

ShieldNet
Cybersecurity Core Training
Course Book

Document Title	ShieldNet Cybersecurity Training Course Book
Release Date	July 2026
Next Review	June 2027 (annual review cycle)
Distribution	Public – Creative Commons BY-NC-ND 4.0
Version	1.0
Author	Michał Zdunowski
Publisher	IS Consulting

Copyright and License

ShieldNet Cybersecurity Core Training – Course Book © 2026 by IS Consulting is licensed under Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International (CC BY-NC-ND 4.0). To view a copy of this license, visit https://creativecommons.org/licenses/by-nc-nd/4.0/

Under this license you are free to share this Course Book, copy it, and redistribute it in any medium or format, provided that you give appropriate credit to IS Consulting, do not use it for commercial purposes, and do not distribute modified versions.

"ShieldNet" and the ShieldNet logo are marks of IS Consulting. Third-party product names, service names, and trademarks mentioned in this book are the property of their respective owners and are used for identification and educational purposes only.

Module 0: Welcome & Orientation

What is This Course and Why Should You Care?

1. Let's Start With a Question

When was the last time you thought about who can see your messages?

Not theoretically, actually thought about it. Who can read the emails sitting in your inbox right now? Who could access your photos if your phone was left on a table? If someone knew your password, what could they do with it?

Most of us don't think about these things until something goes wrong. And by then, it's usually too late to undo the damage.

This course exists to change that. Not by making you paranoid, and not by turning you into a technical expert. But by giving you something more valuable: a clear, practical understanding of how the digital world works, where the risks are, and what you can actually do about them.

Cybersecurity is not a technical subject. It is a human one.

The biggest security failures in history were not caused by unbreakable code or invisible hackers. They were caused by someone clicking a link they shouldn't have, using the same password on every account, or assuming that their organization was too small to be a target. The solutions to those failures are not technical. They are habits, awareness, and judgment, exactly what this course teaches.

2. Who This Course is For

This course is genuinely for everyone.

Not 'everyone in a technical role'. Not 'everyone with a relevant degree'. Everyone. If you use a smartphone, have an email address, or work anywhere that uses a computer, this course is for you. There are no prerequisites. You do not need to know what an IP address[1] is, what encryption means, or what a firewall[2] does. Those things will be explained clearly when they come up, using plain language and real examples.

---

[1] **IP address:** A numerical address that identifies a device on a network, so that data can be sent to the right place.

[2] **Firewall:** A barrier that controls which network traffic is allowed in or out of a device or network, blocking unwanted connections.

Here is who has taken courses like this before:

- A 15-year-old curious about how hackers actually work.
- A 60-year-old accountant who keeps getting suspicious emails and wants to know what to do.
- A small business owner who just hired three new staff and wants everyone to be on the same page.
- A hospital receptionist who handles patient data every day and wants to understand their responsibilities.
- A software developer who knows the technical side but has never thought carefully about the human and organizational side of security.

All of them finished the course. All of them said the same thing: “I wish I had known this sooner.”

3. What Cybersecurity Actually Is

Before we go any further, let’s sort out the word itself. ‘Cybersecurity’ sounds technical and intimidating. It isn’t. Here is a definition that actually makes sense:

> **Cybersecurity, defined simply**
> Cybersecurity is the practice of protecting the things you care about in the digital world your information, your accounts, your devices, and your ability to keep using them from people who want to access, damage or misuse them without your permission.

That’s it. The word ‘cyber’ just means ‘digital’. Security means protection. Put them together and you get: protecting your digital stuff from harm.

The ‘stuff’ worth protecting has a name: digital assets. And you have more of them than you probably realize.

- **Your accounts:** Email, social media, banking, shopping, healthcare apps, work systems. Each one is a door. If the wrong person gets through it, the consequences range from annoying to devastating.
- **Your data:** Passwords, messages, photos, documents, your location history, your browsing history, your health records. Some of this feels trivial. None of it actually is.

- **Your devices:** Your phone, your laptop, your smart TV, your work computer. If any of these are compromised, they can be used as a tool against you or against the people you communicate with.
- **Your ability to function:** If your email is locked, your files are encrypted, or your payment system stops working, the disruption is real regardless of what data was or wasn't stolen.

4. How This Course Is Structured

The course is organized into 20 modules across five parts, plus this orientation module (Module 0) and one final bridge module. You can study at your own pace, in your own order although going from start to finish makes sense because each part builds on the one before it.

Here is the full map of what you will cover:

Part 1 · Understand the Digital World
M1 · Your digital life: data, devices and why attackers want them
M2 · Confidentiality, integrity, availability: the three things worth protecting
M3 · Risk: what it is, why we can't eliminate it, and how we think about it
Part 2 · Know Your Enemies: How Attacks Actually Work
M4 · Phishing and social engineering: hacking humans
M5 · Malware: when software becomes a weapon
M6 · Passwords and account takeover: the keys to your kingdom
M7 · Networks and the internet: how data travels and where it goes wrong
M8 · Who are the attackers: Motivations, targets and methods
Part 3 · Build Your Defenses: Practical Protection
M9 · Strong authentication: proving who you are
M10 · Controlling access: who gets in, what they can do
M11 · Keeping devices safe: updates, locks and good habits
M12 · Encryption: scrambling data so only the right people can read it
M13 · Your data and privacy: what you share, with whom, and why it matters
M14 · Trusting third parties: apps, services and the supply chain
Part 4 · When Things Go Wrong: Responding and Recovering

M15 · Spotting and reporting incidents: your early warning role
M16 · Backups and recovery: why ‘it’s saved’ is never enough
M17 · Data breaches: what happens, what it means, what you do
Part 5 · Security as a Mindset: Habits, Culture and Staying Current
M18 · Safe digital habits: the small things that make a big difference
M19 · Security is everyone’s job: your role in a safer organization
M20 · Staying ahead: how security evolves and how you keep up
Bridge · From Concepts to Practice
M21 · A first look at the ShieldNet framework

Each module runs for around 8–12 minutes. Most people complete the entire course in three to four sessions. There are no deadlines. The platform saves your progress automatically, so you can stop and return at any point without losing where you were.

A note on jargon

Every time a technical term appears in this course, it will be explained in plain language at that moment. You will also find a full glossary at the back of this coursebook. If you ever read something and think ‘I have no idea what that means’, the glossary is your first stop and if it’s not there, that is a mistake we want to fix.

5. The Practice Questions

At the end of each module from Part 1 onwards, there are four practice questions. These are not tests. They are thinking prompts designed to help you check whether the key ideas from that module have landed.

When you answer a practice question, you receive immediate feedback explaining why the correct answer is correct, and why the wrong answers are wrong. This is more valuable than simply seeing a score. The goal is for every question to teach you something, whether you got it right or not.

The practice questions are not graded and do not affect your exam score. Use them honestly. If you get something wrong and understand why after reading the explanation, that is a good outcome. If you get something right but are not sure why, re-read that section of the module before moving on.

6. The Final Exam and Your Badge

After completing all 21 modules, you will be ready to take the final assessment. Passing it earns you the ShieldNet Cybersecurity Core Certified badge a digital credential you can share on LinkedIn, add to your CV, and use to demonstrate that you have completed a structured, assessed cybersecurity literacy program.

What You Need To Know	Details
Number of questions	40
Time allowed	60 minutes
Passing score	75% (30 out of 40)
Attempts	Up to 3 attempts
Between attempts	24-hour cooling-off period after each attempt
Question type	Scenario-based: 'what would you do if...' no trick questions
What it tests	Real-world judgment and recognition not memorization of facts
On passing	Badge issued automatically via Certifier.io within minutes

The most important thing to understand about the exam: every question is a scenario. You will be presented with a realistic situation, an email that arrived, a decision to make, something that happened at work, and asked what the right response is. There are no questions asking you to name a regulation or recall a definition. The exam measures whether you can recognize a threat and respond sensibly, not whether you have memorized a textbook.

7. One Last Thing Before You Start

Cybersecurity has a reputation for being scary. News stories about data breaches, nation-state hackers, and AI-powered attacks can make it feel like there's nothing ordinary people can do.

That reputation is wrong.

The overwhelming majority of successful cyberattacks across individuals, small businesses, hospitals, and governments, succeeded not because the attacker was technically brilliant, but because a basic, preventable mistake was made. A password reused one too many times. An email link clicked without a second thought. A software update ignored for six months.

The good news is that fixing basic, preventable mistakes is entirely within your control. You do not need to be a cybersecurity professional. You do not need to understand how computers work at a technical level. You need to know enough to make better decisions every day and that is exactly what the next 21 modules will give you.

Let's begin.

Module 0: Summary

By the end of this module, you should be able to:

- ✓ Describe what this course teaches and who it is for.
- ✓ Explain what the five parts of the course cover, in sequence.
- ✓ Describe the badge you can earn and what you need to do to pass the exam.
- ✓ Explain what 'cybersecurity' actually means in plain language, no jargon.
- ✓ Name two things that count as 'digital assets' in your own life.

Part 1: Understand the Digital World

Module 1: Your Digital Life

Data, Devices and Why Attackers Want Them

1. A Story to Start With

In 2019, a woman in the UK received a phone call from her bank's fraud department. Someone had just tried to transfer £4,200 from her account. The bank had blocked it this time.

She had not clicked any suspicious links. She had not given her password to anyone. She had not even visited her bank's website recently. What had happened?

Three years earlier, a retail website she had shopped on once had been breached. Her email address and password were stolen. She had used the same password on her bank account. The attackers had simply tried her leaked credentials[3] on hundreds of banking websites until one worked. It took an automated program about four seconds.

She considered herself careful with technology. She was right she was more careful than most people. And it still nearly happened to her.

This module is about understanding why. Not to make you anxious, but to show you exactly what your digital life looks like from an attacker's perspective and why that perspective is very different from your own.

2. What Is a Digital Asset?

An asset is anything that has value. A car is an asset. Your house is an asset. Your savings are an asset. In the digital world, the things that have value are less visible but they are just as real.

A digital asset is any piece of information, any account, or any device that has value to you or to someone else. Here is the important part: the value does not have to be obvious to you for it to be real.

Your accounts

Every account you have email, social media, banking, shopping, health, streaming, work is a digital asset. Each one is a door. Behind that door sits information,

[3] **Credential:** A piece of information that proves who you are to a system, most often a username and password.

purchasing power, or access to other systems. The value varies enormously, but every account has some.

Your email account is almost certainly your most valuable digital asset, even though it may not feel like it. Here is why: most other accounts use your email address as a backup. If an attacker controls your inbox, they can use 'forgot my password' to reset your banking app, your PayPal, your work systems, your cloud storage everything that sends a reset link to your email. Your inbox is the master key.

Your data

Your name, date of birth, phone number, address, financial details, health records, messages, photos, location history, browsing history, purchase history. Much of this feels mundane. It is not.

Individually, each piece seems harmless. Together, they build a profile that can be used to impersonate you, steal from you, manipulate you, or sell to people who do those things for a living. Data has a market. That market is active and well-organized. The table below shows what stolen data is worth on criminal marketplaces.

What Was Stolen	What Attackers Can Do With It	Estimated Dark Web Value
Full name + date of birth	Used to open bank accounts or phone contracts in your name	**€5–40**
Email address + password	Direct access to your inbox and every service that password reset goes to	**€10–80**
Credit card details (full)	Used for fraudulent purchases before you notice	**€10–20 per card**
Social media account (active)	Used to scam your contacts, spread misinformation, or run ads	**€5–15**
Online banking credentials	Direct access to transfer money from your account	**€40–200+**
Medical records	Used for insurance fraud, blackmail, or identity theft	**€50–250**
Corporate email account	Gateway into company systems, supplier fraud, data theft	**€50–500+**

These prices are not theoretical
Security researchers regularly infiltrate dark web marketplaces to document what stolen data sells for. The figures above are based on real observed prices from multiple research reports. They fluctuate with supply and demand which means large breaches that flood the market with a particular type of data temporarily lower prices, while rare or fresh data commands a premium. Your data is a commodity.

Your devices

Your phone, laptop, and home router[4] are digital assets too. Not because of what they are worth in cash, but because of what they can do when compromised. A hacked phone can monitor your calls, read your messages, track your location, and access every app you have open. A compromised laptop can be used to attack other systems, mine cryptocurrency, or act as a relay point in criminal operations, often without slowing down noticeably. You might be paying for someone else's crime without knowing it.

3. 'I Have Nothing to Hide'

This is the most common reason people give for not taking security seriously. It feels rational. It is not.

The 'nothing to hide' argument rests on a false assumption: that attackers are interested in your secrets. Most are not. They are interested in what your data, accounts, and devices can do for them.

The 'nothing to hide' myth, unpacked
Your email account is valuable not because of your messages, but because it resets passwords for everything else you own.
Your social media account is valuable not because of what you post, but because your contacts trust you. A compromised account sends convincing scam messages to people who will click them because they think it is you.
Your device is valuable not because of your files, but because it has processing power, a network connection, and credentials stored in it.
Your identity is valuable not because of who you are, but because a criminal can use it to open credit cards, take out loans, or commit fraud that lands at your door.

[4] **Router:** The device that connects your home or office network to the internet and directs traffic between your devices and the wider network.

Even if none of that convinces you about yourself, consider the people around you. Your contacts, colleagues, and family are connected to you digitally. When your account is compromised, you become a pathway to them. The most convincing phishing[5] messages often come from people the victim already trusts because a real account belonging to a real connection has been taken over.

Security is not just personal. It is communal. When you protect your accounts, you also protect everyone who trusts you.

4. How Attackers Actually Find You

The story at the start of this module might have given the impression that someone specifically targeted that woman. They did not. That is the point.

The overwhelming majority of attacks on individuals are not targeted they are automated and opportunistic. No human being sat down and decided to go after her specifically. An automated program worked through a list of leaked credentials and tried each one against a list of banking websites. The process required no human attention until something worked.

The scale of automated attacks

When a large company suffers a data breach, the stolen data millions of usernames and passwords is quickly sold and distributed on criminal marketplaces. Within days, automated tools are testing those credentials against hundreds of popular websites. This is called credential stuffing. It succeeds not because the attackers are skilled, but because people reuse passwords and because the tools are fast.

In a single day, a credential stuffing campaign can test millions of username/password combinations across thousands of websites. The success rate does not need to be high. Even a 0.1% success rate on a list of ten million leaked credentials means 10,000 compromised accounts.

---

[5] **Phishing:** A fraudulent message, usually email, that pretends to come from a trusted source to trick you into clicking a link, opening an attachment, entering credentials, or sending money.

The digital breadcrumbs you leave behind

Every action you take online leaves a trace. The technical term is 'digital footprint', but 'digital breadcrumbs' is more honest: each individual crumb is tiny and harmless, but the trail they form is a detailed map of who you are.

- **Search history:** What you search for reveals your interests, concerns, health worries, financial situation, and location patterns.
- **Social media:** Your employer, your friends, your family, your daily routine, your pet's name (often used as a password or security answer), your mother's maiden name, where you went to school.
- **Shopping:** Your address, your payment methods, what you buy, when you travel (because you order things to be delivered while you're away).
- **Apps:** Your location, your sleep patterns, your exercise routes, your food preferences, your financial habits.

Individually, these feel trivial. Combined, they give an attacker or anyone paying for data brokers'[6] services an extraordinary amount of leverage. Social engineering[7] attacks (which we cover in Module 4) become far more convincing when the attacker already knows your name, your employer, your manager's name, and the fact that you booked a holiday last week.

What you can do right now

Search your email address at haveibeenpwned.com a free, legitimate service that tells you if your details have appeared in a known data breach. If they have, change the password on that account and on any other account that uses the same password.

Open your most-used apps and check what permissions they have. Does your notes app need access to your location? Does a game need access to your contacts? If a permission does not make sense for what the app does, remove it.

Think about what password reset emails would go to your main email address. Those are the accounts an attacker could access if they got into your inbox.

---

[6] **Data broker:** A company that collects and sells personal data gathered from many sources, often without people's direct knowledge.

[7] **Social engineering:** Manipulating people into giving up information or taking unsafe actions by exploiting trust, urgency, authority, or curiosity, rather than technical weaknesses.

5. The Key Ideas From This Module

Before moving on to Module 2, make sure these ideas have landed:

- Your digital assets have real value to others, regardless of how you personally value them.
- Your email account is your most critical account because it resets everything else.
- Most attacks are automated and opportunistic, not targeted at you specifically. Being unprotected is what makes you a target.
- The 'nothing to hide' argument misunderstands what attackers want. They want utility, not secrets.
- The digital breadcrumbs you leave across the internet build a profile that can be used against you or the people connected to you.

ShieldNet thread going further

The ideas in this module connect to two concepts in the ShieldNet Cybersecurity Standard. The practice of identifying and classifying your digital assets is formalized in control [KP3] (Inventory Assets & Data) the starting point for any security program. The practice of thinking about what could go wrong with those assets is formalized in [KP4] (Assess Risks Regularly). If you ever want to explore how organizations put these principles into practice at a professional level, those are good places to start.

Module 1: Summary

By the end of this module, you should be able to:

- ✓ Explain why 'I have nothing to hide' is a dangerous assumption, using at least one concrete example.
- ✓ Name three categories of digital asset and describe why each has value to an attacker.
- ✓ Describe the difference between a targeted attack and an automated, opportunistic one.
- ✓ Explain why your email account is often the most valuable account an attacker can compromise.
- ✓ Describe what 'digital breadcrumbs' are and give two examples from your own daily life.

Module 2: Confidentiality, Integrity, Availability

The Three Things Worth Protecting

1. Three Scenarios

Before any definitions, three things happened. All three are cybersecurity failures. See if you can spot what is different about each one.

Scenario A

A journalist's confidential source list (names, contact details, locations) is stolen from an encrypted laptop when the laptop is left in a café. The attacker now knows who the journalist has been speaking to. Nothing has been changed. The files are intact. But the wrong person now has access to information they should never have seen.

Scenario B

A patient checks into a hospital for surgery. The surgical team reviews her records and sees she has no known allergies. In fact, she is severely allergic to a common anesthetic but someone, at some point, deleted the allergy entry from her record. Nothing was stolen. The file is accessible and looks perfectly normal. But the information inside it is wrong.

Scenario C

A small town's water treatment facility is attacked by ransomware. The engineers who control the purification systems cannot access any of their monitoring tools. The plant is still physically operational. No data has been stolen or changed. But no one can check whether the water is safe, and they cannot adjust the treatment process. The systems are locked.

Three failures. Three very different consequences. And three different answers to the question: 'What exactly went wrong?' Each one maps to a different principle in what security professionals call the CIA triad.

2. The CIA Triad

CIA stands for Confidentiality, Integrity, and Availability. It is the most widely used framework for thinking about what security is trying to protect not because it is the only way to look at it, but because it is remarkably complete. Almost every

cybersecurity failure you will ever encounter can be described in terms of these three principles.

Here is how each one maps to the scenarios above and what it means in plain language.

C	**Confidentiality: only the right people can see it** Confidentiality means that information is accessible only to those who are supposed to have access to it. It is the principle most people associate with security keeping secrets secret. Scenario A is a confidentiality failure: the journalist's source list was seen by someone who should never have had access to it.
I	**Integrity: it hasn't been changed without authorization** Integrity means that information is accurate and has only been changed by people who are authorized to change it and that those changes are recorded. Scenario B is an integrity failure: the patient's allergy record was altered (or deleted) without authorization, and nobody could tell. The file looked normal. That is what makes integrity failures so dangerous: they are invisible until they cause harm.
A	**Availability: you can access it when you need it** Availability means that information and systems can be accessed by authorized people when they need them. Scenario C is an availability failure: the water treatment engineers had every right to access their systems, but they couldn't. No data was stolen or changed. But the inability to access critical systems in real time created a genuine danger.

3. The Full Picture

Here is a reference table that shows all three principles side by side. It is worth spending a moment with this before moving on.

Principle	Plain Meaning	Everyday Example	How it's Protected	When it's Broken
Confidentiality	Only the right people can see it	Your medical records are visible only to your doctor, not to your neighbor	Encryption, access controls, passwords	Someone reads your private messages · A company sells your data without permission · A criminal accesses your bank details

Principle	Plain Meaning	Everyday Example	How it's Protected	When it's Broken
Integrity	It hasn't been changed without permission	The bank balance you see is accurate and hasn't been altered by anyone	Checksums[8], audit logs[9], version control	A hacker changes a payment destination · A virus corrupts a file · Someone edits a contract after it was signed
Availability	You can access it when you need it	Your hospital can access your records during an emergency, not just when it's convenient	Backups, redundancy, disaster recovery	Ransomware locks all files · A DDoS attack takes a website offline · A power cut destroys unbacked up data

Why all three matter equally

It is tempting to think of confidentiality as the 'main' security goal because breaches involving stolen data make the news most often. But availability failures can be just as severe: a hospital that cannot access patient records during a medical emergency, a factory whose control systems are locked by ransomware, a business that cannot issue invoices because its systems are down. And integrity failures can be the most quietly catastrophic of all: wrong medical dosages, altered financial records, fabricated evidence. The triad is a triangle, not a hierarchy.

4. When All Three Break at Once

In practice, major attacks often violate more than one principle simultaneously.

Consider a ransomware attack on a small accounting firm. The attackers first spend two weeks quietly inside the firm's network, reading client financial records (confidentiality violation). They alter several invoice records to redirect payments to their own accounts (integrity violation). Then they encrypt all files and demand

[8] **Checksum:** A short value calculated from a file that changes if the file changes, used to detect whether data has been altered.

[9] **Audit log:** A record of who did what and when in a system, used to detect and investigate suspicious activity.

payment (availability violation). By the time the firm realizes what happened, all three principles have been broken and untangling which data was seen, which was changed, and which needs to be restored is a weeks-long forensic exercise.

This kind of multi-stage attack is increasingly common. Understanding the triad helps you ask the right questions after an incident: it is not just 'what was stolen?' but also 'what might have been changed?' and 'what can we still access and trust?'

5. How the Triad Shows Up in This Course

You do not need to label every module or topic as 'a confidentiality issue' or 'an integrity issue' as you go through the course. But knowing the triad changes how you think about every security story you encounter in the news, at work, or in these modules.

When you hear about a data breach, the natural question shifts from 'whose fault was it?' to 'which of these three things failed, and how?'. That is a more useful question. It points towards solutions rather than blame. And it makes the dozens of specific threats and defenses in the rest of this course much easier to understand, because they all ultimately serve one or more of these three goals.

- Encryption protects confidentiality.
- Access controls protect all three: they stop the wrong people from reading (confidentiality), changing (integrity), or blocking access to (availability) information.
- Backups protect availability.
- Audit logs protect integrity: they create a record of who changed what, so alterations can be detected.
- Multi-factor authentication protects all three: by making it much harder for an attacker to gain access in the first place.

As you work through the rest of this course, you will find that almost every defense connects back to one of these three principles. The CIA triad is not an abstract concept to memorize. It is a lens that makes everything else clearer.

ShieldNet thread going further

The CIA triad is the conceptual foundation of the ShieldNet Cybersecurity Standard and of virtually every professional cybersecurity framework in the world. In ShieldNet, the controls

in the SHIELD & BUILD zone focus heavily on confidentiality (access controls, encryption) and integrity (hardened configurations, secure development). The REACT & RECOVER zone focuses on availability (business continuity planning, backups, recovery). The WATCH & PATCH zone protects all three by detecting failures before they cause harm. If you want to explore how organizations operationalize these principles, the ShieldNet Core Standard is a practical starting point.

Module 2: Summary

By the end of this module, you should be able to:

- ✓ Define confidentiality, integrity and availability in plain language without referring to the acronym.
- ✓ Give a real-world example of each principle being violated.
- ✓ Explain why availability matters even when no data is stolen.
- ✓ Describe a scenario where all three principles are broken simultaneously.
- ✓ Explain why integrity is often the least obvious failure but sometimes the most dangerous.

Module 3: Risk

What It Is, Why We Can't Eliminate It, and How We Think About It

1. You Already Understand Risk

You make risk decisions every day. You probably made several before you got to this module.

You decided whether to carry an umbrella based on whether rain seemed likely and how much it would inconvenience you. You locked your car door before going into a shop. You looked both ways before crossing the road even on a quiet street. You might have chosen a busy, well-lit route home rather than a shortcut through a dark alley.

None of those decisions required a framework or a spreadsheet. They were intuitive assessments of two things: how likely is something bad to happen, and how bad would it be if it did? That is risk thinking. Cybersecurity just applies that same thinking to the digital world.

This module gives you the vocabulary to do it clearly, so that when you hear terms like 'threat', 'vulnerability', or 'risk assessment', you are not confused by jargon you recognize concepts you already understand.

2. Five Words That Do a Lot of Work

In cybersecurity, five terms are used constantly. They are often used loosely or interchangeably in conversation, but they have precise meanings that matter. Getting them straight makes every future discussion clearer.

Term	Plain Meaning	Home Analogy	Organization Example	Personal Example
Threat	Something that could cause harm	Heavy rain	A phishing email targeting your staff	A criminal who has bought your leaked credentials
Vulnerability	A weakness that a threat could exploit	A cracked roof tile	No spam filter on your email system	You use the same password on every account
Risk	The combination of threat + vulnerability	Flooding inside the house	Staff clicking a malicious link due to no spam filter	Attacker uses your leaked password to log into your bank

Term	Plain Meaning	Home Analogy	Organization Example	Personal Example
Impact	The harm that actually happens if the risk occurs	Water damage to belongings	Ransomware deployed; systems locked for a week	Money taken from your account
Likelihood	How probable is it that this risk occurs?	High, it rains often	Medium, phishing is common but some staff are cautious	High, automated tools test leaked credentials immediately

The most important distinction: threat vs risk

A threat exists whether you do anything about it or not. Rain is a threat to your belongings whether your roof has a crack or not. A risk is what happens when a threat meets a weakness. If your roof is solid, rain is a threat but not a significant risk. If your roof has a crack directly above your wardrobe, it is both. This distinction matters because it tells you where to act: you cannot control whether threats exist, but you can control your vulnerabilities.

3. Likelihood and Impact: Not All Risks Are Equal

Once you have identified a risk, you need to work out how much attention it deserves. Two factors determine this: how likely is it to happen, and how bad would it be if it did?

Likelihood

Likelihood is the probability that a threat will actually exploit a vulnerability and cause harm. It is affected by how common the threat is, how exposed your vulnerability is, and whether you have anything in place that might stop it.

A small bakery's website being targeted by a nation-state hacking group is theoretically possible but has an extremely low likelihood: tuserhat group has more valuable targets. The same bakery's staff clicking a phishing email has a much higher likelihood: phishing campaigns are mass-distributed and indiscriminate.

Impact

Impact is the severity of harm if the risk actually occurs. It covers operational disruption (how long you can't function normally), financial loss (direct theft, fines,

recovery costs), reputational damage (loss of customer trust), and legal consequences (regulatory penalties).

The same event can have very different impacts on different organizations. A two-day system outage might be a minor inconvenience for a hobby website and a life-threatening situation for a hospital's patient monitoring system.

The combination: risk level

Risk level is a product of both factors. A high-likelihood, high-impact risk is a priority. A low-likelihood, low-impact risk may not warrant significant investment. But the relationship is not always simple:

- High impact, low likelihood: A fire destroying your office has a low probability but catastrophic impact. You insure against it and keep fire extinguishers. The cost of preparation is low relative to the cost of being unprepared.
- High likelihood, low impact: Spam email arrives every day. The impact of any single spam message is trivial. A spam filter is cheap and worth implementing, but you do not lose sleep over every message.
- High likelihood, high impact: Phishing attacks targeting your staff are common and can cause serious harm. This combination demands active attention: training, technical controls, and clear procedures.

A useful mental test

When assessing any risk, ask two questions: 'If this happened tomorrow, how bad would it be?' (impact) and 'How often does this kind of thing happen to organizations like ours?' (likelihood). If both answers are concerning, that risk goes to the top of the list. If one answer is reassuring, the risk is probably manageable. This two-question test will serve you well throughout the rest of this course and beyond.

4. Zero Risk Is Not the Goal

Here is something that surprises many people when they first engage seriously with security: the goal is not to eliminate risk. It is to manage risk.

Zero risk is impossible. If you want to eliminate the risk of your laptop being stolen, you could lock it in a safe that is bolted to the floor. But then you cannot use it. If you want to eliminate the risk of your email being hacked, you could delete your email account.

But then you cannot communicate. Every security measure involves a trade-off between protection and usability.

The question is never 'how do we reach zero risk?'. It is 'what level of risk are we willing to accept, and what are we willing to do to get there?' This is called risk tolerance, and it varies enormously. A nuclear power plant has an extremely low risk tolerance for anything affecting its safety systems. A small podcast creator has a higher tolerance for the risk of their social media account being briefly compromised.

Understanding your own risk tolerance and being honest about it is the foundation of sensible security decisions. Trying to protect everything equally is a recipe for wasting resources. Protecting the things that matter most, proportionately to how much they matter, is how good security actually works.

5. Four Ways to Respond to a Risk

Once you have identified and assessed a risk, you have four options. These responses apply equally at home, at work, and in any organization of any size.

Response	What it means	Home Analogy	Organization Example	Personal Example
Reduce	Take steps to make the risk less likely or less harmful	Install a smoke alarm, keep a fire extinguisher	Enable MFA to make account takeover much harder	Turn on two-factor authentication on your accounts
Accept	Acknowledge the risk exists but decide it is tolerable	No smoke alarm in garden shed – acceptable for its value	Accept that some phishing will always get through; rely on staff awareness	Decide your old gaming account doesn't need a strong password
Transfer	Shift the financial impact to someone else	Home insurance covers fire damage	Cyber insurance; contractual liability clauses with suppliers	Use credit card instead of debit card for online purchases – better fraud protection
Avoid	Stop doing the thing that creates the risk entirely	Stop storing petrol in the house	Don't collect customer data you don't need	Delete old accounts you no longer use

In practice, most risk management involves a combination of all four responses. You reduce the most likely and most impactful risks, transfer some financial exposure

through insurance or contracts, accept the residual risks[10] that are too minor or too expensive to address, and avoid the riskiest activities where you have a reasonable alternative.

Accepting a risk is not the same as ignoring it

Risk acceptance is a conscious, documented decision: 'We have assessed this risk, we understand its likelihood and impact, and we have decided the cost of reducing it further outweighs the benefit.' That is legitimate risk management. Ignoring a risk never assessing it, never discussing it, hoping it goes away is not. The difference matters when something goes wrong: an organization that consciously accepted a risk is in a very different legal and ethical position from one that simply never thought about it.

6. Risk in the Rest of This Course

Everything in Parts 2 through 5 of this course is, at heart, a discussion of specific risks and how to manage them. Phishing is a risk. Weak passwords are a vulnerability. Ransomware is a threat. Not having backups is what turns a ransomware attack from a manageable crisis into a catastrophe.

The vocabulary you have built in this module threat, vulnerability, risk, likelihood, impact will appear constantly. When you encounter a new security concept, try asking: what is the threat this addresses? What vulnerability does it reduce? How does it change the likelihood or impact of a risk? Those questions will cut through the technical noise and take you straight to what matters.

ShieldNet thread going further

Risk management is the central activity in the ShieldNet Cybersecurity Standard's KNOW & PLAN zone. Control [KP4] (Assess Risks Regularly) formalizes exactly what this module describes: identify threats and vulnerabilities, assess likelihood and impact, decide how to respond, and review annually. The vocabulary table in section 3.2 maps directly to the language used in the ShieldNet Risk Register template (Annex A, Template A-2). If you are ever involved in a formal risk assessment at your organization, that template is a practical starting point.

[10] **Residual risk:** The risk that remains after protections are in place. Some risk almost always remains.

Module 3: Summary

By the end of this module, you should be able to:

- ✓ Explain the difference between a threat, a vulnerability, and a risk using a concrete example.
- ✓ Describe how likelihood and impact combine to determine whether a risk deserves attention.
- ✓ Name the four ways an organization or individual can respond to a risk, with an example of each.
- ✓ Explain why 'zero risk' is neither achievable nor the goal of security.
- ✓ Give an example of a high-impact but low-likelihood risk that still warrants preparation.

Completing Part 1

You have now covered the three foundational ideas that underpin every module in this course:

Module 1: your digital assets have real value and most attacks are automated and opportunistic.

Module 2: security protects three things confidentiality (who can see it), integrity (is it accurate), and availability (can you access it).

Module 3: risk is a combination of likelihood and impact, cannot be eliminated entirely, and must be consciously managed.

Part 1 Knowledge Check

Module 1 Practice Questions
Q1. You receive an email from a company telling you that your account was included in a data breach. Your username and password were exposed. You don't remember using that site in years and don't think the account matters. What is the most important action to take first? a. Delete the email if you don't use the account, there's no risk. b. Change the password on that account immediately, and check whether you used the same password anywhere else. c. Reply to the email asking for more details about which data was exposed. d. Wait a few days to see if anything suspicious happens before taking action.
Q2. A friend says: 'I don't worry about cybersecurity because I'm not important enough for anyone to target me.' Which response best explains why this thinking is flawed? e. Everyone is important attackers value all data equally. f. Most attacks are automated and look for easy targets, not specific people. Being unprotected makes you more likely to be hit, not less. g. Cybercriminals only target wealthy individuals, so your friend is correct if they have little money. h. Your friend is right that small individuals are rarely targeted, but companies they work for might be.
Q3. An attacker gains access to someone's email account. Beyond reading their emails, what else does this typically allow the attacker to do? i. Nothing email access only lets them read messages, not take further action. j. They can use the email account to send spam to the victim's contacts. k. They can use 'forgot my password' links to reset credentials for banking, shopping, social media and other accounts linked to that email address. l. They can access all files stored on the victim's computer via the email account.
Q4. Which of the following best describes a 'digital breadcrumb'? m. A type of malware that records everything you type. n. A small piece of data a location check-in, a search term, a purchase, a message that individually seems harmless but contributes to a detailed profile of who you are. o. A security technique used to track suspicious behavior on a network. p. An encrypted file that protects sensitive information.

Module 2 Practice Questions
Q1. A hacker breaks into a hospital's computer system and does not steal any data. Instead, they change several patients' blood type records from A+ to O-. No one notices immediately. Which principle of the CIA triad has been violated? a. Confidentiality someone unauthorized accessed the records. b. Availability the records are no longer accessible to doctors. c. Integrity the data has been altered without authorization, and the changes are undetected. d. All three equally a breach always violates all three principles.
Q2. A ransomware attack encrypts all files on a small company's server. The attacker demands payment to restore access. The company has no backups. No data was stolen or changed. Which principle has been most directly violated? e. Confidentiality: the attacker can now read all the company's files. f. Integrity: the files have been permanently altered by encryption. g. Availability: the company can no longer access its own data when it needs it. h. None: if no data was stolen, there is no cybersecurity failure.
Q3. You are paying a supplier via your company's online banking. The bank's website is fully available and your credentials are secure. However, an attacker previously altered the supplier's bank account number stored in your system. You complete the transfer. The money goes to the attacker. Which principle failure caused this outcome? i. Availability: the banking system should have been taken offline during the attack. j. Confidentiality: the attacker read the supplier's bank details. k. Integrity: the bank account data was silently changed, and the system had no way to detect it. l. None: if the transfer was completed successfully, no security failure occurred.
Q4. Which statement best explains why integrity failures are sometimes more dangerous than confidentiality failures? m. Integrity failures always involve more data than confidentiality failures. n. When integrity is broken, you may not know it you act on wrong information with confidence, which can be more harmful than knowing your data was seen by someone. o. Integrity failures are more visible and easier to detect than confidentiality failures. p. Confidentiality is only important for personal data, whereas integrity matters for all data.

Module 3 Practice Questions
Q1. A company stores customer passwords in plain text in its database. An attacker discovers a software vulnerability that allows access to the database. Which statement correctly identifies the threat and the vulnerability? a. Threat: the software vulnerability. Vulnerability: the attacker. b. Threat: the attacker. Vulnerability: the software flaw that allows database access. c. Threat: storing passwords in plain text. Vulnerability: the database itself. d. Threat: the database. Vulnerability: the lack of encryption on stored passwords.
Q2. A security team identifies two risks. Risk A: a meteor strike destroys the server room (impact: catastrophic, likelihood: extremely rare). Risk B: a phishing email causes a staff member to reveal their password (impact: serious, likelihood: very common). Which risk should receive more immediate attention and why? e. Risk A, because the potential impact is catastrophic. f. Risk B, because risk is determined by both likelihood and impact combined a common, serious risk demands more practical attention than a catastrophic but near-impossible one. g. Both equally, because any risk that could cause harm must be treated as a priority. h. Neither, because both risks are outside the organization's control.
Q3. A small online shop decides not to collect or store customer payment card details, instead redirecting all payments through a third-party processor. From a risk management perspective, which response to risk does this best illustrate? i. Reduce: the shop has made card theft less likely by using a third party. j. Transfer: the financial liability for card fraud has been shifted to the payment processor. k. Avoid: by never holding card data, the shop eliminates that specific risk entirely. l. Accept: the shop acknowledges the risk and proceeds with payments anyway.
Q4. Which statement most accurately describes the goal of cybersecurity risk management? m. To eliminate all risks before they can cause any harm. n. To identify, prioritize, and reduce risks to an acceptable level knowing that some residual risk will always remain. o. To transfer all cybersecurity risks to insurance companies and third-party providers. p. To avoid any activity that carries a cybersecurity risk.

Part 2: Know Your Enemies

Module 4: Phishing and Social Engineering

Hacking Humans

1. The Easiest Way Into Any System

Breaking into a computer system by finding and exploiting a technical vulnerability is difficult, time-consuming, and increasingly hard as security tools improve. Tricking a human into opening a door is often much easier.

This is the fundamental insight behind phishing and social engineering: the most reliable attack surface is not the firewall, the software, or the network. It is the person using them. People want to be helpful. People respond to urgency. People trust authority. People make mistakes when they are busy, tired, or distracted. Attackers have understood this for decades and built an entire industry around exploiting it.

Phishing is not a niche technical attack. It is the most commonly reported cyber incident type across Europe year after year. It is how most ransomware gets deployed. It is how most corporate data breaches begin. It is the attack you are statistically most likely to face. Which means understanding exactly how it works and being able to spot it is one of the most practically valuable things this course can give you.

2. How Phishing Works

A phishing attack has a simple structure. The attacker sends a message, most commonly an email, that appears to come from a trusted source. The message creates a reason for the recipient to take an action: click a link, open an attachment, enter credentials, or transfer money. That action either installs malware[11], steals login details, or initiates a fraudulent transaction.

The word ‘phishing’ is a deliberate misspelling of ‘fishing’ and the analogy is accurate. The attacker casts a message into a large body of people and waits for someone to bite. In a mass phishing campaign, the email goes to thousands or millions of recipients. Even if only 0.5% of recipients fall for it, that is thousands of successful attacks from a single campaign.

Spear phishing: when it gets personal

[11] **Malware:** Malicious software designed to harm, spy on, or take control of a device. Viruses, ransomware, spyware, and trojans are all types of malware.

Standard phishing is mass-distribution and relatively generic. Spear phishing is targeted. The attacker researches a specific individual using LinkedIn, the company website, social media, and previous data breaches and crafts a message tailored to that person. It might reference their actual manager by name, mention a real project they are working on, or appear to come from a supplier they actually use.

Spear phishing is far more convincing and far more dangerous. It is how corporate espionage begins. It is how high-value financial fraud is executed. And because it looks so credible, even careful, security-aware people get caught.

Whaling: targeting the biggest fish

Whaling is spear phishing aimed at senior leaders CEOs, CFOs, board members. The stakes are higher because so is the access. A CFO who transfers money based on a convincing fake email from the CEO ('business email compromise' or BEC) can lose hundreds of thousands of euros in a single transaction. This type of fraud has cost organizations worldwide billions of euros in total losses.

3. The Psychology Behind It: Why Smart People Fall for It

Phishing does not succeed because the victims are foolish. It succeeds because it is engineered to bypass the mental shortcuts all human beings use to navigate the world quickly. Understanding the psychological mechanisms makes you significantly harder to deceive.

- Authority: We are conditioned to comply with requests from authority figures. An email appearing to come from the CEO, HMRC, the EU cybersecurity agency, or the police creates an instinct to comply without questioning. Attackers impersonate exactly these figures.
- Urgency: When we believe we must act immediately, we stop reasoning carefully. 'Your account will be suspended in 2 hours' is designed to prevent you from taking the time to check whether the email is genuine. Urgency is the attacker's most powerful tool.
- Fear: 'Your card has been used for a suspicious transaction' or 'Legal action will be taken if you do not respond' activates the threat response, which again prioritizes speed over careful thought.
- Familiarity: An email that looks exactly like a previous genuine email from your bank, or a message that mentions your colleague's name, reduces your natural

suspicion. Familiarity signals safety. Attackers replicate that familiarity meticulously.

- Social proof: Seeing that 'other users have already updated their details' or being told 'this is required by all employees' creates the impression that compliance is normal and expected, making non-compliance feel like the outlier behavior.

The key insight about urgency

Real organizations almost never demand immediate action under threat of severe consequences via an unsolicited email. Your bank will not close your account in two hours if you don't click a link. HMRC will not issue a warrant if you don't call back within the hour. The EU cybersecurity authority will not delete your email account by midnight. When a message creates that kind of pressure, the pressure itself is the red flag.

4. Spotting a Phishing Attempt: The Red Flags

No checklist catches every phishing attempt: attackers constantly evolve their methods. But the following red flags appear in a very high proportion of phishing attacks. Developing the habit of checking for them takes seconds and catches most attempts.

Red Flag	What it Looks Like	Why it Works
Urgency and pressure	"Your account will be suspended in 24 hours" · "ACT NOW" · "Last chance"	Panic overrides careful thinking. The less time you feel you have, the less likely you are to stop and question.
Mismatched sender	Email from 'Amazon Support' arrives from amaz0n-billing@gmail.com · The display name looks fine but the actual address does not	Most email clients show the display name by default. Many people never check the underlying address.
Suspicious or disguised links	microsoft-security-alert.ru · paypal.com.verify-account.net · a shortened URL like bit.ly/xK93pQ	The real domain is always the part immediately before the first single slash. 'paypal.com.verify-account.net' is owned by verify-account.net, not PayPal.
Requests for sensitive information	"Please confirm your password to verify your identity" · "Enter your bank details to unlock your account"	Legitimate services never ask for your password by email. Ever. If they do, it is a scam.

Red Flag	What it Looks Like	Why it Works
Generic greeting	"Dear Customer" · "Hello User" · "Dear Account Holder"	Real companies know your name. Generic greetings often indicate a mass-sent attack without personalization.
Grammar and formatting errors	Inconsistent fonts, spelling mistakes, awkward phrasing, mismatched logos	Less reliable than it once was AI has improved attacker writing quality but still a useful signal when present.
Unexpected attachments	An invoice you didn't request · A 'delivery failed' notice with a PDF · A 'shared document' you weren't expecting	Attachments are one of the most common malware delivery mechanisms. If you weren't expecting it, verify before opening.

The domain check is the most reliable signal

The real domain in a URL or email address is always the part immediately before the first single slash and for email, it is the part after the @ symbol.

paypal.com → legitimate PayPal domain

paypal.com.verify-account.net → the real domain is verify-account.net (not PayPal)

microsoft-login.security-alert.ru → the real domain is security-alert.ru (not Microsoft)

support@amazon.billing-dept.com → the real domain is billing-dept.com (not Amazon)

Practice this check until it is automatic. It takes two seconds and cuts through even sophisticated phishing.

5. Beyond Email: Social Engineering in All Its Forms

Phishing via email is the most common form, but social engineering the broader practice of manipulating people to bypass security takes many forms. Knowing the variants makes you harder to deceive regardless of which channel the attacker chooses.

Technique	What the Attacker Does	Real Example	How To Counter It
Pretexting	Creates a believable fictional scenario to extract information or action	Caller claims to be from IT support and needs your login to fix a 'critical issue' with your account	Verify identities independently. Call the real IT number, not the one they give you.
Impersonation	Pretends to be someone the victim trusts: a	Email appears to be from your CEO asking for an	For unusual financial requests, always verify by

Technique	What the Attacker Does	Real Example	How To Counter It
	colleague, a supplier, a bank, a regulator	urgent wire transfer while they are 'traveling'	phone using a number you already have not one in the message.
Baiting	Leaves something enticing for the victim to interact with	A USB drive labeled 'Salary Information Q4' left in a company car park or reception area	Never plug in a USB device you found or were given unexpectedly. Report it to IT instead
Quid pro quo	Offers something in return for information or access	'I can fix your slow computer just give me remote access for ten minutes'	Unsolicited offers of help, especially involving system access, are almost always suspicious.
Vishing (voice)	Phishing over the phone calls, not emails	Caller claims to be from your bank's fraud team, creates urgency about a 'suspicious transaction', asks you to confirm your card number to 'cancel' it	Banks never ask for your full card number, PIN, or password by phone. Hang up and call back on the official number.
Smishing (SMS)	Phishing via text message	'Your parcel could not be delivered. Pay €1.99 to reschedule: [link]' especially common around holiday periods	Delivery companies do not charge card fees via SMS link. Go directly to the courier's official website.

6. What to Do: Stop, Check, Report

The right response to a suspicious message is always the same three steps. Doing them in this order matters.

Step 1: Stop

Do not click. Do not reply. Do not download the attachment. The moment you feel urgency or pressure from a message, treat that feeling as a warning sign, not a prompt to act. Pause. Take a breath. The few seconds this takes cost you nothing if the message is genuine. It costs you everything if it is not.

Step 2: Check

Verify the message through a separate, trusted channel. If the email claims to be from your bank, call the number on the back of your bank card not any number in the email.

If it appears to be from a colleague, send them a separate message or call them directly. If it claims to be from a company, go directly to that company's official website by typing the address yourself do not follow the link in the message.

Check the sender's actual email address, not just the display name. Hover over any links (on desktop) to see where they actually lead before clicking. Look for the domain check from section 4.

Step 3: Report

If you believe a message is a phishing attempt, report it. In most organizations, this means forwarding it to IT or security, or using a built-in 'report phishing' button in your email client. On personal email, you can mark it as phishing or spam. Reporting helps protect everyone else who might receive the same message.

If you have already clicked a link or entered credentials, report it immediately. The sooner your IT team or bank knows, the faster they can act to limit the damage. Do not wait out of embarrassment phishing catches experienced, careful people constantly. What matters is the speed of response, not the appearance of infallibility.

If you think you fell for it: act fast, not perfectly

The worst response to falling for a phishing attack is silence. Change your password immediately on any account you entered credentials for. Tell your IT team or manager. Check whether any other accounts use the same password and change those too. Contact your bank if any financial information was involved. The first hour after a phishing incident matters enormously most damage is reversible if caught quickly, and most of it becomes irreversible if left unaddressed.

7. Why MFA Changes the Calculation

Even a perfectly executed phishing attack that successfully steals your username and password is significantly limited if your account is protected by multi-factor authentication. This is because the attacker now has your credentials but still cannot log in the second factor (a code from your phone, a biometric check, a hardware key) is something they do not have.

This does not make phishing harmless some phishing attacks include a real-time relay that forwards your MFA code before it expires, and some forms of MFA are weaker than

others. But for the vast majority of attacks, MFA turns a stolen password from a complete account compromise into a failed login attempt. It is the single most effective control against phishing-based account takeover.

Module 9 covers authentication in depth. For now, the takeaway is straightforward: MFA is the backstop that limits the damage of phishing, and enabling it on your accounts is one of the most impactful security actions available to you as an individual.

ShieldNet thread going further

Phishing is addressed directly in two ShieldNet controls. [LL1] (Train and Test Staff) requires regular security awareness training, including phishing simulation exercises because trained people spot phishing attacks that untrained people miss. [SB3] (Enable Multi-Factor Authentication) is the technical backstop that limits damage when phishing succeeds. Together, these two controls address both the human and the technical dimensions of the phishing threat.

Module 4: Summary

By the end of this module, you should be able to:

- ✓ Describe how a phishing attack works and why urgency is the attacker's most powerful tool.
- ✓ Identify at least five red flags that suggest an email or message may be a phishing attempt.
- ✓ Explain the difference between phishing, smishing, and vishing.
- ✓ Describe what pretexting and impersonation are and give an example of each.
- ✓ State the three-step response to a suspicious message: stop, check, report.
- ✓ Explain why MFA limits the damage even when a phishing attack successfully captures a password.

Module 5: Malware

When Software Becomes a Weapon

1. A Story About a Monday Morning

It was a Monday morning in May 2017. Staff at the UK's National Health Service were arriving at work, switching on their computers, and finding the same message on the screen: a red lock icon, a countdown timer, and a demand for the equivalent of £230 in Bitcoin. Their files were encrypted. Patient records were inaccessible. Operating rooms could not function. Ambulances were turned away. Approximately 80 NHS trusts were affected, 19,000 appointments were canceled, and the estimated cost to the NHS alone was £92 million.

The attackers were not specifically targeting the NHS. They were not even specifically targeting the UK. WannaCry was a ransomware worm that spread automatically across the internet, exploiting a vulnerability in unpatched[12] Windows systems. It hit whoever had not applied a two-month-old security update. It hit NHS trusts, Spanish telecoms companies, German railway departure boards, and a Russian interior ministry in the same 24 hours.

This is what malware looks like at scale. It is not targeted, surgical, or personal. It is often indiscriminate, fast-moving, and catastrophic for whoever happens to be in its path. Understanding what malware is, how it gets in, and how to keep it out is not optional knowledge. It is basic digital literacy.

2. What Malware Is

Malware is short for 'malicious software' any program or piece of code designed to cause harm. The harm varies enormously: some malware steals data quietly for months without you knowing; some encrypts your files and demands payment; some hijacks your computer to attack other systems; some simply displays unwanted adverts.

[12] **Patch:** A software update that fixes a security flaw or bug. Applying patches quickly is one of the most effective defenses.

What all malware has in common is that it runs on your device without your genuine informed consent, and it serves the attacker's interests rather than yours. The word covers a wide family of distinct tools, each designed for a different purpose.

Type	What it Does	How it Usually Arrives	What You Notice
Virus	Attaches itself to files or programs and spreads when those files are opened or shared	Infected USB drives, pirated software, email attachments	Files behaving strangely, programs crashing, unexpected slowdowns
Ransomware	Encrypts your files so you cannot access them, then demands payment for the decryption key	Phishing emails, unpatched software vulnerabilities, compromised remote access	Files suddenly unreadable, ransom note appears on screen, system becomes unusable
Spyware	Secretly monitors your activity: keystrokes, screenshots, webcam, browsing then sends it to the attacker	Disguised as legitimate software, bundled with free downloads, malicious ads	Often nothing designed to be invisible. Occasional slowdowns or unexplained data usage
Trojan	Appears to be legitimate software but contains hidden malicious functionality	Fake software updates, cracked applications, links promising free tools	Programme behaves as expected on the surface; malicious activity happens in background
Worm	Spreads automatically across networks without needing a file to attach to; can carry other malware as payload	Unpatched network vulnerabilities, open file shares	Sudden network slowdown, unusual outbound traffic, other devices on the same network becoming infected
Adware	Displays unwanted advertising; often also tracks browsing behavior and sells the data	Bundled with free software installers, browser extensions	Popup adverts, browser homepage changed, search results look different

Malware is delivered, not conjured

Malware does not appear on your device by magic. It always requires a delivery mechanism: an email attachment you open, a link you click, a USB drive you plug in, a software vulnerability that lets it in without any action from you. Understanding how

malware arrives is the key to preventing it because most delivery mechanisms can be disrupted by relatively simple habits.

3. Ransomware: The Most Disruptive Threat to Most Organizations

Of all malware types, ransomware deserves the most attention for one simple reason: it has caused more operational disruption, more financial loss, and more harm to ordinary people's lives through hospitals, schools, councils, and emergency services being taken offline than any other type of attack.

Understanding how a ransomware attack unfolds, stage by stage, explains both why it is so damaging and exactly where defenses can interrupt it.

Stage	Name	What Happens	What You Can Do
1	**Entry**	Attacker gains initial access usually via phishing email, compromised credentials, or an unpatched vulnerability in internet-facing software	Block: MFA, software updates, spam filtering, staff phishing awareness
2	**Spread**	Malware moves laterally through the network, discovering other systems, escalating privileges, identifying backup locations	Limit: network segmentation, least privilege[13] access, monitoring for unusual lateral movement[14]
3	**Preparation**	Attacker identifies and often deletes or encrypts accessible backup copies before triggering the main attack, which is why online backups alone are not sufficient	Protect: offline or immutable backups[15] that cannot be reached from the main network
4	**Encryption**	Files are encrypted rapidly across all reachable systems; ransom note is deployed	Detect early: endpoint detection tools, anomaly monitoring for rapid file changes

[13] **Least privilege:** The principle of giving each person or system only the access they need to do their job, and nothing more.
[14] **Lateral movement:** When an attacker who has gained a foothold moves sideways through a network to reach more valuable systems.
[15] **Immutable backup:** A backup that cannot be changed or deleted for a set period, so ransomware cannot encrypt or destroy it.

Stage	Name	What Happens	What You Can Do
5	**Demand**	Ransom demand appears typically in cryptocurrency to avoid tracing. Often accompanied by threat to publish stolen data (double extortion[16])	Respond: do not pay without professional advice; contact incident response experts immediately
6	**Recovery**	Organization either pays and hopes for decryption, restores from clean offline backups, or rebuilds from scratch	Prepare now: tested offline backups are the only reliable route to recovery without paying

Why hospitals and schools are disproportionately targeted

Ransomware attackers target organizations where operational disruption creates maximum pressure to pay quickly: hospitals that cannot access patient records, schools that cannot function without administrative systems, councils that cannot process benefits or housing. These organizations often have older, unpatched systems and limited IT budgets. They also have strong incentives to restore operations quickly rather than spend weeks rebuilding from scratch.

This is not a coincidence. It is a business model. The attackers are making rational economic calculations about which targets are most likely to pay.

Double extortion: when encryption is not enough

Modern ransomware attacks frequently combine encryption with data theft. Before encrypting files, the attackers copy sensitive data to their own servers. If the organization refuses to pay, the attackers threaten to publish the stolen data publicly which may include patient records, employee information, client data, or commercially sensitive material. This 'double extortion' approach increases the pressure to pay even for organizations that have working backups.

Should you pay the ransom?

Law enforcement agencies across Europe and the US generally advise against paying ransoms, for three reasons: payment funds further attacks, there is no guarantee the

[16] **Double extortion:** A ransomware tactic that both encrypts your files and threatens to publish the stolen data unless you pay.

attackers will provide a working decryption key, and paying once marks you as a payer making you a target again.
In practice, some organizations pay because they have no other viable route to recovery. This is a decision that should be made with professional legal and incident response advice, never alone and never hastily.
The only reliable alternative to payment is a tested, offline backup that the ransomware could not reach. That backup must exist before the attack, not after it.

4. How Malware Gets In: The Delivery Mechanisms

Knowing how malware arrives gives you specific, actionable targets for your defenses. The delivery mechanisms in order of frequency are:

- Phishing emails with malicious attachments or links: the dominant delivery method. Module 4 covered this in detail. Every red flag from that module applies here.
- Unpatched software vulnerabilities: the WannaCry attack exploited a vulnerability that Microsoft had already patched. Every unpatched system is an open door.
- Malicious downloads: pirated software, fake system utilities, free tools from unofficial sources. Cracked applications are one of the most reliable malware delivery vectors.
- Infected USB drives: physical delivery of malware, often through social engineering (the 'lost USB drive' baiting technique from Module 4).
- Compromised websites: malicious code embedded in otherwise legitimate-looking websites that executes when you visit them ('drive-by downloads').
- Supply chain compromise: malware embedded in legitimate software updates from a trusted vendor. Less common but very difficult to defend against individually.

5. The 3-2-1 Backup Rule

If there is one concept from this module to commit to memory, it is the 3-2-1 backup rule. It is the simplest, most effective defense against ransomware for both individuals and organizations.

The 3-2-1 rule
3: Keep at least 3 copies of your data (the original plus 2 backups).
2: Store backups on at least 2 different types of media or in 2 different locations (e.g. an external hard drive and a cloud service).
1: Keep at least 1 copy completely offline or air-gapped[17], inaccessible from your main network. This is the copy that survives ransomware.
The offline copy is the critical element. An external hard drive that is disconnected when not in use, a cloud storage service with immutable versioning enabled, or a tape backup stored offsite all qualify. A second hard drive plugged into the same computer, a network-attached storage device on the same network, or a cloud drive that syncs automatically does not.

For individuals, the 3-2-1 rule is easy to implement: use a cloud backup service (iCloud, Google Drive, OneDrive, Backblaze) as one copy, and an external hard drive that you disconnect after backing up as another. For organizations, the requirements are more formal but the principle is identical.

One more thing that cannot be said often enough: test your backups. Restore a file from your backup today, before you need it. A backup that has never been tested is an assumption. Assumptions are not evidence.

6. Practical Defenses

Malware is not inevitable. The combination of good habits and basic technical controls blocks the vast majority of malware infections before they happen.

Defense	What it Does	How to Apply it
Keep software updated	Patches close the vulnerabilities that malware exploits. An unpatched system is an open invitation.	Enable automatic updates on your operating system and all applications. Do not dismiss update prompts.
Use reputable anti-malware[18]	Detects and removes known malware before it can execute or spread.	Modern operating systems include built-in protection (Windows

[17] **Air-gapped:** Kept physically disconnected from networks, so an attacker on the network cannot reach it. Often used for backups.
[18] **Anti-malware:** Software that detects and removes malicious programs before they can run or spread.

Defense	What it Does	How to Apply it
		Defender, macOS XProtect). Keep it enabled.
Maintain offline backups	Protects your data even if ransomware encrypts everything on your network.	Follow the 3-2-1 rule: 3 copies, on 2 different media, with 1 stored offline or air-gapped.
Test your backups	An untested backup is an assumption. Many organizations discover their backups don't work during the crisis.	Regularly restore a test file from backup to confirm the process actually works end to end.
Be cautious with downloads and attachments	Most malware requires you to run or open something. Your skepticism is a defense.	Only download software from official sources. Verify unexpected attachments before opening them.
Avoid pirated software	Cracked applications are one of the most reliable malware delivery mechanisms.	The cost of legitimate software is almost always less than the cost of a malware infection.
Enable Multi-Factor Authentication	Limits attackers' ability to use stolen credentials to access systems and deploy malware remotely.	Enable MFA on all accounts, especially email, remote access (VPN)[19], and administrative accounts.

The single most impactful action for most people

Enable automatic software updates and stop dismissing them. The majority of successful malware infections exploit vulnerabilities for which patches already exist. WannaCry exploited a vulnerability that had been patched two months earlier. The organizations that applied the patch were not affected. The ones that did not were. Staying updated is not a complex technical task it is a decision to let your device do something it is already designed to do.

ShieldNet thread going further

Malware defenses map directly to three ShieldNet controls. [SB4] (Protect User Devices) covers anti-malware and endpoint protection. [WP3] (Apply Patches Quickly) addresses the vulnerability-closing that prevents malware from exploiting known weaknesses ShieldNet

[19] **VPN:** A Virtual Private Network, which creates an encrypted tunnel for your internet traffic, protecting it on untrusted networks and hiding it from others on the same network.

requires patches within 14 days, and within 48 hours for actively exploited critical vulnerabilities. [KP6] (Plan for Continuity) requires business continuity and disaster recovery planning including tested backup and restoration procedures the organizational equivalent of the 3-2-1 rule.

Module 5: Summary

By the end of this module, you should be able to:

- ✓ Name four types of malware and describe what each one does.
- ✓ Explain in plain language how ransomware works, from initial entry to ransom demand.
- ✓ Describe why attackers target backups during a ransomware attack, and what the 3-2-1 backup rule means.
- ✓ Identify three specific actions you can take personally to reduce your exposure to malware.
- ✓ Explain why keeping software updated is one of the most effective defenses against malware.
- ✓ Describe what ‘double extortion’ means in the context of ransomware.

Module 6: Passwords and Account Takeover

The Keys to Your Kingdom

1. The Problem With Passwords

We were told to use passwords to protect our accounts. Then we were told to make them complex upper and lower case, numbers, symbols. Then to make them unique for every account. Then to change them regularly. Then not to write them down. Then to use a password manager. Then to use multi-factor authentication on top of all of that.

No wonder people end up using 'Password1!' on everything.

The fundamental problem is that good password security as traditionally taught is genuinely difficult for humans to do, while being increasingly easy for automated tools to defeat. A modern password-cracking rig can test billions of combinations per second. The word 'complex' has been redefined by computers to mean something entirely different from what it means to a person.

This module explains how passwords get stolen, what makes a password actually strong (rather than just technically complex), and most importantly the practical approaches that solve the problem without requiring you to memorize 80 different impossible strings of characters.

2. How Passwords Get Stolen

There are six main ways attackers acquire your credentials. Understanding them shows you exactly which habits close which doors.

Method	How it Works	What The Attacker Gets	How Common
Data breach	A service you use is hacked and its user database is stolen. Your email and password hash[20] (or plain text) are exposed.	Your email address paired with your password for that service usable immediately if not hashed, or crackable offline if hashed weakly	Extremely common. Billions of credentials are in circulation from past breaches.

[20] **Password hash:** A scrambled version of a password that websites store instead of the real password, so the original is not kept in plain form.

Method	How it Works	What The Attacker Gets	How Common
Credential stuffing	Automated tools test leaked username/password pairs against hundreds of websites. Only needs one reused password to succeed.	Access to every account where you reused that password: email, banking, shopping, work systems	Automated and continuous. Runs 24/7 against major platforms.
Password guessing / spraying	Tries common passwords (123456, password, qwerty) against many accounts, or tries many passwords against one target account.	Access to accounts with weak or predictable passwords	Very common against accounts with no lockout policy.
Keylogging	Malware records every keystroke as you type, capturing passwords as you enter them.	Every password you type while the malware is active real-time capture	Common via phishing-delivered malware
Phishing	You are directed to a fake login page that looks identical to the real one. You type your credentials into the attacker's form.	Your username and password, plus sometimes MFA codes if a real-time relay is used	The most widely used credential theft method. Covered in depth in Module 4
Shoulder surfing	Someone physically observes you entering a password in a café, on a train, at a shared workspace	Whatever password you typed	Low-tech but effective in public or open-plan environments.

The credential stuffing chain reaction

Here is how a single data breach at a small retail website turns into a banking fraud. Step 1: the retail site is breached and your email plus password are stolen. Step 2: automated tools test that email/password combination against 500 popular websites. Step 3: your email provider accepts the login. Step 4: from your inbox, the attacker uses 'forgot my password' to reset your banking password. Step 5: your bank account is accessed. This entire chain can complete in under 30 minutes after the initial breach, with no human involvement after Step 1. Password reuse is the single link that makes this chain possible.

3. What Makes a Password Actually Strong?

The conventional wisdom uppercase, lowercase, numbers, symbols produces passwords that are hard for humans to remember and not as hard for computers to crack as you might think. Modern cracking tools know about character substitutions (a→@, o→0, e→3) and common patterns (capitalize the first letter, put the number and symbol at the end). 'P@ssw0rd!' is not a strong password.

What actually matters to a computer trying to crack your password is length and unpredictability. A longer, genuinely random password takes exponentially more time to crack than a shorter, seemingly complex one.

Password	Why it's weak or strong	Time to crack (rough estimate)	Verdict
password	One of the most commonly used passwords in the world. Appears in every breach list.	Milliseconds	❌ Very weak
P@ssw0rd1	Letter substitutions (a→@, o'0) are well-known to cracking tools and add minimal security.	Seconds to minutes	❌ Weak.
Summer2024!	A predictable pattern: common word + year + symbol. Easy for tools trained on real passwords.	Minutes to hours	⚠ Marginal
horse-battery-staple-7	Four random words joined by hyphens. Long, memorable, and very hard to crack.	Millions of years	✅ Strong
j#Kp!2mNqR8&vL	14 random characters mixing upper, lower, numbers and symbols. Impossible to remember but ideal for a password manager.	Billions of years	✅ Very strong

The passphrase approach

Four or more unrelated random words strung together a passphrase gives you a long, memorable, and genuinely strong password. The classic example is 'correct horse battery staple' (from a well-known security comic). The words do not need to make grammatical sense. What matters is that they are random (not 'my dog's name is Biscuit', but 'lamp-ocean-cathedral-seventeen') and that you use a different passphrase for each account.

4. The Password Manager: Solving the Problem Properly

The honest reality is that no human being can maintain strong, unique passwords for dozens of accounts from memory. The math does not work. If you are trying to do it mentally, one of the following is almost certainly true: you are reusing passwords, you are using weak passwords, or both.

A password manager is software that generates and stores strong, unique passwords for every account you have. You need to remember only one password the master password that unlocks the manager itself. The manager handles everything else: generating a random 20-character password for each site, storing it securely, and filling it in automatically when you log in.

How password managers work

Your passwords are stored in an encrypted vault. The vault is locked with your master password, which the password manager itself never sees or stores it is used only to decrypt the vault locally on your device. Even if the password manager company's servers are breached, the attackers get encrypted data that is useless without your master password.

When you visit a website, the manager recognizes it and fills in your credentials automatically. This has an additional security benefit: it will not fill in credentials on a fake website, because the domain does not match. Password managers are therefore a partial defense against phishing as well.

Choosing and setting up a password manager

- Well-regarded options include Bitwarden (free and open-source), 1Password, Dashlane, and the built-in managers in iOS (iCloud Keychain) and Android/Chrome (Google Password Manager). All of the major options are substantially more secure than trying to remember passwords yourself.
- Set a strong master password this is the one password you must remember. A long passphrase works well here.
- Enable multi-factor authentication on the password manager itself. This is the single most important security setting for your password manager.

- Gradually migrate your existing accounts: whenever you log in to a service, let the manager save or generate a new strong password for it. You do not need to change everything at once.

The one objection: what if the password manager is hacked?
This concern deserves a direct answer. A good password manager with a strong master password and MFA is far harder to breach than the dozens of websites where you currently store reused passwords. The alternative reusing passwords across accounts virtually guarantees that a breach at any one of those sites gives attackers access to all of them. The risk of a well-designed password manager being breached in a way that exposes your passwords is significantly lower than the near-certainty of credential stuffing succeeding if you reuse passwords.

5. What Happens After an Account Is Taken Over

Understanding what attackers do once they have your credentials explains why account takeover is so damaging and why recovery can be so difficult.

If They Got Your...	They Can Immediately...	Why it Matters
Email account	Reset passwords for every service linked to that email; read all your messages; impersonate you to your contacts; access any files shared with that address	Email is the master key. Losing email access is losing access to everything else.
Banking or payment app	Transfer money; set up new payees; apply for credit; change contact details to lock you out	Direct financial loss. Can take weeks to reverse, if ever fully.
Work account or email	Send emails as you; access company files and systems; launch attacks on your colleagues; commit fraud using your identity	Can cause serious professional and legal consequences beyond just your own data.
Social media	Message your friends and family with convincing scams; post content in your name; sell the account; use it to access other services you logged into via that account	Your contacts trust you. A message from 'you' is far more convincing than a cold approach.

If They Got Your...	They Can Immediately...	Why it Matters
Password manager (if unprotected)	Access every password stored inside it: a single breach givies complete access to your entire digital life	This is why the master password and MFA on your password manager are the most critical credentials you have.

The common thread across all of these scenarios is speed. Account takeovers happen fast. Automated tools act on stolen credentials immediately. The window between a breach occurring and an attacker acting on it is often measured in minutes, not hours. This is why prompt action when you suspect a compromise changing passwords, enabling MFA, contacting your bank matters so much.

6. MFA: The Backstop That Changes Everything

Multi-factor authentication was introduced in Module 4 as a defense against phishing. Here it appears again, because it is equally critical as a defense against credential theft. The principle is the same: even if an attacker has your password, they still need your second factor.

For most accounts, the second factor is a six-digit code from an authenticator app that changes every 30 seconds. The attacker has the password but not the phone. They cannot log in.

Not all MFA methods are equal. From strongest to weakest:

- Hardware security keys (YubiKey, Google Titan) a physical device you plug in or tap. Near-impossible to phish remotely.
- Authenticator app codes (Google Authenticator, Microsoft Authenticator, Authy) time-based codes that require possession of your phone. Strong and practical for most people.
- Push notifications (approve/deny via app) convenient but vulnerable to 'MFA fatigue' attacks where the attacker sends dozens of approval requests until the user approves one by accident.
- SMS codes (one-time codes sent by text) better than nothing, but vulnerable to SIM-swapping attacks where an attacker convinces a mobile carrier to transfer your number.
- No MFA a stolen password is a complete account compromise.

The practical recommendation for most people: use an authenticator app for your most important accounts (email, banking, work systems, password manager) and SMS codes as a fallback for services that do not offer an app option. Anything is better than nothing. Authenticator apps are better than SMS. Hardware keys are the strongest option for very high-value accounts.

7. Three Actions You Can Take Today

This module has covered a lot of ground. Here are the three most impactful things you can do immediately:

- Check haveibeenpwned.com[21]: Enter your email address to see whether it has appeared in a known data breach. If it has, change the password on that account and any account using the same password. This takes five minutes and gives you a clear starting point.
- Set up MFA on your most important accounts: Start with your primary email account. Download an authenticator app (Microsoft Authenticator, Google Authenticator, or Authy all free). Follow the instructions in your email provider's security settings to link the app. This takes ten minutes and dramatically improves the security of your email which, as we established, is the key to everything else.
- Start using a password manager: Choose one from the options in section 6.4 and set it up with a strong master password and MFA. Begin migrating your accounts as you log in to them over the next few weeks. Within a month, your most-used accounts will have unique, strong passwords that you did not have to memorize.

ShieldNet thread going further

Passwords and account security map to two ShieldNet controls. [SB1] (Control User Access) requires unique accounts for every person and service, with access rights limited to the minimum necessary the organizational expression of the unique-password principle. [SB3] (Enable Multi-Factor Authentication) requires MFA on all remote logins and important accounts, covering administrators, email, VPN, and cloud dashboards. These controls exist in organizations for the same reason the advice in this module exists for individuals: credential reuse and absence of MFA are the two most exploited weaknesses in account security.

[21] **haveibeenpwned.com:** A free service that tells you whether your email address or passwords have appeared in known data breaches.

Module 6: Summary

By the end of this module, you should be able to:

- ✓ Explain what credential stuffing is and why password reuse makes it so effective.
- ✓ Describe the difference between a weak password and a strong one, with a specific example of each.
- ✓ Explain what a password manager is and why using one is the most practical solution to the password problem.
- ✓ State what an attacker can typically do after gaining access to an email account.
- ✓ Describe how MFA protects an account even after the password has been stolen.
- ✓ Name three actions you can take today to improve your personal password security.

Module 7: Networks and the Internet

How Data Travels and Where It Can Go Wrong

1. The Invisible Infrastructure

Every time you open a webpage, send a message, or stream a video, your data travels across a complex global infrastructure that most people never think about. It leaves your device, passes through your router, crosses your internet provider's network, bounces through multiple servers, and arrives at its destination all in a fraction of a second.

Most of the time this works invisibly and reliably. But that journey creates multiple points where something can go wrong, where data can be intercepted, or where an attacker can position themselves between you and your destination.

This module does not require you to understand how networks work at a technical level. What it does require is enough understanding to make sensible decisions about the risks you face: when to use public Wi-Fi and when not to, what a VPN actually does, and why the little padlock in your browser matters more than most people realize.

2. A Few Concepts Worth Understanding

You do not need a networking qualification to understand internet security. But a handful of concepts appear constantly and are worth having a clear mental model for.

Concept	Plain Meaning	Everyday Example	Why it Matters
IP address	A unique number assigned to every device on a network like a postal address for data	Every house has a street address. Every device has an IP address.	IP addresses are logged by every website and service you visit. They can be used to identify your approximate location and, with a court order, your identity.
DNS	The system that translates human-readable website names (google.com) into the numerical IP addresses computers actually use	A phone book that converts a name into a phone number.	DNS requests are often unencrypted, revealing which websites you visit to your internet provider or any network observer even if the websites themselves use HTTPS.

Concept	Plain Meaning	Everyday Example	Why it Matters
Router	A device that connects your local network (home, office) to the wider internet and directs traffic between them	A post office sorting hub receives packages, figures out where they're going, and sends them on	A compromised router can intercept or redirect all traffic passing through it. Home routers with default passwords are a common attack target.
Packet	Data traveling across the internet is broken into small chunks called packets, sent separately, and reassembled at the destination	Sending a long letter by cutting it into ten sections and posting each one in a separate envelope.	Unencrypted packets can be read by anyone on the network path between you and the destination. HTTPS encryption makes the contents unreadable even if intercepted.
Protocol	A set of rules governing how computers communicate like a shared language both sides must speak	The conventions that make a phone call work: one person speaks, the other listens, then they switch.	Insecure protocols (HTTP, older SSL versions) expose data. Secure protocols (HTTPS with TLS 1.2+) encrypt it.

The postal system analogy for the internet

Think of the internet as a global postal system. Your device is a house with an address (IP address). The router is your local post office. Data is broken into envelopes (packets) and sent separately, each routed to the right destination by the postal system. The phone book that translates names to addresses is DNS. HTTPS is like sending your letters in sealed, tamper-evident envelopes that only the recipient can open. HTTP is like sending postcards anyone who handles them along the way can read them.

3. HTTP vs HTTPS: The Padlock That Actually Matters

When you visit a website, it uses one of two protocols: HTTP or HTTPS. The difference is fundamental to your security.

HTTP: the postcard

HTTP (HyperText Transfer Protocol) sends data in plain text. Anyone on the network path between you and the server your ISP, a router you pass through, someone on the same Wi-Fi network can read the content. Any credentials you type, any form you fill

in, any page you load is visible in plain text. Today, using HTTP for anything that involves personal data or login credentials is indefensible.

HTTPS: the sealed envelope

HTTPS (the S stands for Secure) encrypts the connection between your browser and the server using a protocol called TLS. Even if an attacker intercepts the data packets, they cannot read the contents. The padlock icon and 'https://' in your browser's address bar confirm an encrypted connection is in place.

> **Important: HTTPS confirms encryption, not legitimacy**
> A common misconception is that a padlock means the website is trustworthy. It does not. It means the connection is encrypted. Criminals routinely obtain valid HTTPS certificates for phishing websites the site fakepaypal.com can have a padlock just as easily as paypal.com. The padlock tells you that nobody in between can read your traffic. It tells you nothing about whether the person at the other end is who they claim to be. Always check the domain name, not just the padlock.

4. Public Wi-Fi: Convenient and Risky

Free Wi-Fi in coffee shops, airports, hotels and stations is one of the most convenient things the internet has given us. It is also one of the most commonly exploited attack surfaces for opportunistic attackers.

The core problem is that public networks are shared. Everyone connected to the same access point is, in a meaningful technical sense, on the same network. On a properly managed network, this is handled with isolation controls. On many public networks, it is not.

Risk	What the Attacker Does	How to Protect Yourself
Eavesdropping on unencrypted traffic	Passively captures all unencrypted data on the network any website using HTTP (not HTTPS) is readable in plain text	Only access sites using HTTPS (look for the padlock). Most modern browsers warn you about HTTP sites. Avoid entering any sensitive information on non-HTTPS pages.
Evil twin access point	Sets up a Wi-Fi hotspot with the same name as a legitimate network (e.g. 'Starbucks WiFi'). Your device connects automatically. All traffic passes through the attacker.	Verify the exact network name with staff. Avoid connecting to networks without a password. Use mobile data instead of public Wi-Fi for sensitive tasks. A VPN encrypts traffic even

Risk	What the Attacker Does	How to Protect Yourself
		through a compromised access point.
Man-in-the-middle	Positions themselves between you and the destination server, relaying traffic while reading or modifying it. Can present fake certificates to decrypt HTTPS traffic on vulnerable systems.	Keep your operating system and browser updated (patches close certificate vulnerabilities). Enable HTTPS-only mode in your browser. Use a VPN on public networks.
Network scanning and exploitation	Scans for other devices on the same public network, looking for open file shares, unpatched services, or devices using default credentials	Enable your device's firewall. Turn off file sharing when on public networks. Keep devices patched. Do not leave remote access services running unnecessarily.

Practical rules for public Wi-Fi

Verify the network name with staff before connecting. Ask 'what's the Wi-Fi name?' do not assume the most prominent network in the list is legitimate.

Avoid accessing banking, work systems, or anything sensitive on public Wi-Fi unless you are using a VPN or your organization's secure remote access solution.

Use your mobile data connection (4G/5G) instead of public Wi-Fi for sensitive tasks when possible. Mobile data is significantly harder to intercept than open Wi-Fi.

Enable HTTPS-only mode in your browser. Modern browsers (Chrome, Firefox, Safari, Edge) all offer this setting. It forces encrypted connections and warns you when a site tries to load over HTTP.

Consider a VPN for regular public Wi-Fi use but understand what it does and does not protect (see section 5).

5. VPNs: What They Do and What They Don't

VPN stands for Virtual Private Network. It is one of the most marketed and most misunderstood tools in consumer security. Understanding what a VPN actually does and crucially, what it does not do lets you use it appropriately rather than relying on it for protection it cannot provide.

A VPN creates an encrypted tunnel between your device and a VPN server. All your traffic travels through that tunnel. From the perspective of anyone on your local network (a café Wi-Fi router, for example), they can see that you are connected to a

VPN server, but not what websites you are visiting or what data you are sending. From the perspective of the websites you visit, your traffic appears to come from the VPN server's IP address, not yours.

	What a VPN DOES Protect	What a VPN does NOT Protect
Traffic content	Encrypts data between your device and the VPN server, protecting it from anyone on your local network (café Wi-Fi, ISP on home broadband)	Once traffic leaves the VPN server, the VPN provider can see it. You are trusting the VPN provider instead of your ISP.
Your IP address	Hides your real IP address from websites and services you visit they see the VPN server's IP instead	Does not make you anonymous. Websites still track you via cookies[22], browser fingerprinting, and logins. The VPN provider knows your real IP.
Malware and phishing	Some VPNs include basic DNS filtering that blocks known malicious domains	A VPN does not protect you from clicking a phishing link, downloading malware, or entering credentials on a fake site. It is not an antivirus.
Work network security	Corporate VPNs connect you securely to your organization's network, allowing access to internal resources from anywhere as if you were in the office	Corporate VPNs route your work traffic through the organization's security systems, which means IT can monitor that traffic by design.

The bottom line on VPNs: they are a useful tool for one specific job protecting your traffic from observation on untrusted networks. They are not a comprehensive privacy or security solution. A VPN does not make you anonymous, does not protect you from phishing, and does not replace other security practices.

For work use, the corporate VPN your organization provides is different from consumer VPNs: it connects you to your organization's internal network and routes work traffic through organizational security controls. Follow your organization's guidance on when it must be used.

6. Your Home Network: The Forgotten Attack Surface

[22] **Cookie:** A small file a website stores in your browser to remember you. Some cookies are necessary; others track your activity for advertising.

Most people pay careful attention to security on work devices and work networks. Fewer people think carefully about their home network even though it is the network their work laptop, their phone, and increasingly their smart home devices all connect to.

Change your router's default credentials

Every router ships with a default administrator username and password. These defaults are often printed on the router itself and are published in public documentation for every model. An attacker who can reach your router through a vulnerability in the router's remote management interface, for example can log in with the default credentials and take complete control of your network traffic.

Log into your router's administration panel (usually accessible at 192.168.0.1 or 192.168.1.1) and change both the admin password and the Wi-Fi password if they are still factory defaults.

Keep your router's firmware updated

Routers run software (firmware) that, like any software, contains vulnerabilities. Router manufacturers release firmware updates to patch these vulnerabilities. Many routers can be set to update automatically enable this if the option exists. A router running three-year-old firmware is running known, unpatched vulnerabilities.

Separate your IoT devices

Smart TVs, home assistants, connected cameras, and other 'Internet of Things' devices often have weaker security than computers or phones. Many home routers support a 'guest network' a separate Wi-Fi network that is isolated from your main one. Putting IoT[23] devices on the guest network means that if one is compromised, it cannot easily reach your laptop or phone.

7. The Key Habits

Networking concepts can feel abstract. The habits that translate this module into daily practice are concrete:

[23] **IoT:** The Internet of Things, the many everyday devices that connect to the internet, such as cameras, doorbells, thermostats, and smart speakers.

- Always check for HTTPS (the padlock and https:// prefix) before entering any personal information or credentials on a website.
- Enable HTTPS-only mode in your browser settings it forces encrypted connections automatically.
- Verify the exact Wi-Fi network name with staff before connecting on public networks.
- Use mobile data instead of public Wi-Fi for sensitive tasks when possible.
- Change your home router's default admin password and Wi-Fi password if you have not already.
- Keep your router's firmware updated, or enable automatic updates if available.
- Use your organization's VPN when working remotely on an untrusted network, as directed by your IT team.

ShieldNet thread going further

Network security maps to two ShieldNet controls. [SB5] (Secure Your Network) requires organizations to use firewalls, block unwanted traffic, and segment networks so that critical systems are isolated from general access the organizational equivalent of the home router hardening[24] and IoT isolation discussed in this module. [SB7] (Encrypt Sensitive Data) requires HTTPS/TLS for data in transit the control that underlies the padlock and HTTPS habits covered in sections 3 and 4.

Module 7: Summary

By the end of this module, you should be able to:

- ✓ Explain in plain language what an IP address and DNS are, and why DNS matters for privacy.
- ✓ Describe what a man-in-the-middle attack is and how HTTPS protects against it.
- ✓ Explain two specific risks of using public Wi-Fi and describe one practical defense for each.
- ✓ Describe what a VPN does and, equally importantly, what it does not protect you from.
- ✓ Explain the difference between HTTP and HTTPS and how to identify a secure connection.
- ✓ State two practical habits for staying safer on any network.

[24] **Hardening:** Reducing a system's weak points by turning off unnecessary features, closing unused access, and applying secure settings.

Module 8: Who Are the Attackers?

Motivations, Targets and Methods

1. The Person on the Other Side

Security is often discussed as if it were a battle against abstract forces: 'threats', 'actors', 'adversaries'. But there are people on the other side of every attack. People with motivations, constraints, tools, and goals. Understanding who they are, not to humanize harmful behavior, but to understand what they want and how they operate, makes security decisions far more practical.

The most dangerous misconception about attackers is that they are all sophisticated, patient, highly skilled individuals targeting you specifically. The reality is more varied, more mundane, and in many ways more useful to understand. Most attacks on most organizations and individuals are carried out by people or automated systems doing the digital equivalent of trying every door handle in a street, looking for one that is unlocked.

Knowing the difference between someone trying every door and someone specifically targeting yours changes how you defend yourself and makes clear why basic security hygiene eliminates the vast majority of risk faced by most people most of the time.

2. The Attacker Landscape

Attackers are not a single category. They range from teenagers running scripts they downloaded online to professional criminal enterprises with HR departments, from disgruntled employees with legitimate system access to state-sponsored intelligence operations with multi-year infiltration campaigns. What they share is intent to cause harm whether for money, politics, revenge, or ideology.

Who they are	Primary motivation	Typical targets	Methods	What stops them
Cybercriminals	Financial gain direct theft, ransomware, fraud, selling stolen data	Anyone with money, data, or systems worth exploiting. Hospitals, businesses, individuals equally	Ransomware, phishing, credential stuffing, business email compromise, fraud	MFA, patching, backups, staff training. They move to easier targets.

Who they are	Primary motivation	Typical targets	Methods	What stops them
Opportunists (script kiddies[25])	Curiosity, notoriety, or low-effort financial gain using tools they did not build	Easy, unprotected targets. They scan the internet for open doors.	Automated scanning tools, publicly available exploit kits, default credential attacks	Basic hardening makes you invisible to automated scans. They do not persist.
Insider threats[26]	Revenge, financial distress, coercion by third parties, or simple negligence	Employers and organizations they have legitimate access to	Misuse of existing access rights, data exfiltration, sabotage, accidental misconfiguration	Least privilege access, monitoring, offboarding
Hacktivists[27]	Political or ideological goals embarrassing organizations, disrupting operations, publicizing causes	Government agencies, corporations, organizations they disagree with ideologically	DDoS attacks, defacement of websites, data leaks, social media campaigns	DDoS protection, incident response planning, PR and communications strategy
Nation-state actors[28]	Political advantage, military intelligence, economic espionage, destabilization	Critical infrastructure, government agencies, defense contractors, key industries	Advanced persistent threats[29] (APTs), supply chain attacks, zero-day exploits, long-term infiltration	Hardened architecture, threat intelligence, government partnerships, defense-in-depth[30]

[25] **Script kiddie:** An unskilled attacker who uses tools and exploits made by others, usually for low-effort, opportunistic attacks.
[26] **Insider threat:** A risk that comes from someone inside the organization, whether malicious, negligent, or simply careless.
[27] **Hacktivist:** An attacker motivated by a political or social cause, who may deface websites or leak data to make a point.
[28] **Nation-state actor:** A well-resourced attacker working for or on behalf of a government, capable of sophisticated and persistent operations.
[29] **APT:** An Advanced Persistent Threat, a skilled and well-funded attacker that gains access and stays hidden in a network for a long time.
[30] **Defense in depth:** Using several layers of protection, so that if one layer fails, others still stand.

Who they are	Primary motivation	Typical targets	Methods	What stops them
Organized crime groups	Large-scale financial gain, often operating as businesses with specialists	High-value organizations: banks, insurers, healthcare, legal firms	Sophisticated multi-stage attacks, money laundering infrastructure, ransomware-as-a-service	Advanced detection, incident response, law enforcement cooperation, insurance

The most common attacker you will ever face

For the vast majority of organizations and individuals, the most likely attacker is a financially motivated cybercriminal or an opportunist using automated tools. These attackers are not targeting you specifically they are running mass campaigns looking for easy wins. An organization with patched systems, MFA, trained staff, and tested backups is not an easy win. The attacker's tool moves on. This is why basic security hygiene has such a high return: it eliminates most of your realistic risk without requiring sophisticated defenses.

3. Opportunistic vs Targeted: A Critical Distinction

The single most practically useful way to think about attacks is the distinction between opportunistic and targeted. It directly answers the question every person and organization asks: 'Why would someone target us?' The answer, for most attacks, is that they did not. You were not targeted. You were found.

	Opportunistic Attack	Targeted Attack
Who is affected	Whoever happens to be vulnerable and reachable no prior knowledge of the victim	A specific organization, system, or individual chosen deliberately
How targets are identified	Automated scanning of the internet for known vulnerabilities, open ports, default credentials	Research using public information (LinkedIn, company website, job postings, previous breaches)
Effort required	Low, largely automated, requires minimal skill, runs continuously	High, requires reconnaissance, custom tools or tactics, patience
What makes you a target	Being unprotected. Default passwords, unpatched software,	Your organization's industry, size, political profile, data holdings, or

	Opportunistic Attack	Targeted Attack
	open ports anything an automated scanner can find.	known relationships with other targets
Primary defense	Basic hygiene: patch, harden, use MFA. Remove easy entry points and automated tools move on.	Depth of defense: monitoring, threat intelligence, incident response capability, supply chain security

Size does not protect you from opportunistic attacks

A common belief is that small organizations or individuals are too small to bother attacking. This is true for targeted attacks a sophisticated criminal gang is unlikely to spend weeks researching a ten-person business. But it is entirely false for opportunistic attacks. Automated scanners do not check the size of an organization before probing its systems. A small accounting firm with an unpatched server is just as visible and just as reachable as a large corporation with the same vulnerability. The scanner does not care. Size is irrelevant to automated tools. Security posture is everything.

4. The Insider Threat: The Risk From Within

Not every security failure comes from outside the organization. Insider threats harm caused by people who already have legitimate access to systems or data are consistently underestimated and consistently costly.

The term covers a wider range of people and behaviors than most imagine:

- Malicious insiders: Current or former employees, contractors, or partners who deliberately misuse their access to steal data, sabotage systems, or assist external attackers. Often motivated by financial distress, grievances, or coercion.
- Negligent insiders: People who cause harm without intending to clicking a phishing link, misconfiguring a system, sharing data with the wrong person, or failing to follow security procedures. This category causes the majority of insider incidents.
- Compromised insiders: Employees whose credentials have been stolen and whose accounts are being used by an external attacker. The person did not do anything wrong, but their access is being misused.

Insider threats are particularly difficult to detect because the activity looks legitimate from a system's perspective. A user accessing files they are authorized to access does not trigger obvious alarms. The defenses that help are not technical in the first place: clear access policies, least-privilege access so people can only reach what they need, prompt revocation of access when someone leaves, and a culture where people feel comfortable reporting concerns.

> **The human dimension of insider risk**
> Most insider incidents do not begin with malice. They begin with a person under pressure financial difficulty, a difficult manager, an organization that has treated them unfairly who makes a decision they would not have made otherwise. This does not excuse the harm. But it does suggest that organizations that invest in their people, treat them well, and give them legitimate channels to raise concerns are less likely to face insider incidents than those that do not. Security is not only a technical problem.

5. Supply Chain Attacks: When Trusted Software Becomes the Threat

One of the most difficult categories of attack to defend against individually is the supply chain attack. The premise is straightforward and troubling: instead of attacking your organization directly, the attacker compromises something your organization trusts a software vendor, an IT service provider, a development tool, an open-source library and uses that trust as the entry point.

Supply chain attacks are concerning precisely because they can succeed against organizations that have done everything right internally. Your systems are patched. Your staff are trained. Your credentials are protected. And then you install a legitimate software update from a trusted vendor, and that update contains malware.

Attack Route	What Happens	Real Example
Compromised software update	Attacker infiltrates a software vendor and injects malware into a legitimate update, which is then distributed to all the vendor's customers	SolarWinds (2020): a malicious update to network management software reached approximately 18,000 organizations including US government agencies
Compromised development tools	Malicious code is injected into the tools developers use to build software, contaminating software before it is even packaged	XcodeGhost (2015): a fake version of Apple's Xcode development tool was used to inject malware into iOS apps,

Attack Route	What Happens	Real Example
		including some that reached the App Store
Compromised third-party service provider	An IT support company, managed service provider, or cloud tool with privileged access to multiple customers is compromised and used as a stepping stone	Kaseya VSA (2021): ransomware deployed through a remote management tool used by IT service providers, reaching around 1,500 businesses in one attack
Malicious open-source package	A developer unknowingly uses a malicious or compromised open-source library, which ships malware inside their application	Numerous npm and PyPI packages have been found to contain credential stealers or backdoors with convincing but fake names

For most people reading this course, supply chain attacks are not something you can personally prevent they happen at a level above individual control. What you can do is support the organizational practices that limit the blast radius[31]: apply the principle of least privilege to software and services as well as users, monitor for unusual behavior from trusted tools, and ensure that vendor security is part of procurement decisions (which is what ShieldNet's [KP7] Vet Suppliers control addresses).

6. Nation-State Actors: Real, But Not Your Most Likely Threat

Nation-state cyberattacks receive disproportionate coverage in the news. They are real, they are sophisticated, and they have caused genuine harm: the disruption of Ukrainian power grids, the theft of intellectual property from defense contractors, the interference in electoral processes. But for the overwhelming majority of organizations and individuals, a nation-state actor is not the threat they should be designing their security program around.

Nation-state actors choose targets for strategic reasons: geopolitical intelligence value, military significance, critical infrastructure leverage, or economic espionage. A small marketing agency, a local council, a school, or an individual professional is not on that list unless they have a specific connection to something that is.

[31] **Blast radius:** How far an attacker can reach once they compromise one account or device. Least privilege keeps the blast radius small.

The practical implication: design your security for the threats you actually face. For most organizations, that means financially motivated criminals and opportunistic automated attacks. The defenses that work against those threats patching, MFA, trained staff, tested backups, access controls also provide a baseline of protection against more sophisticated actors. Start there.

7. What This Means for How You Think About Security

Completing Part 2 gives you a more accurate mental model of the threat landscape than most people including many people working in organizations carry around. Three ideas should stick from this module:

- Most attacks are not targeted at you. They are automated, indiscriminate, and looking for easy opportunities. Basic hygiene removes you from the easy-opportunity category.
- The people who do target specifically whether criminals, insiders, or sophisticated actors all rely at some point on a human mistake or a technical weakness. There is no attack that bypasses both a well-prepared person and a well-maintained system simultaneously.
- Understanding who is attacking and why allows proportionate response. Not every organization needs nation-state-level defenses. Most organizations need solid, consistent fundamentals applied well. That is what Part 3 provides.

ShieldNet thread going further

The attacker landscape directly informs two ShieldNet controls. [KP4] (Assess Risks Regularly) asks organizations to identify the threats most relevant to their specific context a healthcare provider faces different likely attackers from a software startup. [SB2] (Secure Hiring and Exit) addresses the insider threat directly: vetting people before they join, and revoking all access on the day they leave. [KP7] (Vet Suppliers) addresses supply chain risk: understanding who your technology providers are and what security standards they meet before you grant them access to your systems.

Module 8: Summary

By the end of this module, you should be able to:

✓ Name four types of attacker, describe their primary motivation, and give an example of the methods they use.

- ✓ Explain the difference between an opportunistic attack and a targeted attack, and describe what makes each one more or less likely to succeed against you.
- ✓ Describe what an insider threat is and explain why it is difficult to defend against.
- ✓ Explain what a supply chain attack is and give one example of how it can affect organizations that did everything 'right' internally.
- ✓ Explain why basic security hygiene (patching, MFA, hardening) is an effective defense against the most common category of attacker.

Completing Part 2

Part 2 is complete. You now have a concrete picture of how attacks happen and who carries them out:

Module 4: Phishing and social engineering exploiting human psychology through urgency, authority and deception.

Module 5: Malware ransomware, spyware, trojans and the 3-2-1 backup rule.

Module 6: Passwords and account takeover credential theft, stuffing, and why MFA changes the calculation.

Module 7: Networks and the internet how data travels, public Wi-Fi risks, and what a VPN actually does.

Module 8: Who the attackers are motivations, targeted vs opportunistic, insider threats, supply chain attacks.

Part 2 Knowledge Check

Module 4 Practice Questions
Q1. You receive an email from 'PayPal Security' (the sender address shows: paypal-security-check@paypal.support.billing-confirm.net). The email says your account has been compromised and asks you to click a link to verify your identity within 2 hours or your account will be permanently suspended. What should you do? a. Click the link quickly, as the 2-hour deadline suggests this is a genuine emergency. b. Reply to the email asking for more information before taking action. c. Do not click the link. The sender domain is not from PayPal. Open your browser, go directly to paypal.com, and log in to check whether there is actually an issue with your account. d. Forward the email to your colleagues to warn them about the scam.
Q2. A colleague calls you unexpectedly, says they are locked out of a shared system, and asks for your login credentials so they can complete an urgent task before a client deadline. You recognize their voice. What is the correct response? e. Provide the credentials, as you recognize the voice and the situation sounds genuine. f. Ask them to send the request by email so you have a written record. g. Refuse to share your credentials regardless of the reason. Offer to help them contact IT support to resolve the lockout instead. h. Ask them a security question to confirm their identity before sharing
Q3. You find a USB drive in your company's reception area. It is labeled 'Staff Pay Review 2026 Confidential'. What should you do? i. Plug it into your computer to check its contents, then hand it to HR if it contains salary information. j. Leave it where it is: it probably belongs to a colleague who will return for it. k. Do not plug it in. Hand it to your IT team or manager and report where you found it. l. Take it to the manager whose name appears to be referenced, so they can review the confidential information.
Q4. A phishing attack successfully tricks an employee into entering their username and password on a fake login page. The organization uses multi-factor authentication (MFA) on all accounts. What is the most likely outcome? m. The attacker now has full access to the employee's account, because they have the credentials. n. The attacker cannot log in, because MFA requires a second factor (such as a code from an authenticator app) that the attacker does not have. o. The attacker can access the account but only for a limited time before the session expires. p. MFA has no effect once credentials are stolen, the account is compromised regardless.

Module 5 Practice Questions
Q1. A hospital's IT systems are hit by ransomware. All files on the main server are encrypted and a ransom note demands €200,000 in cryptocurrency. The IT team checks the backup system and finds the backups were also encrypted, because they were stored on a network drive accessible from the main server. What fundamental backup principle was not followed? a. The backups were not encrypted with a strong enough algorithm. b. The backups were not stored offline or in an isolated location inaccessible from the main network, so ransomware was able to reach and encrypt them. c. The backups were taken too infrequently daily backups would have prevented the encryption. d. The hospital should have used cloud backups instead of a network drive.
Q2. A user downloads what appears to be a legitimate video editing application from a third-party website. The application works as advertised, but over the following weeks the user's online banking credentials are stolen and used fraudulently. Which type of malware best explains this scenario? e. Ransomware: the application encrypted the user's credentials. f. Worm: the application spread to other devices on the network. g. Trojan: the application appeared legitimate but contained hidden malicious functionality, likely a keylogger or credential stealer. h. Adware: the application displayed advertising that contained the malicious content.
Q3. During a ransomware attack investigation, forensic analysts find that the attackers had been inside the network for three weeks before triggering the encryption. During that time, they identified and deleted all accessible backup copies. Why is this preparation stage so significant? i. It allows the attackers to understand the organization's data better, enabling a higher ransom demand. j. It ensures the organization cannot restore their data from backups, making payment the only apparent route to recovery and dramatically increasing the chance the ransom will be paid. k. It prevents the organization from detecting the attack until encryption begins. l. It allows the attackers to encrypt the backups rather than deleting them, creating a more complete compromise.
Q4. Which combination of defenses most directly addresses the two highest-impact malware risks: ransomware encrypting your files, and malware exploiting software vulnerabilities to gain access? m. Anti-malware software and avoiding public Wi-Fi. n. Offline tested backups (to recover from ransomware) and keeping software updated (to close vulnerabilities before they can be exploited). o. Strong passwords and multi-factor authentication. p. Firewall rules and network segmentation.

Module 6 Practice Questions
Q1. A user has the same password on their email, their online banking, and a retail website they used once years ago. The retail website suffers a data breach and the user's email and password are stolen. What can the attacker now do, even without any further technical skill? a. Access only the retail website account, since that is the one that was breached. b. Access the email and banking accounts by trying the same password on those services this is credential stuffing, and it succeeds because the password was reused. c. Nothing immediately, they would need to crack the password before using it. d. Access the retail website only; the other accounts use the same password but different usernames.
Q2. Which of the following passwords is strongest, and why? e. P@ssw0rd2024!: it uses a mix of uppercase, lowercase, numbers and symbols. f. correct-horse-battery-staple: four random words creating a long, unpredictable passphrase. g. Liverpool1892!: a meaningful phrase with a capital letter and punctuation. h. xK9#mP: six random characters with high complexity.
Q3. Someone argues that using a password manager is risky because 'if it gets hacked, the attacker gets all your passwords at once.' Which response best addresses this concern? i. This is a valid concern password managers should only be used for low-importance accounts. j. Password managers store passwords in encrypted form and are far harder to breach than the dozens of websites where you currently reuse passwords. The risk of one password manager breach is lower than the near-certainty of credential stuffing succeeding when passwords are reused. k. Password managers are completely secure and cannot be hacked under any circumstances. l. The concern is valid, which is why you should write passwords down on paper instead.
Q4. An attacker steals a user's email password through a phishing attack. The account has multi-factor authentication enabled using an authenticator app. What happens when the attacker tries to log in? m. The attacker logs in successfully because they have the correct password. n. The attacker is blocked because they cannot complete the MFA step they do not have access to the user's authenticator app. o. The attacker receives an error message telling them the account is protected by MFA, revealing that security is in place. p. The MFA sends a notification to the user's phone, but the attacker can bypass it by calling the phone company.

Module 7 Practice Questions
Q1. You are in a coffee shop and connect to a Wi-Fi network called 'CoffeeHouse_Free'. You did not ask staff for the network name. You then log in to your work email. A security researcher at a nearby table has set up a rogue access point with the same name and is intercepting all traffic. You are using HTTPS for your email. What protection does HTTPS provide in this scenario? a. HTTPS provides no protection once connected to the evil twin, all traffic is visible to the attacker. b. HTTPS encrypts the content of your email traffic, so even though the attacker can see that you are connecting to your email provider, they cannot read the emails themselves or your login credentials. c. HTTPS automatically detects the rogue access point and warns you before any data is transmitted. d. HTTPS is only effective on home networks, not public Wi-Fi.
Q2. A colleague says: 'I use a VPN, so I'm safe from phishing attacks.' Which response most accurately addresses this claim? e. This is correct VPNs encrypt all traffic and therefore prevent phishing attacks from reaching your device. f. A VPN protects your network traffic from eavesdropping, but it does not protect you from clicking a phishing link, downloading malware, or entering your credentials on a fake website. Those threats require different defenses. g. This is correct only if the VPN includes built-in antivirus software. h. VPNs are not relevant to phishing at all they operate at different layers of the network.
Q3. You visit a website and your browser shows a padlock icon and 'https://' in the address bar. What does this confirm, and what does it NOT confirm? i. It confirms the website is legitimate and owned by a trustworthy organization. j. It confirms the connection between your browser and the server is encrypted, but it does not confirm the website is legitimate. Criminals can obtain valid HTTPS certificates for fake websites. k. It confirms the website has been verified by a government cybersecurity agency. l. It confirms no one can see which website you are visiting, including your internet service provider.
Q4. Your home router is still using the default username and password that came in the box three years ago. Why is this a security risk, even though only your family uses the home network? m. It is not a risk home networks are not targets for sophisticated attackers. n. Default router credentials are widely known and published online. An attacker who can reach your router for example, through a remotely exploitable vulnerability can log in, intercept traffic, redirect DNS requests to malicious servers, or use your connection for their own purposes. o. The risk is minimal because ISPs monitor home routers and would detect any compromise. p. It is a risk only if you use the router for work purposes.

Module 8 Practice Questions
Q1. A small bakery's website is defaced overnight. The attacker replaces the homepage with a political message. The bakery has no known political enemies and holds no sensitive data. Which type of attacker most likely carried out this attack? a. A nation-state actor conducting political espionage. b. An organised crime group seeking financial gain. c. An opportunist or hacktivist using automated scanning tools to find vulnerable websites, with no specific interest in the bakery. d. An insider threat from a disgruntled former employee.
Q2. An organization patches all known software vulnerabilities within 48 hours of release, uses MFA on all accounts, and has hardened all internet-facing systems. Which category of attacker does this posture most effectively deter? e. Nation-state actors, because they rely on known vulnerabilities. f. Opportunistic attackers, who use automated tools to scan for easy targets. Finding no easy entry point, their tools move on to less-protected systems. g. Insider threats, because patching removes their ability to escalate privileges. h. All attacker categories equally good hygiene stops every type of attack.
Q3. A software company is attacked not because of any weakness in its own systems, but because a widely-used third-party library it includes in its product was found to contain malware injected by an attacker months earlier. What type of attack does this illustrate? i. A phishing attack targeting the software company's developers. j. A supply chain attack the attacker compromised a trusted component used by the software company, reaching the company's customers without ever directly attacking the company itself. k. An insider threat from a developer who introduced the malicious library. l. A ransomware attack delivered through the update mechanism.
Q4. A long-serving employee is made redundant and feels unfairly treated. Two weeks after their departure, unusual data transfers are detected from a shared cloud drive that the employee still had access to. Which combination of controls, if they had been in place, would most directly have prevented this? m. Multi-factor authentication and strong passwords on the cloud drive. n. Regular patching of the systems the employee used. o. Prompt revocation of all access on the employee's last working day, combined with monitoring for unusual access patterns. p. Network segmentation to isolate the cloud drive from other systems.

Part 3: Build Your Defenses

Module 9: Strong Authentication

Proving Who You Are

1. The Lock on Every Door

Before any attacker can steal your data, deploy ransomware on your systems, or send fraudulent emails as you, they need one thing: access. Authentication is the process that decides who gets access and who does not. It is the lock on every digital door you own.

For most of history, that lock was a password. A single secret that, if known, opened the door completely. The problem as Parts 1 and 2 of this course have made abundantly clear, is that passwords are stolen constantly, guessed automatically, leaked in breaches, and reused catastrophically.

Multi-factor authentication (MFA) does not fix the password problem. It makes the password irrelevant as the sole line of defense. Even if an attacker has your password, they also need your second factor and that second factor is something they almost certainly do not have. This single change reduces the risk of account takeover by over 99% for most attack types. It is the most impactful action available to most people and most organizations for the least effort.

This module explains how authentication works, why different methods have different strengths, and gives you a clear, prioritized plan for what to enable and where.

2. The Three Factors of Authentication

Every authentication method in existence from a PIN to a retina scan to a hardware key falls into one of three categories. These categories are called authentication factors, and understanding them explains both why MFA is stronger than any single method and why different combinations have different strengths.

Factor	What it means	Examples	Key weakness
Something you know	A secret stored in your memory	Password, PIN, security question answer, passphrase	Can be guessed, stolen via phishing, exposed in a breach, or observed over your shoulder
Something you have	A physical or digital object in your possession	Your phone (for an authenticator app or SMS	Can be lost or stolen though the attacker also

Factor	What it means	Examples	Key weakness
		code), a hardware key (YubiKey), a smart card, a bank card	needs your password to use it alone
Something you are	A physical characteristic unique to you	Fingerprint, face scan, iris pattern, voice recognition	Cannot be changed if compromised. Performance varies with environmental conditions (wet finger, dim light)

Why two factors beat one

A password alone protects you only as well as that password is protected. If it is stolen, guessed, or leaked, you have nothing left. A second factor from a different category means an attacker must compromise two completely separate things simultaneously your password AND your phone, or your password AND your hardware key. These are independent. Stealing one gives nothing without the other. This is why MFA is not just incrementally better than a password it is categorically better.

3. MFA Methods: Not All Are Equal

Multi-factor authentication is available in several forms, and they are not equally secure. Understanding the differences lets you choose the right method for each account rather than treating all MFA as identical.

Method	How it Works	Phishing Resistant?	Usability	Recommended for
Hardware security key	Physical USB or NFC device. You plug in or tap it when prompted. Cryptographically proves you have the device.	✅ Yes: the key checks the real domain and refuses to respond to fakes	Very easy once set up. Requires carrying the key.	High-value accounts: work admin, financial systems, senior staff
Authenticator app (TOTP)	App generates a 6-digit code that changes every 30 seconds. You type the current code when logging in.	⚠ Mostly: a real-time phishing relay can capture codes but this is uncommon and complex	Easy. Requires unlocking your phone and opening the app.	Most people for most accounts. Best practical choice for everyday use

Method	How it Works	Phishing Resistant?	Usability	Recommended for
Push notification	A notification appears on your phone asking you to approve or deny the login. You tap 'Approve'.	⚠ Partially: vulnerable to MFA fatigue attacks (see callout)	Very easy. Single tap to approve	Acceptable where TOTP is unavailable. Enable 'number matching' where possible
SMS code	A one-time code sent to your phone by text message. You type it in	⚠ Partially: vulnerable to SIM-swapping and interception	Easy. No app needed.	Better than nothing. Use when no other option exists. Not for high-value accounts.
Biometric (fingerprint / face)	Your device uses your physical characteristic to confirm it is you before releasing a stored credential	✅ Yes: the credential stored on the device is what authenticates, not the biometric itself	Very easy. Built into most modern devices.	Unlocking devices and apps. Excellent for convenience alongside another factor.
No MFA	Password only.	❌ No: a stolen password = complete account access	Easy but insecure.	Not recommended for any account you care about.

MFA fatigue: when convenience becomes a vulnerability

Push notification MFA (the 'tap Approve on your phone' method) is convenient but has a specific weakness: an attacker who has your password can send approval requests to your phone continuously until you approve one.

This attack works because approval requests look identical whether you initiated them or not, and people approve them out of habit, confusion, or frustration after receiving dozens.

The defense: enable 'number matching' or 'additional context' in push MFA settings. This displays a number on the login screen that you must match on your phone before approving making blind approval impossible. If your MFA app supports it, turn this on.

The simpler defense: if you receive an MFA request you did not initiate, deny it and immediately change your password. Someone has your credentials.

4. Where to Enable MFA: A Prioritized List

Not all accounts are equally important to protect. This table lists account types in priority order. Start at the top and work down. Do not wait until you have time to do everything enabling MFA on your email today is more valuable than a plan to eventually secure everything.

Priority	Account Type	Why
Critical	Primary email account	Email resets every other account. Losing email = losing everything linked to it. Enable MFA here first, before anything else.
Critical	Password manager	The vault containing every other password. If this is compromised, all other accounts are compromised.
Critical	Banking and financial apps	Direct access to money. Most banks offer MFA; many require it. Use an authenticator app if available rather than SMS.
High	Work accounts and email	Access to professional data, systems, and the ability to act as you to colleagues and clients.
High	Social media accounts	Your contacts trust messages from you. A compromised account is used to scam them.
Medium	Shopping and retail accounts	Saved payment methods and delivery addresses. Less critical if no card is stored.
Medium	Cloud storage (iCloud, Google Drive, Dropbox)	Often contains documents, photos, and files you would not want accessed or deleted.

Email is always first

If you enable MFA on only one account in your life, make it your primary email. Everything flows from there. Your email is used to reset passwords for your bank, your work systems, your cloud storage, your social media, and every other service you use. Securing your email

with MFA does not just protect your inbox, it protects every account that relies on it as a recovery mechanism.

5. Passkeys: The Password's Replacement

Passwords have been the dominant authentication method for sixty years. Their replacement is now being rolled out by every major platform: passkeys. Understanding what passkeys are and why they are more secure than passwords helps you make better decisions as the authentication landscape changes over the next few years.

Feature	Traditional Password	Passkey
What you remember	A secret string you must memorize or store	Nothing: the passkey is stored securely on your device
How login works	Type the password into the website's form	Your device confirms your identity (fingerprint, face, PIN) and cryptographically signs the login
Can it be phished?	Yes, typing a password into a fake site gives it to the attacker	No, the passkey only works on the real site. It refuses to authenticate to fakes.
Can it be breached?	Yes, if the site stores passwords poorly, they can be stolen en masse	No, the site never holds your secret. Only your device does.
Where it works today	Everywhere	Growing rapidly: Google, Apple, Microsoft, GitHub, many banks and services.

Passkeys are supported on most modern devices and are increasingly offered as an option by Google, Apple, Microsoft, GitHub, PayPal, and many others. When a service offers you the option to set up a passkey, it is worth doing. You will log in faster and with stronger security than any password-plus-MFA combination.

Passkeys and the future of authentication

Passkeys will not replace passwords overnight too many services still require them, and many people have not yet adopted passkeys where they are available. But the direction of travel is clear: the industry is moving towards authentication that cannot be phished, does not require memorization, and does not expose secrets to servers. For now, a strong

passphrase plus an authenticator app is the practical standard. Within a few years, passkeys will likely become the norm for most major services.

6. Setting Up MFA: The Practical Steps

Setup varies slightly by platform but follows the same pattern for almost every service.

Step 1: Download an authenticator app

Microsoft Authenticator, Google Authenticator, and Authy are all free, widely supported, and reliable. Download one of these before you start you will need it for the next steps. Authy has the advantage of encrypted cloud backup, meaning you can recover your codes if you lose your phone.

Step 2: Go to your account's security settings

In your email provider, bank, work system, or any other service, look for 'Security', 'Privacy', or 'Account Settings'. Most major platforms have a dedicated section for two-factor or multi-factor authentication. Enable it.

Step 3: Scan the QR code or enter the setup key

The service will display a QR code. Open your authenticator app, tap 'Add account' or the '+' button, and scan the code. The app will immediately start generating 6-digit codes that refresh every 30 seconds. Enter the current code to confirm setup.

Step 4: Save your recovery codes

Every service provides emergency recovery codes when you set up MFA, typically 8 to 10 single-use codes. These allow you to log in if you lose access to your authenticator app. Save them somewhere secure and offline: printed and stored physically, or in a notes section of your password manager. Do not store them in your email.

7. What to Do If You Lose Your Second Factor

The most common concern about MFA is: 'What happens if I lose my phone?' This is a legitimate question with a clear answer, provided you have prepared.

- Recovery codes: if you saved them during setup (Step 4 above), use one to log in and then re-enroll a new device.
- Backup authenticator: you can register more than one device with most services. Set up your authenticator app on both your phone and a tablet, for example.

- Authy backup: if you use Authy and enabled encrypted cloud backup, you can restore your codes on a new device.
- Account recovery: most services have an account recovery process that involves verifying your identity through email, a backup phone number, or identity verification. This takes longer but works.

The practical takeaway: save your recovery codes. This single action prevents the most common MFA lockout scenario. Print them, store them in a password manager, or keep them somewhere safe. Do not skip this step when setting up MFA on any account.

ShieldNet thread going further

Strong authentication is addressed in ShieldNet control [SB3] (Enable Multi-Factor Authentication), which requires MFA on all remote logins and important accounts at minimum administrators, email, VPN, and cloud dashboards. This module covers the same ground from a personal perspective. The organizational requirement in [SB3] exists because individual accounts, when compromised through weak authentication, become the entry point for attacks on the entire organization. Your personal MFA habits directly support your organization's security posture.

Module 9: Summary

By the end of this module, you should be able to:

- ✓ Explain the three authentication factors (something you know, have, are) and give an example of each.
- ✓ Describe how an authenticator app works and explain why it is more secure than an SMS code.
- ✓ Explain what MFA fatigue is and describe how to protect against it.
- ✓ List the accounts where MFA should be enabled as a critical priority, in the correct order.
- ✓ Explain what a passkey is and why it is resistant to phishing.
- ✓ Name two actions you can take today to improve your authentication security.

Module 10: Controlling Access

Who Gets In, What They Can Do

1. Getting In vs What You Can Do Once You're In

Module 9 covered authentication: proving who you are. This module covers what comes next: once a system knows who you are, it decides what you are allowed to do. This second step is called authorization, and it is just as important as the first.

Think of it in terms of a hospital. Authentication is the ID badge check at the entrance. It confirms that you are a member of staff and have a right to be in the building. But once you are inside, not everyone should be able to walk into the operating room, access the pharmacy, or read all patient records. What you can do inside the building depends on your role. A porter, a nurse, and a surgeon all pass the same entrance check but have access to very different areas.

Most security thinking focuses on keeping attackers out. Access control recognizes that attackers sometimes get in through stolen credentials, phishing, or compromised accounts, and asks: once they are in, how much damage can they do? The answer depends almost entirely on how well access was controlled.

2. Authentication vs Authorization

These two words are often confused. The distinction is worth being precise about, because the defenses are different.

	Authentication	Authorization
The question it answers	Who are you?	What are you allowed to do?
What it controls	Whether you can get in at all	What you can see and do once you are in
Analogy	Showing your passport at the airport to confirm your identity	Your boarding pass specifying which seat you may sit in and which lounge you may enter
In practice	Your username and password, plus MFA	Your role, permissions, and access rights within a system

	Authentication	Authorization
What happens when it fails	An attacker gets past the login screen	A user or attacker who got past authentication can access more than they should

> **Why both matter**
> Strong authentication without proper authorization is like a heavily fortified front door on a building where every room inside is unlocked and labeled. An attacker who gets through authentication by stealing credentials, for example immediately has access to everything unless authorization limits what they can reach. This is why MFA and least privilege are complementary, not interchangeable. You need both.

3. The Principle of Least Privilege

Least privilege is the single most important concept in access control. It is also one of the most consistently violated, because following it requires ongoing effort rather than a one-time setup.

The principle is simple: every person, application, or system should have access to exactly what they need to do their job and nothing more. Not 'probably what they need'. Not 'what their predecessor had'. Not 'everything, to be safe'. Exactly what is needed, and no more.

The reason is equally simple: access that exists can be exploited. Access that does not exist cannot. If an accounts payable clerk's account is compromised, the damage is contained to what that account could reach. If the same clerk had been given administrator rights for convenience, the damage is total.

Role	What They Need Access To	What They Should NOT Have
Accounts payable clerk	The finance system to raise and approve invoices within their limit; supplier contact records; the company bank portal to view statements	HR salary records; the ability to create new bank payees; administrator access to any system; access to all customer data
Customer service agent	The customer database (read-only for most records); the ticketing	The ability to modify customer financial records; access to other

Role	What They Need Access To	What They Should NOT Have
	system; product information; their own email	employees' files; system configuration settings
IT support technician	Administrator access to the specific systems they support; the IT asset register; the helpdesk system	Access to HR records; financial systems beyond what is needed to support them; permanent elevated access (use time-limited admin sessions instead)
New starter (first week)	Access to the specific systems needed for their role; read access to team documents; company email	Administrator rights on any system; access to confidential data not relevant to their role; VPN access if not required for their job
Contractor (short-term project)	Access to the specific project systems and files required; a time-limited account that expires at project end	Broad file system access; access to systems outside the project scope; access that persists after the contract ends

The blast radius principle

Security professionals talk about 'blast radius' the area of damage an attacker can cause from a single compromised account. Least privilege minimizes blast radius. A compromised account with limited access causes limited harm. A compromised account with administrator rights causes unlimited harm. Reducing the blast radius of any individual account is one of the highest-return security investments an organization can make, and it costs nothing except the effort of being deliberate about permissions.

4. Common Over-Permission Patterns

In practice, organizations consistently make the same access control mistakes. Understanding them makes them easier to spot and challenge when you encounter them.

Common Pattern	Why it Happens	Why it Matters
Everyone gets admin rights	It is easier to give everyone admin access than to manage individual permissions. IT teams under pressure take the path of least resistance.	When any account is compromised, the attacker immediately has full system control. Ransomware, data exfiltration, and sabotage all become trivially easy.

Common Pattern	Why it Happens	Why it Matters
Access never gets removed	Nobody tracks when roles change or people leave. The leaving process does not include a structured access revocation step.	Former employees and contractors retain access they should not have. Dormant accounts with old credentials are prime targets, often less monitored than active accounts.
Shared accounts for convenience	Teams share a single login to avoid managing individual accounts (e.g. a shared 'admin' account, a shared social media login).	When something goes wrong, there is no way to know who did what. Accountability disappears. Shared credentials also spread exponentially when people leave.
Access granted broadly at onboarding	It is faster to copy an existing employee's access profile than to think carefully about what the new person actually needs.	New starters arrive with access accumulated over years by their predecessor. Every unnecessary permission is an unnecessary risk.
No regular access review[32]	Nobody has time. Access reviews feel like administrative overhead rather than security work.	Permissions drift over time. People accumulate access as their roles evolve, but rarely lose it when it is no longer needed.

The leaver problem is the most underestimated risk

Research consistently shows that a significant proportion of data breaches involve accounts belonging to people who have already left the organization. These accounts are often overlooked because they are no longer active in day-to-day operations, are less likely to be monitored, and may be known to others (former colleagues, partners) who can still use them. The fix is structural: offboarding must include a mandatory, checklist-driven process for revoking all access on the last working day. Not the following week. Not 'when IT gets around to it'. The same day.

5. Access Reviews: The Ongoing Work

Least privilege is not a configuration you set once. It requires regular review, because access drifts over time. People change roles, take on new responsibilities, move

[32] **Access review:** A regular check of who has access to what, so that unnecessary or outdated access can be removed.

between teams, and accumulate permissions along the way. Without periodic review, an organization's access controls gradually diverge from the principle of least privilege.

What an access review involves

At its simplest, an access review asks three questions for every user account: Does this person still work here? Is their current role the same as when their access was last set? Does the access they have match what their current role requires? For many small organizations, this is a spreadsheet exercise that takes a few hours once or twice a year. For larger organizations, it involves dedicated tools and formal sign-off processes.

Service accounts deserve special attention

Service accounts, accounts used by applications, automated processes, and integrations rather than people, are frequently overlooked in access reviews. They are often set up with broad permissions for convenience and then forgotten. Abandoned service accounts connected to old systems are a prime target for attackers, precisely because nobody is watching them. Include service accounts in every access review.

What triggers an immediate review

Some events should trigger an immediate access review without waiting for the scheduled cycle:

- Someone leaves the organization or changes role.
- A security incident[33] occurs: to understand what the compromised account could reach.
- A new system or application is deployed: to ensure it does not inherit over-broad permissions.
- A supplier relationship ends: to ensure contractor and supplier accounts are removed.

6. Access Control in Your Personal Digital Life

The principle of least privilege applies just as much to your personal accounts and apps as it does to organizations. You make access control decisions every day: which

[33] **Security incident:** Any event that may harm the confidentiality, integrity, or availability of systems or data, such as a malware infection or a lost laptop.

apps you allow to access your location, which services you connect to your Google or Apple account, which people you share files with. Applying least-privilege thinking to these decisions significantly reduces your personal risk.

Habit	What it Means in Practice	Why it Matters
Review app permissions regularly	Check which apps on your phone have access to your location, contacts, microphone, camera, and messages. Remove permissions that do not make sense for the app's function.	Apps with unnecessary permissions collect data you did not consciously share. A torch app does not need your contacts. A game does not need your location.
Use separate email addresses	Maintain a primary email for important accounts (banking, work) and a secondary one for newsletters, shopping, and services you trust less.	If the secondary email is breached or flooded with spam, your primary email and everything linked to it remains unaffected.
Revoke access to old connected apps	In Google, Apple, Facebook, and Microsoft account settings, there is a list of third-party apps you have granted access to. Review and remove any you no longer use.	Apps you connected years ago may still have access to your account data. If those apps are breached, your account data goes with them.
Don't share account credentials	Avoid sharing passwords even with trusted family or colleagues. If shared access is needed, use proper sharing features (shared folders, team accounts) rather than shared passwords.	When something goes wrong, shared credentials make it impossible to determine who acted. They also mean you cannot change your password without breaking someone else's access.
Log out of shared or public devices	Always log out when using a computer that is not yours library computers, hotel business centers, a colleague's machine.	Staying logged in on a shared device leaves your account accessible to the next user, regardless of how trustworthy they seem.

The connected apps audit

Most people have dozens of third-party apps connected to their primary accounts that they have forgotten about.

To find them: in Google: go to myaccount.google.com, then 'Security', then 'Third-party apps with account access'.

In Apple: go to Settings > your name > Password & Security > Apps Using Apple ID.

In Facebook/Meta: go to Settings > Security and Login > Apps and Websites.

Remove any app you do not recognize, no longer use, or cannot explain why it needs access to your account. This takes ten minutes and removes a significant number of unnecessary exposure points.

7. The Link Between Access Control and Every Other Defense

Access control is not a standalone topic. It connects directly to almost every other module in this course:

- Module 6 (passwords): even the strongest password only protects an account as far as that account's permissions allow. A strong password on a least-privilege account is far safer than a strong password on an administrator account.
- Module 9 (authentication): MFA and least privilege together are the most effective double layer of defense against account compromise. MFA slows attackers down. Least privilege limits what they can do if they get through.
- Module 8 (insider threats): the most effective defense against malicious insiders is ensuring they can only reach what they genuinely need. Over-privileged accounts make insider incidents significantly more damaging.
- Module 5 (ransomware): ransomware spreads across networks using whatever access the compromised account has. An account with network-wide file permissions gives ransomware network-wide reach. Least privilege directly limits ransomware's blast radius.

Access control is the connective tissue of security. Getting it right does not require expensive tools or complex processes. It requires being deliberate: about what access each person needs, about reviewing that access regularly, and about removing it promptly when it is no longer needed.

ShieldNet thread going further

Access control maps to two ShieldNet controls. [SB1] (Control User Access) requires unique user accounts for every person and service, with each account granted the minimum access rights it needs the direct organizational expression of least privilege. It also requires regular removal or adjustment of access when roles change. [SB2] (Secure Hiring and Exit) addresses the leaver problem: screening before people join and prompt revocation of all access on the day they leave. Template A-8 (Access Review Log) in Annex A is the artefact organizations use to evidence that access reviews are happening regularly.

Module 10: Summary

By the end of this module, you should be able to:

- ✓ Explain the difference between authentication and authorization using a concrete analogy.
- ✓ Define the principle of least privilege and give an example of what it looks like in practice for a specific role.
- ✓ Describe three common over-permission patterns and explain why each one creates risk.
- ✓ Explain why dormant accounts (belonging to people who have left) are a security risk.
- ✓ List three personal access control habits and explain the security benefit of each.

Module 11: Keeping Devices Safe

Updates, Locks and Good Habits

1. Your Device Is the Battlefield

Everything else in this course, your accounts, your data, your communications, passes through your devices. Your phone knows where you are, who you talk to, and what you buy. Your laptop contains your work files, your browser history, your saved passwords, and your access to corporate systems. Your tablet connects you to your bank, your health records, and your family.

Attackers understand this. A compromised device is not just an inconvenience it is a window into everything you do digitally. And the most common ways devices get compromised are not sophisticated exploits dreamed up by elite hackers. They are unpatched software vulnerabilities, absent screen locks, and absent encryption. Problems with known solutions that require nothing more than consistent habits to prevent.

This module covers the practical baseline that every device you own or use for work should meet. Not perfection. Not enterprise-grade security operations. A clear, verifiable baseline that eliminates the vast majority of device-level risk.

2. Why Software Updates Are a Security Issue, Not an Annoyance

The update notification sitting in the corner of your screen is not asking you to download new features. It is telling you that a security flaw has been discovered in your software, that the flaw has been fixed, and that until you apply the fix, your device has a known, documented vulnerability that attackers can exploit.

This is not hypothetical. The WannaCry ransomware attack described in Module 5 exploited a Windows vulnerability that had been patched by Microsoft two months earlier. The organizations that applied the patch were not affected. The ones that dismissed the update notification were. The gap between a patch release and active exploitation of the underlying vulnerability is shrinking: attackers now reverse-engineer patches to understand what was fixed and develop exploits within days.

Type of Update	What it Fixes	How Urgent	What if I Ignore
Security patch	A known vulnerability that could be exploited	Critical: apply immediately or within	Your device or software becomes a known,

Type of Update	What it Fixes	How Urgent	What if I Ignore
	to gain access, run malicious code, or steal data	48 hours for actively exploited vulnerabilities	documented target. Exploit code is often publicly available within days of a patch release.
Bug fix	Software behavior that does not work as intended, which may include instability or data loss	High: apply within a few weeks	Instability, crashes, or data integrity issues. Some bugs have security implications that are only apparent later.
Feature update	New functionality, improvements to existing features, interface changes	Normal: apply during regular maintenance cycles	Missing new capabilities, but no immediate security impact unless the update also includes security fixes.
Operating system upgrade	A major version change (e.g. Windows 10 to Windows 11, iOS 16 to iOS 17) with accumulated improvements and new security foundations	Important: especially when the old version reaches end-of-life[34]	Once a version reaches end-of-life, security patches stop. Running end-of-life software is running known, permanently unpatched vulnerabilities.

The update prompt is not optional

Every time you dismiss an update notification, you are making a security decision. You are deciding that the inconvenience of restarting your device now outweighs the risk of running known, unpatched vulnerabilities. For most security patches, that calculation is wrong. Enable automatic updates on every device you own. Let the device update overnight when you are not using it. The five minutes of inconvenience costs less than the cost of being compromised.

3. The Device Protection Baseline

[34] **End-of-life (EOL):** The point at which software or a device no longer receives security updates, which makes it increasingly unsafe to use.

Six measures together constitute a well-protected device. This table shows what each one is, how to verify it is in place, and why it matters. Check your own devices against this list.

Protection Measure	Your Laptop / Desktop	Your Phone / Tablet	Why it Matters
Automatic updates enabled	✅ Enable in Settings > Update	✅ Enable in Settings > General > Software Update (iOS) or Settings > System > System Update (Android)	Closes security vulnerabilities without requiring you to remember to check.
Screen lock with strong PIN or password	✅ Use a password (not just a 4-digit PIN) with auto-lock after 5 minutes	✅ Use biometric + a 6-digit PIN minimum. Set auto-lock to 1–2 minutes.	Prevents physical access to your device and data if lost or stolen.
Full-disk encryption[35] enabled	✅ Windows: BitLocker[36] (check via Settings > Privacy & Security). macOS: FileVault[37] (System Settings > Privacy & Security).	✅ iOS: enabled automatically when a passcode is set. Android: usually enabled by default on modern devices.	Makes data on a lost or stolen device unreadable without the password.
Anti-malware active	✅ Windows Defender is built in and sufficient for most users. macOS has XProtect built in. Keep both enabled.	⚠ Less critical on mobile (sandboxed[38] apps), but avoid sideloading[39] apps outside official stores.	Detects and blocks known malware before it can execute or spread.
Remote wipe capability enabled	✅ Windows: Find My Device in account settings. macOS: Find My in iCloud.	✅ iPhone: Find My iPhone in iCloud. Android: Find My	Allows you to erase all data remotely if the device is lost or stolen.

[35] **Full-disk encryption:** Encryption that protects everything on a device's storage, so the data is unreadable if the device is lost or stolen.
[36] **BitLocker:** Microsoft's built-in full-disk encryption for Windows.
[37] **FileVault:** Apple's built-in full-disk encryption for macOS.
[38] **Sandboxing:** Running a program in an isolated space, so that if it is malicious it cannot affect the rest of the system.
[39] **Sideloading:** Installing apps from outside the official app store, which bypasses the store's safety checks.

Protection Measure	Your Laptop / Desktop	Your Phone / Tablet	Why it Matters
		Device in Google account.	
Firewall enabled	✅ Windows Defender Firewall: on by default. macOS: System Settings > Network > Firewall.	✅ Built-in on both iOS and Android. No action needed on modern devices.	Blocks unsolicited inbound network connections to your device.

Check your devices right now

Open your laptop's settings and verify: automatic updates are on, BitLocker or FileVault is enabled, and the screen locks after no more than 5 minutes.

On your phone: check that your OS is up to date, a 6-digit PIN or biometric is required to unlock, and Find My iPhone / Find My Device is enabled.

If any of these are not in place, the next ten minutes fixing them will be the most impactful ten minutes of this course.

4. The End-of-Life Problem

Every piece of software and every operating system eventually reaches 'end of life', the point at which the vendor stops releasing security updates. After that date, any vulnerability discovered in that software remains permanently unpatched. Attackers know the end-of-life dates. They stockpile exploits for end-of-life software specifically, because they know the vulnerabilities will never be fixed.

Software / System	End-of-life Date	What That Means	Action
Windows 10	Already end-of-life	Microsoft stops releasing security patches. All future vulnerabilities remain permanently unpatched.	Upgrade to Windows 11 or migrate to a supported OS.
Windows 7 / 8.1	Already end-of-life	Thousands of documented, publicly known vulnerabilities with no patches available. Actively exploited by attackers.	Replace immediately. Running these is indefensible for any system with internet access.

Software / System	End-of-life Date	What That Means	Action
iOS / Android (2+ versions behind)	Varies by device	Older versions stop receiving security updates before newer ones. The specific cutoff depends on the device manufacturer.	Update to the latest supported version. If your device no longer supports the current OS, consider replacing it.
Unsupported browsers (old Chrome, Firefox, Safari, IE)	Varies	The browser is the primary interface with the internet. An unpatched browser is an open door to drive-by malware and credential theft.	Keep your browser updated. Internet Explorer is end-of-life do not use it for anything.

The practical implication: if any device you use for work or personal banking is running end-of-life software, it is not a matter of if it will be exploited but when. The investment in upgrading or replacing the device is almost always less than the cost of recovering from a compromise.

5. Physical Security: The Lock on the Lid

Digital security often focuses on network and software threats while underestimating the simplest physical risks: a device left unattended, a screen left unlocked, a laptop stolen from a bag.

Screen lock and auto-lock

A screen lock with auto-lock after a few minutes of inactivity is one of the simplest and most effective security measures available. It protects against opportunistic physical access: someone picking up your unlocked phone, someone sitting at your unattended laptop. The PIN or password should be strong enough that it cannot be guessed quickly. A 4-digit PIN is 10,000 combinations. A 6-digit PIN is 1,000,000. A biometric plus a 6-digit PIN is better still.

Never leave devices unattended in public

A laptop in a coffee shop, a phone on a restaurant table, a tablet left on a train seat. Theft is the most obvious risk, but not the only one. An unattended, unlocked device can be accessed by someone in seconds, credentials harvested, malware installed,

files copied. The habit of locking your device before stepping away, every time, costs nothing.

Be careful with USB and charging

Public USB charging points at airports, hotels, coffee shops have been used to deliver malware to devices through a technique called 'juice jacking'. Modern devices often prompt you to trust the connection when plugging into an unknown USB port. Always choose 'charge only' if given the option, and carry your own charger or a USB data blocker ('USB condom') if you regularly use public charging.

6. Personal Devices at Work: The BYOD Challenge

Bring Your Own Device (BYOD) using personal phones, laptops, or tablets to access work systems is now standard in most organizations. It is convenient, saves costs, and reflects how people actually work. It also introduces security risks that neither the individual nor the organization always manages well.

The core problem is a mismatch of expectations: the organization assumes work data is being handled on a device that meets minimum security standards; the individual may not know what those standards are or may not have applied them to a personal device they also use for gaming, personal banking, and family photos.

If You Use Personal Devices for Work...	The Organization Needs to Know...	You Need to Apply...
Your personal phone receives work email or accesses work systems	Which personal devices are used for work purposes and what data they can access	The same screen lock, encryption, and update standards as a work device
You store work files on personal cloud storage (personal Google Drive, Dropbox, iCloud)	Where work data is being stored, so it can be protected and included in data retention policies	Access controls and MFA on that cloud storage; do not mix personal and work files in unsecured shared folders
You use a personal laptop for remote work	Whether that laptop meets minimum security standards before it accesses the corporate network	Anti-malware, full-disk encryption, OS updates, and screen lock as a minimum; ideally a corporate VPN

The work-life separation principle

The cleaner the separation between work and personal use on a device, the lower the risk. Ideally: work email and work files on a work-managed device or a dedicated work profile; personal apps, personal email, and personal files on personal accounts. Where full separation is not possible, at minimum ensure that work data (emails, files, messages) is stored in work-controlled services rather than being copied to personal cloud storage or personal apps. If your organization provides a work profile or MDM (mobile device management) configuration for your phone, follow it.

7. Jailbreaking, Rooting, and Why They Matter

Some users choose to 'jailbreak' their iPhone or 'root' their Android device removing the manufacturer's restrictions to install unauthorized apps, customize the interface, or access system-level functionality. From a security perspective, this is significant.

The security model of both iOS and Android relies on a layered set of protections: sandboxed apps that cannot access each other's data, verified app stores that screen for malware, and operating system protections that prevent apps from escalating their own privileges. Jailbreaking or rooting removes these protections entirely. Apps installed on a jailbroken device can access data from other apps, can run with elevated privileges, and are not subject to app store security review.

For personal devices, the decision is a personal one. For devices used for work accessing company email, files, or systems jailbroken or rooted devices represent an unacceptable security risk that most organizations explicitly prohibit in their BYOD policies.

8. Two Actions to Take Today

- Enable automatic updates on every device you own: Go to Settings on your phone, laptop, and any other device you use regularly. Find the update settings and turn on automatic updates. This takes five minutes across all your devices and is the single highest-return action in this module.
- Check full-disk encryption on your laptop: On Windows: search for 'BitLocker' in the Start menu. On macOS: go to System Settings > Privacy & Security > FileVault. If it is off, turn it on. On a modern SSD, encryption completes in the background within a few hours and has no impact on performance.

ShieldNet thread going further

Device security maps directly to two ShieldNet controls. [SB4] (Protect User Devices) requires all endpoints to have anti-malware, host firewalls, patches, and device login passwords with auto-lock the exact baseline covered in section 11.3. [WP3] (Apply Patches Quickly) requires organizations to apply security patches promptly, with a 14-day standard deadline and a 48-hour target for critical, actively exploited vulnerabilities. The personal patching habits in this module are the individual expression of the same principle.

Module 11: Summary

By the end of this module, you should be able to:

- ✓ Explain why software updates matter for security and describe what happens when end-of-life software is used.
- ✓ List the six key device protection measures and describe how to verify each one is in place on your own devices.
- ✓ Explain what full-disk encryption does and why it matters specifically for lost or stolen devices.
- ✓ Describe the risks of using personal devices for work and name two steps that reduce those risks.
- ✓ Explain what ‘jailbreaking’ or ‘rooting’ a device does to its security model.
- ✓ Name two actions you can take today to improve your device security.

Module 12: Encryption

Scrambling Data So Only the Right People Can Read It

1. The Locked Box

Imagine you need to send a valuable document to someone across the country. You could hand it to a courier and hope nobody opens it on the way. Or you could put it in a locked box, send the box, and share the key separately with the recipient. Even if the courier is curious, dishonest, or robbed, they cannot read the document without the key.

That is encryption. It takes readable information and transforms it into scrambled, unreadable noise. Only someone with the correct key can unscramble it back into something useful. The scrambling can be extraordinarily complex modern encryption is mathematically impossible to reverse without the key within any practical timeframe but the concept is that simple.

Encryption is already working silently around you everywhere: when you check your bank balance, when you send a WhatsApp message, when you unlock your laptop, when your company's files are stored in the cloud. You do not need to understand the mathematics. You need to understand where it applies, what it protects, and, just as importantly what it does not.

2. Two Types You Need to Know: In Transit and At Rest

Encryption appears in two fundamental contexts, and understanding both is necessary for a complete picture.

Encryption in transit

When data travels across a network from your browser to a website, from your phone to a server, from one email provider to another, it passes through infrastructure that is not yours. Without encryption, anyone on that path can read it. With encryption in transit (the technology behind HTTPS), the data is scrambled before it leaves your device and can only be unscrambled by the intended destination.

This is why the padlock in your browser matters. HTTPS uses a protocol called TLS (Transport Layer Security) that encrypts everything exchanged between you and the website. Your login credentials, your payment card details, your search queries, all scrambled in transit, unreadable to anyone intercepting the packets.

Encryption at rest

Data sitting on a hard drive, a server, or in cloud storage is 'at rest'. Without encryption at rest, anyone who physically accesses the storage medium or compromises the server can read every file. With encryption at rest, the stored data is scrambled and unreadable without the decryption key.

Full-disk encryption on your laptop (covered in Module 11) is encryption at rest. Database encryption protecting millions of customer records is encryption at rest. Cloud storage providers encrypting your uploaded files are encryption at rest.

> **Why you need both**
> In-transit encryption protects your data while it is moving. At-rest encryption protects your data while it is sitting still. An attacker who intercepts network traffic cannot read encrypted data in transit. An attacker who steals a hard drive cannot read encrypted data at rest. Each protects against a different attack scenario. A service that encrypts data in transit but stores it unencrypted is vulnerable to server breaches. A service that encrypts data at rest but sends it unencrypted is vulnerable to interception. Best practice requires both.

3. End-to-End Encryption: When Even the Platform Can't Read It

Standard encryption in transit protects your data from everyone except the platform it passes through. When you send an email via Gmail, Google encrypts the connection between you and their servers. But Google can read the email content once it arrives at their servers because they hold the decryption keys. This is by design: it allows spam filtering, search indexing, and account recovery.

End-to-end encryption (E2E) is different. The message is encrypted on your device before it is sent, and only the recipient's device holds the key to decrypt it. The platform that carries the message the server in the middle never has the keys. It stores and forwards encrypted data it cannot read.

	Standard Encryption	End-to-End Encryption
Who can read the content	You, the recipient, and the service provider (they hold the keys).	Only you and the recipient. The platform cannot read it even if compelled.

	Standard Encryption	End-to-End Encryption
What happens if the platform is breached	Encrypted data may be accessible if the attacker also gets the keys	Encrypted data is unreadable without the recipient's private key, which never leaves their device
Examples	Gmail (Google can read your emails), standard cloud storage, most corporate email systems	Signal, WhatsApp (for messages), iMessage (between Apple devices), ProtonMail
Best for	General use good enough for most communication and storage	Sensitive personal communication, confidential documents, anything you genuinely need kept private from the platform provider

Signal vs WhatsApp: both E2E, different trust models

Both Signal and WhatsApp use end-to-end encryption for messages. The content of messages is protected in both. The difference is metadata and trust: WhatsApp is owned by Meta, which collects metadata (who you message, when, how often) even if it cannot read message content. Signal is operated by a non-profit, collects minimal metadata, and its code is fully open-source and independently audited. For most personal communication, WhatsApp's E2E encryption is sufficient. For sensitive or high-stakes communication, Signal is the stronger choice.

4. Where Encryption Applies in Your Daily Life

Encryption is already present in most of the digital tools you use. Understanding where it is and where it might be missing helps you make better decisions about what to send and store where.

Where Encryption Applies	What it Protects	How to Tell it's Working	What to Do When it's Missing
Websites (HTTPS)	Everything you send to and receive from a website: login credentials, payment details, form submissions, page content	Padlock icon and 'https://' in your browser address bar	Do not enter any personal information or credentials on HTTP pages. Modern browsers warn you heed the warning.

Where Encryption Applies	What it Protects	How to Tell it's Working	What to Do When it's Missing
Email in transit	Email content while it travels between mail servers	Most modern email providers (Gmail, Outlook) encrypt in transit automatically. You cannot easily verify this as a user.	Use a reputable email provider that supports TLS. If sending highly sensitive documents, consider encrypting the attachment itself rather than relying on transport encryption.
Messaging apps (end-to-end)	Message content from your device to the recipient's device. Even the messaging platform cannot read it.	WhatsApp, Signal, and iMessage all use end-to-end encryption by default. Look for the lock icon or the 'encrypted' label in app settings.	If you need strong confidentiality for sensitive conversations, use Signal. Standard SMS and many messaging apps do not offer end-to-end encryption.
Device storage (disk encryption)	All data stored on your device's drive. Protects your data if the device is lost, stolen, or the drive is removed.	Check via BitLocker (Windows) or FileVault (macOS) settings. iOS encrypts automatically when a passcode is set.	Enable full-disk encryption as described in Module 11. On modern devices this takes minutes to set up.
Cloud storage	Files stored in cloud services. Encrypted in transit and usually at rest on the server.	All major providers (iCloud, Google Drive, OneDrive, Dropbox) encrypt data in transit and at rest.	Be aware that cloud providers hold the encryption keys for most standard plans, meaning they can technically access your files. For highly sensitive data, consider client-side encryption before uploading.
VPN tunnel	All traffic between your device and the VPN server, protecting it from observation on your local network	Your VPN app will show a connected/active status	Use a VPN on untrusted networks (public Wi-Fi) as covered in Module 7. Remember it does not protect content once it leaves the VPN server.

5. What Encryption Does and Doesn't Protect

Encryption is a powerful tool with real limits. Understanding those limits is as important as understanding the protection it provides.

✅ Encryption DOES Protect You From...	❌ Encryption Does NOT Protect You From...
An attacker intercepting your data in transit on a network (man-in-the-middle)	Entering your own credentials on a phishing site: you decrypt the connection yourself when you log in
Someone reading data on a lost or stolen encrypted device	Malware already running on your device it captures data before encryption takes place
A data breach at a company that stored your data encrypted at rest	A service that holds your encryption keys if they are compromised, your data can be decrypted
Your internet provider reading the content of encrypted web traffic	Metadata: who you communicate with, when, and how often even if the content is encrypted
Someone physically removing your hard drive and reading it on another machine	Account takeover an attacker who logs in legitimately with your credentials sees your decrypted data

The most important limit: encryption protects data, not decisions

Encryption cannot protect you from your own actions. If you type your password into a convincing phishing site, the HTTPS padlock on that fake site confirms the connection is encrypted it does nothing to protect the credentials you just handed to an attacker. If malware is running on your device, it captures your data before it is encrypted. Encryption is a transport and storage protection. Human judgment is a separate layer that no technology can replace.

6. Key Management: The Overlooked Half of Encryption

Encryption is only as secure as the key that unlocks it. This is the most consistently underestimated aspect of encryption, both for individuals and organizations. A perfectly encrypted file is worthless to an attacker without the key and worthless to you too, if you lose it.

Scenario	The Key Management Question	What Goes Wrong Without it
Full-disk encryption on your laptop	Where is the recovery key stored? If you forget your password, you need it to decrypt the drive.	Without the recovery key, a forgotten password means permanent, irreversible data loss. Store the recovery key somewhere safe and separate from the device.
Password manager vault	The master password is effectively the encryption key. What happens if you forget it?	Most password managers cannot recover your vault if you forget the master password by design. Set up recovery options (emergency kit, recovery email) when you first create the account.
Business file encryption	Who holds the keys, and what happens if the key holder leaves?	Files encrypted by a departing employee become permanently inaccessible if key management was not documented. Always use centralized key management for business data.
Cloud storage with client-side encryption	You hold the key. If you lose it, the cloud provider cannot help you they do not have a copy.	Permanent data loss. For most users, standard cloud encryption (where the provider holds keys) is a better trade-off than the risk of losing your own keys.

The key management principle

Keys must be stored separately from the data they protect. An encrypted hard drive whose recovery key is stored in a text file on the same drive defeats the encryption. An encrypted database whose decryption key is in the same server directory defeats the encryption. An encrypted ZIP file sent to a recipient with the password in the same email defeats the encryption. Always separate the key from the lock. If you cannot do this, reconsider whether encryption is providing the protection you think it is.

7. Practical Encryption Habits

Encryption requires relatively little active management. For most people, it works in the background. The habits that matter are about verifying it is in place and not accidentally undermining it.

- Check for HTTPS before entering any credentials or personal information on a website. The padlock and https:// prefix confirm an encrypted connection. Module 7 covered this; it is worth repeating.
- Use end-to-end encrypted messaging (Signal or WhatsApp) for sensitive personal conversations. Do not assume standard SMS provides any meaningful security.
- Ensure full-disk encryption is enabled on your laptop and that your phone has a passcode set (which activates its built-in encryption). Verified in Module 11.
- When sending sensitive files by email, encrypt the file itself (a password-protected ZIP or PDF) and share the password through a different channel (a text message, a phone call). Do not send the password in the same email as the encrypted file.
- Save encryption recovery keys. Whether for BitLocker, FileVault, or your password manager, store recovery information somewhere safe and separate from the device it protects.
- Be thoughtful about what you store in cloud services. Most cloud storage encrypts your data, but the provider holds the keys. For highly confidential documents, consider whether cloud storage is appropriate at all.

ShieldNet thread going further

Encryption is addressed in ShieldNet control [SB7] (Encrypt Sensitive Data), which requires HTTPS/TLS for data in transit and strong encryption for data at rest, with proper key management. It specifically calls out encrypted backups a detail that many organizations overlook. The control also connects to [SB5] (Secure Your Network) for the VPN encryption aspect covered in Module 7. For organizations developing software or products, [SB8] (Develop & Acquire Securely) requires that encryption is built in from the design stage rather than added afterwards.

Module 12: Summary

By the end of this module, you should be able to:

- ✓ Explain what encryption does in plain language, using the locked box analogy or equivalent.
- ✓ Describe the difference between encryption in transit and encryption at rest, with an example of each.
- ✓ Explain what end-to-end encryption means and why it offers stronger privacy than standard encryption.
- ✓ List three things encryption protects you from and two things it does not.

- ✓ Describe what key management means and why it matters, using one concrete example.
- ✓ Explain what HTTPS confirms and, importantly, what it does not confirm.

Module 13: Your Data and Privacy

What You Share, With Whom, and Why It Matters

1. The Product You Did Not Know You Were Selling

In 2010, a technology investor made an observation that has since become one of the defining phrases of the digital age: 'If you're not paying for the product, you are the product.' It is a simplification, but a useful one.

Every major free digital service, search engines, social media platforms, email, maps, video streaming, is built on a business model that monetize your attention and your data. The service is free because the real transaction is not happening between you and the platform. It is happening between the platform and advertisers, who pay for access to detailed profiles of people's interests, habits, and vulnerabilities.

This is not inherently sinister. People make conscious trade-offs: free email in exchange for some data collection is a bargain many people find acceptable. The problem is when the trade-off is not transparent, when the data is used in ways people did not expect, or when the accumulated profile becomes a tool for manipulation, discrimination, or exploitation.

This module is about understanding what personal data is, how it flows, what rights you have over it, and what practical steps you can take to limit collection where you choose to. Not paranoia informed decisions.

2. What Personal Data Actually Is

Under GDPR, personal data is defined as any information relating to an identified or identifiable natural person. That definition is deliberately broad, and it covers far more than most people instinctively think of as 'personal data'.

Category	Examples	Why it is SENSITIVE
Basic identifiers	Full name, date of birth, home address, phone number, email address, national ID number	Enough to impersonate you, open accounts in your name, or pass security questions
Financial data	Bank account numbers, payment card details, credit scores, salary information, tax records	Direct pathway to financial fraud and identity theft

Category	Examples	Why it is SENSITIVE
Special category data	Health and medical records, racial or ethnic origin, political opinions, religious beliefs, biometric data (fingerprints, face scans), sexual orientation, criminal records	Explicitly given the highest protection under GDPR because misuse can cause discrimination, harm, or persecution. Requires explicit consent or specific legal basis to process.
Behavioral data	Browsing history, search queries, location history, purchase history, app usage patterns, social media interactions	Reveals your habits, relationships, vulnerabilities, and preferences. Used for profiling and targeted advertising; valuable to criminals for social engineering.
Communications data	Email content, message history, call logs, who you communicate with and when	Reveals relationships and private thoughts; can be used for blackmail, social engineering, or professional harm
Device and technical data	IP addresses, device identifiers, operating system, browser type, cookie identifiers	Used to track you across websites and build profiles even without knowing your name

The aggregation problem

Each individual piece of data in the table above might seem harmless in isolation. Your first name: harmless. Your employer: harmless. Your approximate neighborhood: harmless. The coffee shop you visit every morning at 8am: harmless. Combined, these four pieces of information create a profile precise enough to physically locate you at a specific time and place. This is the aggregation problem the reason why data minimization[40] matters even for data that individually seems trivial. The harm is not in any single piece. It is in what emerges when they are combined.

[40] **Data minimization:** The principle of collecting and keeping only the personal data you actually need, and no more.

3. How Your Data Flows Without You Noticing

Most people have a vague sense that 'companies collect data about them'. Fewer understand the specific mechanisms. Understanding them makes you a more conscious participant.

Cookies and tracking pixels

A cookie is a small file stored on your device by a website that allows the site to recognize you on future visits. Tracking cookies go further: they are placed by third-party advertising networks and follow you across multiple websites, building a profile of your browsing behavior. When you click 'Accept all cookies' without reading the options, you are typically consenting to this cross-site tracking. The 'Reject all' or 'Manage preferences' options reduce it significantly.

A tracking pixel is an invisible image embedded in a webpage or email. When it loads, it reports back to the sender: you opened this email, at this time, on this device, in this approximate location. Email marketing tools use these to measure engagement. You can reduce their effectiveness by disabling automatic image loading in your email client.

Data brokers

Data brokers are companies whose entire business model is collecting, aggregating, and selling personal data. They gather information from public records, social media, purchase histories, app data, voter registers, and hundreds of other sources. They combine these into detailed profiles and sell them to marketers, insurance companies, employers, lenders, and increasingly to anyone willing to pay.

You almost certainly have a profile with multiple data brokers, even if you have never heard of them. EU residents have the right under GDPR to request deletion of their data from data brokers (the right to erasure). Exercising this right is time-consuming but available. Several services automate the process for a subscription fee.

App permissions and device sensors

Mobile apps routinely request permissions that go well beyond what the app needs to function. A flashlight app that requests access to your contacts is not serving you better it is harvesting your address book. A free game that wants your location at all times is not improving gameplay it is selling location data. Reviewing and revoking

unnecessary permissions (covered in Module 10) is one of the most direct ways to reduce data collection from your phone.

4. GDPR in Plain English

The General Data Protection Regulation is EU law that gives individuals rights over their personal data and places obligations on organizations that collect and process it. You do not need to be a lawyer to benefit from it. The rights it grants are concrete and exercisable.

The core principle behind GDPR is accountability: organizations must be able to demonstrate that they have a lawful reason to collect your data, that they collect only what they need (data minimization), that they keep it only as long as necessary, and that they protect it properly. When they fail to do these things, they can face significant fines, up to 4% of global annual turnover for the most serious breaches.

Your Right	Examples	How to Exercise it
Right to be informed	Organizations must tell you what data they collect, why, how long they keep it, and who they share it with usually in a privacy notice	Read privacy notices before signing up to services. Look for plain-language summaries at the top.
Right of access	You can request a copy of all personal data an organization holds about you (a Subject Access Request, or SAR). They must respond within one month, usually free of charge.	Email or write to the organization's data protection contact. State you are making a Subject Access Request[41] under GDPR Article 15.
Right to be rectification	You can ask an organization to correct inaccurate personal data they hold about you	Contact the organization, identify the inaccuracy, and request correction. They must respond within one month.
Right to erasure	'The right to be forgotten', in certain circumstances, you can ask an organization to delete your personal data	Applies when the data is no longer needed, you withdraw consent, or the processing was unlawful. Not absolute some organizations have legitimate reasons to retain data.

[41] **Subject Access Request:** A formal request under GDPR for a copy of the personal data an organization holds about you, which it must usually provide within one month.

Your Right	Examples	How to Exercise it
Right to data portability	You can request your personal data in a machine-readable format to transfer to another service	Useful when switching banks, email providers, or social media platforms. Request your data export from account settings.
Right to object	You can object to your personal data being used for direct marketing, profiling, or certain other purposes	Unsubscribe from marketing lists. Contact the organization directly to object to profiling or automated decision-making affecting you.

When to use a Subject Access Request

A Subject Access Request (SAR) is your formal request for a copy of all personal data an organization holds about you. It is most useful when:

You want to know what a company, employer, or institution holds about you before making a significant decision.

You suspect data about you is inaccurate and want to see what they actually hold.

You are involved in a dispute (employment, insurance, financial) and need to understand what information the other party has.

To make a SAR: send a written request (email is fine) to the organization's data protection officer or privacy contact. State clearly that you are making a Subject Access Request under UK/EU GDPR Article 15. They must respond within one month.

5. Data Minimization as a Personal Habit

GDPR's data minimization principle collect only what you need applies to organizations by law. But it is equally useful as a personal habit. Data you do not share cannot be collected, breached, or misused.

What you share when signing up for services

When a service asks for your date of birth, consider whether it needs your actual date of birth or just confirmation that you are over a certain age. When it asks for your home address for a digital product, question whether that is actually required. When a newsletter asks for your phone number, ask why a newsletter needs your phone number. Providing minimum necessary information and being willing to provide false information for fields that are not legally required and not essential to the service reduces your data footprint.

Using aliases and secondary identities

Many privacy-conscious people maintain a separate email address for services they trust less, use a PO box or relay address for physical mail from commercial organizations, and use browser extensions or Apple's Hide My Email feature to generate unique email aliases that forward to their real inbox. If one alias is breached or sold, the impact is contained. If the alias starts receiving spam, it can be deleted without affecting the primary email.

What you share publicly on social media

Social media profiles are among the most accessible sources of personal data about individuals. Your employer, your location, your daily routine, your family members, your pet's name, your car, your home's exterior all potentially visible to anyone, including attackers researching spear phishing targets. Periodically audit what is publicly visible on your profiles and adjust privacy settings accordingly.

6. Taking Control: Practical Privacy Settings

Privacy protection does not require abandoning the services you use. It requires spending time in the settings that most platforms bury several menus deep. Here is where to look.

Platform / Service	Key Privacy Settings to Review	What They Control
Google account	myaccount.google.com → Data & Privacy → History settings, Ad personalization, Third-party apps	Turn off web & app activity, location history, and YouTube history if you prefer not to have them tracked. Review and remove third-party apps with access.
Facebook / Instagram (Meta)	Settings → Privacy, Settings → Ads, Settings → Apps and Websites	Limit who sees your posts and profile. Turn off off-Facebook activity tracking. Remove apps you no longer use.
iPhone / iOS	Settings → Privacy & Security → each app's permissions; App Tracking Transparency	Review and restrict location, contacts, microphone, camera access per app. Enable 'Ask App Not to Track' for all apps.
Android	Settings → Privacy → Permission Manager; Settings → Google → Ads	Review permissions by type (see all apps with location access). Opt-out

Platform / Service	Key Privacy Settings to Review	What They Control
		of ads personalization. Reset advertising ID regularly.
Browser	Settings → Privacy & Security in Chrome, Firefox, Safari, or Edge	Enable tracking protection (Firefox Strict mode is strong). Clear cookies regularly. Use private browsing for sensitive searches.
Email	Unsubscribe from mailing lists. Use a secondary email for signups. Check for email trackers.	Reduce data harvesting via email. Services like Hey, ProtonMail, or email aliasing (SimpleLogin, Apple Hide My Email) limit tracking.

Cookie consent: reject all is almost always available

When a website shows a cookie consent banner, look for 'Reject all' or 'Manage preferences'. EU law (under the ePrivacy Directive and GDPR) requires that rejecting cookies must be as easy as accepting them though many sites bury the option or make it deliberately harder to find. If you see only an 'Accept all' button with no easy way to decline, that is itself a legal violation you can report to the relevant data protection authority. Your browser's built-in privacy settings or an extension like uBlock Origin will block most tracking before it starts.

7. Privacy and Security: Why They Are Connected

Privacy and security are sometimes treated as separate concerns. They are not. Every piece of personal data you share increases your attack surface.

The location data your phone shares with apps can be used to determine your home address, your workplace, your daily routine, and when you are away from home. The social media profile that shows your employer, your colleagues' names, and your recent travel creates the raw material for a spear phishing attack that would fool almost anyone. The data broker profile that shows your interests, your financial situation, and your relationships gives an attacker leverage for social engineering.

Privacy protection is threat reduction. Limiting data collection does not just protect your personal autonomy it directly reduces the quality of information available to people who want to attack, defraud, or manipulate you. The fewer accurate data

points an attacker has, the less convincing their impersonation, the less targeted their approach, the more likely their attempt fails.

ShieldNet thread going further

Data privacy maps to two ShieldNet controls. [SB9] (Minimize Data Collection) requires organizations to collect and retain only the data they need, anonymize or delete it when no longer required, and configure systems to enforce retention policies the organizational expression of the personal data minimization habits in this module. [KP8] (Build Security into Projects) includes the requirement to embed privacy by design into new systems and products, connecting to GDPR's data protection by design principle (Article 25). These controls exist because organizations that collect less data have smaller breach impact, fewer compliance obligations, and a smaller attack surface.

Module 13: Summary

By the end of this module, you should be able to:

- ✓ Define personal data and explain why behavioral data (browsing history, location) is sensitive even when it seems trivial.
- ✓ Explain the 'free product' model and describe what users typically provide in exchange for free digital services.
- ✓ Name three rights that individuals have under GDPR and describe how to exercise one of them.
- ✓ Explain what data minimization means and give a practical example of applying it.
- ✓ Describe two specific steps you can take to reduce data collection about you in your digital life.
- ✓ Explain why privacy and security are connected, using the concept of the attack surface.

Module 14: Trusting Third Parties

Apps, Services and the Supply Chain

1. Everything You Install Is a Trust Decision

Every app you install, every service you sign up for, every browser extension you add, every 'Login with Google' you click each one is a trust decision. You are granting a third party some level of access to your device, your data, or your accounts. Most of the time, that trust is well-placed. Sometimes it is not.

The risk is not theoretical. In 2021, a widely-used VPN app on the Google Play Store was found to have been quietly modified after its initial publication to collect user data and forward it to third parties. In 2020, a popular browser extension with millions of users was discovered to be harvesting complete browsing histories and selling them. In 2023, a free PDF tool downloaded by millions of people turned out to be adware that redirected search results and installed additional unwanted software.

None of these were downloaded from shady websites. They were all available through official channels, with good ratings, for extended periods. The question is not whether to trust third parties at all that is unavoidable in modern digital life. The question is how to evaluate that trust and limit the exposure when trust turns out to have been misplaced.

2. Official Stores Are Not a Safety Guarantee

App stores from Apple and Google provide a degree of vetting: they scan for known malware, verify developer identities, and review apps before listing them. This is worth something. But it is not a guarantee of safety.

Malicious apps regularly appear in official stores despite review processes. They may pass initial review as legitimate tools and only become malicious after an update that bypasses re-review. They may use permission combinations that are technically allowed but practically harmful. They may use names or icons that closely mimic trusted apps, deceiving users into downloading the wrong version.

The fake app problem

Search for a popular app in any app store and you will often find several results with similar names, similar icons, and similar descriptions. The real WhatsApp, the real Google Maps, the real banking app and several impostors. The safe approach: always navigate to the app

via the developer's official website and follow the download link there, rather than searching in the store. The developer's website will link to the genuine app listing.

3. How to Evaluate an App or Service

The following six questions, asked before installing any app or signing up to any service, catch the vast majority of problematic tools before they cause harm.

Question to Ask	Green Flags	Red Flags
Who made it?	A known, established developer or company. A verified developer badge in the app store. A real website with contact information.	Unknown developer with no web presence. A name very similar to a well-known app ('Whatsapp Free', 'G00gle Maps'). No privacy policy linked.
What permissions does it request?	Permissions that make sense for the app's stated function. A navigation app wanting location. A camera app wanting camera access.	Permissions that have no obvious connection to the app's function. A calculator wanting contacts. A wallpaper app wanting microphone access.
What do reviews and ratings say?	Large number of genuine, varied reviews over time. Consistent quality feedback. Established in the store for a significant period.	Very few reviews. Many reviews on a single date (purchased reviews). Reviews that focus on the app working but mention unexpected behavior.
Does it have a privacy policy?	A clear, accessible privacy policy that explains what data is collected and why. The policy is specific, not generic.	No privacy policy. A policy that is clearly a generic template with no app-specific information. A policy that claims to share data with 'partners' without naming them.
What is the update history	Regular updates over an extended period. The developer responds to user feedback. Recent security patches noted in update descriptions.	Last update was years ago. No response to user complaints. Sudden spike in negative reviews after an update.
How is it monetized?	Clear paid model, or a clear freemium model with transparent advertising. The business model makes sense for the app's type.	Free with no obvious revenue source. A business model that is unclear or unstated. Free apps in categories where development costs are substantial.

The permission test

The single most reliable quick check is the permissions list. Ask: 'For what this app does, why would it need this?' A weather app needs your location. It does not need your contacts, your microphone, or access to your files. A photo editor needs camera access. It does not need to read your SMS messages. If you cannot construct a plausible explanation for why the app's stated function requires a specific permission, deny that permission, or choose a different app.

4. Third-Party Risk by Level

Not all third parties carry equal risk. The risk depends on what access you grant them, what data they can reach, and what happens if they are compromised. Understanding this lets you apply proportionate scrutiny rather than treating every app identically.

Risk Level	Type of Third Party	Why The Risk is Higher	What to Check
Critical	Password managers, identity providers (login with Google/Apple), security tools	These have privileged access to credentials or act as the gateway to all other accounts. A compromise here is a total compromise.	Use only well-established providers with strong security track records. Enable MFA. Review what each can access.
High	Cloud storage, email providers, banking apps, work productivity tools	Store or process sensitive personal or financial data. A breach exposes significant information.	Stick to reputable, established providers. Review sharing settings. Enable MFA. Know where your data is stored.
Medium	Shopping apps, streaming services, social media, fitness trackers	May hold payment details, personal preferences, location history, or contacts. A breach is inconvenient and potentially damaging.	Use unique passwords (password manager). Limit permissions. Review privacy settings. Remove when no longer used.
Lower	Games, utilities, reference apps, tools	Limited access to sensitive data. A	Still check permissions and developer

Risk Level	Type of Third Party	Why The Risk is Higher	What to Check
	with no account or cloud component	compromise affects only that app's function.	reputation. Avoid from unofficial sources.

The 'Login with Google' concentration risk

'Login with Google', 'Login with Apple', and 'Login with Facebook' are convenient and, for the individual services they protect, more secure than reusing passwords.

The risk is concentration. If the central account (Google, Apple, or Facebook) is compromised, every service linked to it through that login is simultaneously compromised.

The mitigation: treat the central account as critical infrastructure. Enable the strongest available MFA on it (authenticator app minimum, hardware key if possible). Review which services are connected via Settings > Security > Connected apps. Remove any you no longer use.

Apple Sign In has a privacy advantage: it can generate unique relay email addresses for each service, meaning the service never knows your real email address.

5. Browser Extensions: A Higher-Risk Category

Browser extensions deserve special attention because their permission model is unusually powerful. An extension with 'read and change all data on websites you visit' permissions which many extensions request as a matter of course can see everything you type into every website, read every page you visit, and in principle intercept any data passing through your browser.

This is a significant level of trust to place in a third party, and it is granted with a single click during installation. Most users do not consider the implications.

Extension Type	The Risk	Best Practices
Ad blockers and privacy tools	Legitimate ad blockers (uBlock Origin, Privacy Badger) are well-audited. However, malicious extensions with similar names exist and ad blockers have 'read and change all data on websites you visit' permissions by default.	Use only the well-known, widely-reviewed versions. Install from the official browser store. Check the developer name exactly.

Extension Type	The Risk	Best Practices
Productivity tools (grammar checkers, PDF editors, etc.)	These tools often read everything you type or every page you visit in order to function. That is a significant amount of sensitive data passing through a third party.	Use only from established providers you trust. Understand that these tools see your content. Disable on sensitive sites (banking, medical, work systems) if possible.
Shopping assistants and coupon finders	These extensions typically send your entire browsing history to the extension provider's servers to identify relevant offers. This is extensive behavioral data collection in exchange for small discounts.	Evaluate whether the trade-off is worthwhile. If using one, use a browser profile dedicated to shopping and not for sensitive browsing.
Extensions you no longer use	Browser extensions can be sold to other developers after acquisition, who then update them with data-harvesting or malicious code. The user who installed a legitimate tool years ago now has malware.	Regularly audit your browser extensions. Remove any you no longer actively use. Be suspicious of any extension that requests unexpected permission changes after an update.

Browser extension hygiene: the five-minute audit

Open your browser's extension management page: chrome://extensions in Chrome, about:addons in Firefox, or Extensions in Safari.

For each extension: do you still use it? Do you remember installing it? Does the developer name look correct?

Remove anything you do not actively use, do not recognize, or cannot explain.

Check the permissions of everything you keep. Look for 'read and change all data on websites you visit' that is a high-trust permission. Is this extension worth that level of trust?

This audit takes five minutes and removes a category of risk that most people have never considered.

6. The Supply Chain Risk for Individuals

Module 8 introduced supply chain attacks from an organizational perspective: attackers compromising trusted software vendors to reach their customers. This risk exists at the individual level too, and it is one of the most difficult to defend against because it does not require any mistake on your part.

When you use a reputable application, you inherit the security of every library, component, and dependency that application relies on. A vulnerability in an open-source library used by dozens of popular applications can expose millions of users simultaneously, even though each user did everything right.

What individuals can realistically do

Complete protection against supply chain attacks is not achievable at the individual level. What is achievable:

- Keep software updated. When a supply chain compromise is discovered and patched, the patch reaches you through an update. Turning on automatic updates means you receive fixes as fast as possible.
- Minimize your software footprint. Every application you install is a potential supply chain exposure. Fewer applications = smaller attack surface. Regularly uninstall applications you no longer need.
- Use reputable, well-maintained applications. Established applications with active development communities respond to supply chain incidents faster and more transparently than abandoned or obscure tools.
- Monitor for breach notifications. Services like haveibeenpwned.com alert you when your email appears in a known breach, including those resulting from supply chain attacks on services you use.

7. When You Stop Using a Service: The Offboarding Habit

Most people are reasonably careful about which services they sign up for. Almost nobody is as careful about leaving. Dormant accounts and forgotten app connections are one of the most commonly overlooked personal security risks.

An account you no longer use still holds your data. It may still have a password you reused elsewhere. It still appears in breach notifications if that service is compromised. And if the service is acquired, its new owners inherit your data and may use it differently from the original terms.

- Delete accounts you no longer use. Most services provide a delete account option in settings. Use it. Deletion is not the same as deactivation: ensure data is actually removed, not just the profile made private.

- Revoke app connections. Before deleting an account used for third-party logins, revoke any connected apps via the account's security settings first.
- Check for data export options. Under GDPR, you have the right to a copy of your data before you delete it. If you want to retain any history, export it first.
- Remove the app from your device. Uninstalling the app does not delete your account or data on the service's servers. Account deletion is a separate step.

ShieldNet thread going further

Third-party trust maps directly to ShieldNet control [KP7] (Vet Suppliers), which requires organizations to screen third-party providers before and during engagement, ensure contracts include security requirements, and prefer certified or reputable suppliers. The personal habits in this module evaluating apps before installing, reviewing permissions, auditing connected services, removing what you no longer use are the individual expression of the same due diligence principle. [SB9] (Minimize Data Collection) also applies: the fewer third parties you connect to your data, the smaller your exposure when any one of them is compromised.

Module 14: Summary

By the end of this module, you should be able to:

- ✓ Explain why installing an app from an official app store does not guarantee it is safe.
- ✓ List four questions to ask when evaluating whether to trust a new app or service.
- ✓ Explain what 'login with Google' or 'login with Apple' means in terms of access and risk.
- ✓ Describe why browser extensions are a higher-risk category of third-party tool.
- ✓ Explain the supply chain risk from the individual user's perspective and describe one thing you can do to reduce it.
- ✓ Name two actions to take when you stop using a service or app.

Completing Part 3

Part 3 is complete. You now have a practical toolkit covering the defenses that matter most.

Module 9: Strong authentication, MFA, passkeys, and the three factors that prove who you are.

Module 10: Access control, least privilege, dormant accounts, and the blast radius principle.

Module 11: Keeping devices safe, updates, screen locks, encryption, and the end-of-life risk.

Module 12: Encryption in transit, at rest, end-to-end, and the key management gap.

Module 13: Your data and privacy, what personal data is, GDPR rights, and data minimization.

Module 14: Trusting third parties, evaluating apps, browser extensions, and the supply chain.

Part 3 Knowledge Check

Module 9 Practice Questions
Q1. An employee receives 15 push notification MFA requests on their phone in rapid succession, all appearing to be from their work account login system. They did not initiate any logins. The notifications stop and ten minutes later they receive a 16th, which they approve out of frustration. What type of attack has just succeeded? a. A SIM-swapping attack, the attacker has taken over the employee's phone number. b. An MFA fatigue attack, the attacker flooded the employee with approval requests until they approved one, bypassing MFA despite having only the password. c. A credential stuffing attack, the attacker tried many passwords until one worked. d. A phishing attack, the employee was tricked into approving the request by a convincing email.
Q2. A user sets up a hardware security key (such as a YubiKey) as their second factor for their email account. An attacker later tricks the user into entering their email password on a convincing fake login page. The attacker now has the password. What happens when they try to complete the login? e. The attacker logs in successfully because they have the password. f. The attacker cannot complete the login because the hardware key performs a cryptographic check that verifies the real domain, it will not respond on a fake site, regardless of whether the attacker has the password. g. The hardware key sends an alert to the user's phone, allowing them to deny the login. h. The attacker is blocked for 24 hours after a failed MFA attempt.
Q3. Someone argues that biometric authentication (fingerprint or face) is risky because 'if your fingerprint is stolen, you can't change it like a password.' Which response most accurately addresses this concern? i. This concern is valid, biometrics should never be used as an authentication method. j. When used on a device, your fingerprint is not sent to a server, it unlocks a cryptographic key stored locally. What could theoretically be stolen is the key, not your fingerprint. And you can revoke and re-enroll biometrics. k. This concern is irrelevant because biometric data is always stored in the cloud where it is fully encrypted. l. The concern is valid, which is why biometrics should only be used as a primary factor, never combined with other methods.
Q4. You are advising a small charity on which accounts to enable MFA on first, given limited time. They use email (Gmail), a cloud accounting package, social media, and a password manager. In which order should they prioritize? m. Social media first (highest public visibility), then email, then accounting, then password manager.

Module 9 Practice Questions
n. Password manager first (most accounts at risk if breached), then email (resets everything else), then accounting (financial data), then social media. o. Email first (resets every other account and is the gateway to all others), then password manager (contains all other credentials), then accounting (financial data), then social media. p. Accounting first (financial data is most sensitive), then password manager, then email, then social media.

Module 10 Practice Questions
Q1. A marketing assistant at a company is given full administrator rights on the company's server 'to make it easier to install the design software they need'. Their account is later compromised via a phishing attack. What access does the attacker now have? a. Access only to the design software, since that is what the admin rights were granted for. b. Full administrator access to the server, they can read, modify, or delete all data, install malware, create new accounts, and disable security controls. c. The same access any normal user would have, because the admin rights are only activated when installing software. d. No access, because the phishing attack would have been blocked by the server's security controls.
Q2. A team member who left the company six months ago still has an active user account in the company's cloud storage. A former colleague remembers the account exists and uses it to copy confidential client files before starting work at a competitor. Which access control failure most directly enabled this? e. The former employee used a weak password that was easy to guess. f. The company did not have multi-factor authentication on the cloud storage. g. The account was never deactivated when the employee left, a failure to revoke access as part of the offboarding process. h. The cloud storage did not have sufficient monitoring to detect unusual downloads.
Q3. You receive a request on your phone asking you to approve access for a new app to connect to your Google account. The app wants permission to: read all your emails, access your Google Drive, and manage your calendar. You do not recognize the app. What is the correct response? i. Approve the permissions, as Google has already verified the app is safe. j. Approve read-only permissions but deny write permissions. k. Deny the access request entirely. Do not grant permissions to apps you do not recognize or have not intentionally connected to your account. l. Approve the request and then review what the app does before deciding whether to keep the permissions.
Q4. An organization uses a single shared 'admin' account that several IT staff members log into when they need to make system changes. A security incident occurs and the organization

Module 10 Practice Questions
needs to determine who made a specific configuration change three weeks ago. What fundamental access control principle does this arrangement violate? m. Least privilege, the shared account has more access than any individual needs. n. Separation of duties, no single person should be able to make changes without another approving them. o. Individual accountability, shared accounts make it impossible to attribute actions to specific people, so there is no audit trail. p. Need-to-know, not all IT staff should have access to the same information.

Module 11 Practice Questions
Q1. A security researcher publishes details of a critical vulnerability in a widely used operating system. The vendor releases a patch the same day. Three weeks later, an organization that has not applied the patch is breached through that exact vulnerability. Which principle of device security was not followed? a. Full-disk encryption, the organization's data was not encrypted at rest. b. Anti-malware, the organization should have used endpoint protection to block the attack. c. Timely patching, security patches for critical vulnerabilities should be applied urgently; three weeks after a publicly known, actively exploited vulnerability is far too late. d. Screen lock, physical access to the device enabled the exploit.
Q2. A staff member's work laptop is stolen from their car. The laptop has a strong login password, full-disk encryption enabled, and Find My Device set up. The thief attempts to access the data by removing the hard drive and connecting it to a different computer. What happens? e. The thief can read all the data, because removing the drive bypasses the login password. f. The thief cannot read the data, because full-disk encryption makes the drive unreadable without the encryption key, regardless of which computer it is connected to. g. The thief can read some data, because full-disk encryption only protects files that have been manually encrypted. h. The organization can prevent access by triggering a remote wipe through Find My Device.
Q3. A user's phone is running an Android version that is two major releases behind the current version. Their device manufacturer no longer supports that version. What is the most significant security implication? i. The phone will run more slowly and some apps may not function correctly. j. The phone will no longer receive security patches, meaning any vulnerabilities discovered from this point forward will remain permanently unpatched on that device. k. The phone's encryption will be weaker than on a current version. l. The phone will be unable to connect to modern Wi-Fi networks.
Q4. An employee uses their personal smartphone to access company email and Teams. They have not enabled a screen lock PIN and their phone does not receive OS updates because it is an old model. What is the most appropriate organizational response? m. Ban the use of personal devices for work entirely. n. Require that personal devices used for work meet minimum security standards screen lock, encryption, and OS updates as a condition of accessing company systems, and provide guidance on how to check these settings. o. Accept the risk, as personal devices are outside the organization's control. p. Install monitoring software on the employee's personal device to enforce compliance.

Module 12 Practice Questions
Q1. A journalist is investigating a sensitive story and needs to communicate securely with a source. They are considering using email via Gmail or Signal for their messages. Which option offers stronger protection for the content of their communications, and why? a. Gmail, because it uses HTTPS which encrypts all communications. b. Signal, because it uses end-to-end encryption only the journalist and source can read the messages. Gmail encrypts data in transit but Google can read the content and may be compelled to provide it to authorities. c. Both are equally secure because both use encryption. d. Gmail, because it stores messages on Google's encrypted servers which are more secure than Signal's.
Q2. A user's laptop is stolen. The hard drive is removed and connected to a different computer. The laptop had full-disk encryption enabled (BitLocker) with a strong password. What can the thief access? e. All files, because removing the drive bypasses Windows login security. f. Only files created after encryption was enabled. g. Nothing, the drive is encrypted and unreadable without the decryption key, regardless of which computer it is connected to. h. Files that were not marked as 'private' in Windows settings.
Q3. An attacker successfully intercepts encrypted HTTPS traffic between a user and their bank. The attacker captures thousands of encrypted data packets. What can they read? i. Everything, because they have captured the full conversation. j. The metadata, which website was visited and when, but not the content of the pages or any credentials entered. k. Nothing useful, the content is encrypted with a key they do not have, making the captured data unreadable. l. Only the username, because passwords are double-encrypted.
Q4. A company encrypts all files on its server but stores the encryption keys in a text file on the same server. The server is then breached. What encryption failure does this illustrate? m. The encryption algorithm used was too weak. n. The files should have used end-to-end encryption instead of at-rest encryption. o. Poor key management, storing the encryption key alongside the encrypted data effectively defeats the encryption. Keys must be stored separately from the data they protect. p. The company should have used a VPN to protect the server.

Module 13 Practice Questions
Q1. A fitness app asks for permission to access your contacts, location at all times, microphone, and camera in order to track your runs and log workouts. Applying the principle of least privilege to app permissions, which of these should you grant? a. All of them, the app needs everything it requests to function correctly. b. Location (for tracking runs) and camera (for logging photos of workouts). Microphone and contacts access does not serve the stated function and should be denied. c. None of them, fitness apps should not require any device permissions. d. Only camera access, because location tracking is always a privacy risk.
Q2. A person discovers that a company holds incorrect information about their credit history. Under GDPR, which right allows them to ask the company to fix this? e. The right to erasure, they can ask the company to delete all data about them. f. The right to data portability, they can transfer their data to a more accurate provider. g. The right to rectification, they can ask the company to correct inaccurate personal data. h. The right to object, they can object to the company processing their data at all.
Q3. A social media platform offers a free service and does not charge users money. Its primary revenue source is advertising. What is the most accurate description of the business model? i. The platform is a charity providing a free public service. j. Users pay with their personal data and attention. The platform collects behavioral data to build advertising profiles, which it sells access to. k. The platform is funded by governments as a public communications infrastructure. l. The platform has no revenue model and relies on investment funding indefinitely.
Q4. Someone argues: 'I don't care about privacy because I have nothing to hide.' Which response best addresses this from a security perspective, beyond the personal privacy argument? m. Privacy is a legal right, so everyone should care about it regardless of their personal views. n. The data you share creates an attack surface. The more an attacker knows about you, your habits, relationships, employer, travel patterns, the more convincingly they can craft a targeted attack, impersonate you, or manipulate people connected to you. o. Privacy only matters if you are doing something illegal, so the argument is largely correct. p. Privacy is important because companies will sell your data without your knowledge.

Module 14 Practice Questions
Q1. You find a free PDF editing app in the official Google Play Store. It has 4.8 stars and 50,000 downloads. It requests permission to access your contacts, microphone, and location. The developer has no website and the app has no privacy policy. Should you install it? a. Yes, the high rating and download count in the official store confirm it is safe. b. No, the absence of a privacy policy, unknown developer with no web presence, and permissions with no connection to PDF editing are significant red flags regardless of the rating. c. Yes, but only grant the PDF-related permissions and deny contacts, microphone and location. d. Yes, apps in official stores have been reviewed by Google and are guaranteed to be malware-free.
Q2. A user installs a grammar checking browser extension to help with their writing. The extension has permission to 'read and change all data on websites you visit'. The user then uses the same browser to log into their online banking. What is the security implication? e. There is no security implication, browser extensions cannot access banking websites. f. The grammar checking extension can read everything on the banking page, including account numbers and any content the user types, if the extension is compromised or malicious, this data could be exfiltrated. g. The extension can only read text the user has selected and asked it to check. h. The banking site's HTTPS encryption prevents the extension from reading the page content.
Q3. You have been using a shopping discount extension in your browser for two years. You notice that after a recent update, it now requests permission to 'read your browsing history'. Previously it did not have this permission. What is the most appropriate response? i. Accept the new permission, the extension has been trustworthy for two years and the developer probably needs this to improve the service. j. Treat the unexpected permission change as suspicious. Research whether the extension has been sold or compromised. If you cannot verify the change is legitimate, remove the extension. k. Accept the new permission only if you can verify the update came from the original developer. l. Report the extension to the browser store and wait for an official response before deciding.
Q4. A colleague says: 'I use "Login with Google" for all my accounts so I only have one password to remember.' What is the most accurate security assessment of this approach? m. This is an excellent approach, Google's security is stronger than individual site passwords. n. This approach has a significant concentration risk: if the Google account is compromised, every service linked to it is also compromised. It should always be combined with strong MFA on the Google account. o. This is risky because Google can see which services the user logs into. p. This approach is no different from using a password manager.

Part 4: When Things Go Wrong

Module 15: Spotting and Reporting Incidents

Your Early Warning Role

1. The Earlier You Spot It, the Less It Costs

Security incidents are not like most problems that improve with time. They get worse. An attacker with access to a system on Monday is doing more damage by Friday than they were on Monday. Ransomware that has been quietly mapping a network for three weeks before encrypting files causes far more damage than ransomware caught in its first hours. A data breach discovered and contained within 24 hours causes less harm legally, reputationally, and practically than one discovered three months later.

The people most likely to notice the first signs of an incident are not always the security team. They are the people closest to the work: the staff member who notices their account has been accessing files they did not open, the receptionist who spots an unusual visitor asking technical questions, the developer who sees unexpected network traffic, the administrator who receives an alert they almost dismissed. You are on the front line of early detection whether you have a security job title or not.

This module is about giving you the knowledge and confidence to act on what you notice. Not to investigate, not to fix it yourself but to recognize the signs and report them fast, with the information that matters.

2. What Counts as a Security Incident?

A security incident is any event that has compromised, or could compromise, the confidentiality, integrity, or availability of information or systems. That definition is broad by design the CIA triad from Module 2 reappears here as the test for whether something is reportable.

People commonly under-report incidents for two reasons: they are not sure something ‘counts’, or they think it was minor enough not to matter. Both of these instincts are usually wrong. Here is a clear taxonomy of what constitutes a reportable incident.

Type of Incident	Examples	Why it Needs Reporting Even if it Seems Minor
Account compromise	Unexpected login alerts, password reset emails you didn't request, activity in your account you don't recognize, contacts saying you sent them strange messages.	A compromised account is a live entry point. Every minute it remains active the attacker can access more systems, send phishing from your identity, or escalate privileges.
Phishing click or credential entry	You clicked a link in a suspicious email, you opened an attachment that behaved oddly, you entered credentials on a site that you now suspect was fake.	Even if nothing obvious has happened yet, the attacker may have your credentials or malware may have been delivered. Early response limits the damage.
Lost or stolen device	A work laptop left on a train, a phone stolen from a bag, a USB drive containing work files lost.	The device may contain unencrypted data, saved credentials, or access to corporate systems. Remote wipe must happen as fast as possible.
Suspicious system behavior	Unexplained slowdowns, programs crashing repeatedly, files that have been moved or changed without explanation, unexpected network activity, antivirus alerts	These can be signs of malware running in the background. Investigating early is far cheaper than discovering ransomware has been deploying for three weeks.
Accidental data disclosure	Sending an email with personal data to the wrong recipient, accidentally sharing a confidential file publicly, a colleague seeing data they should not have	Under GDPR, personal data breaches must be assessed and potentially reported to the regulator within 72 hours. Delay makes compliance harder and harm greater.
Unusual access or activity	A colleague's account accessing files it normally would not, large file downloads at unusual times, login from an unexpected location, new admin accounts appearing	Could be a compromised account, an insider incident, or early-stage ransomware reconnaissance. Early detection prevents escalation.

Uncertainty is not a reason to delay reporting

The single most important principle in incident reporting is this: you do not need to be certain that an incident has occurred before you report it. 'I think I may have clicked something I shouldn't have' is a valid report. 'I'm not sure, but my account seems to be behaving oddly' is a valid report. The job of the security team is to investigate and

determine whether something happened. Your job is to give them the information they need to do that, as early as possible.

3. Warning Signs: What to Watch For

Most incidents are invisible at first. But many leave traces that a watchful person can spot. The following warning signs are worth knowing, not so that you become paranoid, but so that when something unusual happens, you have a framework for deciding whether it is worth reporting.

Warning Sign	What it Might Indicate	What to Do
You cannot log in with your usual credentials	Your password may have been changed by an attacker who has already taken over the account.	Use account recovery immediately. Report to IT or security if a work account. Check your email for recent password reset or login activity notifications.
You receive MFA codes you did not request	Someone has your password and is attempting to log in to your account right now	Do not approve any push notifications. Change your password immediately using a different device. Report to IT if a work account.
Your contacts report receiving odd messages from you	Your account has been taken over and is being used to send phishing or scam messages to your contacts.	Treat as full account compromise. Change password, enable MFA, check for unauthorized activity, warn your contacts not to act on messages received.
Files have been renamed with a strange extension	Ransomware is encrypting your files. This is one of the earliest visible signs.	Disconnect from the network immediately, do not shut down. Report to IT urgently. Do not attempt to decrypt yourself.
Your device is running much slower than usual	Possible malware activity, cryptocurrency mining, or background data exfiltration.	Run an antivirus scan. If the slowdown is severe or accompanied by other signs, report to IT rather than trying to diagnose yourself.
You see an unfamiliar charge on your card or bank statement	Payment credentials may have been stolen through a phishing attack, a compromised merchant, or card skimming.	Contact your bank immediately. Report the charge as fraudulent. Check whether any other accounts linked to the same payment method show unusual activity.

The instinct worth trusting

Security professionals consistently report that in retrospect, someone in the affected organization noticed something odd before the incident was formally discovered, and said nothing, assuming it was not their place to raise it or that they were probably mistaken. Trust your instinct. If something seems wrong, the cost of being wrong and reporting it is a short conversation. The cost of being right and staying silent can be catastrophic.

4. What NOT to Do: The Mistakes That Make Things Worse

When people suspect something has gone wrong, the instinctive responses are often exactly the wrong ones. Understanding why helps you resist the impulse.

What People Often Do	Why it Makes Things Worse	What to Do Instead
Wait to see if it resolves itself	Attackers move fast. Every hour of delay gives them more time to exfiltrate data, spread to other systems, or establish persistence that survives password changes.	Report immediately, even if you are not certain something bad has happened. False alarms are far less costly than late responses.
Stay silent out of embarrassment	Security incidents happen to careful, experienced people constantly. Silence guarantees the harm grows. Speaking up gives the organization a chance to contain it.	Report to your manager, IT team, or security contact. Frame it factually: 'I think I may have clicked something I shouldn't have' is enough.
Try to fix it yourself without telling anyone	You may inadvertently destroy forensic evidence, alert the attacker that they have been detected (causing them to accelerate), or miss the full scope of the compromise.	Preserve everything. Do not delete files, do not clear logs, do not reinstall the operating system. Report first, let the experts decide what to do.
Shut down the device immediately	For some malware (particularly ransomware in progress), shutting down can actually trigger full encryption of remaining files. Forensic evidence in RAM is also lost on shutdown.	Disconnect from the network (unplug the cable, disable Wi-Fi) rather than shutting down. This stops the spread without destroying evidence or triggering shutdown-triggered payloads.

What People Often Do	Why it Makes Things Worse	What to Do Instead
Pay a ransom without telling anyone	Payment should only happen after professional incident response advice. Paying without expertise may violate sanctions laws, fund criminal organizations, and provide no guarantee of recovery.	Contact your organization's IT team or an incident response professional before any decision about payment. Decisions made alone in a crisis are rarely good ones.

The disconnect-not-shutdown rule

This deserves emphasis because it contradicts instinct. When you see ransomware symptoms files being renamed, a ransom note appearing, your computer becoming unresponsive the natural reaction is to shut the computer down to stop it. Do not. Instead, physically disconnect the network cable or disable Wi-Fi. This isolates the machine from the network (stopping spread and C2 communication) without triggering shutdown-activated payloads and without destroying volatile memory evidence that forensic investigators may need. Then report immediately and do not touch the machine further.

5. How to Report: What to Include

An effective incident report does not need to be long or technically precise. It needs to give the responder enough information to understand what happened, when, and what has been done since. The following five elements are sufficient for an initial report:

- What happened (as best you can describe it): A factual description of what you observed. 'I received an email from what appeared to be our bank, clicked a link, and was taken to a login page where I entered my credentials before realizing the URL was wrong.'
- When it happened: The approximate time and date. If you are not sure, give a range. The timeline helps incident responders correlate your report with system logs.
- Which systems or accounts are involved: The specific device, account, system, or file that was affected or might have been. This tells responders where to look first.

- What you have done since: Have you changed your password? Disconnected from the network? Tried to remove a file? This affects what the responders need to do and what evidence may still be available.
- Who else knows about it: Have you told anyone else? This prevents parallel investigation efforts and helps establish whether the incident is broader than it initially appears.

> **If you have no formal incident reporting channel**
> In a small organization without a dedicated security team, report to your manager or the most senior person available.
> If personal accounts are involved (personal email, personal banking), report directly to the service provider's fraud or security team. Every major service has one.
> For GDPR-notifiable incidents (personal data breaches), the organization's Data Protection Officer or privacy contact must be informed.
> If criminal activity is suspected (ransomware, fraud, data theft for sale), law enforcement should be involved, your national CERT and local cybercrime unit are the right contacts.

6. The No-Blame Culture: Why It Matters

The single biggest barrier to early incident reporting is fear of blame. People who clicked a phishing link, lost a device, or accidentally disclosed data often stay silent because they are afraid of the consequences: disciplinary action, embarrassment, being seen as careless.

This silence is catastrophic from a security perspective. Every hour of unreported incident is an hour the attacker spends undetected. Organizations that punish people for reporting incidents get fewer reports, later. That is the worst possible outcome.

A no-blame culture does not mean there are no consequences for genuinely reckless behavior. It means that honest mistakes, promptly reported, are treated as learning opportunities rather than disciplinary events. It means people know they can say 'I think I made a mistake' without immediately fearing for their job. It means the security team is approachable, not intimidating.

If you are a manager reading this: the response you give to the first security incident reported to you sets the tone for every future report. A calm, practical, grateful response gets you more reports. An angry or punitive response gets you silence, and eventually, a much larger incident that went unreported for weeks.

ShieldNet thread going further

Incident detection and reporting maps to two ShieldNet controls. [RR2] (Detect and Escalate Incidents) requires organizations to establish clear criteria for what constitutes an incident, ensure all staff know how to report signs of a potential incident immediately, and set up an internal emergency contact method for rapid escalation. [LL1] (Train and Test Staff) includes awareness training that covers what to report and how, because people cannot report what they do not recognize. The no-blame culture principle is embedded in both: effective detection depends on people feeling safe enough to speak up.

Module 15: Summary

By the end of this module, you should be able to:

- ✓ Define what a security incident is and give three examples that are often under-reported.
- ✓ Explain why early reporting matters more than certainty about what has happened.
- ✓ Describe five warning signs that suggest a security incident may be in progress.
- ✓ Explain why you should disconnect a device from the network rather than shut it down during a suspected ransomware attack.
- ✓ Describe what a no-blame reporting culture means and why it matters for organizational security.
- ✓ State the single most important action when you suspect an incident has occurred.

Module 16: Backups and Recovery

Why 'It's Saved' Is Never Enough

1. The Backup That Was Not There When It Was Needed

In May 2021, Ireland's national health service, the HSE, was hit by a ransomware attack that encrypted approximately 80,000 devices. The attack effectively shut down the entire national health IT infrastructure. Appointments were canceled, patient records were inaccessible, diagnostic equipment could not be used. It took months to fully recover and cost an estimated €600 million.

Backups existed. They were insufficient. Some were on systems the attacker had already reached. Some had never been tested. Some covered individual servers but not the whole environment. The gap between 'we have backups' and 'we can recover from this' turned out to be enormous.

This is the gap this module is about. A backup is not a recovery. A backup is a potential recovery, conditional on whether it was taken recently enough, whether it actually captured the right data, whether it is stored somewhere the attacker could not reach, and whether anyone has verified that restoration actually works. This module walks through every point where that chain can break, and what to do about each one.

2. The 3-2-1 Rule

The 3-2-1 rule was introduced in Module 5 in the context of ransomware. It is worth examining in more detail here because it is the single most reliable framework for backup resilience, and because each element addresses a different failure mode.

The 3-2-1 rule in full

3: Keep at least three copies of your data. The original plus two backups. This protects against any single copy failing, becoming corrupted, or being unavailable.

2: Store copies on at least two different types of media or in two different locations. Internal hard drive plus external drive. Local server plus cloud. This protects against a single failure mode (a drive type failing, a location being physically destroyed) taking out all copies simultaneously.

1: Keep at least one copy completely offline or in an immutable, air-gapped location. A disconnected external drive. A cloud service with immutable versioning. Tape stored offsite. This is the copy that survives ransomware, ransomware cannot encrypt what it cannot reach.

The '1' is the most important and most commonly missing element. Most organizations that think they are following 3-2-1 have three copies in three locations, all of them reachable from the network. That is not 3-2-1. That is three copies of the same vulnerability.

3. How Backups Fail: Six Ways to Lose Your Safety Net

Understanding how backups fail is more useful than a checklist of what to do, because the failures are specific and each has a specific prevention.

How The Backup Fails	Why it Happens	How To Avoid it
The backup was stored on the same network as the primary data	Ransomware reaches and encrypts all connected storage simultaneously. A network drive, a USB drive left plugged in, and a cloud folder that auto-syncs are all reachable.	Follow the 3-2-1 rule: at least one copy must be offline or air-gapped. Disconnected external drives, cloud services with immutable versioning, or tape stored offsite all qualify.
The backup was never tested	Nobody verified that the backup process actually worked. Misconfigured backup jobs, full storage, corrupted archives, or failed transfers mean nothing was actually saved	Test restoration regularly. Restore an actual file from backup at least once every three months. Test a full system restoration annually if critical systems are backed up.
The backup was too old	The last successful backup was weeks or months ago. Everything created or changed since is gone.	Define a Recovery Point Objective (RPO): the maximum acceptable data loss. Set backup frequency to match. Most organizations need at least daily backups of critical data.
The backup was encrypted by the attacker before it could be used	Sophisticated attackers specifically target and delete or encrypt backup systems before triggering ransomware. This is the preparation stage described in Module 5.	Immutable backups, where data cannot be modified or deleted once written, are the defense. Most cloud providers offer versioned, immutable storage options.
The restored backup contained the malware	If the attacker was present for weeks before encryption, the malware may be embedded in backups taken during that period.	Understand how long the attacker may have been in the system before restoring. Work with incident response professionals to identify a clean restore point.

How The Backup Fails	Why it Happens	How To Avoid it
The backup existed but nobody knew how to restore it	Restoration procedures were never documented. The person who set up the backup has left. The restore process requires software that is no longer installed.	Document restoration procedures step by step. Verify at least annually that the procedures still work with current tools and that more than one person knows how to execute them.

Immutable backups: the ransomware-proof option

An immutable backup is one that, once written, cannot be modified or deleted not even by an administrator. Most major cloud storage providers offer 'object lock' or 'versioned backup' features that provide immutability. A ransomware attacker who reaches your cloud backup storage cannot encrypt or delete immutable copies, because the storage system physically prevents modification. For organizations serious about ransomware resilience, immutable cloud backups are the current gold standard.

4. Types of Backup: Matching the Approach to the Need

Different backup types suit different needs. Understanding the trade-offs helps you or your organization choose the right approach for each system or dataset.

Backup Type	What it Captures	Pros	Cons
Full backup	A complete copy of all selected data at that point in time	Simple to restore, everything is in one place. Easy to verify.	Takes longer and uses more storage than other types. Impractical to run hourly.
Incremental backup	Only data that has changed since the last backup of any kind	Fast and storage-efficient. Can run frequently (hourly) without significant overhead.	Restoration requires the last full backup plus every incremental since. More complex and slower to restore.
Differential backup	All data that has changed since the last full backup	Faster than full, simpler to restore than incremental, only need the last full plus the latest differential.	Grows in size over time until the next full backup is taken.

Backup Type	What it Captures	Pros	Cons
Cloud backup (continuous / versioned)	Near-continuous capture of file changes with version history retained	Frequent recovery points. Accessible from anywhere. Managed by the provider. Immutable versioning available on most platforms.	Requires internet access for restoration. Storage costs scale with data volume. Provider trust is required.
Snapshot	A point-in-time image of a system or virtual machine state	Very fast to take and restore. Good for systems that must recover quickly.	Typically stored on the same infrastructure as the primary system, vulnerable to the same ransomware unless replicated offsite.

In practice, most organizations use a combination: full backups weekly, incremental or differential backups daily, and continuous cloud backup for the most critical data. The approach is chosen based on how much data can be lost (RPO) and how quickly systems must be restored (RTO), which are covered in the next section.

5. RPO and RTO: Knowing What You're Protecting

Two questions define what 'adequate' backup and recovery looks like for any system. Every organization should answer them for each critical system before an incident occurs, not during one.

Concept	Plain English Definition	Example
Recovery Point Objective (RPO)	The maximum amount of data loss you can tolerate, expressed as time. How old can your most recent backup be and still be acceptable?	An e-commerce company processes thousands of orders per hour. Losing more than 15 minutes of order data is unacceptable. RPO = 15 minutes. Backups must run at least every 15 minutes.
Recovery Time Objective (RTO)	The maximum amount of time you can tolerate being without a system or service. How long can you be down before it becomes a crisis?	A hospital cannot operate its patient management system for more than 2 hours before patient safety is at risk. RTO = 2 hours. Recovery processes must restore the system within 2 hours.

Concept	Plain English Definition	Example
The gap between RPO/RTO and reality	Most organizations define RPO and RTO aspirationally but never test whether their backup and recovery processes actually meet them.	A company states RTO = 4 hours but has never done a full restore test. In practice, restoration takes 18 hours. The gap between stated and actual RTO is only discovered during a real incident.

Test your RTO before you need it

The most common finding in post-incident reviews is that the stated Recovery Time Objective bore no relationship to the actual time needed to restore. This gap exists because RTOs are set aspirational and tested rarely or never. A simple test: choose one critical system, simulate a failure, and time how long it takes to restore from backup. The number you get is your real RTO. If it is longer than your business can tolerate, that is a gap to fix before the attacker finds it for you.

6. Personal Backups: The 3-2-1 Rule at Home

The principles that apply to organizational backups apply equally to your personal data. Losing years of photos, documents, and files because a hard drive failed or ransomware hit your home computer is not a theoretical risk.

What to back up personally

- Photos and videos: irreplaceable and often the most valuable personal data.
- Documents: tax records, contracts, insurance documents, creative work.
- Password manager data: your password manager likely has its own backup and export mechanism, use it.
- Device configuration: apps, settings, and content on your phone can be restored from an iCloud or Google account backup.

A practical personal 3-2-1 setup

- Copy 1: your primary device (laptop or phone).
- Copy 2: an automatic cloud backup service, iCloud, Google Photos, OneDrive, or Backblaze for computers. These run continuously in the background with no action required.

- Copy 3: a periodic backup to an external hard drive that you disconnect and store safely. Monthly is sufficient for most personal data. This is your offline copy.

The cloud sync trap

Cloud sync (Dropbox, Google Drive, iCloud Drive) is not a backup. When ransomware encrypts your local files, cloud sync uploads the encrypted versions and overwrites the originals in the cloud. You now have three copies of encrypted, useless files. A true cloud backup service keeps versioned history that allows you to restore to a point before the encryption. Check that your cloud service offers version history and know how to access it before you need it.

7. Business Continuity: Keeping Operating When Systems Are Down

Recovery from a backup restores your data. Business continuity is broader: it is about how your organization keeps functioning during the period between an incident occurring and full systems being restored. For complex incidents, that period can be days or weeks.

Concept	Plain English Definition	Why it Matters
Business continuity plan (BCP)	A documented plan for how the organization will continue critical operations during and after a disruption, even if normal systems are unavailable	Without a plan, every decision gets made in chaos under pressure. A plan made in advance, even a basic one, significantly reduces response time and decision quality.
Critical processes	The specific functions that, if unavailable, would cause the most harm. Not all processes are equally critical.	Organizations that try to protect everything equally protect nothing well. Identifying the top 5–10 critical processes focuses recovery effort where it matters most.
Manual workarounds	Alternative ways of performing critical functions without the normal digital systems.	A hospital that can switch to paper-based patient tracking during a system outage keeps operating. One that has no manual process stops completely.
Communication plan	A pre-established list of who needs to be contacted during an incident, how to reach them when normal communication systems may be affected, and what to tell them	During a cyberattack, email and phone systems may be compromised or unavailable. Knowing in advance how to contact

Concept	Plain English Definition	Why it Matters
		key people without relying on those systems is essential.

Even a basic business continuity plan, a single document that lists your five most critical processes, how you would perform each manually if systems were unavailable, who to call when normal communication is down, and where your offline backup copies are, is enormously valuable in a crisis. The value of that document is entirely in it being written before the crisis, not during it.

ShieldNet thread going further

Backups and business continuity map to two ShieldNet controls. [KP6] (Plan for Continuity) requires organizations to develop a basic business continuity and disaster recovery plan covering data backups, restoration procedures, and who does what in a crisis, exactly the content of this module. [RR4] (Recover Systems) covers the response side: restoring operations from backups, verifying systems are clean before reconnecting them to the network, and returning to normal operations in a controlled sequence. Template A-13 (BC/DR Test Log) in Annex A records the testing that proves these processes actually work.

Module 16: Summary

By the end of this module, you should be able to:

- ✓ Explain the 3-2-1 backup rule and describe what qualifies as the 'offline' copy.
- ✓ Name three ways a backup can fail when you need it most, and describe one action that prevents each.
- ✓ Define Recovery Point Objective (RPO) and Recovery Time Objective (RTO) in plain language.
- ✓ Explain why testing backups is as important as taking them.
- ✓ Describe what 'immutable backups' means and why they are important for ransomware protection.
- ✓ Explain what a business continuity plan is and why even a basic one is better than none.

Module 17: Data Breaches

What Happens, What It Means, What You Do

1. A Breach Is Not the End

In September 2017, Equifax, one of the largest credit reporting agencies in the world, disclosed that the personal data of approximately 147 million people had been stolen. Names, dates of birth, Social Security numbers, addresses, and in some cases driver's license details. The breach had gone undetected for 78 days. The root cause was an unpatched vulnerability in a software component that a publicly available fix had been available for two months.

The damage was vast: hundreds of millions of dollars in fines and settlements, the resignation of the CEO and CISO, and lasting harm to the individuals whose most sensitive identity data was now in criminal hands. But Equifax survived. Most organizations that suffer breaches do survive, if they respond properly. The organizations that do not survive are typically those that compounded the original breach with a botched response: concealment, delay, inadequate communication, and failure to notify as required by law.

This module is about understanding what a data breach actually is, what organizations are legally obligated to do when one happens, and what you should do as an individual, whether you are the person whose data was breached, or the person at the organization who needs to respond.

2. What a Personal Data Breach Is

Under GDPR, a personal data breach is defined as a security incident that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data. The definition maps directly to the CIA triad introduced in Module 2.

Type of Breach	What Happened	Typical Harm caused
Confidentiality breach	Personal data was accessed or disclosed to someone who should not have it, through a hack, an accidental email, misconfigured access controls, or insider misuse	Identity theft, fraud, embarrassment, discrimination, physical danger (e.g. exposure of a domestic abuse victim's address)

Type of Breach	What Happened	Typical Harm caused
Integrity breach	Personal data was altered without authorization, medical records changed, financial details modified, identity falsified	Harm from decisions made on wrong information: wrong medical treatment, incorrect credit scoring, false criminal records
Availability breach	Personal data was lost or made temporarily unavailable, ransomware encrypting patient records, a device lost containing the only copy of data	Inability to deliver services, delayed medical treatment, loss of business records, legal non-compliance

Most breaches are not dramatic hacks

Media coverage of breaches focuses on sophisticated attacks against large organizations. In practice, the majority of personal data breaches reported to supervisory authorities involve far less dramatic causes: emails sent to the wrong recipient, documents left in public places, files accidentally made publicly accessible through misconfigured cloud storage, laptops lost on public transport, or staff accessing data they should not have. The legal obligations apply regardless of how the breach happened.

3. What Organizations Must Do: The GDPR Obligations

When a personal data breach occurs, GDPR places specific obligations on the organization. These are not optional and apply to all organizations that process personal data of EU or UK residents, regardless of size.

Obligation	What GDPR Requires	The Consequences of Failing
Notify the supervisory authority	When a breach is likely to result in a risk to individuals' rights and freedoms, the organization must notify its national data protection authority (e.g. CNIL in France, UODO in Poland) within 72 hours of becoming aware of the breach.	Fines of up to €10 million or 2% of global annual turnover for procedural violations. Late notification is itself a separate violation.
Notify affected individuals	When the breach is likely to result in a HIGH risk to individuals' rights and freedoms, the organization must also notify the affected people 'without undue delay'. The notification must explain what	Failure to notify individuals when required is a separate GDPR violation. Individuals who suffer harm from a breach they were not told about may have grounds for compensation claims.

Obligation	What GDPR Requires	The Consequences of Failing
	happened, what data was involved, likely consequences, and what measures are being taken.	
Document all breaches	ALL personal data breaches must be documented internally, regardless of whether they meet the threshold for notification. The documentation must include facts, effects, and remedial action taken.	The documentation requirement applies even to breaches that do not need to be reported externally. Failure to maintain records is a compliance failure and leaves the organization unable to demonstrate proportionate response.
Assess risk and act proportionately	Not every breach requires external notification. The 72-hour clock starts from when the organization becomes aware, and the obligation to notify depends on a risk assessment. Organizations must be able to show they assessed the breach and made a reasoned decision.	Organizations that routinely over-notify (reporting trivial incidents) or under-notify (failing to report significant ones) both face scrutiny. The assessment must be documented and defensible.

The 72-hour clock: what it really means

The 72-hour notification window starts from when the organization becomes 'aware' of the breach, not from when the breach occurred. This distinction matters enormously.

If a breach occurred three months ago but was only discovered today, the 72-hour clock starts today.

If the breach is discovered on a Friday afternoon, the 72 hours run through the weekend. There is no weekend exemption.

If the organization cannot complete the notification within 72 hours, it can send a provisional notification explaining that the investigation is ongoing. Waiting for complete information before notifying at all is not acceptable.

Organizations that discover a breach and then spend time deciding whether they have to notify are already using up their notification window. The risk assessment and notification preparation must happen simultaneously.

4. The Breach Response Timeline

What should happen in the hours and days after a breach is discovered follows a clear sequence. The exact actions depend on the scale and nature of the breach, but the structure is consistent.

Hours	What Should Be Happening	Legal Obligations	Common Mistakes
0 to 24	Detect and contain: disconnect affected systems, preserve evidence, convene incident response team, begin assessment	72-hour clock starts from the moment the organization becomes 'aware' of the breach	Destroying evidence. Concealing the breach. Not escalating fast enough. Trying to fix without assessing first.
24 to 48	Assess scope: what data was involved, how many people affected, what risk does this create for individuals?	If the breach meets the threshold (risk to individuals' rights and freedoms), notification to the supervisory authority must be prepared	Under-assessing the scope. Assuming breach is smaller than it is before investigation is complete.
48 to 72	Notify supervisory authority if required. Continue remediation. Begin drafting individual notifications if high risk confirmed.	Supervisory authority must be notified within 72 hours. The notification can be provisional if full information is not yet available, do not delay to wait for complete information.	Missing the 72-hour deadline by waiting for the full picture. The initial notification can say 'investigation ongoing'.
72h+	Notify affected individuals without undue delay if high-risk breach confirmed. Continue remediation. Document everything.	Individual notification must follow 'without undue delay' for high-risk breaches. Document all breach decisions and actions.	Underestimating what constitutes a high-risk breach for individuals. Poor communication that causes panic or insufficient guidance.

What a breach notification to individuals must contain

When an organization notifies affected individuals, the communication must include:
A clear description of what happened (in plain language, not legal or technical jargon).
What categories of data were involved and approximately how many individuals affected.
The likely consequences of the breach for individuals.
The measures the organization has taken or proposes to take to address the breach.
Contact details for a named person or team where individuals can ask questions.

Specific advice on what individuals should do to protect themselves (change passwords, monitor accounts, etc.).

5. What You Should Do as an Individual

Being told your personal data has been breached is unsettling. The right response depends on what type of data was involved and what risk it creates. The table below gives specific guidance for the most common scenarios.

Situation	Immediate Actions	Longer-Term Actions
You receive a breach notification from a service	Read it carefully to understand what data was exposed. Change your password for that service immediately, even if not asked to. Enable MFA if not already active.	Check whether you use the same password on other services (credential stuffing risk from Module 6). Monitor for unusual activity in any account that could be affected. Report any fraud to your bank or relevant service.
Your financial data was involved	Contact your bank immediately. Ask them to monitor your account for unusual activity and, if payment card details were exposed, consider requesting a new card.	Check your credit report for any new credit applications you did not make. Consider placing a credit freeze with credit reference agencies if identity theft is suspected.
Your login credentials were exposed	Change the password on the affected service immediately. Change it on every other service where you used the same password (this is why a password manager matters).	Use haveibeenpwned.com to check whether your email appears in other known breaches. Enable MFA on the affected account and on your email as a priority.
Sensitive personal data was exposed (health, ID, address)	Assess the specific harm. For health data: limited immediate action but be alert to insurance fraud or blackmail attempts. For address/ID: be alert to identity theft and physical security if the exposure was targeted.	Consider whether to report to the police if the exposure was deliberate. Contact the information commissioner in your country if you believe the organization's response was inadequate. Seek legal advice if you suffered material harm.
You discover your organization has suffered a breach	Report to your information security team or manager immediately. Preserve all evidence. Do not attempt to fix or conceal the breach.	Support the GDPR assessment and notification process. Cooperate with any external investigation. Review

Situation	Immediate Actions	Longer-Term Actions
	Activate the incident response process from Module 15.	and update controls to prevent recurrence.

Check haveibeenpwned.com proactively

You do not have to wait to be notified of a breach. The website haveibeenpwned.com aggregates data from hundreds of known breaches and lets you enter your email address to see whether it has appeared in any of them. It is free, legitimate, and operated by a well-known security researcher. Set up the notification feature so you are alerted automatically if your email appears in a future breach. This is one of the most practical personal security tools available.

6. If You Think an Organization Has Failed in Its Response

Organizations do not always handle breach notifications well. They may notify too late, provide inadequate information, downplay the severity, or fail to notify at all. As an individual whose data was involved, you have recourse.

Make a complaint to the supervisory authority

Every EU member state has a national data protection supervisory authority. In Poland it is UODO (Urząd Ochrony Danych Osobowych). You can make a complaint to the supervisory authority if you believe an organization has not met its GDPR obligations, including its breach notification duties. The authority has the power to investigate and, where warranted, impose fines.

Seek compensation

Under GDPR Article 82, individuals who have suffered material or non-material damage as a result of a GDPR breach have the right to claim compensation from the responsible organization. Non-material damage includes distress, anxiety, and loss of control over personal data, not just direct financial loss. Class actions on behalf of large groups of affected individuals have become increasingly common in the UK and EU.

Exercise your GDPR rights

Following a breach, you may wish to exercise your right of access (to understand what data was involved), your right to erasure (if the data is no longer needed), or your right

to rectification (if the breach revealed that inaccurate data was held). These rights were covered in Module 13.

7. How Breaches Connect to Everything Else in This Course

A data breach is not an isolated event. It is the outcome when one or more of the defenses covered in Parts 2 and 3 failed. Working backwards through a breach scenario reveals exactly which controls were absent:

- The breach happened because of a phishing attack - Module 4 (recognizing and reporting phishing).
- The breach happened because of an unpatched vulnerability - Module 11 (keeping devices and software updated).
- The breach happened because credentials were reused and credential stuffing succeeded - Module 6 (passwords and MFA).
- The breach was worse because the attacker had access to more data than they needed - Modules 10 and 13 (access control and data minimization).
- The breach was worse because it went undetected for months - Module 15 (spotting and reporting incidents).
- The recovery was slower than it needed to be because backups were not tested - Module 16 (backups and recovery).

Every module in this course addresses a specific point in the chain that leads to, amplifies, or prolongs a breach. A breach is not bad luck. It is the result of a specific combination of things that went wrong, and most of those things have specific, learnable countermeasures.

ShieldNet thread going further

Breach notification maps directly to ShieldNet controls [RR5] (Notify Regulators) and [RR6] (Inform Affected Users). [RR5] requires notifying the relevant supervisory authority and other regulators within the timeframes set by law, the 72-hour GDPR window and the 24-hour initial notice for significant incidents under NIS2. [RR6] requires informing affected customers or individuals without undue delay when a breach creates a high risk for them, with specific guidance on what the notification must contain. Together these controls operationalize exactly the obligations described in this module.

Module 17: Summary

By the end of this module, you should be able to:

- ✓ Define a personal data breach and explain the three types using the CIA triad.
- ✓ State the two GDPR notification obligations and the key thresholds and timelines for each.
- ✓ Describe five steps an individual should take when they receive a breach notification affecting their credentials.
- ✓ Explain why the 72-hour notification clock starts when the organization 'becomes aware', not when the breach occurred.
- ✓ Describe what an individual can do if they believe an organization's breach response was inadequate.
- ✓ Explain why documenting a breach matters even for incidents below the notification threshold.

Completing Part 4

Part 4 is complete. You now have a practical toolkit for responding when incidents occur:

Module 15: Spotting and reporting incidents, recognizing warning signs and the no-blame reporting culture.

Module 16: Backups and recovery, the 3-2-1 rule, why backups fail, RPO/RTO, and business continuity.

Module 17: Data breaches, what they are, what organizations must do, and what individuals should do.

Part 4 Knowledge Check

Module 15 Practice Questions
Q1. A staff member accidentally sends an email containing a customer's name, address, and purchase history to the wrong recipient. The recipient replies immediately saying they have deleted it. The staff member decides not to report it because 'no harm was done'. What is wrong with this decision? a. Nothing, if the recipient confirmed deletion, the incident is resolved. b. The staff member should have checked with IT before deciding not to report. c. Under GDPR, accidental disclosure of personal data is a notifiable personal data breach that must be assessed and potentially reported to the data protection authority within 72 hours. The organization cannot make that assessment if it is not told about the incident. d. The staff member should have reported it only if the email contained sensitive financial data.
Q2. A user notices their files are being renamed with a '.locked' extension. They recognize this as a ransomware sign. They are about to shut down their computer to stop the encryption. What should they do instead, and why? e. Shut down immediately, turning off the computer stops all processes including the encryption. f. Disconnect the computer from the network without shutting it down. This stops the malware from spreading to other systems and communicating with the attacker's server, while preserving forensic evidence in memory and avoiding potential shutdown-triggered payloads. g. Run an antivirus scan to remove the ransomware before it can encrypt more files. h. Save all open files and then shut down to prevent further damage.
Q3. An employee clicked a link in what they now believe was a phishing email three days ago but did not report it because nothing seemed to happen. They have now been asked to complete security awareness training about phishing. During the training, they realize what they did. What should they do? i. Nothing, if nothing happened in three days, the click was probably harmless. j. Report it to IT immediately, even though three days have passed. The attacker may have been in the system for three days undetected. Early action now is still better than continued inaction. k. Complete the training and treat it as a learning experience without reporting the past incident. l. Only report it if they notice something suspicious happening on their computer.
Q4. A manager is told by a team member that they think they may have introduced a security incident. The manager responds: 'You should have been more careful, do you know how much this could cost?' What is the problem with this response from a security perspective? m. The response is appropriate, staff need to understand the consequences of security mistakes. n. The response creates a culture where staff are afraid to report incidents. Future incidents will be hidden to avoid blame, leading to slower detection, greater harm, and worse outcomes for the organization.

Module 15 Practice Questions
o. The response should have focused on the technical aspects of the incident rather than the human error. p. The response is only problematic if the manager was not aware of the organization's security policies.

Module 16 Practice Questions
Q1. A company backs up all its files nightly to a dedicated backup server on the same local network. Ransomware attacks the primary server, spreads across the network, and encrypts both the primary files and the backup server. Which element of the 3-2-1 rule was not followed? a. The '3' element: the company only had two copies of the data. b. The '2' element: both copies were on the same type of media. c. The '1' element: there was no offline or air-gapped copy inaccessible from the main network. d. The backup frequency was insufficient: backups should run hourly, not nightly.
Q2. A small business owner says 'we back up to the cloud every night, so we're covered if ransomware hits.' What is the most important follow-up question to ask? e. 'Which cloud provider do you use?' f. 'Have you ever actually restored a file from that backup, and did it work?' g. 'Do you also have a local backup in addition to the cloud?' h. 'Is the backup encrypted?'.
Q3. An organization's Recovery Time Objective for its main customer database is 4 hours. During a ransomware incident, the IT team begins restoration and discovers it will take 14 hours. What does this gap reveal? i. The organization should have had a shorter RPO. j. The backup process was misconfigured and captured incomplete data. k. The stated RTO was aspirational but was never tested against the actual restoration process. The real recovery capability does not match the documented objective. l. The organization needs to invest in faster backup hardware.
Q4. During a ransomware investigation, forensic analysts determine that the attacker had been inside the network for 22 days before triggering encryption. The organization's most recent backup was taken 5 days ago. Why is this backup potentially unsafe to restore from? m. The backup is too old: too much data has been lost. n. The backup may contain the malware or attacker's tools, since the attacker was present for 17 days before that backup was taken. Restoring from it could re-introduce the attacker into the environment. o. Ransomware always encrypts backups before triggering, so this backup is likely already encrypted. p. The backup was taken after the attacker arrived, so it contains data modifications the attacker made.

Module 17 Practice Questions
Q1. A company discovers on Tuesday morning that its customer database was accessed by an unauthorized third party at some point over the previous weekend. The database contains names, email addresses, and hashed passwords. When does the 72-hour GDPR notification clock start? a. From the moment the breach actually occurred, sometime over the weekend. b. From Tuesday morning, when the company became aware of the breach. c. From the moment a formal investigation is launched and confirms that a breach occurred. d. There is no 72-hour requirement for breaches involving only hashed passwords.
Q2. A healthcare provider suffers a breach in which patient medical records, including diagnoses, medications, and home addresses, are accessed by an unauthorized person. Under GDPR, which combination of notification obligations applies? e. Document the breach internally only, health data is protected by medical confidentiality, not GDPR. f. Notify the supervisory authority within 72 hours AND notify the affected patients, because this involves special category data with high risk of harm to individuals. g. Notify the supervisory authority only, individual notification is only required for financial data breaches. h. No notification is required unless the data has already been misused.
Q3. You receive an email from a shopping website telling you that a security incident may have exposed your name, email address, and the password you used when you registered. You use the same password on your email account and two other shopping sites. What is the most important first action? i. Reply to the notification email asking for more details about exactly what was exposed. j. Change the password on the affected shopping site only, the breach was limited to that site. k. Change your password on the affected site AND on every other account where you used the same password, starting with your email account, because a stolen password can be used for credential stuffing on any site where it was reused. l. Wait to see whether you notice any suspicious activity before taking action.
Q4. An employee accidentally sends a spreadsheet containing the names, salaries, and home addresses of all 85 employees to the entire company instead of just to the HR team. The email is recalled within minutes and all but three recipients confirm they have deleted it. The organization decides not to document the incident because 'it was resolved quickly'. What is wrong with this decision? m. Nothing, if the email was recalled and most recipients deleted it, the breach was effectively contained. n. The organization should have notified the employees whose data was disclosed. o. GDPR requires all personal data breaches to be documented internally, regardless of severity or outcome. Failure to document is itself a compliance violation, and undocumented incidents cannot demonstrate proportionate response to regulators. p. The organization should have notified the supervisory authority within 72 hours.

Part 5: Security as a Mindset

Module 18: Safe Digital Habits

The Small Things That Make a Big Difference

1. Knowledge Without Habits Is Just Trivia

You have now covered seventeen modules of cybersecurity knowledge. You understand how phishing works, why ransomware is so damaging, what MFA does, how encryption protects data in transit and at rest, what GDPR requires when a breach occurs, and dozens of other concepts that most people never think about carefully.

None of it matters if you do not act on it.

Security is not an exam you pass once and forget. It is a set of practices that compound over time. A person who pauses before clicking every link, uses a password manager, locks their screen when they step away, and reports suspicious activity promptly is dramatically more secure than a person with extensive theoretical knowledge who does none of those things. Habits are the difference between knowing and being.

This module is about making the transition from knowing to doing. It introduces the small, consistent behaviors that, practiced daily, make security a natural part of how you work and live rather than an extra burden on top of everything else.

2. The Seatbelt Analogy

Forty years ago, wearing a seatbelt was optional, unusual, and seen by many as inconvenient or unnecessary. Today, it is automatic for most people. You get in the car, you put on the seatbelt, you do not think about it. The habit has become so embedded that the absence of it, getting in a car without buckling up, now feels wrong.

Security habits follow the same arc. The first few weeks of locking your screen every time you step away feels deliberate and slightly effortful. After two months, doing it without thinking feels normal. Not doing it starts to feel odd. The habit has been installed.

The goal of this module is not to tell you to try harder. It is to identify the specific habits that have the highest return, explain exactly what they look like in practice, and give you enough context to understand why they matter so that the motivation to maintain them is internal rather than imposed. Habits built on understanding are more durable than habits built on rules.

3. Six Core Daily Habits

The following six habits, applied consistently, address the most common attack vectors and provide the most significant reduction in personal and professional risk for the least effort. They are not a complete security program, that is what the rest of this course is for. They are the baseline that everything else builds on.

Habit	What it Looks Like in Practice	What it Protects Against
One-second pause before clicking	Before clicking any link or opening any attachment, in email, messaging apps, or social media, pause one second and ask: was I expecting this? Does the sender look right? Does the URL match where I expect to go?	Phishing, malware delivery, credential theft. The vast majority of successful phishing attacks succeed because the recipient clicks without pausing. One second changes the calculation.
Lock your screen when you step away	Every time you leave your desk, your workstation, or put down your phone in a public place, lock the screen. On Windows: Win+L. On macOS: Ctrl+Cmd+Q. On phone: press the power button.	Physical access to your accounts, data, and systems. A locked screen takes three seconds. An unlocked screen in an office takes three seconds for someone passing to read, photograph, or access your work.
Use unique passwords via a password manager	If you are not already using a password manager, set one up this week. Let it generate a new strong password for each account. You should never know what most of your passwords actually are.	Credential stuffing. Every account with a unique password is a firebreak, a breach at one service cannot cascade to others.
Keep software updated	Before posting on social media, consider who can see it and whether it reveals something that could be used against you: your location, your routine, your relationships, your employer, your home. Apply the same pause to sharing files and data at work.	Social engineering, targeted phishing, physical security risks, data breaches. Information shared publicly is information available to attackers.
Think before you share	Report to your information security team or manager immediately. Preserve all evidence. Do not attempt to fix or conceal the breach.	Support the GDPR assessment and notification process. Cooperate with any external investigation. Review and update controls to prevent recurrence.

Habit	What it Looks Like in Practice	What it Protects Against
	Activate the incident response process from Module 15.	
Report anything suspicious	If something seems odd, an unusual email, an unexpected login alert, a colleague behaving strangely around systems, a suspicious caller, report it. You do not need to be certain. You need to flag it.	Delayed detection of incidents. Early reporting consistently leads to better outcomes. The cost of a false alarm is a short conversation. The cost of silence can be weeks of undetected attacker access.

The one-second rule

The single habit that prevents more incidents than any other is the briefest: one second of conscious thought before clicking, opening, or responding to anything unexpected. This is not paranoia, it is the application of the threat recognition from Part 2 to real-world decisions. Urgency, unexpected senders, requests for credentials, suspicious URLs, all of these are visible in one second if you look. The attacker's greatest weapon is your automatic, unconsidered response. One second removes that weapon.

4. Clean Desk, Clear Screen

Physical security is the aspect of digital security most people overlook entirely. The focus on network threats, malware, and phishing can create a blind spot for the simplest risks: information visible to the wrong person because it was left in view.

The clean desk principle

A clean desk policy means not leaving sensitive information physically visible when you are not at your desk: printed documents, notebooks with passwords or confidential information, post-it notes with login details, USB drives. The risk is not primarily theft, it is observation. Someone passing your desk, sitting nearby in a café, or visiting the office for a meeting can read or photograph information in seconds without anyone noticing.

In practice: lock sensitive documents away when you step away for more than a few minutes. Take printouts from the printer promptly, shared office printers are one of the most common sources of accidental information disclosure. Shred rather than bin documents containing personal data or confidential information.

The clear screen principle

An unattended, unlocked screen is a physical access vulnerability. In an open-plan office, a hotel lobby, a coffee shop, or on a train, your screen is visible to anyone nearby. An unlocked screen means anyone passing can read, photograph, or interact with your work in seconds.

Three habits close this gap completely: lock your screen every time you step away (Win+L or Ctrl+Cmd+Q), set your screen to auto-lock after five minutes of inactivity, and position your screen so it is not directly visible to anyone passing behind you in public places. A privacy screen filter, a physical overlay that limits the viewing angle, is worth considering for regular public working.

5. Shadow IT: When Convenience Creates Risk

Shadow IT refers to the use of technology systems, software, or services outside the knowledge or approval of the organization's IT function. It is almost always driven by good intentions: someone finds a tool that makes their job easier and starts using it without going through what feels like a slow approval process.

The security problem with shadow IT is not that the tools are necessarily bad. It is that data processed outside approved systems is outside the organization's security controls, backup processes, data retention policies, and legal compliance frameworks. The organization does not know the data is there, cannot protect it, and may be in breach of GDPR or other regulations as a result.

Common Scenario	The Security Risk it Creates	Better Alternative
Using a personal cloud drive for work files	Work data sits outside organizational security controls, backup processes, and access policies. When the employee leaves, the data stays in their personal account. If the personal account is breached, work data is exposed.	Use organization-provided cloud storage (SharePoint, OneDrive for Business, Google Workspace). If a personal drive is genuinely more convenient, ask IT why the official option is not meeting your needs.
Installing unapproved software on a work device	Software installed outside the organization's approval process may not have been security-vetted. It may have vulnerabilities, collect data, or create conflicts with security tools.	Request the software through IT. If it is a legitimate business need, IT can usually accommodate it. The approval process exists for good reasons and takes less time than recovering from a malware infection.

Common Scenario	The Security Risk it Creates	Better Alternative
Sending work documents to a personal email for remote access	Work data passes through and is stored in a personal email account outside organizational control. It may be retained there indefinitely, across devices, and under different security standards.	Use the organization's remote access tools (VPN, remote desktop, cloud collaboration platforms). If these do not work well for your needs, tell IT, that is useful feedback.
Using a consumer messaging app for work discussions containing sensitive information	Sensitive work conversations in WhatsApp, personal iMessage, or similar apps are stored on personal devices, backed up to personal cloud accounts, and outside the organization's data retention and legal hold policies.	Use organization-approved communication tools (Teams, Slack with business account, encrypted email). For urgent situations, a personal message saying 'call me' is fine. Sensitive content should stay in approved channels.

Shadow IT is a symptom, not just a problem

When people use shadow IT, it usually means the approved tools are not meeting their needs. A team that uses WhatsApp for project communication because Teams is difficult to use, or an employee who saves files to personal Dropbox because the corporate VPN is too slow, is giving IT a useful signal: the official tools need improvement. The security-conscious response to shadow IT is not just to prohibit it but to understand why it is happening and fix the underlying problem.

6. Public and Shared Environments

Working outside the office, in coffee shops, airports, hotels, coworking spaces, or on public transport, is increasingly normal. Each environment brings specific risks that a few simple habits address.

Public spaces

- Position your screen so it is not easily visible to people behind or beside you.
- Use a VPN when connecting to public Wi-Fi for work tasks (covered in Module 7).
- Do not hold sensitive phone or video calls where others can hear confidential information. A hallway conversation or a call taken in a café can expose more than a network interception.
- Be aware of who is near you when typing passwords or PINs.

Shared or borrowed computers

- Never save passwords in a browser on a shared or borrowed computer.
- Always log out of all accounts before returning a shared device or leaving a workstation.
- Do not assume a browser's 'private' or 'incognito' mode makes a shared computer safe, it prevents browser history but not keyloggers[42] or other monitoring tools.
- If you have accidentally saved credentials on a shared computer, change the affected passwords immediately from a different device.

7. Social Media Security: A Brief Audit

Social media profiles are simultaneously one of the richest sources of personal information available to attackers and one of the most neglected areas of personal security practice. An annual or semi-annual audit of your social media presence takes under an hour and significantly reduces your attack surface.

What to Check	Why it Matters	How to Action it
Who can see your posts and profile	Public posts are visible to attackers doing reconnaissance for spear phishing, employers, and anyone else with an internet connection	Set posts to 'Friends' or equivalent. Set profile fields (employer, location, phone) to private or friends-only. Review each platform's privacy settings individually.
What your profile reveals when public	Even with posts private, your profile may show your employer, your city, your profile photo, and who your connections are, enough for a targeted attack	Google your own name and see what appears. Check what is visible when logged out of your account. Remove or limit anything that provides more detail than necessary.
Old accounts you no longer use	Dormant accounts still hold your data and may use an old reused password. They receive no security attention. If breached, you may not notice.	Search for accounts associated with your email addresses. Delete accounts you no longer use, most platforms provide a deletion option in Settings > Account.

[42] **Keylogger:** A tool, usually malicious, that records every key you type in order to capture passwords and other sensitive information.

What to Check	Why it Matters	How to Action it
Whether MFA is enabled	Social media accounts are high-value targets for takeover, your contacts trust messages from you	Enable an authenticator app for login on all social media platforms you actively use. Check security settings on each platform.
Connected apps with access to your account	Quiz apps, third-party schedulers, and old connected tools may still have read/write access to your profile and feed	Review connected apps in account security settings. Remove any you no longer use or do not recognize. This was covered in Module 10, apply the same principle here.

8. Making Habits Stick

Understanding which habits matter is necessary but not sufficient. The harder question is how to build habits that persist beyond the first week after completing a security course.

Attach habits to existing routines

The most reliable way to build a new habit is to attach it to something you already do. Lock your screen when you stand up to get coffee, the standing triggers the lock. Review your password manager when you pay a bill online, the payment triggers the review. Check your email's security settings when you clear your inbox on a Friday, the inbox review triggers the security check. Pairing a new behavior with an established trigger removes the need to remember to do it.

Make the secure option the default option

The most powerful habit-support mechanism is an environment where the secure option requires no effort and the insecure option requires extra steps. Enable automatic updates so you do not have to choose to update. Use a password manager so generating a unique password requires less effort than reusing one. Set your screen to auto-lock so security happens without action. When security is the path of least resistance, it becomes the automatic choice.

One habit at a time

The temptation after completing a security course is to try to change everything at once. This almost always fails. Behavior change research consistently shows that focusing on one habit at a time until it is automatic produces better outcomes than

attempting several simultaneously. Choose the habit from section 13 that addresses your biggest current gap and focus on it for two weeks before adding another.

ShieldNet thread going further

The habits in this module map to four ShieldNet controls. [SB4] (Protect User Devices) covers screen locks and device security. [WP3] (Apply Patches Quickly) covers the update habit. [SB6] (Establish a Clear Desk and Clear Screen Policy) formalizes the physical security practices from section 18.4. [LL1] (Train and Test Staff) recognizes that awareness training, like this course, is only the beginning: regular reinforcement, simulated phishing exercises, and security culture initiatives are what make the learning stick at scale.

Module 18 : Summary

By the end of this module, you should be able to:

- ✓ Explain why security habits are more valuable than security knowledge that is not acted on.
- ✓ Describe the ‘one-second rule’ and explain what it protects against.
- ✓ Define shadow IT and give two examples of how it creates security risk.
- ✓ Explain what a clean desk policy is and describe the security problem it solves.
- ✓ Describe three specific steps in a social media security audit.
- ✓ Explain the difference between security as a personal mindset and security as a set of rules imposed from outside.

Module 19: Security Is Everyone's Job

Your Role in a Safer Organization

1. The IT Team Cannot Do This Alone

Most people think of cybersecurity as something the IT department handles. There is a firewall somewhere. Someone monitors the logs. The antivirus is managed centrally. If something goes wrong, you call IT. In this mental model, security is a specialist function that happens in the background, and everyone else just needs to not get in the way.

This model is wrong, and increasingly dangerously so. Modern attacks are designed specifically to bypass technical controls by targeting the people who operate them. Phishing does not attack the firewall. Business email compromise[43] does not exploit a software vulnerability. Insider incidents do not trigger an antivirus alert. The attack surface that matters most is not the perimeter of the network, it is the behavior of every person inside it.

A security team can build excellent technical defenses and still watch those defenses fail because a staff member clicked a link, shared a password, or stayed silent about something they noticed. Conversely, a security team with modest technical resources can maintain genuinely good security outcomes if the people they support are alert, informed, and willing to act. Security is a team sport. The security team is the coach, not the only player.

2. What Security Teams Can and Cannot Do

Understanding the limits of what technical security controls can achieve helps clarify why individual behavior is not optional. The following comparison is not a criticism of security teams, it is an honest account of what technology can and cannot protect against.

What a Security Team CAN Do	What a Security Team CANNOT Do Alone
Set policies and technical controls	Make every individual follow them without active buy-in

[43] **Business Email Compromise (BEC):** A scam in which an attacker poses as a trusted colleague, supplier, or executive over email to trick an organization into transferring money or changing payment details.

What a Security Team CAN Do	What a Security Team CANNOT Do Alone
Configure spam filters and phishing detection	Catch every phishing email before it reaches the inbox
Implement MFA across all systems	Force individuals to choose strong master passwords or protect personal devices
Deploy endpoint protection[44] and monitoring	See what happens in unmonitored channels (personal email, messaging apps, shadow IT)
Design an incident response plan	Execute it effectively if staff do not know how to report incidents or what they should not do
Run access control policies	Prevent every instance of someone sharing credentials or bypassing controls for convenience
Train staff annually	Sustain security behavior without daily reinforcement from management and peers

The human layer is not a weakness to manage, it is a capability to develop

Security awareness training is sometimes framed as 'patching the human', as if people are a vulnerability to be fixed. This framing is both inaccurate and counterproductive. A genuinely security-aware person is not a patched vulnerability, they are an active defense layer. They notice things automated systems miss, exercise judgment in situations no policy anticipated, and create the early warning that allows rapid response. The goal is not to make people less likely to make mistakes. It is to make people more capable of recognizing threats and more confident about responding to them.

3. Your Responsibilities by Role

Security responsibilities are not uniform across an organization. They scale with access, authority, and the sensitivity of the systems or data someone interacts with. The following table maps specific responsibilities to common roles.

[44] **Endpoint protection:** Security software on devices (endpoints) that detects and blocks threats such as malware.

Your Role	Your Specific Security Responsibilities	Why This Role Matters
Every staff member	Follow security policies, use approved tools, lock screens, report suspicious activity, complete required training, use strong unique passwords and MFA, be alert to phishing and social engineering	You are the last line of defense that technical controls cannot replace. An attacker who tricks you bypasses every technical measure. Your vigilance and habits directly protect your colleagues and your organization.
Manager or team lead	Model good security behavior visibly, respond to reported incidents without blame, reinforce security expectations in team communications, raise systemic security issues upward, ensure departing team members' access is revoked promptly	Culture flows from management behavior. If managers dismiss security as IT's problem, their teams will too. If managers treat security incidents without blame, their teams will report more. Your behavior sets the standard.
System or data owner	Know what data your system holds and its sensitivity, ensure appropriate access controls, participate in access reviews, respond to data breach obligations relevant to your systems, ensure third parties with access meet required standards	You are accountable for the systems and data in your area. Regulatory obligations, GDPR, NIS2, ultimately require someone to take responsibility for specific systems and datasets. That is you.
New starter	Complete required security training promptly, ask about policies before using workarounds, report any pressure to bypass security controls, understand how to contact the IT or security team	New starters are statistically higher-risk targets for social engineering because attackers know they are less familiar with the organization's normal patterns. Your caution in the first weeks matters more than average.
Leaver or contractor at end of engagement	Return all devices and physical access materials, do not retain copies of organizational data on personal systems, ensure your manager initiates the access revocation process on your last day	Dormant accounts and retained data from former employees are a consistent source of security incidents. Responsible offboarding is a professional obligation, not just a policy compliance checkbox.

Credentials are never a team resource

One of the most common security violations in organizations, at every level, is sharing credentials. 'Can I use your login just this once?', 'We all share the admin password', 'The team account details are in the shared document'. These arrangements destroy accountability, prevent meaningful access control, and mean that when something goes wrong it cannot be attributed to a specific action by a specific person. If someone needs access, they get their own account. That is the only acceptable arrangement. The inconvenience of requesting access is always less than the cost of a shared credential breach.

4. Security Culture: What It Is and Why It Matters

Security culture is the set of values, behaviors, and norms that determine how people in an organization actually behave around security, not what the policy says, but what people actually do when nobody is watching, when it is inconvenient, and when there is pressure to cut corners.

Policy compliance and security culture are not the same thing. An organization where staff complete annual security training because they are required to and otherwise give security no thought has compliance. An organization where staff pause before clicking links because they understand why it matters, report suspicious things because they feel safe doing so, and challenge unusual requests because they see it as their job to do so has culture. Culture is what happens when the policy document is closed.

Signs of a STRONG Security Culture	Signs of a WEAK Security Culture
People report suspicious emails even when unsure, and are thanked for it	People stay silent about incidents out of fear of blame or embarrassment
Security training is seen as genuinely useful, not a compliance checkbox to rush through	Annual security training is completed in under ten minutes by clicking through without reading
Managers visibly follow the same security rules as everyone else	Senior staff are exempt from security policies or enforce them only on others
Security concerns are raised and acted on in project planning, not discovered after launch	Security is bolted on at the end of projects or after an incident has occurred
Staff can name their IT security contact and know how to report an incident	Most staff do not know how to report a security incident or who to contact

Signs of a STRONG Security Culture	Signs of a WEAK Security Culture
People question unusual requests, even from apparent authority, before complying	Requests from apparent senior figures are followed without verification because questioning them feels uncomfortable
New security tools are explained and rolled out with context, not just mandated	Security policies arrive as unexplained mandates that people work around as quickly as possible

Culture is set from the top

Security culture is not primarily shaped by training or posters. It is shaped by leadership behavior. When a senior leader asks IT to bypass MFA because it is inconvenient for them, the signal sent to every observer is that security is for other people. When a CEO praises someone publicly for reporting a phishing simulation catch, the signal is that security awareness is valued. When a manager responds to an incident report with blame, the signal is that silence is safer than honesty. Leaders do not need to be security experts. They need to model the behavior they want to see.

5. The Security Champion: Amplifying the Message

In many organizations, a small number of people take a particular interest in security and voluntarily act as informal bridges between the security team and their colleagues. These people are sometimes formally recognized as 'security champions' or 'security advocates', and their impact on organizational security culture is disproportionate to their numbers.

A security champion does not need to be technical. What they provide is:

- A trusted, accessible contact for colleagues who have security questions but do not know how to approach the IT team.
- Local reinforcement of security training: they remind their team of good practices in the context of real work, not abstract scenarios.
- Early signal to the security team about emerging risks, confusions, or compliance gaps that would not otherwise be visible.
- A model of security-conscious behavior that normalizes it for the people around them.

If the concept of a security champion program exists in your organization, it is worth exploring. If it does not, the behaviors described above are worth practicing regardless of whether there is a formal title attached to them. Anyone who takes an interest and helps those around them is performing the function, labeled or not.

6. Three Conversations Worth Having

The most practical output from this module is not a set of personal habits, those were covered in Module 18. It is a set of conversations. Security culture is built in conversations, not in policies. Here are three worth initiating.

With your team: normalize reporting

The next time something security-related comes up in your team, a suspicious email, an unexpected request, a system behaving oddly, use it as an opportunity to talk openly about how to respond. The goal is to make 'I wasn't sure, so I reported it' a normal, valued thing to say rather than something that feels risky.

With your manager: clarify what 'good' looks like

Ask your manager how security incidents should be reported in your team, and what the expected response is. If your manager does not know, that is itself useful information. If the answer suggests a blame-based culture, the conversation about no-blame reporting from Module 15 is worth raising constructively: 'I've been reading that early reporting leads to much better outcomes, could we discuss how we handle this as a team?'

With the IT or security team: introduce yourself

Most security teams work in relative isolation from the wider organization. They set policies, respond to incidents, and rarely hear from staff except when something has gone wrong. Introducing yourself, 'I've just completed our security training and I'm keen to understand how I can report incidents and what I should watch out for in my specific role', takes five minutes and establishes the kind of relationship that makes future reporting easier and faster.

7. From Compliance to Commitment

There is a meaningful difference between being secure because you have to be and being secure because you understand why it matters and have chosen to make it part of how you work. The first is fragile: it produces the minimum required behavior and

fails the moment oversight is removed. The second is durable: it produces behavior that persists because the motivation is internal.

The goal of this course has been the second. Not a list of rules to follow because a training policy requires it, but a genuine understanding of the threat landscape, the defenses that work, and the role every person plays in making them effective. Security knowledge that is truly understood becomes security judgment, the ability to recognize a situation that the policy document did not anticipate and make a good decision anyway. That judgment is what no technical control can replace, and what no attacker can fully predict or bypass. It is what makes you, regardless of your job title or technical background, a genuine security asset.

ShieldNet thread going further

Security culture maps directly to ShieldNet control [LL1] (Train and Test Staff), which requires security awareness training for all staff and regular phishing simulation exercises to test and reinforce learning. It also connects to [KP4] (Assess Risks Regularly), which requires management engagement with security as a business priority, the organizational expression of the leadership behavior this module describes. The role accountabilities in section 19.3 mirror the accountability table in the ShieldNet Core Standard Section 4, which assigns specific security responsibilities to the Board, InfoSec Coordinator, System Owner, All Staff, and Third-Party Providers.

Module 19: Summary

By the end of this module, you should be able to:

- ✓ Explain why security teams cannot protect an organization alone, regardless of their technical capability.
- ✓ Describe two specific security responsibilities that apply to every staff member.
- ✓ Explain what a security culture is and describe two observable signs that distinguish a strong culture from a weak one.
- ✓ Describe how manager behavior shapes team security behavior, with a specific example.
- ✓ Explain what ‘security champion’ means and describe one action a security champion might take in their team.
- ✓ State one specific security responsibility that is unique to someone leaving an organization.

Module 20: Staying Ahead

How Security Evolves and How You Keep Up

1. This Course Is a Starting Point, Not a Destination

You have now covered twenty modules of cybersecurity knowledge: the CIA triad, risk, phishing, malware, passwords, networks, attackers, authentication, access control, device security, encryption, privacy, third parties, incidents, backups, data breaches, habits, and security culture. That is a substantial foundation.

It will not stay current forever.

Cybersecurity is one of the few fields where the landscape changes meaningfully year on year. Not in ways that make everything you have learned obsolete, the fundamentals of risk management, the importance of MFA, the value of tested backups, the danger of phishing, none of these will change. But the specific techniques attackers use, the tools available to both sides, the regulatory requirements organizations must meet, and the new attack surfaces created by new technologies all shift continuously.

This module gives you a realistic picture of what changes, what stays constant, and what a sustainable approach to staying current actually looks like for someone who is not a security professional, without turning security awareness into a second career.

2. What Changes, What Stays Constant

The most useful mental model for navigating a changing landscape is distinguishing between what evolves and what endures. This distinction reduces anxiety: you do not need to track every new development if you hold the constants clearly.

What Changes Over Time	What Stays Constant
Attack techniques evolve, new malware families, new phishing tactics, new exploitation methods	The attacker's goals remain the same: access, data, disruption, money
The tools attackers use become more sophisticated and accessible (including AI-powered attacks)	The fundamental weaknesses they exploit remain consistent: unpatched software, weak credentials, human trust
New technologies create new attack surfaces (IoT devices, cloud, AI systems, connected vehicles)	The defenses that work remain consistent: patching, strong authentication, access control, backups, training

What Changes Over Time	What Stays Constant
Regulations evolve, new laws, updated requirements, expanded scope	The underlying principles of data protection, risk management, and proportionate response remain stable
Specific threats become more or less prominent as attackers follow money and opportunity	The importance of early detection and rapid response does not change regardless of what the threat is
The security tools and products available to organizations improve	The human element, judgment, awareness, and culture, remains the decisive factor

The fundamentals compound

The defenses that work against today's attacks, MFA, patching, tested backups, phishing awareness, access control, incident reporting, are the same defenses that worked against last year's attacks and will work against next year's. An attacker who finds MFA in place cannot use stolen credentials. Ransomware that finds offline backups cannot extort. Phishing that meets a skeptical, pausing recipient fails. The fundamentals do not expire. Staying current means keeping up with new expressions of old problems, not learning an entirely new discipline every year.

3. Emerging Trends Worth Understanding

A handful of developments in the current threat landscape deserve specific attention because they represent meaningful shifts rather than incremental evolution. Understanding them at a conceptual level is enough, you do not need technical depth, but you should know they are happening.

Trend	What it Means in Practice	What it Means For You
AI-enhanced attacks	Large language models enable attackers to produce highly convincing phishing emails at scale, with perfect grammar, personalized content, and context-aware messaging. Voice cloning enables convincing vishing attacks using a real person's voice.	The grammar-and-spelling red flag from Module 4 is becoming less reliable. Domain checks and process verification (call back on a known number) matter more than ever. Urgency and authority are still the key signals.
Ransomware as a service (RaaS)	Ransomware is now available as a commercial product, criminal groups	The number of ransomware attacks is growing faster than the number of

Trend	What it Means in Practice	What it Means For You
	lease ransomware tools and infrastructure to less-skilled operators in exchange for a percentage of ransoms. This dramatically lowers the barrier to entry for attackers.	attackers. Tested backups, patching, and MFA remain the most effective defenses regardless of which ransomware variant is used.
Passkeys and passwordless authentication	The shift away from passwords to passkeys (covered in Module 9) is accelerating. Major platforms are pushing passkey adoption, and within a few years passwords may become the exception rather than the norm for consumer services.	Enable passkeys wherever they are offered. They are strictly better than passwords plus MFA for most threat models. The transition will happen gradually, there is no urgency, but no reason to resist either.
Regulation catching up with technology	The EU AI Act, the Cyber Resilience Act (CRA), and NIS2 represent a wave of regulation extending cybersecurity requirements to new sectors and new types of product. More organizations will have formal compliance obligations than before.	If your organization develops software, connected products, or operates in newly regulated sectors, expect new security requirements in the coming years. The ShieldNet framework is designed to align with these regulations.
Supply chain attacks at greater scale	Software supply chain attacks, compromising trusted tools, libraries, and updates, are growing in frequency and sophistication as attackers recognize the leverage of compromising widely-used components.	Individual defenses remain limited (keep software updated, minimize footprint). The organizational response, vendor vetting, software bill of materials, monitoring for unusual behavior from trusted tools, becomes more important.

AI and social engineering: the key adjustment

Generative AI has made it significantly easier to produce convincing phishing content at scale. The grammar-and-spelling heuristic that appeared in Module 4 is becoming less reliable as a standalone check.

What this means in practice: rely more heavily on the structural red flags that AI cannot easily fake. Did you expect this message? Does the request follow your organization's normal process? Is the sender asking you to act urgently outside normal channels? Can you verify the request through a separate, known channel?

The one-second pause from Module 18 matters more than ever. AI improves the quality of the lure. It does not change the fundamental structure of a phishing attempt: unexpected message, creates urgency, requests action that bypasses normal process.

4. How to Stay Informed Without It Becoming a Job

The security industry produces an enormous volume of content: threat reports, vulnerability advisories, incident analyses, product announcements, regulatory guidance. Reading all of it is a full-time occupation. Reading none of it leaves you disconnected from meaningful developments.

The practical approach for a non-specialist is a light-touch, curated routine that takes less than thirty minutes a week and provides genuine signal rather than noise.

Source Type	Specific Examples	What it Gives You
National cybersecurity agencies	ENISA[45] (EU), NCSC (UK), ANSSI (France), BSI (Germany), CERT Polska (Poland), all publish free advisories, threat reports, and guidance	Authoritative, non-commercial information about current threats and defensive guidance. NCSC's weekly threat reports are particularly accessible and practical.
Breach and vulnerability tracking	haveibeenpwned.com (personal breach notifications), ENISA Vulnerability Database (EUVD), CISA Known Exploited Vulnerabilities catalog (KEV), CVE database (cve.mitre.org)	Early warning when your data appears in a breach; a current list of actively exploited vulnerabilities that organizations should prioritize patching.
Security news accessible tier	Krebs on Security. The Record, Bleeping Computer	Readable, non-technical coverage of significant incidents, new attack techniques, and security industry developments. Suitable for a weekly scan.
Your organization's own security team	Internal security bulletins, alerts about current phishing campaigns targeting your sector, updates when policies change	The most directly relevant information for your specific context and role. Make sure you are subscribed to whatever internal security communications exist

[45] **ENISA:** The European Union Agency for Cybersecurity, which provides guidance, threat information, and support across the EU.

Source Type	Specific Examples	What it Gives You
Professional development	ShieldNet educational framework, ISC2, CompTIA (Security+), SANS Institute, Coursera and edX	Structured learning for people who want to deepen their knowledge beyond literacy.

A minimal viable information diet

Subscribe to your national cybersecurity agency's alerts (free, authoritative, non-commercial).

Enable breach notifications on haveibeenpwned.com for your email addresses.

Scan one security news source (Krebs on Security or The Record) once a week, headlines only unless something is directly relevant to your work.

Complete refresher training when your organization offers it, and ask for it if they do not.

When a major incident makes mainstream news (a large ransomware attack, a significant data breach, a new regulation), read one article about it. Understanding real-world context is more valuable than abstract threat intelligence.

That is it. Thirty minutes a week, maximum. Sustainability matters more than comprehensiveness.

5. If You Want to Go Further

This course is designed for universal literacy, the knowledge every person needs regardless of their role. Some people who complete it will find that they want to go deeper. The following routes are worth knowing about.

ShieldNet Education Framework

First European educational framework that matches its courses to European Cybersecurity Skills Framework.

CompTIA Security+

A widely recognized industry certification that goes a step beyond the CC in technical depth. Particularly relevant for people moving into IT roles with security components. Paid examination, significant study investment required.

SANS Institute

The SANS Institute offers some of the most rigorous technical security training available. More expensive and more demanding than entry-level certifications, but the

quality is consistently high. Suitable for people actively moving into security-specialist roles.

Practical skills

For people who learn by doing, platforms like TryHackMe and Hack The Box offer guided, hands-on security exercises at various skill levels. These go well beyond literacy into practical security skills, but the gamified format makes them accessible and engaging for beginners.

> **You do not have to become a security professional to be a security asset**
> The path from this course to a security specialist role is long and not necessary for most people. What is both achievable and genuinely valuable is being the person in your team or organization who understands what is happening, applies good habits consistently, notices things, and speaks up. That person, at any level of any organization, is worth more to security outcomes than a distant policy document or a technical control that nobody monitors.

6. The Annual Security Refresh

The most practical commitment to ongoing security awareness is not continuous reading, it is an annual structured review. Once a year, ideally triggered by a fixed date (the start of the year, your professional review, your organization's training cycle), spend a couple of hours on the following:

- Review your passwords: Check haveibeenpwned.com for your email addresses. Update the password manager. Ensure the accounts you use most have unique, strong passwords and active MFA.
- Review your device security: Check that automatic updates are enabled on all devices. Verify that full-disk encryption is active on laptops. Confirm remote wipe capability is set up on phones.
- Review your connected apps and permissions: Audit third-party apps connected to Google, Apple, and social media accounts. Remove what you no longer use. Review app permissions on your phone.
- Review your backup status: Restore a file from your backup to confirm it actually works. Check that the offline copy is current.

- Scan major developments of the past year: Read one annual threat report from your national cybersecurity agency. Update your understanding of what has changed.
- Complete any refresher training offered by your organization: If none is offered, ask why. Organizations that do not invest in security awareness training are carrying unnecessary risk.

Two hours, once a year. Less time than a dental check-up, and considerably more consequential for some people's digital health.

ShieldNet thread going further

Staying current maps to ShieldNet control [LL1] (Train and Test Staff), which requires security training at least annually and recommends phishing simulation exercises to test and reinforce awareness. It also connects to [LL2] (Learn from Incidents and Near Misses), which requires organizations to review security incidents for lessons and update training and controls accordingly. The 'staying ahead' mindset at the individual level mirrors the continuous improvement cycle that [LL2] builds into organizations. Module 21, the final module, introduces how ShieldNet itself operationalizes these principles at the organizational level.

Module 20: Summary

By the end of this module, you should be able to:

- ✓ Explain what stays constant in cybersecurity even as specific threats and tools change.
- ✓ Name two authoritative sources of security information available free of charge and describe what each provides.
- ✓ Explain how AI is changing the phishing threat and describe one defense that remains effective.
- ✓ Describe what 'Ransomware as a Service' means and explain why it increases the volume of attacks.
- ✓ Explain why completing this course is a starting point rather than a destination, and name one specific action for staying current.

Part 5 Knowledge Check

Module 18 Practice Questions
Q1. A staff member receives an email appearing to be from their bank, asking them to verify their account details urgently. They are busy and about to click the link before they pause and notice the sender's address is from a domain they do not recognize. They do not click and report it to IT. Which habit made the critical difference in this scenario? a. Using a password manager, which would have refused to fill in credentials on a fake site. b. Having MFA enabled, which would have prevented account takeover even if credentials were entered. c. The one-second pause before clicking, taking a moment to check the sender and URL before acting on an urgent prompt. d. Keeping their software updated, which would have blocked the phishing email at the network level.
Q2. A project manager saves work documents to their personal Dropbox account so they can access them easily from their home computer. The documents include client contracts and financial projections. What is the primary security risk this creates? e. Dropbox is not secure enough to hold business documents. f. The project manager's personal Dropbox account is outside the organization's security controls, access policies, and backup processes. If their personal account is breached or the employee leaves, the organization loses control of sensitive client data. g. Personal cloud storage does not provide version history for documents. h. The documents may be accidentally shared publicly if the Dropbox folder is misconfigured.
Q3. A staff member leaves their workstation unlocked when they go to make coffee. A colleague sits at the desk briefly and notices the screen shows a confidential HR spreadsheet. Which clean desk / clear screen principle was not followed, and what is the simplest prevention? i. The colleague should have looked away, the responsibility is on the observer, not the absent staff member. j. The staff member should have logged out of their computer rather than just stepping away. k. The staff member should have locked their screen before stepping away (Win+L or Ctrl+Cmd+Q on macOS), which would have required a password to access the computer in their absence. l. The workstation should have been in a private room rather than an open office.
Q4. Someone argues: 'I don't need to worry about my social media privacy because I never post anything sensitive.' Which response best addresses the security dimension of this claim? m. This is correct, if you do not post sensitive content, your social media presence creates no security risk. n. Even without sensitive posts, a public profile can reveal your employer, location, daily routine, relationships, and photo, enough information for a targeted phishing or social engineering attack. The risk is not in what you post, but in what your presence reveals about you. o. This is partially correct, the risk is only significant for people in high-profile roles.

Module 18 Practice Questions
p. The only real risk from social media is account takeover, which is prevented by MFA regardless of what you post.

Module 19 Practice Questions
Q1. An organization deploys state-of-the-art spam filtering, endpoint protection, and MFA across all systems. A staff member then receives a well-crafted spear phishing email that bypasses the spam filter, clicks the link, enters their credentials on a convincing fake login page, and because MFA push notifications were enabled, eventually approves one after receiving fifteen requests in a row. What does this scenario illustrate about the limits of technical security controls? a. The technical controls failed, better technology would have prevented this. b. Technical controls significantly raise the bar but cannot replace human judgment. The spam filter reduced risk; MFA required the attacker to also manipulate the person; but a human decision, approving the MFA push, ultimately enabled the breach. Security awareness and human behavior are not optional supplements to technical controls. c. The organization should have used a different MFA method. d. Staff should not have access to external email on work devices.
Q2. A manager discovers that a team member clicked a phishing link and may have exposed credentials. The manager responds: 'Good thing you told me, let's get IT involved immediately and work out what we need to do. Thanks for flagging it quickly.' What is the security impact of this response? e. It is too lenient, the team member should face consequences to deter future carelessness. f. It reinforces the no-blame reporting culture, making it more likely that future incidents, which will inevitably occur, are reported promptly rather than concealed, enabling faster response and less damage. g. It sets a bad precedent by rewarding careless behavior. h. It has no impact on security, what matters is the technical response, not the managerial reaction.
Q3. A new colleague asks you to share your login credentials temporarily because they are having trouble accessing a shared system and have a deadline in an hour. They are friendly, seem stressed, and you have worked with them for two weeks. What is the correct response? i. Share the credentials temporarily and ask them to change them back once the deadline has passed. j. Decline to share credentials regardless of the reason, and instead help them contact IT support or your manager to resolve the access issue through proper channels. k. Share the credentials but change your password as soon as the deadline has passed. l. Ask your manager whether it is acceptable to share credentials in this specific situation
Q4. Which of the following best describes the difference between compliance with security policies and a genuine security culture?

Module 19 Practice Questions
m. Compliance means following rules; culture means going beyond minimum requirements to actively protect the organization because you understand why it matters and see security as part of your role. n. Compliance is sufficient, if everyone follows the policies, culture is irrelevant. o. Culture is what the security team creates; compliance is what everyone else is expected to maintain. p. There is no meaningful difference, both describe the same desired outcome.

Module 20 Practice Questions
Q1. A colleague argues: 'I completed security training two years ago, so I'm covered.' Which response best addresses this? a. This is correct, foundational security knowledge does not expire. b. Security training two years ago covered the threats and tools of two years ago. AI-enhanced phishing, new ransomware variants, updated regulations, and new attack surfaces have emerged since. Staying current requires periodic refreshing, not a one-time effort. c. Security training should be repeated annually regardless of changes, purely for compliance purposes. d. Two years is within the acceptable refresh cycle, most training is valid for three to five years.
Q2. An attacker uses an AI tool to generate a highly personalized phishing email targeting a specific employee. The email contains no spelling errors, references real projects the employee is working on (gathered from LinkedIn), and appears to come from a supplier the employee recognizes. The old red flag of 'look for grammar errors' would not have helped. Which defense remains most effective against this attack? e. Spam filters with AI-powered detection, which can identify AI-generated content. f. The one-second pause combined with domain verification and process-based checks, verifying unexpected requests by contacting the apparent sender through a known, separate channel rather than replying to the email. g. Employee awareness that attackers use AI tools, which makes the employee immune to AI-generated content. h. Using a VPN, which hides the employee's location from attackers doing reconnaissance.
Q3. Ransomware as a Service (RaaS) has made ransomware attacks more common by lowering the barrier to entry. Which combination of defenses most directly limits the impact of a ransomware attack, regardless of which RaaS variant is used? i. Advanced threat detection software and a dedicated security operations center. j. Tested offline backups (to recover without paying) and MFA on all accounts (to limit the attacker's ability to spread through compromised credentials). k. Employee training on recognizing ransomware symptoms and disconnecting infected machines. l. Cyber insurance that covers ransomware payments and recovery costs.

Module 20 Practice Questions
Q4. You have just completed this course. Which approach best describes what 'staying current' should look like going forward? m. Completing this entire course again in twelve months. n. Subscribing to a weekly threat intelligence feed and reading every advisory in full. o. A light-touch ongoing practice: subscribing to your national cybersecurity agency's alerts, enabling breach notifications on haveibeenpwned.com, completing refresher training when offered, and paying attention to major security news stories, while continuing to apply the habits and principles from this course. p. Waiting for your organization to update its security policies and following the new guidance when it arrives.

Module 21: From Concepts to Practice

A First Look at ShieldNet

1. You Have Already Learned ShieldNet

Every module in this course has been tagged with a ShieldNet thread, a brief note at the end of each module showing how the topic connects to specific controls in the ShieldNet Cybersecurity Standard. If you followed those threads, you have already encountered almost every ShieldNet control at least once, framed in the context of understanding why it matters rather than what it requires.

This final module does something different. It steps back from the individual topics and shows you the whole structure: what the ShieldNet Standard is, how it is organized, how its five Action Zones map to the arc of this course, and what using ShieldNet in practice actually looks like for the organizations and individuals it is designed to serve.

The goal is not to make you a ShieldNet expert, that is what the Core Standard document and the sector Add-Ons are for. The goal is to make you someone who, when ShieldNet comes up in a professional context, in a supplier questionnaire, a job description, a board-level discussion, or a customer contract, understands what it is, where it came from, and what it asks of the people and organizations that adopt it.

2. What ShieldNet Is

The ShieldNet Cybersecurity Standard is a practical, plain-language cybersecurity framework developed by IS Consulting for small-to-medium organizations operating in the EU regulatory environment. It consists of 48 mandatory controls organized into five Action Zones, written specifically to be implementable by organizations without a dedicated security team, the vast majority of European businesses and institutions.

Three features distinguish ShieldNet from other cybersecurity frameworks:

- Plain language: Every control is written in plain English with a clear Why field explaining the business rationale. There is no assumption of technical expertise. A competent operations manager can read, understand, and begin implementing ShieldNet without specialist translation.
- EU regulatory alignment: Every control is anchored to specific EU laws such as GDPR, NIS2, the Cyber Resilience Act, the AI Act. Implementing ShieldNet does not

just improve security posture: it simultaneously builds a documented compliance trail for the regulations that apply to most European organizations.

- Modular design: The Core Standard provides the 48 universal controls. Sector Add-Ons extend it for specific industries (healthcare, e-commerce, education, water, heating and cooling). The Cybersecurity Management System (CMS) layer adds OKR-based governance for organizations that want to drive continuous improvement. Each layer builds on the previous one without replacing it.

Who ShieldNet is designed for

ShieldNet is designed for any organization that wants to demonstrate a credible, proportionate approach to cybersecurity but does not have the resources to implement a major framework like ISO 27001 from scratch. It is particularly relevant for organizations that need to meet NIS2 or GDPR obligations, respond to customer or partner security questionnaires, prepare for sector-specific regulatory requirements, or simply build genuine security capability rather than paper compliance.

3. The Five Action Zones

The 48 controls in the Core Standard are organized into five Action Zones. Each zone groups controls by the stage of security activity they represent. The zones also correspond to the five parts of this course, not by design in the original standard, but because the underlying logic is the same: understand first, build defenses, watch for problems, respond when they occur, and keep improving.

Zone	Tagline	What it Covers	Course Modules it Connects to
KNOW & PLAN	*'Know your assets, risks, and obligations – and plan ahead for security.'*	Asset inventory, risk assessment, regulatory compliance mapping, supplier vetting, business continuity planning, security roles and responsibilities	M1 (digital assets), M3 (risk), M8 (attacker landscape), M13 (data and privacy), M16 (business continuity)
SHIELD & BUILD	*'Shield your technology and build it strong – keep attackers out from the start.'*	Access control, MFA, secure hiring and exit, device protection, network security, secure development, data	M9 (authentication), M10 (access control), M11 (device security), M12 (encryption), M13

Zone	Tagline	What it Covers	Course Modules it Connects to
		minimization, software updates	(privacy), M14 (third parties)
WATCH & PATCH	*'Watch for signs of trouble, and patch problems quickly to stay secure.'*	Vulnerability monitoring, patch management, security monitoring and logging, threat intelligence	M11 (patching), M15 (spotting incidents), M20 (staying current)
REACT & RECOVER	*'React fast when incidents strike, and recover to business-as-usual quickly.'*	Incident response planning, detection and escalation, forensic preservation, system recovery, regulator and customer notification	M15 (incident reporting), M16 (backups and recovery), M17 (data breaches)
LEARN & LIFT	*'Learn from every experience and lift your cybersecurity maturity continuously.'*	Staff training and testing, incident review and lessons learned, continuous improvement, maturity assessment	M18 (habits), M19 (security culture), M20 (staying current)

The Action Zone taglines are fixed and canonical

Each zone has a specific tagline that appears throughout the ShieldNet document family. Knowing them is useful for recognizing the framework in professional contexts:

KNOW & PLAN: 'Know your assets, risks, and obligations – and plan ahead for security.'

SHIELD & BUILD: 'Shield your technology and build it strong – keep attackers out from the start.'

WATCH & PATCH: 'Watch for signs of trouble, and patch problems quickly to stay secure.'

REACT & RECOVER: 'React fast when incidents strike, and recover to business-as-usual quickly.'

LEARN & LIFT: 'Learn from every experience and lift your cybersecurity maturity continuously.'

4. How This Course Maps to the Standard

Every module in this course has supported at least one ShieldNet control. The following table makes those connections explicit. Use it as a reference if you want to understand which controls an organization would be working on when dealing with topics from specific modules.

Module	Primary Topic	ShieldNet Controls it Supports
M1	Your Digital Life	[KP3] Asset & Data Inventory, [KP4] Assess Risks Regularly
M2	CIA Triad	Underpins all 48 controls, the conceptual foundation of the entire framework
M3	Risk	[KP4] Assess Risks Regularly
M4	Phishing	[LL1] Train and Test Staff, [SB3] Enable MFA
M5	Malware	[SB4] Protect User Devices, [WP3] Apply Patches Quickly, [KP6] Plan for Continuity
M6	Passwords	[SB1] Control User Access, [SB3] Enable MFA
M7	Networks	[SB5] Secure Your Network, [SB7] Encrypt Sensitive Data
M8	Attackers	[KP4] Assess Risks Regularly, [SB2] Secure Hiring and Exit, [KP7] Vet Suppliers
M9	Authentication	[SB3] Enable Multi-Factor Authentication
M10	Access Control	[SB1] Control User Access, [SB2] Secure Hiring and Exit
M11	Device Security	[SB4] Protect User Devices, [WP3] Apply Patches Quickly
M12	Encryption	[SB7] Encrypt Sensitive Data
M13	Data and Privacy	[SB9] Minimize Data Collection, [KP8] Build Security into Projects
M14	Third Parties	[KP7] Vet Suppliers, [SB9] Minimize Data Collection
M15	Incident Reporting	[RR2] Detect and Escalate Incidents, [LL1] Train and Test Staff
M16	Backups	[KP6] Plan for Continuity, [RR4] Recover Systems
M17	Data Breaches	[RR5] Notify Regulators, [RR6] Inform Affected Users
M18	Habits	[SB4] Protect User Devices, [WP3] Apply Patches Quickly, [LL1] Train and Test Staff
M19	Security Culture	[LL1] Train and Test Staff, [KP4] Assess Risks Regularly

Module	Primary Topic	ShieldNet Controls it Supports
M20	Staying Current	[LL1] Train and Test Staff, [LL2] Learn from Incidents

5. The Control Structure: A Sample

Every ShieldNet control follows an identical four-field structure. Understanding that structure helps you read the standard fluently. Here is what each field contains, illustrated with a real control.

[SB3] Enable Multi-Factor Authentication

Control text: The organization must enable multi-factor authentication (MFA) on all remote logins and important accounts, at minimum covering administrators, email, VPN, and cloud dashboards.

Why: Passwords alone are no longer sufficient protection for important accounts. MFA ensures that a stolen password cannot immediately be used to access your systems, the attacker would also need a second factor (such as a code from an authenticator app) that they do not have. Even a basic phishing attack that captures credentials is neutralized by MFA.

Evidence examples: MFA enabled on email platform (screenshot or policy document), MFA enabled on VPN, MFA enabled on cloud management consoles, MFA policy document approved by management.

Legal anchors: NIS2 Art. 21(2)(j), GDPR Art. 32(1)(b), CRA Annex I(1)(f).

If you completed Module 9 of this course, every element of that control is already familiar. The control text states the requirement. The Why explains the business rationale (which Module 9 explored in depth). The evidence examples tell an auditor or reviewer what to look for. The legal anchors connect the control to the specific EU regulations it satisfies. This structure is consistent across all 48 Core controls and all sector Add-On controls.

6. The Annex A Templates

ShieldNet is designed to be evidence-based: organizations do not just implement controls, they document the implementation so that it can be reviewed, audited, and improved over time. Annex A of the ShieldNet Standard provides 13 ready-to-use templates that correspond to the most important evidence artefacts.

The most important templates to know

- A-1 Asset & Data Inventory: Lists all significant assets (systems, data sets, applications) with their owner, sensitivity level, and location. Required by control [KP3]. Starting point for almost everything else.
- A-2 Risk Register: Documents identified threats, vulnerabilities, risk ratings, and chosen responses. Required by control [KP4]. The vocabulary from Module 3, threat, vulnerability, likelihood, impact, feeds directly into this template.
- A-10 Incident Contact List: Names and contact details for internal and external contacts during an incident: IT lead, management, legal, data protection authority, key suppliers. Required by control [RR1].
- A-11 Incident Log: Records all security incidents and near misses with timeline, scope, and actions taken. Required by controls [RR2] and [LL2].
- A-13 BC/DR Test Log: Records backup and recovery tests, confirming that restoration procedures work. Required by control [KP6]. The annual backup test from Module 16 is what fills this template.

You do not need to memorize all 13 templates. What matters is understanding the principle: ShieldNet connects requirements (controls) to evidence (templates) to legal obligations (anchors) in a single coherent system.

7. What ShieldNet Looks Like in Practice

The gap between reading a framework and implementing it is one that many organizations never cross. ShieldNet is designed to be narrow. Here is what adoption actually looks like at different organizational scales.

ShieldNet Component	What it Looks Like in a Small Organization	What it Looks Like in a Medium Organization
Core Standard (48 controls)	A single person (the InfoSec Coordinator, who may also be the office manager) works through the controls with the Annex A templates, producing a risk register, asset inventory, and incident response plan. Takes a few days spread over a month.	A small internal security team or a dedicated InfoSec Coordinator leads the implementation, with system owners accountable for specific controls in their area. Formal management sign-off at the Board or senior management level.
Annex A templates	Fill in the asset inventory (A-1), risk register (A-2), and incident contact list (A-10) first, these three alone	All 13 templates completed, version-controlled, and reviewed at least annually. Templates integrated into

ShieldNet Component	What it Looks Like in a Small Organization	What it Looks Like in a Medium Organization
	provide significant value and are required for most of the subsequent controls.	onboarding, project planning, and supplier management processes.
Sector Add-Ons	A small healthcare practice adopts the Healthcare Add-On controls relevant to their patient data. A boutique e-commerce business adopts the E-commerce Add-On for card and customer data handling.	Sector controls integrated into the main security program. Where the organization spans multiple sectors (a healthcare provider that also has an online shop), the relevant Add-Ons are combined.
Annual review cycle	Once a year, the InfoSec Coordinator revisits the risk register, checks whether anything significant has changed (new systems, new staff, new threats), and updates the controls accordingly.	Quarterly risk reviews for high-priority areas, annual full review. Internal audit function reviews compliance. External assessment or penetration test every two to three years.

The size matrix: Core, Core + Optional, Core + Mandatory

ShieldNet calibrates its requirements to organizational size and sector sensitivity:
Micro organizations in low-sensitivity sectors: Core Standard only.
Small organizations in moderate-sensitivity sectors: Core + Optional sector controls.
Medium organizations in high-sensitivity sectors (healthcare, finance, critical infrastructure): Core + Mandatory sector controls + recommended audit.
This proportionality is deliberate. A five-person bakery and a 200-person healthcare provider face different threats, hold different data, and operate under different regulations. ShieldNet applies minimum necessary controls to each rather than treating them identically.

8. ShieldNet and the EU Regulatory Landscape

One of ShieldNet's explicit design goals is to serve as a practical implementation path for EU cybersecurity regulations. The three most significant current frameworks are:

NIS2 Directive

The Network and Information Security 2 Directive extends mandatory cybersecurity obligations to a much wider range of sectors than its predecessor. Organizations in scope must implement risk management measures, report significant incidents within 24 hours, and ensure supply chain security. ShieldNet's 48 controls map directly to NIS2 Article 21 requirements.

GDPR

The General Data Protection Regulation requires appropriate technical and organizational measures to protect personal data. The SHIELD & BUILD zone controls, particularly [SB1] through [SB9], address the Article 32 obligation for security of processing. The REACT & RECOVER controls, particularly [RR5] and [RR6], address breach notification. Module 17 covered this in depth.

Cyber Resilience Act (CRA)

The Cyber Resilience Act establishes security requirements for products with digital elements, software and connected hardware sold in the EU. Organizations that develop or distribute such products must demonstrate security by design, vulnerability management processes, and incident reporting. ShieldNet's [KP8] (Build Security into Projects) and [WP3] (Apply Patches Quickly) directly address CRA requirements.

Understanding that ShieldNet is designed to satisfy multiple regulatory requirements simultaneously is important context for anyone who will encounter it in a supplier questionnaire, a procurement process, or a compliance review. Implementing ShieldNet is not a separate task from meeting regulatory obligations, for most organizations, it is the same task.

9. What Comes Next

You have now completed all 21 content modules of the ShieldNet Core Training. From Module 1's exploration of digital assets and why attackers want them, through five parts covering the threat landscape, practical defenses, incident response, and security as a mindset, to this final bridge module connecting the learning to the ShieldNet Standard, you have covered more ground than most people in most organizations ever will.

The Final Assessment that follows tests your understanding through 40 scenario-based questions drawn from across all five parts of the course. The questions are

designed to test judgment and application, not memorization. If you have engaged with the modules, you are ready.

One last thought before you go into the assessment. Security knowledge is genuinely valuable. But knowledge applied is what makes the difference. The person who comes out of this course and actually uses a password manager, actually pauses before clicking, actually reports the suspicious email, actually tells their team what they learned, that person has not just passed a course. They have become harder to attack. And in a world where most attacks succeed because they find an easy target, being harder to attack is a meaningful contribution to everyone around you.

Module 21: Summary

You have completed the ShieldNet Core Training content. Before the final assessment, here is what to carry forward:

- ✓ The five Action Zones are the structure through which ShieldNet organizes all 48 controls.
- ✓ Every module in this course connects to one or more ShieldNet controls, the course and the standard are designed to reinforce each other.
- ✓ ShieldNet is a starting point, not a ceiling. The Core Standard covers the universal baseline. Sector Add-Ons, the CMS, and external certification programs build on it.
- ✓ The skills you have developed, recognizing phishing, applying MFA, understanding risk, reporting incidents, protecting devices, are immediately applicable regardless of whether your organization ever formally adopts ShieldNet.