

Introduction to Security

AP Cybersecurity ■ Unit 1

AP Cybersecurity



What we will cover

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

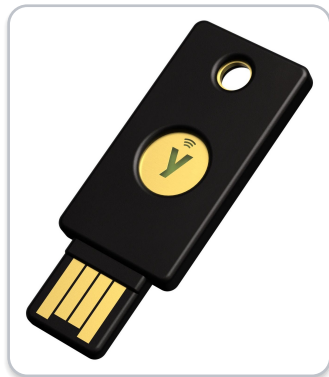
1

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.



A hardware key resists the phishing that tricks people

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



*One-time codes help, but people can still be talked
into sharing them*

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 **imperson-
ate** 冒充 them

A one-time pass- word 一次性密码

handed over – the ad-
versary 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.

Making an account hard to take

Multifactor authentication

Multifactor authentication (MFA) beats any password policy: the attacker needs the second factor as well.

One-time password

A **one-time password (OTP)** from an app is safer than one by SMS, which a SIM swap can intercept.

VPN

A **virtual private network (VPN)** encrypts traffic to its exit point – useful on an untrusted network, and no protection against a phishing page.

What is coming

Large language models (LLMs) write fluent phishing in any language, so the spelling mistakes people were taught to look for are gone.

A **denial of service (DoS)** attacks availability rather than secrecy – the third leg of the CIA triad, and the one most often forgotten.

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.

Identify the wireless mechanism

A school investigates three separate incidents. Choose the attack and cite the fact that supports your answer.

- A An unauthorised access point copies the school's network name. Students connect to it, and an adversary captures their traffic.
- B An adversary's transmitter emits a strong signal on the wireless network's frequency. Legitimate devices cannot communicate with the access point.
- C An adversary drives around the building recording network beacons and the locations where the signal reaches outside. No connection is made.

Which case imitates an identity, which denies access, and which gathers information?

Explain what the adversary is doing

A: Evil twin 双胞胎恶意热点. The fake **access point 接入点** copies the real **SSID 服务集标识符** to attract connections. Capturing traffic is the aim; copying a name does not make the device trustworthy.

B: Jamming 干扰攻击. Radio interference prevents legitimate wireless communication: a **denial of service 拒绝服务**. The evidence is the interfering transmitter, not an outage alone.

C: War driving 战争驾驶. The adversary maps wireless beacons and signal reach. Joining the network is not required. An authorised wireless survey can use similar observations; purpose and permission matter.

Does the right network name prove safety?

Two access points display the same school SSID. One is school-owned; the other belongs to an adversary. A student says:

“The name matches, so I know this is the school’s network. If I use HTTPS, nothing can go wrong.”

Identify the two overclaims. Explain what encrypted HTTPS protects, and name a separate step for checking which network to join.

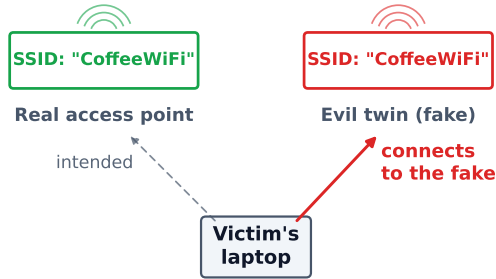
Separate identity, content and access

A matching name is a check, not proof. An evil twin can copy it. Use the school's trusted connection instructions and confirm uncertainties with staff through a separate trusted channel.

Valid encrypted HTTPS protects content in transit. Capturing that traffic does not reveal its plaintext. It does not establish ownership of the hotspot or guarantee that every destination is trustworthy.

A fake network can still interfere with access or direct users toward a phishing site. Read the scenario: identify what is protected and what risk remains.

Three wireless attacks, in detail



Captured valid HTTPS traffic keeps its content encrypted.
AP Cybersecurity · U1 · evil-twin attack: fake AP copies the real SSID

a copied SSID captures the victim

An evil-twin access point copies the real network's name so victims connect to the attacker

Protecting yourself on public networks

Check the exact network name; a match alone does not prove ownership

Use valid **en-crypted** 加密的 HTTPS; it protects content in transit

Consider a trusted **VPN** 虚拟专用网络: it protects traffic carried through its tunnel

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.

Suspicious Website Logins

A **password attack** 密码攻击 is any attempt to log in using guessed or stolen passwords.

- many failed logins in a short time,
- login attempts at unusual hours,
- login attempts from unknown devices.
- Create passwords that are **long, random, and unique** - a **password manager** 密码管理器 can generate and store them for you.

Understanding Social Engineering

Adversary's pressure tactics

**Intimidation
(threat of harm)**

**Urgency
(act now!)**

**Pretexting
(a fake reason)**

**Victim
acts before
thinking**

Harmful outcomes

**Reveals a password
or OTP**

Downloads malware

**Gives personal info
(impersonation)**

AP Cybersecurity · U1 · social engineering: pressure tactics -> victim action

Social engineering uses psychological pressure to make a victim act before they think

Exam tips

- When a question asks you to rank risks, remember **high risk = high impact AND easy to exploit**. A parking-lot Wi-Fi leak matters less than an **open internal port that lets an adversary spoof a device**.
- Learn the social-engineering tactics by name - **intimidation, urgency, pretexting, authority, consensus, scarcity, familiarity** - and be ready to spot which one an email is using.
- **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”.
- For “how to make authentication stronger”, **MFA** is almost always part of the answer, plus long/unique passwords from a manager.
- AI is **dual-use**: the same tool (LLMs, code analysis) appears on both the attack and the defense 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