

Introduction to Security

AP Cybersecurity ■ Unit 1

AP Cybersecurity



Introduction to Security

What we will cover

- 1 Social engineering
- 2 Password attacks & authentication
- 3 Adversaries & public networks
- 4 AI-based attacks
- 5 AI in cyber defence

1

Social engineering

The weakest part is the human

Social engineering 社会工程学 tricks people into breaking security. The **adversary** 对手 does not break the code – only the person.

The goal is **elicitation** 套取信息 – getting sensitive information out of someone without them realising.



Security key

Two feelings the adversary leans on

Intimidation 恐吓

a threatened bad result
– fear pushes you to act

Urgency 紧迫感

an invented deadline – when
rushed, we stop thinking



Security token

Worked example – naming the tactics

A phishing email

“Over 90% of staff have already verified their account – confirm yours in the next hour or lose payroll access.” Two tactics are stacked: “in the next hour” → **urgency**
“over 90% of staff have already” → **consensus**

Naming each tactic –
not just calling the email
“suspicious” – is exactly
what an exam answer
needs.

The impact on a victim

Personal details

name, address, pet, birthday – later used to answer **challenge questions** 安全问题 and **impersonate** 冒充 them

A one-time password 一次性密码

handed over – the adversary logs in as them

Malware 恶意软件

downloaded – it steals data from the browser

2 Passwords

Password attacks – the warning signs

In an online **password attack** 密码攻击 the adversary tries passwords against a **real** login page. The logs show it:

- many failed logins in a short time
- attempts at unusual hours
- attempts from unknown devices

Adversaries succeed because people choose **weak** 弱 passwords: a word + a two-digit year + a symbol (Summer24!), or a pet's name.

Those patterns are so common that a **dictionary** 字典 of likely passwords can be built from facts about you and tried automatically.

Making authentication stronger

Long, random, unique
a **password manager** 密码管理器 generates and stores them

No meaning
avoid names, dates and meaningful words

MFA 多因素身份验证
extra proof on top of the password

For “how would you make authentication stronger?”, MFA is almost always part of the answer – plus long, unique passwords from a manager.

3 Public networks

Know your adversary

Adversaries differ by skill:

Low-skilled – buy ready-made tools, reuse known **exploits** 漏洞利用

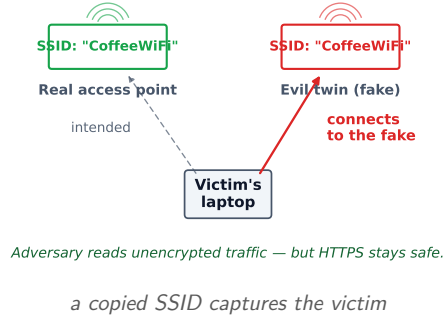
High-skilled – write their own tools, find brand-new **zero days** 零日漏洞

Their **motivation** 动机 varies too: greed, revenge, politics, or belief.

When ranking risks: high risk = high impact AND easy to exploit. A parking-lot Wi-Fi leak matters less than an open internal port.

Three wireless attacks

- **Evil twin** 双胞胎恶意热点 – a fake **access point** 接入点 copying the real **SSID** 服务集标识符
- **Jamming** 干扰攻击 – flooding the air so nobody can connect: a **denial of service** 拒绝服务
- **War driving** 战争驾驶 – driving around detecting networks and where signal leaks outside



Encryption still protects you on an evil twin: the adversary sees your traffic but cannot read HTTPS. Say what is exposed – not just “it’s unsafe”.

Protecting yourself on public networks

Check the network name matches exactly the one you intend to join

Prefer **en-crypted** 加密的 sites – HTTPS stays unreadable

Consider a **VPN** 虚拟专用网络 – it encrypts all traffic to the operator

4

AI

AI-based attacks

- a **deepfake** 深度伪造 avatar impersonates someone on a call
- **LLMs** 大语言模型 write **phishing** 钓鱼 emails in **perfect** language – removing the clumsy wording that once gave scams away
- back-end: prompts that pull secret data out of an LLM, **poisoning** training data, scanning for targets, writing malware

Defences: agree a **shared secret** 共享秘密 word with close contacts; enable MFA (a **cloned voice alone** cannot log in); never type sensitive data into a chatbot; double-check AI output against non-AI sources.

AI in cyber defence – the same tool, the other side

AI can review firewall rules and access settings and recommend safer options – though a human expert must always check before applying.

Its biggest advantage is scale: a medium network makes millions of events a day, far too many for people to read.



AI is dual-use: the same tool appears on both the attack and the defence side. Read the question carefully to see which side it asks about.

5

Recap

Unit 1 – key takeaways

1 Name the tactic

urgency, consensus, intimidation –
not just “suspicious”

2 Authentication

long, unique, from a manager –
plus MFA

3 Evil twin

a copied SSID; HTTPS still
cannot be read

4 AI is dual-use

the same tool attacks and defends
– which side is asked?

Check yourself

- 1 “Reply within the hour” – name the tactic.
- 2 On an evil twin, can the adversary read your HTTPS traffic?
- 3 What makes a risk HIGH?
- 4 Name one defence against a cloned-voice call.

Answers 1. urgency 2. no – it stays encrypted 3. high impact AND easy to exploit
4. a shared secret word, or MFA