MODULE 1 · FREE COURSE

What Is Cybersecurity?



What we protect, the core ideas behind security, and who attacks and why

Start Your Cybersecurity Career

In this module you will learn



What cybersecurity protects
People, information, systems and services



The CIA triad
Confidentiality, integrity and availability



Threat, vulnerability and risk
The three words every security job uses



Who attacks and why
Criminals, hacktivists, nation states and insiders

01

Module 1 of 8
What Is Cybersecurity?

About 20 minutes

Why it matters: Japan, October 2026

In five weeks, ransomware, data theft and an exploited software flaw pushed Japan to declare a state of emergency in cyberspace.

500+

cyber incidents in Japan in 2026, a new record

495

organisations hit by one cloud ransomware attack

9 Oct

government declares a cyberspace emergency

Source: ZNexora Tech, “Japan’s October 2026 Cyber Emergency”

What cybersecurity protects



People

Staff, customers and their personal data



Information

Records, designs, money and secrets



Systems

Computers, phones, networks and cloud services



Services

Hospitals, banks, trains and power that society relies on

The CIA triad: three goals of security



Confidentiality

Only the right people can see information. Example: your medical records stay private.



Integrity

Information stays accurate and is not secretly changed. Example: a bank transfer amount cannot be altered.



Availability

Systems work when people need them. Example: a hospital system stays online during an emergency.

Threat, vulnerability and risk



Threat

Someone or something that could cause harm

A burglar

Vulnerability

A weakness that could be used

An unlocked window

Risk

The chance of harm × how bad it would be

Likely break-in, valuables lost

Security teams cannot remove every threat, so they reduce vulnerabilities and impact to lower the risk.

Who attacks, and why



Cybercriminals

Want money: ransomware, fraud, selling stolen data. The most common attackers.



Hacktivists

Want attention for a cause: website defacement, leaks, service disruption.



Nation-state groups

Want secrets or influence: espionage and attacks on critical infrastructure.



Insiders

Employees or partners who cause harm, by mistake or on purpose.

Common myths about cybersecurity

Myth	Reality
“We are too small to be a target.”	Most ransomware victims in Japan are small and medium-sized companies.
“Security is only the IT team’s job.”	One click by anyone can start an attack. Everyone has a role.
“Antivirus is enough.”	Good security combines people, processes and several layers of technology.
“You need to be a coder to work in security.”	Many roles focus on analysis, risk, communication and governance.

Quick check

1. A hospital system goes offline during an attack. Which part of the CIA triad is affected?

2. An unpatched server is a threat, a vulnerability or a risk?

3. Which type of attacker is most often after money?

Answers are in the lesson article.

Key takeaways

- Cybersecurity protects people, information, systems and the services society relies on.
- Security has three goals: confidentiality, integrity and availability.
- Risk = how likely harm is × how bad it would be. Defenders lower it.

Next: Module 2 · How Attacks Work