

CYBER SECURITY AWARENESS

Building your Digital Shield: A Practical Guide to Personal Cybersecurity

Hong Kong Baptist University



Speaker

Jason Lee
PwC's Dark Lab
Cyber Threat Intelligence Lead

What we'll cover today

01 Understanding the threats targeting you

02 Your identity: spotting threats and protecting privacy

03 Accounts, devices and everyday hazards

04 Safeguarding your online presence

05 Key takeaways and call to action



01

Understanding the Threats Targeting You



The 2026 Cyber Threat Landscape

1

Logging in, not breaking in

Adversaries increasingly exploit credentials and session tokens to bypass defences.



2

Identity is the key battleground

Identity-centric attacks now take pole position across threat motivations.



4

AI accelerates the race

AI is used by both attackers and defenders to increase speed and scale.



How do these threats look like?

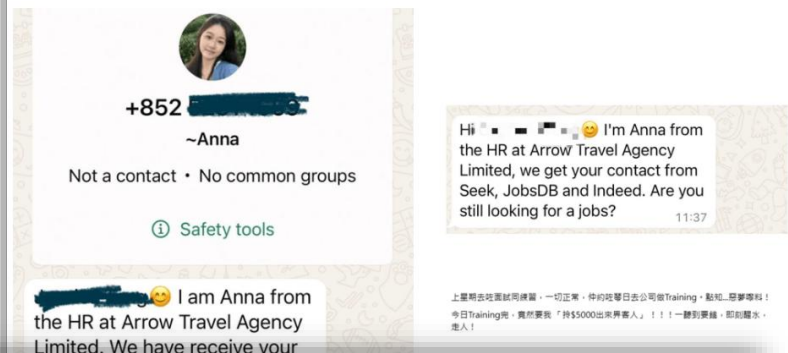
Fake Police Uniforms and Pretend Official Trap: Postgraduate Student Loses Over HK\$1 Million

2025-11-11



Student duped out of \$190,000 in English-language job scam

SOCIAL BUZZ 01-04-2026 13:40 HKT



Over 72,000 students and staff at Hong Kong educational institutions affected in Canvas hack

How do these threats look like?

Year of 2025 Ten Most Alarming Scams

Number of Cases

Total Losses (HKD)



Online Shopping Scam

12,505

\$395.1M



Online Investment Scam

5,135

\$3,583.5M



Impersonate Customer Service Scam

4,440

\$636.4M



Online Employment Fraud

4,095

\$880.8M



"Guess Who" Scam

2,048

\$132.5M

Year of 2025 Ten Most Alarming Scams

Number of Cases

Total Losses (HKD)



Advance Fee Fraud

1,811

\$148M



Compensated Dating Scam

1,122

\$50.2M



Online Romance Scam

1,093

\$469.3M



Phishing Scam

1,093

\$113.9M



Pretend Officials Scam

1,060

\$887.1M

Why attackers want your accounts and private data



Email

Lets them reset the password on every other account



Data

ID scans and photos let them impersonate you



Money

Cards and e-wallets they can drain directly



Trust

Your name used to scam others

Attackers do not break in. They log in.

How do cybercriminals target us?

THREAT 01

ClickFix



A fake “prove you are human” check asks you to paste and run a command — and you infect your own device.

THREAT 02

Smishing



A text posing as a courier, a bank or your boss. Read within minutes, on a screen that hides the real address.

THREAT 03

Quishing



A QR code is a link you cannot read. Filters often miss it, and it lands on your personal phone.

THREAT 04

MFA fatigue



Approval prompts you never requested, again and again, until you tap Approve to stop the noise.

THREAT 05

Email bombing



Thousands of sign-up emails at once, burying the one real alert about a password or payment change.

THREAT 06

Stolen logins



Password-stealing software empties your saved passwords — and the cookies that keep you signed in.

THREAT 07

Invoice fraud



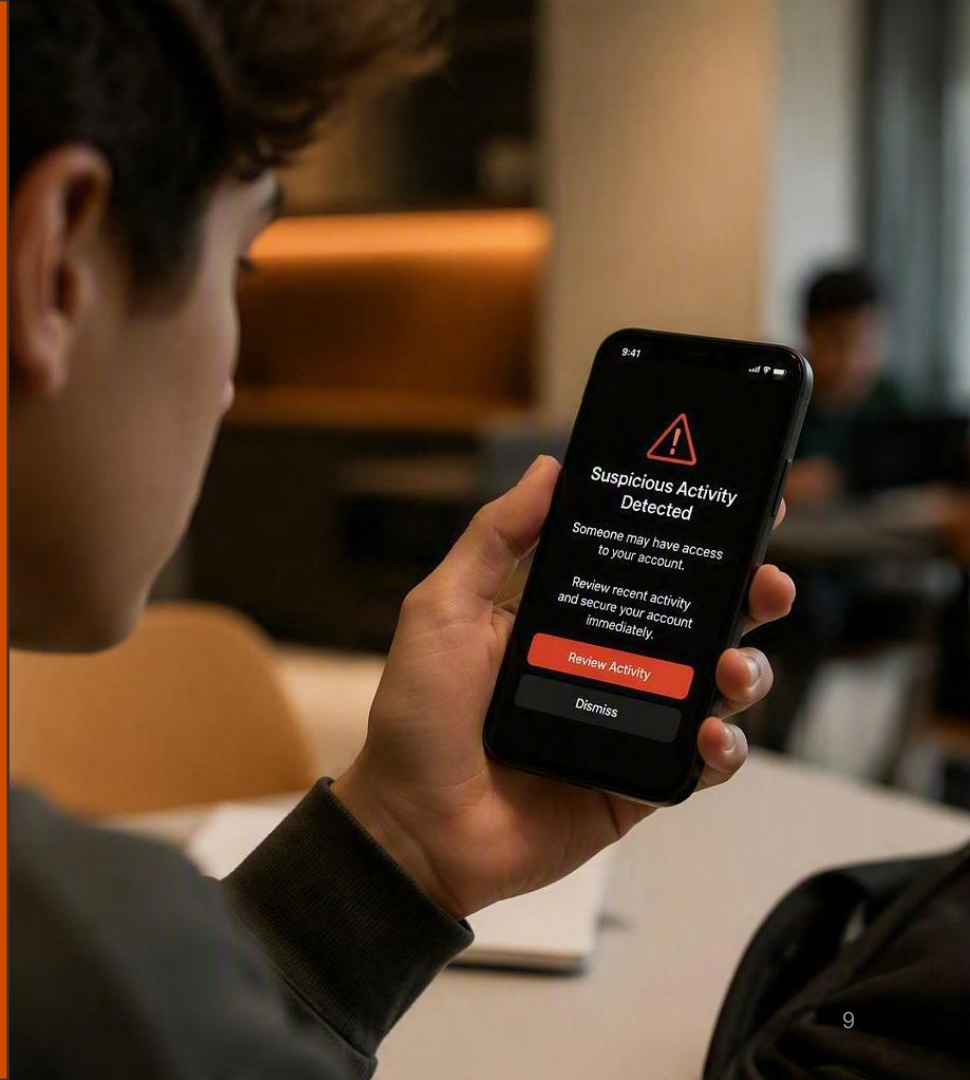
No malware. Just a convincing message about money — changed bank details, an urgent supplier payment.

All seven rely on the same thing: one hurried moment of trust. Slow down, verify through a channel you already know, and report it.

02

Protecting Your Identity

Red flags • Privacy habits • Social media settings

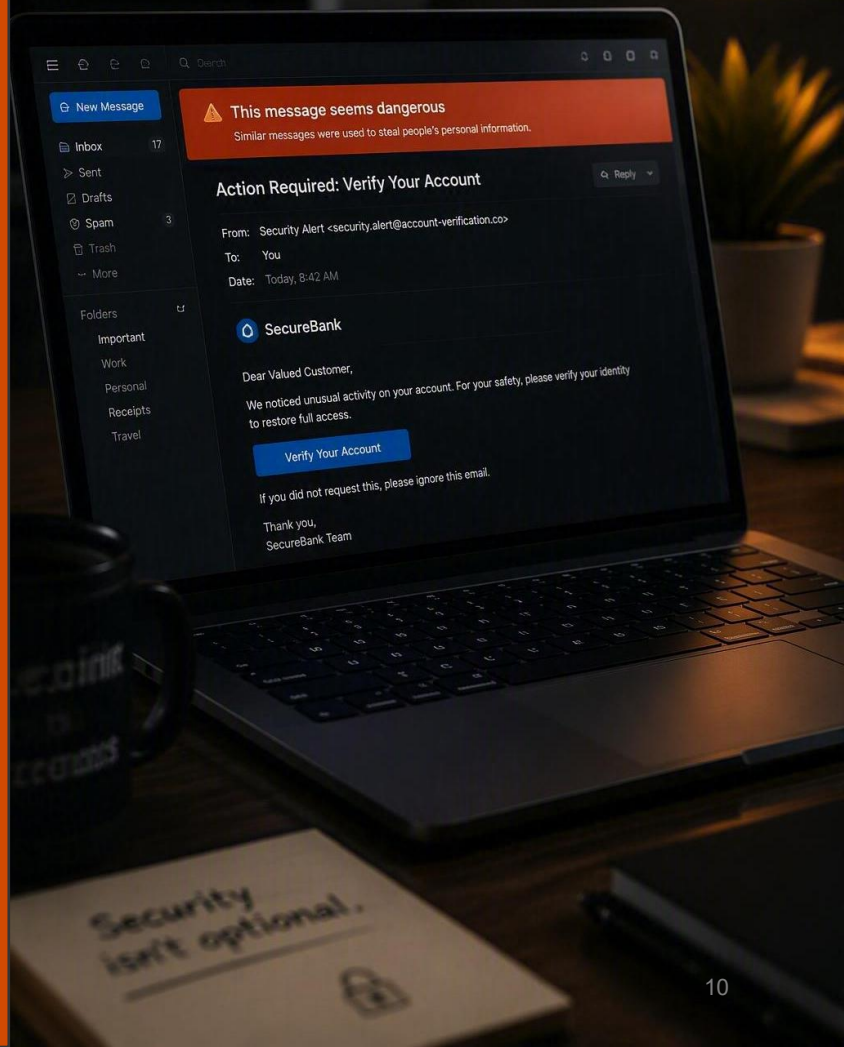


SPOTTING THREATS

Red flags in your inbox or instant messages

- Urgency and threats
- Sender address does not match the name
- Links and attachments you never asked for
- Requests for codes, money or gift cards

More to be shared later, hence this section is intentionally shortened!





SPOTTING THREATS

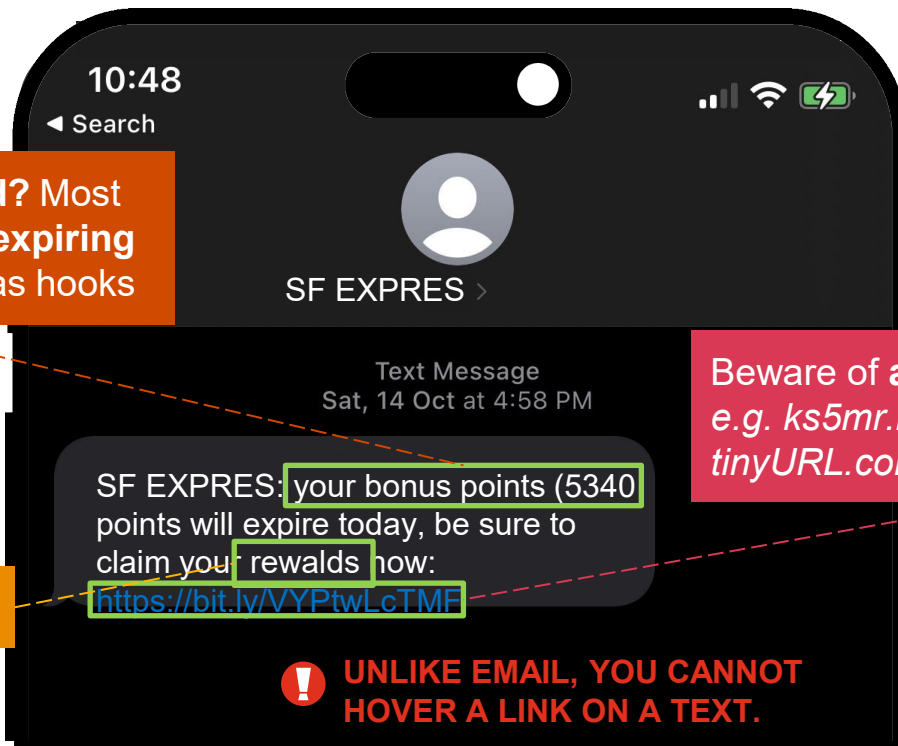
Fake calls, texts and websites

- Parcel, refund and wrong-number messages
- Callers posing as police, banks or customs

Deepfaked voices are cheap. Verify another way.

Spotting a Smishing Message

Is this an expected award? Most scammers use gift card, expiring rewards, unpaid fines...as hooks



Beware of any shortened link.
e.g. *ks5mr.info*, *bit.ly*, *goo.gl*, *ow.ly*,
tinyURL.com, *t.co*...

Alert! Spelling errors



**UNLIKE EMAIL, YOU CANNOT
HOVER A LINK ON A TEXT.**

Did you receive any of these recently?

【中銀生活】閣下嘅中銀賬戶生活體驗會員即將到期，截止今日收取2131HKD。如有疑問請致電：[23338391](tel:23338391)

系統檢測到您賬戶出現安全風險，請立即前往wotas-app.com進行安全認證，否則賬號將失去訪問/使用權限

Wednesday 1 Jul • 12:24 pm

Sending with [SmarTone HK](#)

Sender can't accept replies. Contact them directly. [Learn more](#)

扣款通知：你嘅「滴滴安全險」續保合約已經生效，每月將會扣款 HKD4,290。如果需要取消服務，請務必聯絡官方線上客服：2572-9980。

Wednesday 1 Jul • 12:24 pm

Sending with [SmarTone HK](#)

Sender can't accept replies. Contact them directly. [Learn more](#)

【HKAlipay】閣下螞蟻保險協議簽訂成功，即日開始按年扣21,600HKD。取消請聯絡：2237-9525避免畀你帶嚟困擾！

16:11

Sender can't accept replies. Contact them directly. [Learn more](#)

Express

⋮

Unread

Tuesday 28 Jul • 5:49 pm

【順豐速運】您好！您包裹就快到喇。請盡快聯絡順豐隊員預約擺件或者安排放邊度：2652-4879

Monday 3 Aug • 11:26 am

【順豐速運】您好！您包裹就快到喇。請盡快聯絡順豐隊員：2652-4882 預約擺件或者安排放邊度。

Friday 7 Aug • 2:16 pm

【順豐速運】您好，您的包裹就快到喇。請盡快致電 2652-4298 聯繫，預約安排司機您的派送時間。

2:16 pm

Sender can't accept replies. Contact them directly. [Learn more](#)

A QR code is a link you cannot read



Check the sticker

Fake codes get pasted over real ones



Preview the link

Read the full domain before opening



Never log in or pay

Open your own app instead



Codes in email

A code asking you to re-verify is phishing

Quishing bypasses email link filtering entirely.

QR CODE SAFETY – SPOTTING THREATS

Spotting a QR Code Phishing

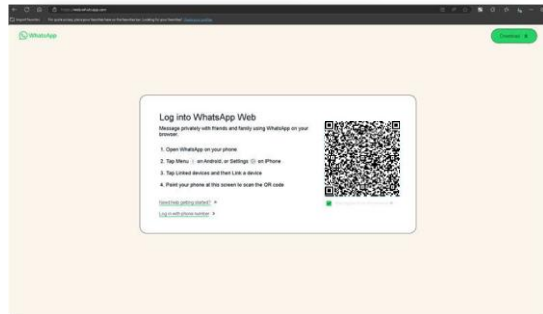
ATTACKER'S BROWSER:

1. Attacker opens legitimate WhatsApp Web login page
2. Attacker enables EvilQR browser extension to dynamically display latest QR code on phishing page



VICTIM'S BROWSER:

3. Unsuspecting Victim visits attacker-controlled phishing page mimicking the WhatsApp Web login page



4. Victim scans QR code, authenticating attacker to login to the victim's WhatsApp account



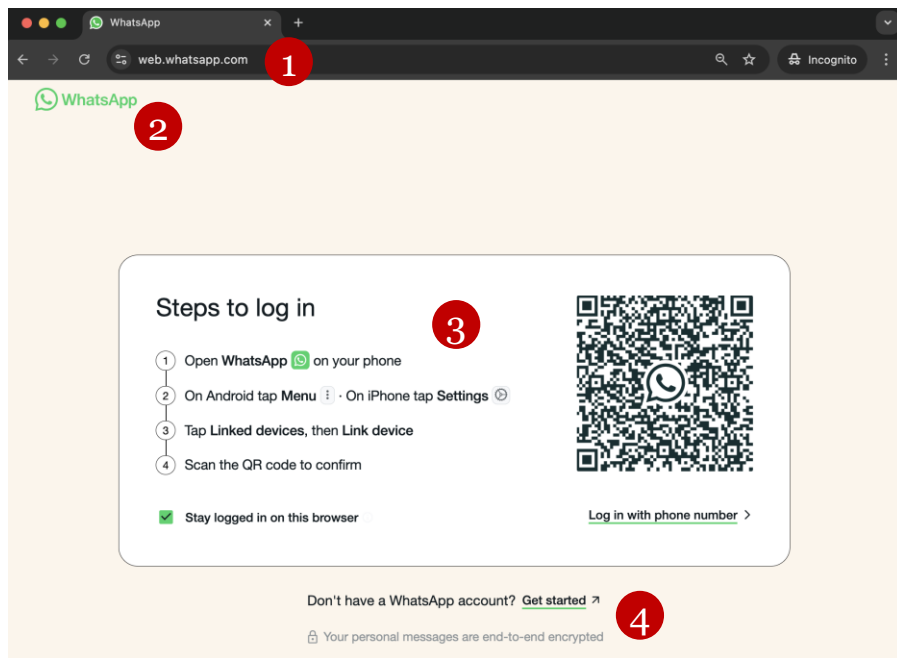
5. Attacker gains full access to victim's WhatsApp

Threat actors create fake website interfaces that look similar to original WhatsApp web interface, and trick user to scan the QR code on the forged website.



Spotting a QR Code Phishing

LEGITIMATE



There are **four (4) differentiators**:

1. If you were to **check the URL** of the phishing page, you would immediately notice it is suspicious and unlikely to be the actual WhatsApp login page.
2. On the legitimate webpage, the **WhatsApp logo and name exist**, which is not observed on the malicious page.
3. **The instruction wordings** differ.
4. The legitimate webpage has **a 'Tutorial' section with advice on 'how to get started'**. It should be noted that whilst this phishing domain does not display this section, other more convincing phishing sites could include this section to further deceive you into trusting their phishing site is legitimate.

Recognising Spam Calls

Hello, this is **Ben from the Immigration Department**. There's some issue with your recent appointment. I'll need your **full name and Date of birth ("DOB") and Identity Cards Number** for your identity verification.



Oh, really? My name is Amy Smith and my date of birth is January 16th, 1980. My Identity Cards Number is Z890934(2).



How to tell if the caller is a scammer?

- **Contacted out of the blue** by a stranger.
- Caller asks for **sensitive details**, such as your personal information, online banking credentials, one-time passwords (OTP)
- The incoming number **contains "+852", "+81", "+1", "+44" etc. telephone country codes prefix**. This means they **originate from overseas** and **"spoofed"**.
- Caller makes claims such as **"law enforcement officer", "compromised accounts", "overdue tax payment"**, to drown you in fear etc.
- The caller makes an **offer that sounds too good** to be true — such as "guaranteed" credit or debt relief.

A uniform on a video call — and the deepfake era ahead

01

The call

A postgraduate finance student in Hong Kong takes a call from an unknown Mainland number: a phone line registered in his name is linked to a fraud case.

02

The uniform

He is put through to the “Xiamen Municipal Public Security Bureau”. On video, the officer displays a police uniform and an officer ID number.

03

The transfers

Told to cooperate with the investigation, he makes repeated transfers to a designated account for “fund verification”.

04

The loss

More than HK\$1 million is gone. Police logged 1,711 scam cases involving university students to September, losing HK\$180 million.

This one needed only a police uniform. Deepfakes can now fake the face and the voice as well.

Why it worked — and why it would work here

Fear switched off his judgement

Being told you are named in a criminal case is terrifying. Panic makes people comply first and think later.

A uniform looked like proof

A uniform, an officer ID number and a live video call are all props. Anyone can buy or fake every one of them.

“Confidential” kept him alone

Told the investigation was secret, he spoke to no one — removing the one thing that stops this: a second opinion.

THE LESSON WE TAKE FROM IT

No real police force asks you to transfer money to prove your innocence. Hang up, check the number yourself, and call the HKPF anti-deception hotline 18222.

Your defence against deep fakes and scams over the phone



Verify on a second channel

If a request arrives by call, verify by message. If by message, verify by call — always using contact details you already have.



Agree a code word

With your family. A word an attacker cannot know, for the moment you need certainty.



Treat urgency as the signal

Rushing you is the one thing every attack must do. When you feel pressure to act now, that is the moment to slow down.



Never break the process

Payments, bank details, password resets and access requests follow the same steps, no matter who is asking.



Assume your voice is copyable

Anything you have said publicly can be cloned. That is not a reason to hide — it is a reason to verify.



Report, don't resolve

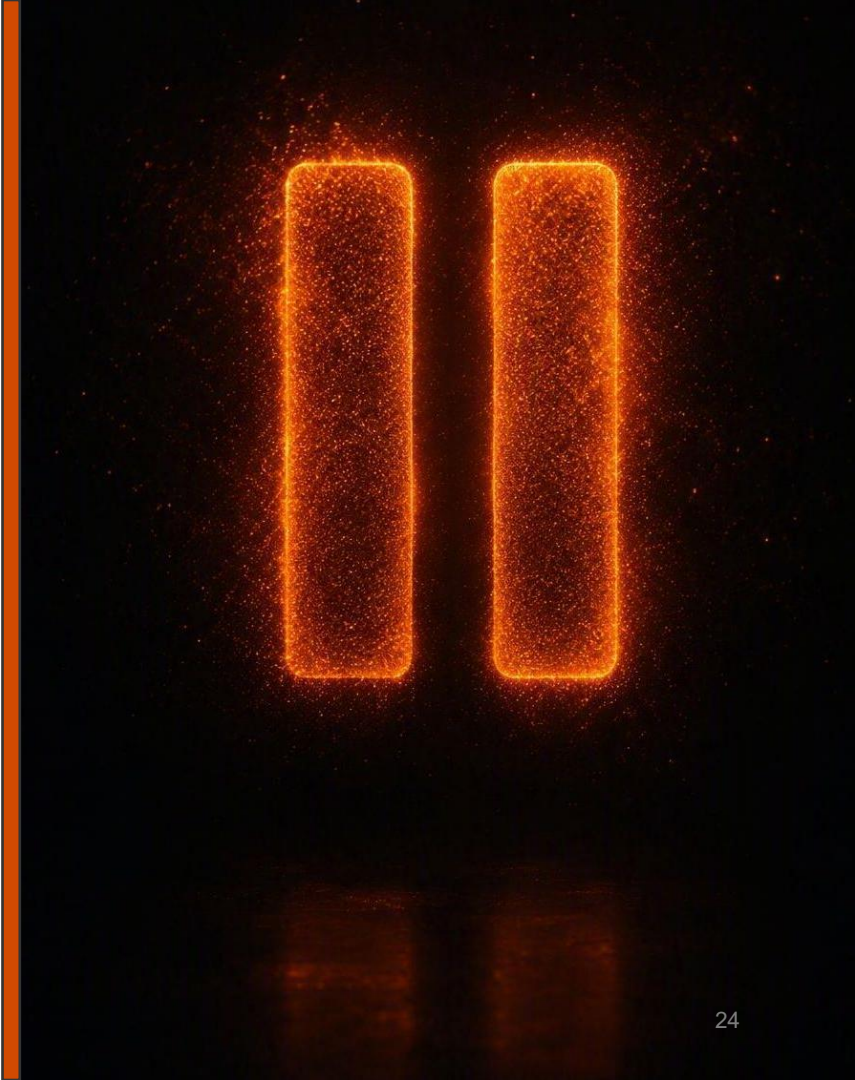
You are not expected to work out whether it was AI. You are only expected to raise it.

YOUR THREE-SECOND HABIT

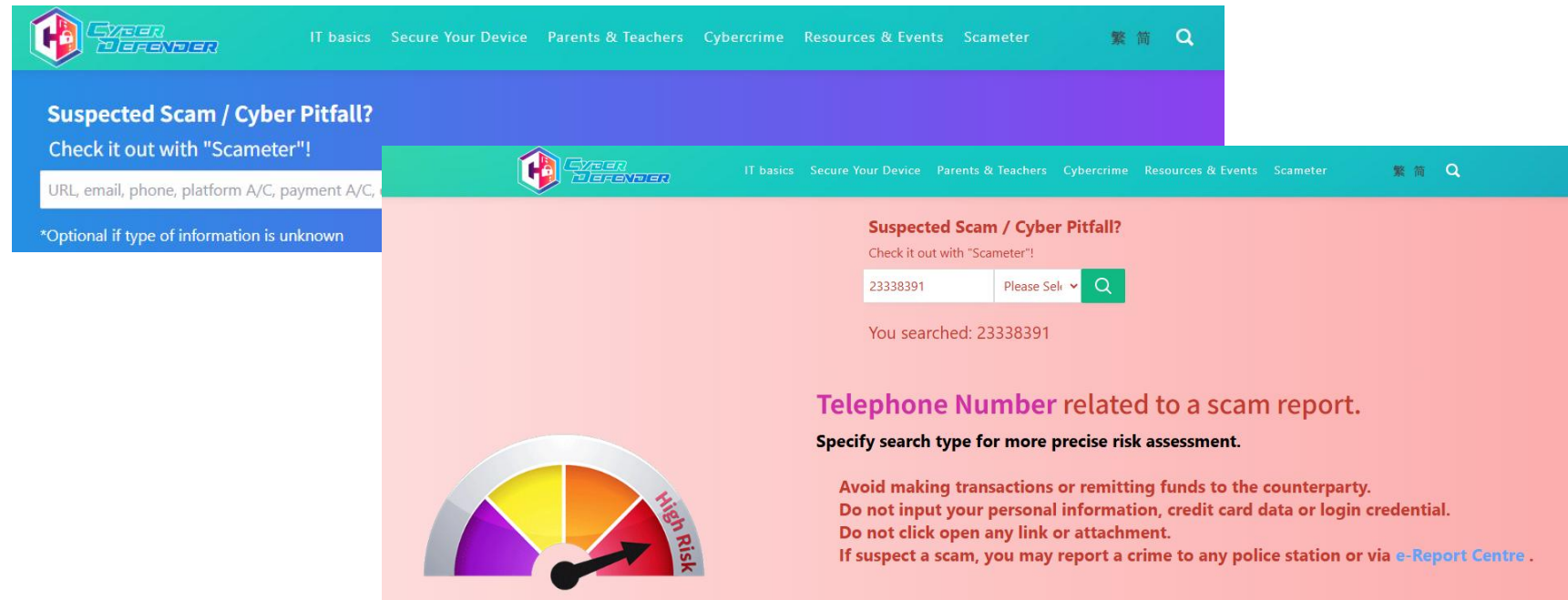
Stop. Think. Verify.

-
- STOP — urgency is the attacker's tool
 - THINK — was I expecting this?
 - VERIFY — use a number you already have

In doubt? Ask the IT Service Desk.



How can you check if you think it is a scam?



The screenshot displays the CyberDefender website's 'Suspected Scam / Cyber Pitfall?' section. The page features a teal header with navigation links: IT basics, Secure Your Device, Parents & Teachers, Cybercrime, Resources & Events, and Scameter. A search icon and language toggle (繁 簡) are also present. The main content area has a purple header with the title 'Suspected Scam / Cyber Pitfall?' and the instruction 'Check it out with "Scameter"!'. Below this is a search form with a text input field containing '23338391', a dropdown menu labeled 'Please Sel...', and a green search button. The results show 'You searched: 23338391'. A large, semi-circular risk gauge is positioned on the left, with segments in purple, yellow, orange, and red. The needle points to the red segment, which is labeled 'High Risk'. To the right of the gauge, the text 'Telephone Number related to a scam report.' is displayed in purple. Below this, a bold instruction reads 'Specify search type for more precise risk assessment.' A list of warnings follows: 'Avoid making transactions or remitting funds to the counterparty.', 'Do not input your personal information, credit card data or login credential.', 'Do not click open any link or attachment.', and 'If suspect a scam, you may report a crime to any police station or via e-Report Centre .'. The URL 'https://cyberdefender.hk/en-us/' is shown at the bottom.

Suspected Scam / Cyber Pitfall?
Check it out with "Scameter"!

URL, email, phone, platform A/C, payment A/C,
*Optional if type of information is unknown

Suspected Scam / Cyber Pitfall?
Check it out with "Scameter"!

23338391 Please Sel. 🔍

You searched: 23338391

Telephone Number related to a scam report.
Specify search type for more precise risk assessment.

Avoid making transactions or remitting funds to the counterparty.
Do not input your personal information, credit card data or login credential.
Do not click open any link or attachment.
If suspect a scam, you may report a crime to any police station or via [e-Report Centre](#) .

<https://cyberdefender.hk/en-us/>

03

Securing Accounts and Devices

Passwords • MFA • Password managers • Devices



ACCOUNT SECURITY

Strong and unique passwords

- Avoid using passwords that are easy to guess
- Aim for 15 characters or more
- Never reuse your HKBU password
- Do not share your password with anyone

Reuse is what makes stolen passwords dangerous.

Check if your password is weak at
<https://howsecureismypassword.net/>

HOW SECURE IS MY PASSWORD?

.....

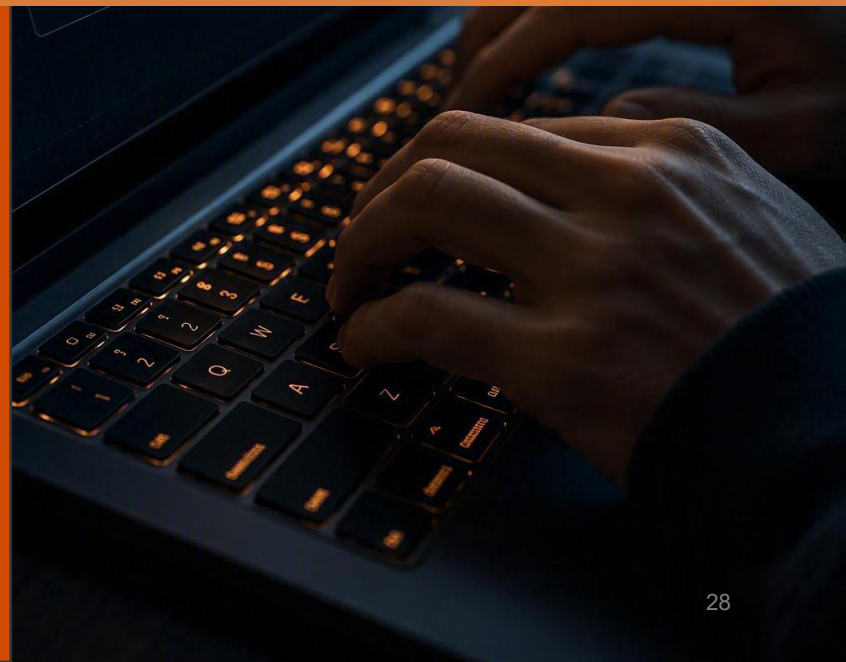
It would take a computer about

2 THOUSAND YEARS

to crack your password

Why not create even stronger passwords with [Dashlane](#)? It's free!

[Tweet Your Result](#)



Common Password Mutations Attacks

1. Password Repetition

E.g. Companyname2021!

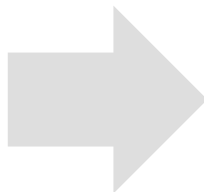
2. Password Mutation

E.g. Companyname2011!

3. Personal information

E.g. johnchan@yourcompanydomain.hk

4. Common Passwords



Hacker

Companyname2021! Companyname2021!

Companyname2011!, Companyname2012!...etc

john2021, johnchan2021, johnchanabcd1234! ..etc

qwertyuiop, covid2019, password ..etc



ACCOUNT SECURITY

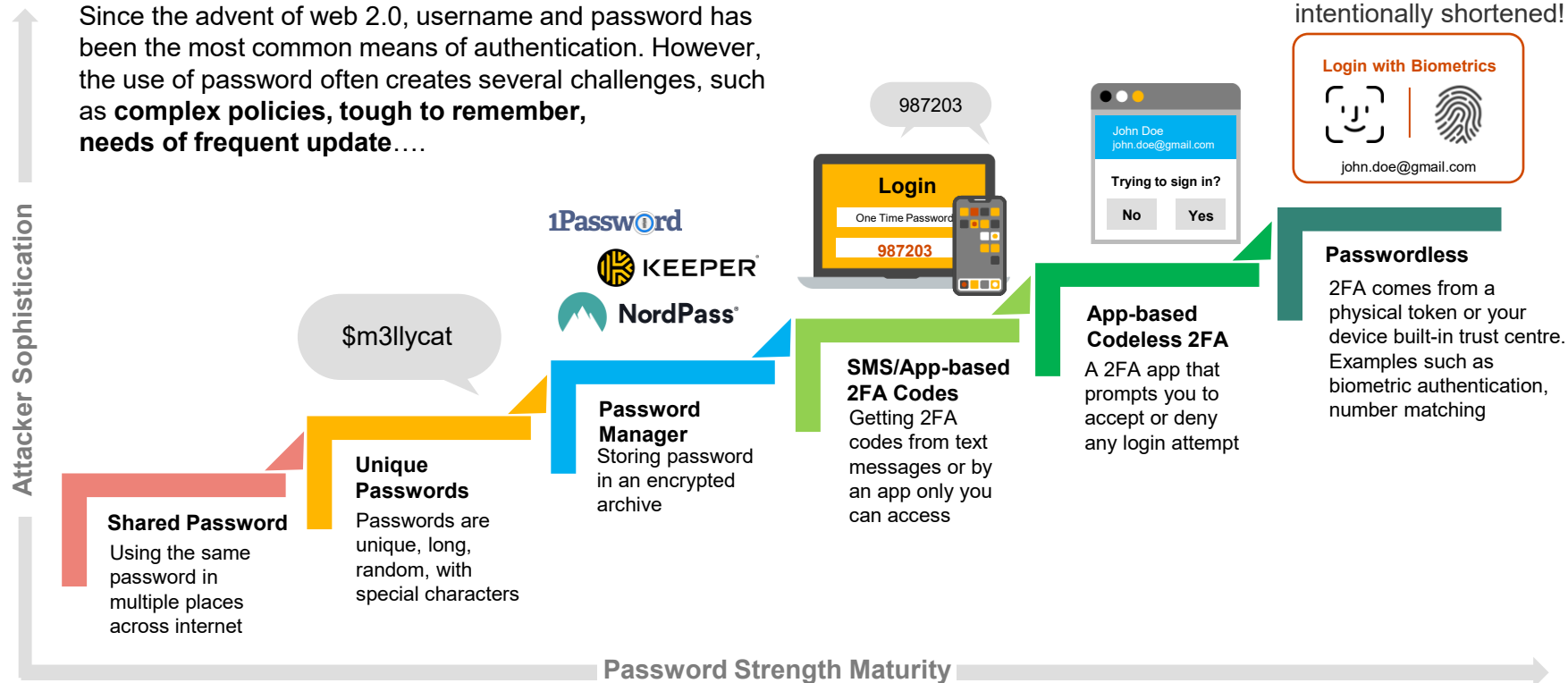
Turn on MFA everywhere

-
- Best: passkeys and hardware keys
 - Good: an authenticator app
 - Last resort: SMS codes
 - Never approve a prompt you did not trigger

A stolen password alone is no longer enough.

Embrace Modern Authentication

Since the advent of web 2.0, username and password has been the most common means of authentication. However, the use of password often creates several challenges, such as **complex policies, tough to remember, needs of frequent update....**



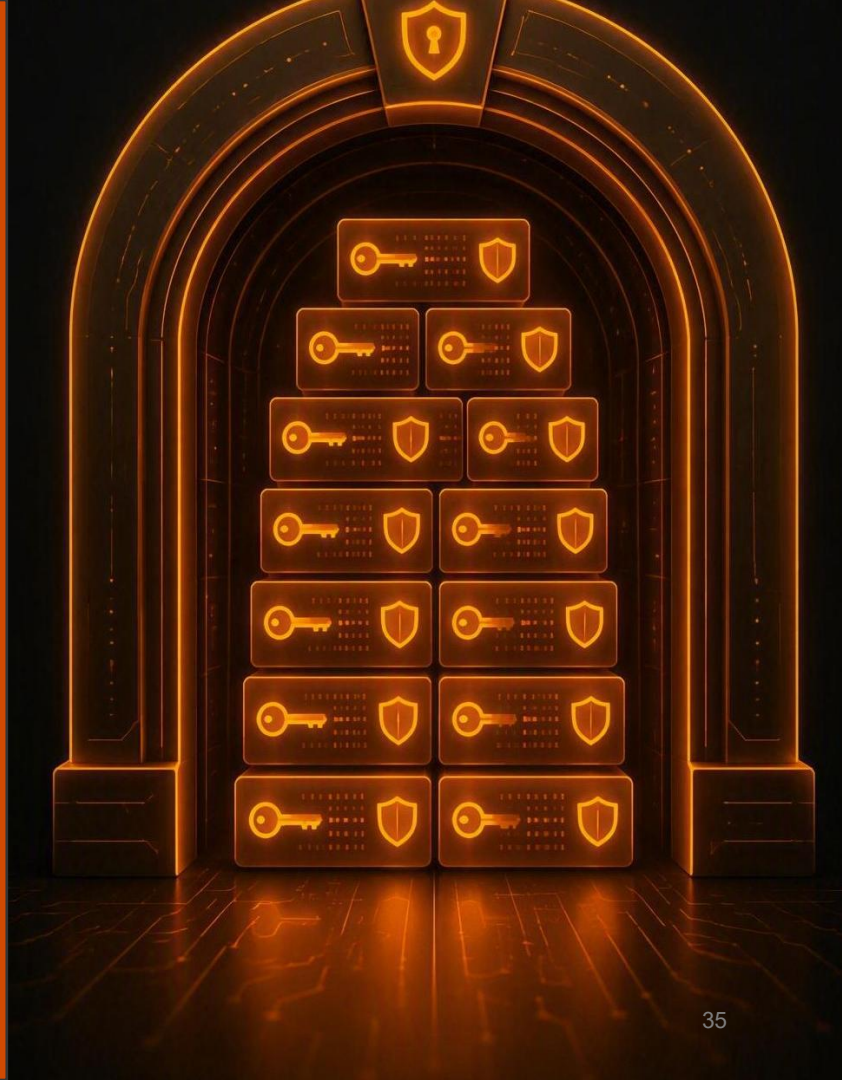
More to be shared later, hence this section is intentionally shortened!

ACCOUNT SECURITY

Use a password manager

- Pick a reputable manager
- Memorise one strong master passphrase
- Protect the vault with MFA
- Start with email, banking and HKBU

Nobody can remember fifty passphrases.





DEVICE SECURITY

Keep your device updated and secure

- Automatic updates on, everywhere
- Full-disk encryption on laptops and phones
- Six digits or more, plus biometrics
- Set up remote find and wipe today

Most attacks exploit flaws patched months ago.

DEVICE SECURITY

Do not jailbreak or root

- App sandboxing disappears
- Security updates stop arriving
- Banking and campus apps refuse to run
- Jailbreak tools are a malware route

Check second-hand devices before you use them.



Four checks before you download an app



Official store

No APK files from chat groups, links or QR codes



Developer

Follow the store link from the brand's site



Reviews

Few installs or copied reviews?
Walk away



Permissions

Read what it wants; a torch needs no contacts

Sideloaded turns your phone into the attacker's device.



PUBLIC WI-FI

Free Wi-Fi is never free

-
- Evil-twin hotspots copy real network names
 - Turn off auto-connect
 - A VPN encrypts, but does not stop phishing
 - Free VPNs often sell your browsing data

04

Safeguarding your Online Presence





PRIVACY PROTECTION

Shrink your digital footprint

- Search for yourself, then clean up
- Never post IDs, tickets or live location
- Revoke apps you no longer use
- Assume every post is permanent

Check haveibeenpwned.com for your accounts.

Lock down your social platforms

Instagram

- Private account
- No location tags
- Hide activity

Facebook

- Privacy Checkup
- Limit past posts
- No search indexing

WhatsApp and WeChat

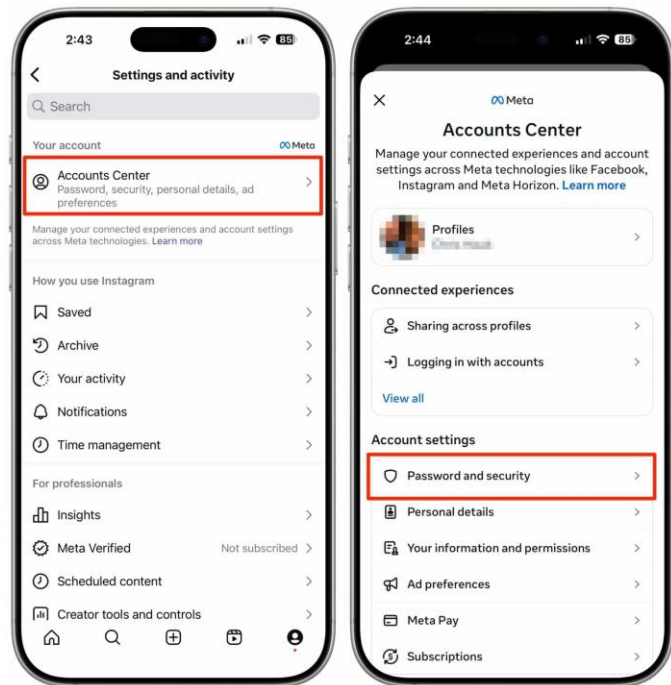
- Contacts only
- Two-step login
- Limit group adds

LinkedIn and X

- Hide connections
- Hide contact details
- Mute activity feed

Everywhere: turn on login alerts and remove old devices. Setup MFA.

Instagram: recommended privacy settings



Account Center > Password and Security

- Two-factor Authentication
- Turn on alerts for new logins and check “Where you’re logged in”
- Regularly perform ‘Security Checkup’

Account Center > Story, live and location

- Location sharing – disable Instagram map

05

Takeaways and Call to Action



Five things to do today

01

Turn on MFA wherever possible

02

Install a password manager; do not use weak passwords

03

Update your devices

04

Run a social media privacy check

05

Stop. Think. Verify.

OUR COMMUNITY

Security is shared

-
- Protect yourself first
 - Pass it on to friends and family
 - Report early — no penalty for a false alarm

No control can protect an account you give away.





Thank you

Any Questions?

Report anything suspicious to the HKBU IT Service Desk.

An abstract graphic on the right side of the slide, consisting of a network of orange dots connected by thin orange lines, resembling a molecular structure or a data network, set against a dark background.