17/10/2025

IT Security Seminar 2025

A Brief Overview of IT Security Insight and Trends of 2025.

Nathan Man & Percy Cheung
October 2025

Digital Security
Progress. Protected.

Agenda

- ➢Phishing and Social Engineering
- ➢Password Security and Management
- ➢Mobile Devices and Security
- ➢IoT Security
- ➢Cloud Service and Security
- ➢Security Impact of AI

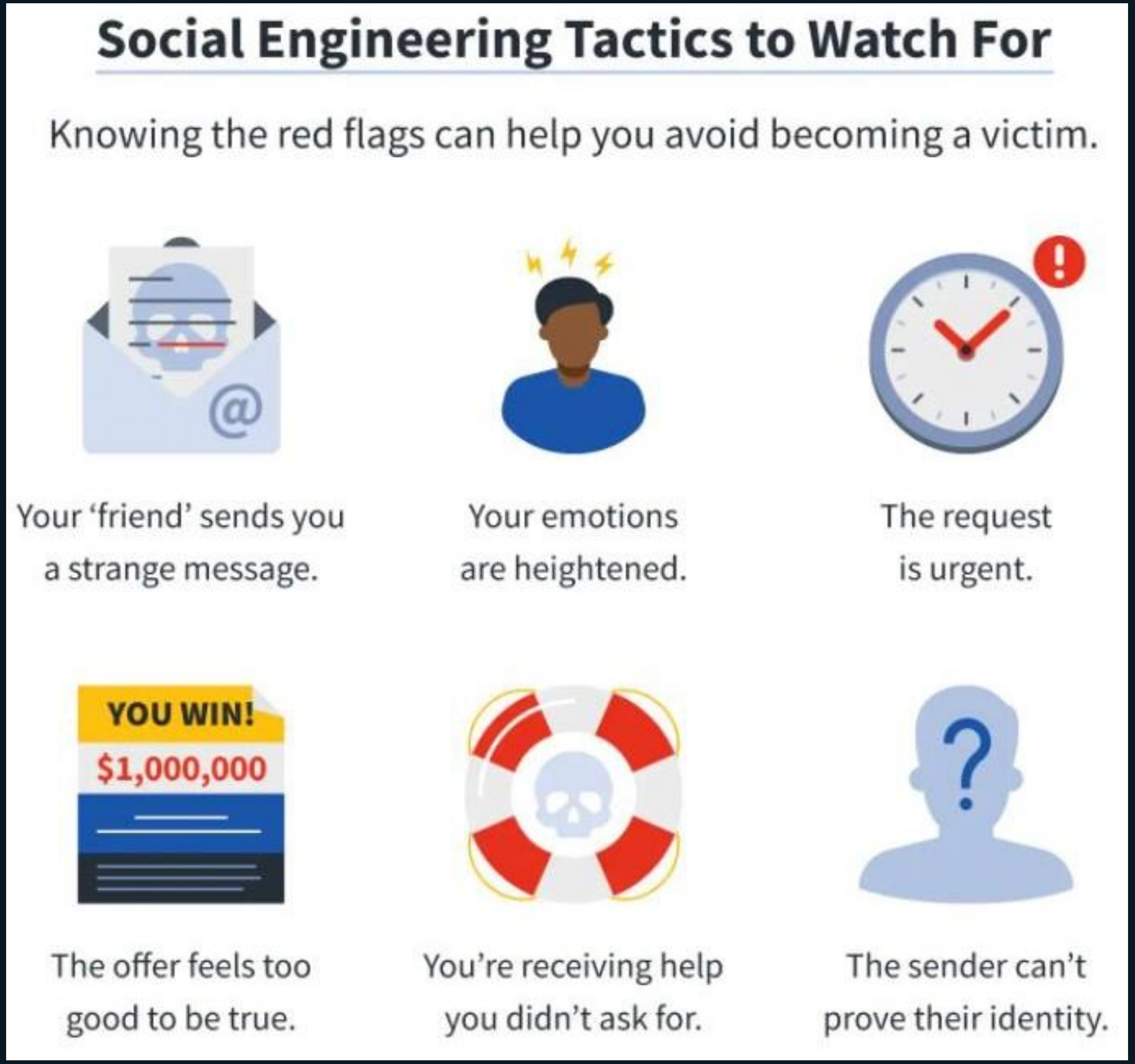
Phishing and Social Engineering

Digital Security
Progress. Protected.

What is Social Engineering?

- A **manipulation technique** that exploits **human psychology** to gain confidential information

- It targets the **human factor** by leveraging emotions like **trust, fear, or urgency.**



Social Engineering Tactics to Watch For

Knowing the red flags can help you avoid becoming a victim.

Your 'friend' sends you a strange message.

Your emotions are heightened.

The request is urgent.

The offer feels too good to be true.

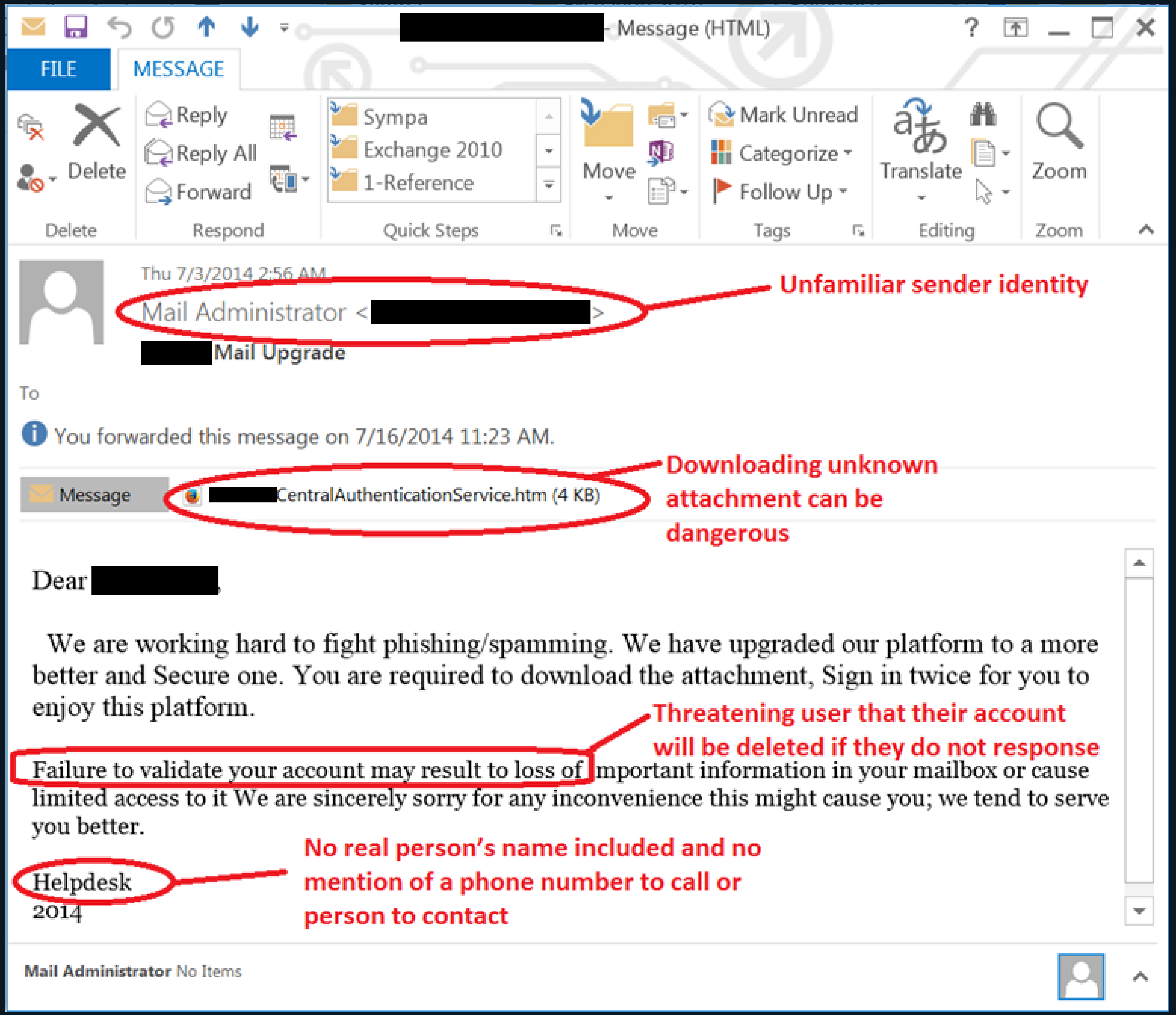
You're receiving help you didn't ask for.

The sender can't prove their identity.

How to Spot Engineering

- **Unexpected Requests:** Be wary of unsolicited requests for sensitive information or unusual actions.

- **Urgency or Pressure:** Watch out for situations that demand an immediate response orask you to bypasssecurity measures.



Thu 7/3/2014 2:56 AM

Mail Administrator <[redacted]>

[redacted]Mail Upgrade

To

You forwarded this message on 7/16/2014 11:23 AM.

[redacted]CentralAuthenticationService.htm (4 KB)

Dear [redacted],

We are working hard to fight phishing/spamming. We have upgraded our platform to a more better and Secure one. You are required to download the attachment, Sign in twice for you to enjoy this platform.

Failure to validate your account may result to loss of important information in your mailbox or cause limited access to it We are sincerely sorry for any inconvenience this might cause you; we tend to serve you better.

Helpdesk
2014

Mail Administrator No Items

Unfamiliar sender identity

Downloading unknown attachment can be dangerous

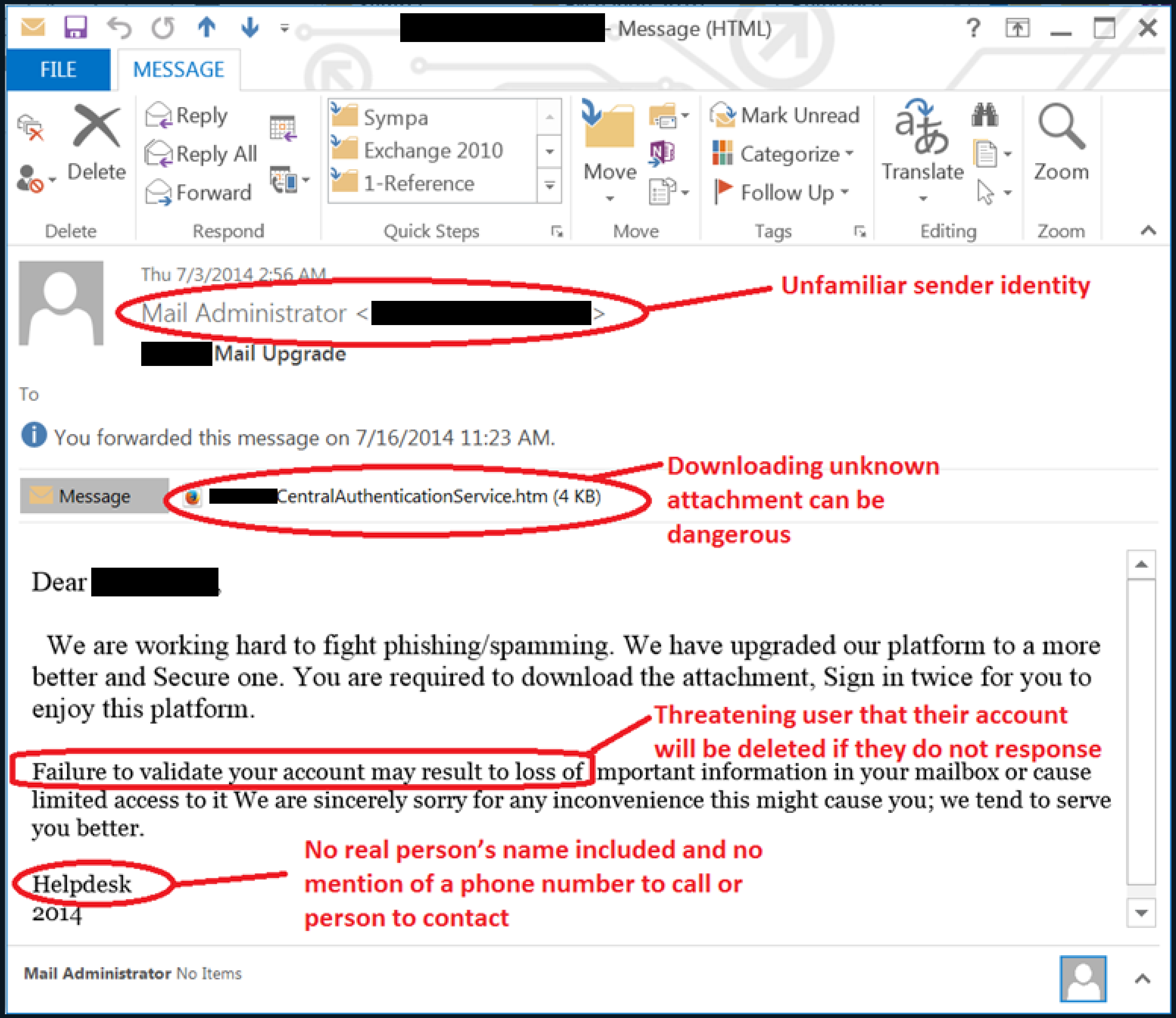
Threatening user that their account will be deleted if they do not response

No real person’s name included and no mention of a phone number to call or person to contact

How to Spot Engineering

- **Suspicious Communication:** Look for messages from unknown sources, unusual email addresses, or those with grammar errors.

- **Trust Your Instincts:** If something feels off or **too good to be true**, it likely is.



[redacted] - Message (HTML)

Thu 7/3/2014 2:56 AM

Mail Administrator <[redacted]>

[redacted] Mail Upgrade

To

You forwarded this message on 7/16/2014 11:23 AM.

[redacted]CentralAuthenticationService.htm (4 KB)

Dear [redacted],

We are working hard to fight phishing/spamming. We have upgraded our platform to a more better and Secure one. You are required to download the attachment, Sign in twice for you to enjoy this platform.

Failure to validate your account may result to loss of important information in your mailbox or cause limited access to it We are sincerely sorry for any inconvenience this might cause you; we tend to serve you better.

Helpdesk
2014

Unfamiliar sender identity

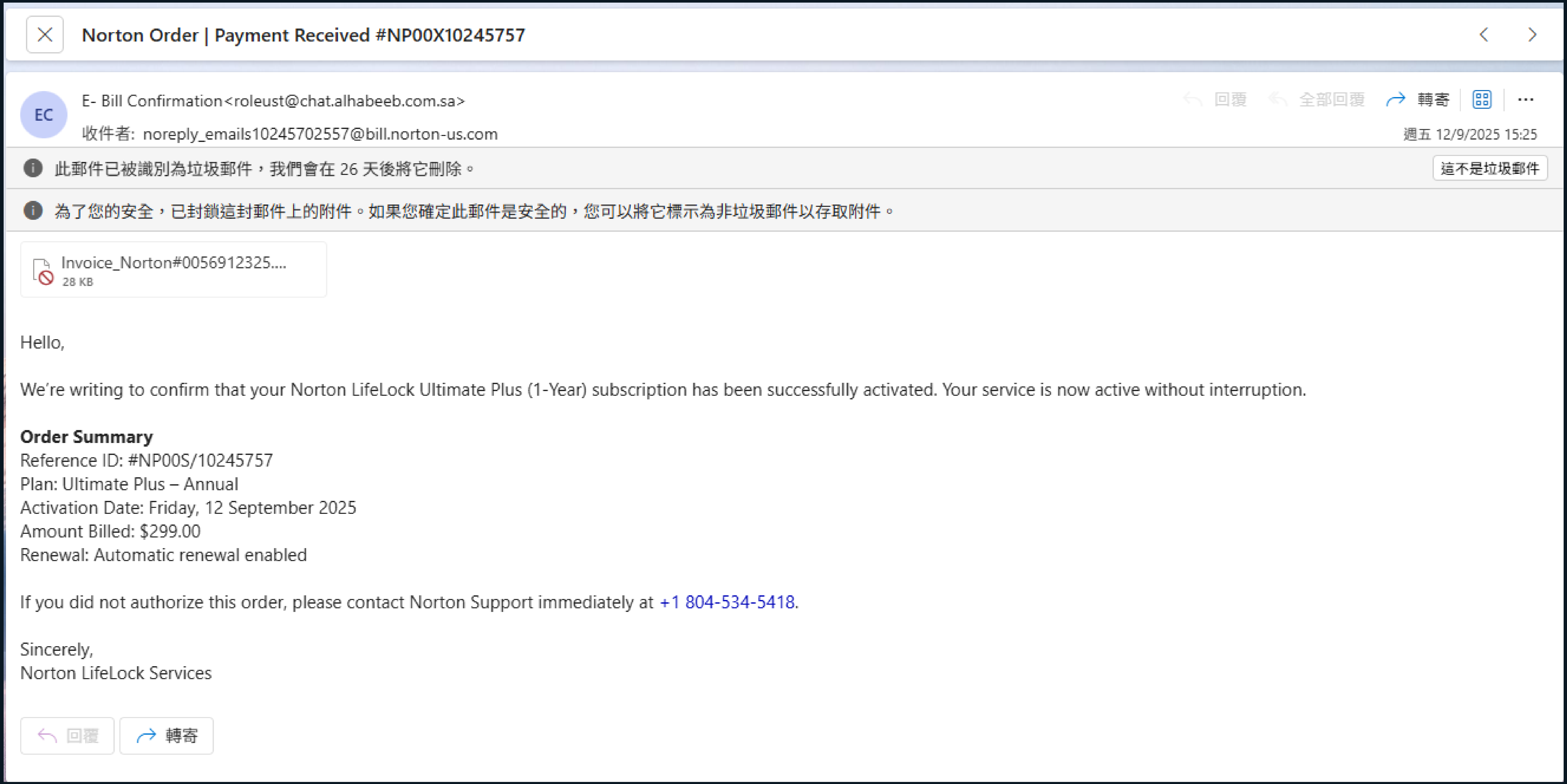
Downloading unknown attachment can be dangerous

Threatening user that their account will be deleted if they do not response

No real person's name included and no mention of a phone number to call or person to contact

Case Studies

By **Email:**



Norton Order | Payment Received #NP00X10245757

E- Bill Confirmation<roleust@chat.alhabeeb.com.sa>

收件者: noreply_emails10245702557@bill.norton-us.com

週五 12/9/2025 15:25

此郵件已被識別為垃圾郵件，我們會在 26 天後將它刪除。

為了您的安全，已封鎖這封郵件上的附件。如果您確定此郵件是安全的，您可以將它標示為非垃圾郵件以存取附件。

Invoice_Norton#0056912325....
28 KB

Hello,

We’re writing to confirm that your Norton LifeLock Ultimate Plus (1-Year) subscription has been successfully activated. Your service is now active without interruption.

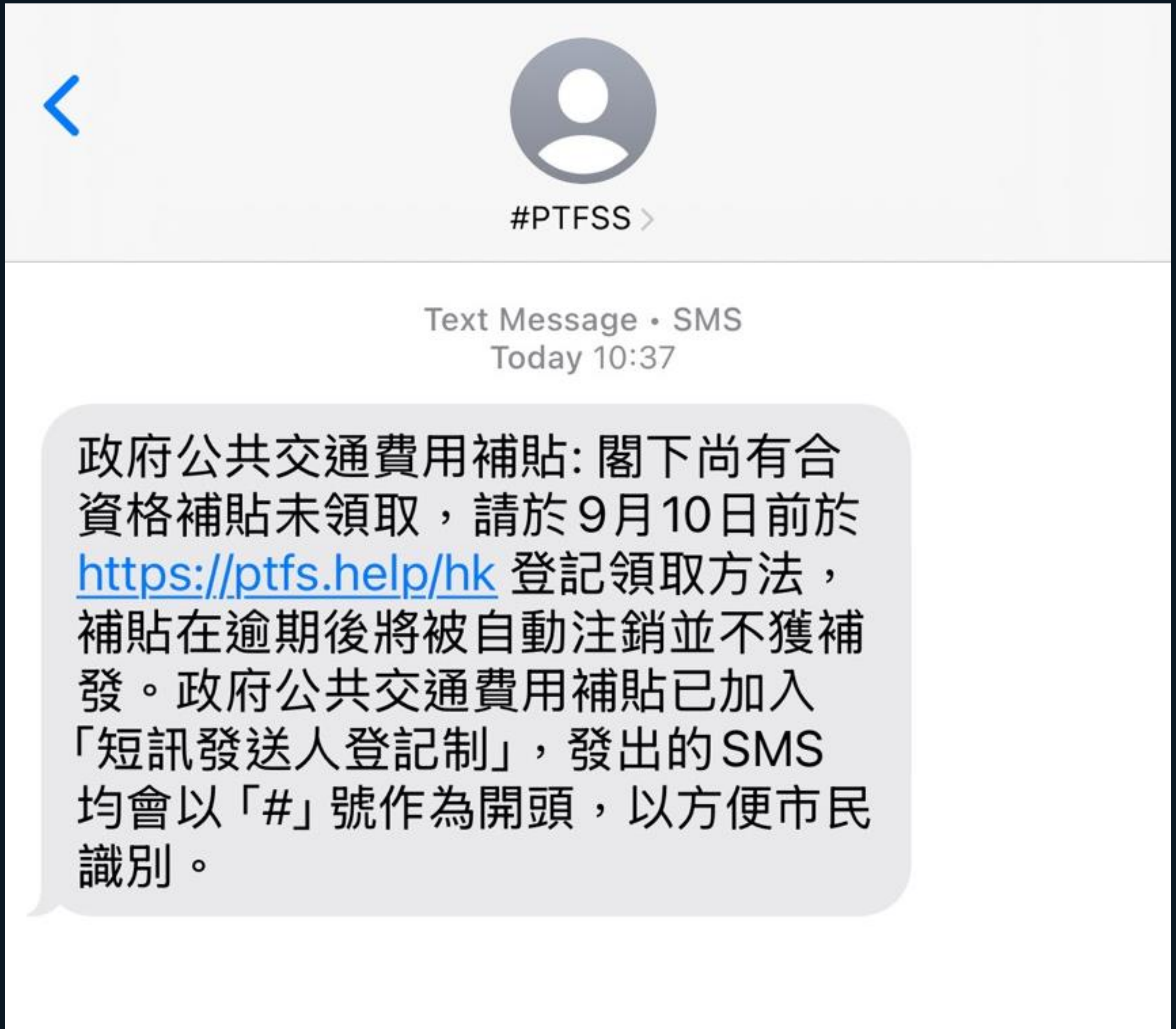
Order Summary
Reference ID: #NP00S/10245757
Plan: Ultimate Plus – Annual
Activation Date: Friday, 12 September 2025
Amount Billed: $299.00
Renewal: Automatic renewal enabled

If you did not authorize this order, please contact Norton Support immediately at +1 804-534-5418.

Sincerely,
Norton LifeLock Services

Case Studies

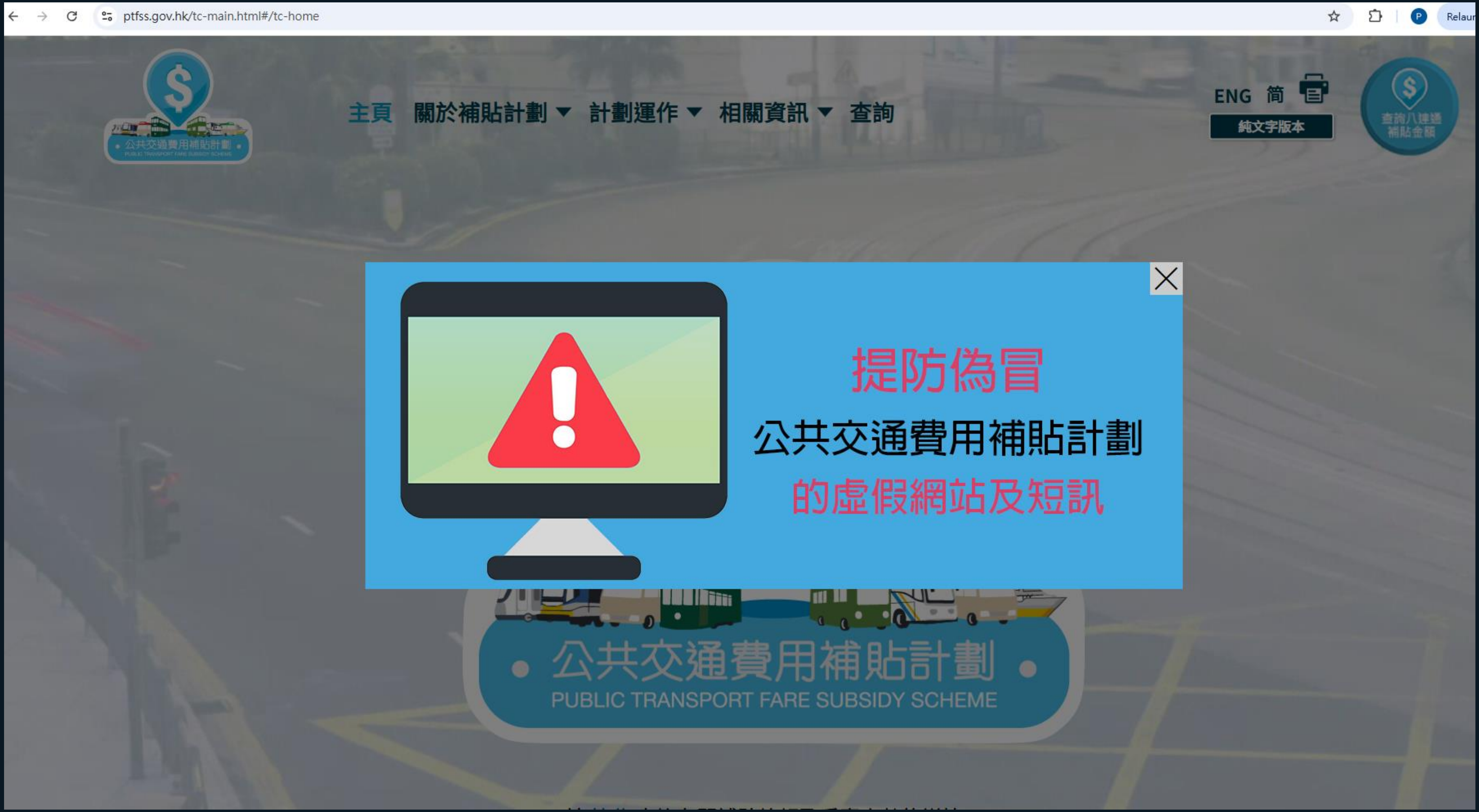
By **SMS**:



Text Message • SMS
Today 10:37

政府公共交通費用補貼: 閣下尚有合資格補貼未領取，請於9月10日前於https://ptfs.help/hk 登記領取方法，補貼在逾期後將被自動注銷並不獲補發。政府公共交通費用補貼已加入「短訊發送人登記制」，發出的SMS均會以「#」號作為開頭，以方便市民識別。

Case Studies



ptfss.gov.hk/tc-main.html#/tc-home

提防偽冒

公共交通費用補貼計劃

的虛假網站及短訊

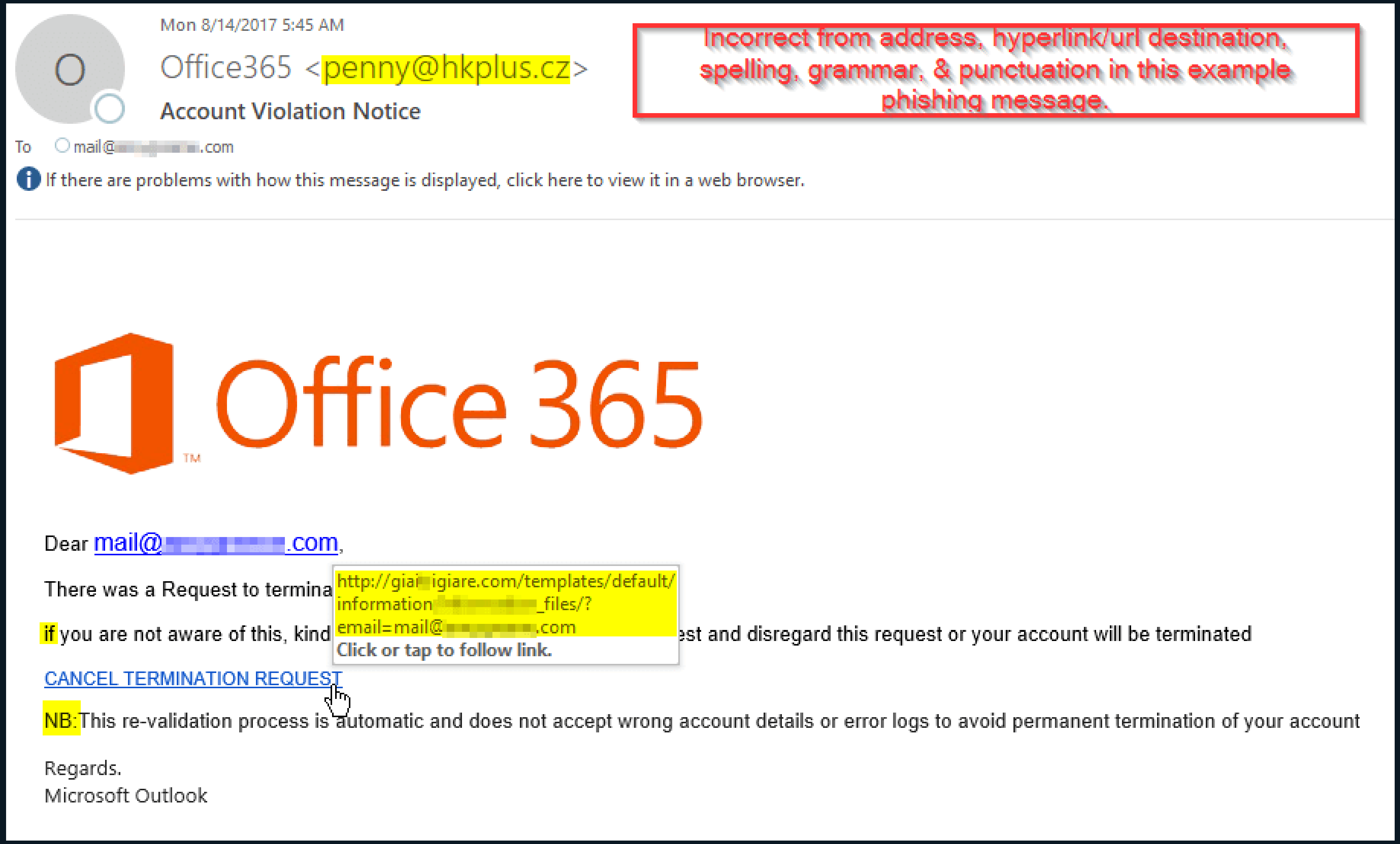
What is Phishing?

- A specific type of **social engineering** attack designed to deceive individuals into providing sensitive information.

- Common forms include **email phishing, SMS phishing (smishing),** and **voice phishing (vishing).**

Example of Phishing

Phishing email



Mon 8/14/2017 5:45 AM

Office365 <penny@hkplus.cz>

Account Violation Notice

To ○ mail@[redacted].com

If there are problems with how this message is displayed, click here to view it in a web browser.

Incorrect from address, hyperlink/url destination, spelling, grammar, & punctuation in this example phishing message.

Office 365

Dear mail@[redacted].com,

There was a Request to termina

http://giai[redacted]igiare.com/templates/default/information[redacted]_files/?email=mail@[redacted].com
Click or tap to follow link.

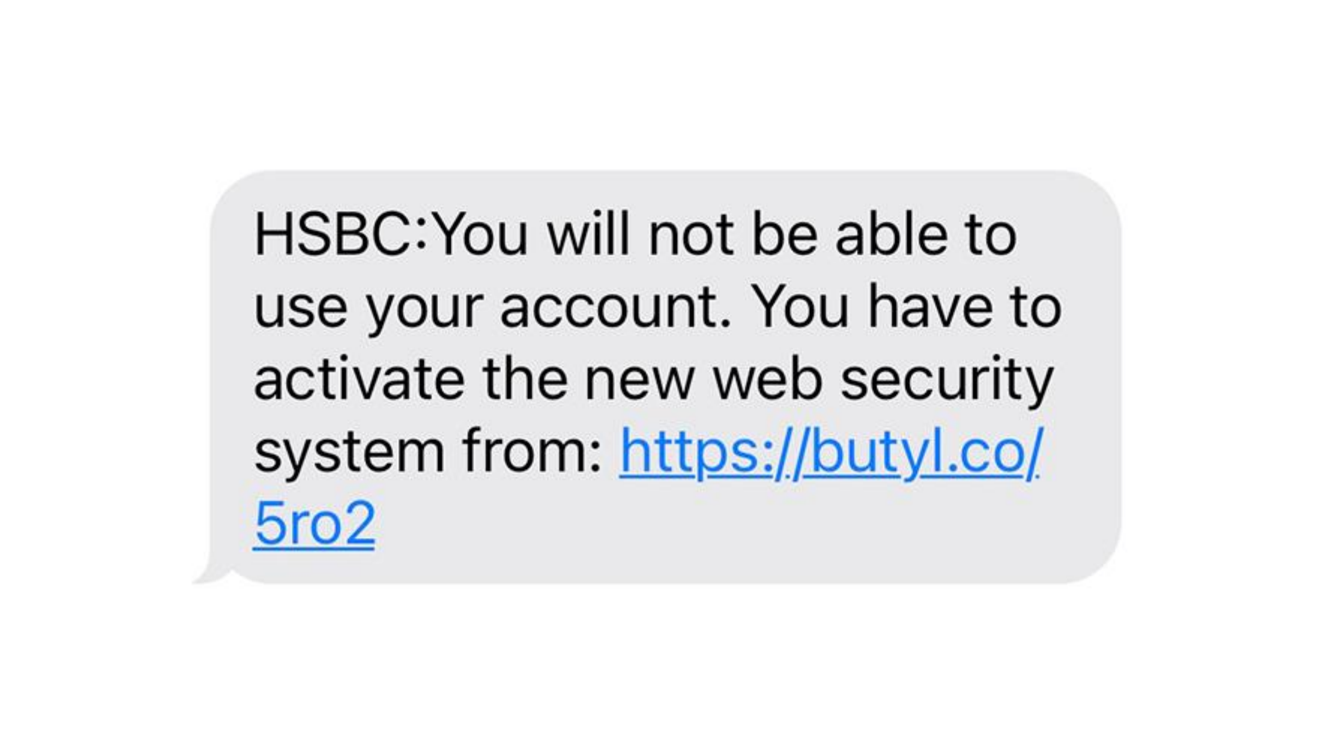
if you are not aware of this, kind est and disregard this request or your account will be terminated

CANCEL TERMINATION REQUEST

NB:This re-validation process is automatic and does not accept wrong account details or error logs to avoid permanent termination of your account

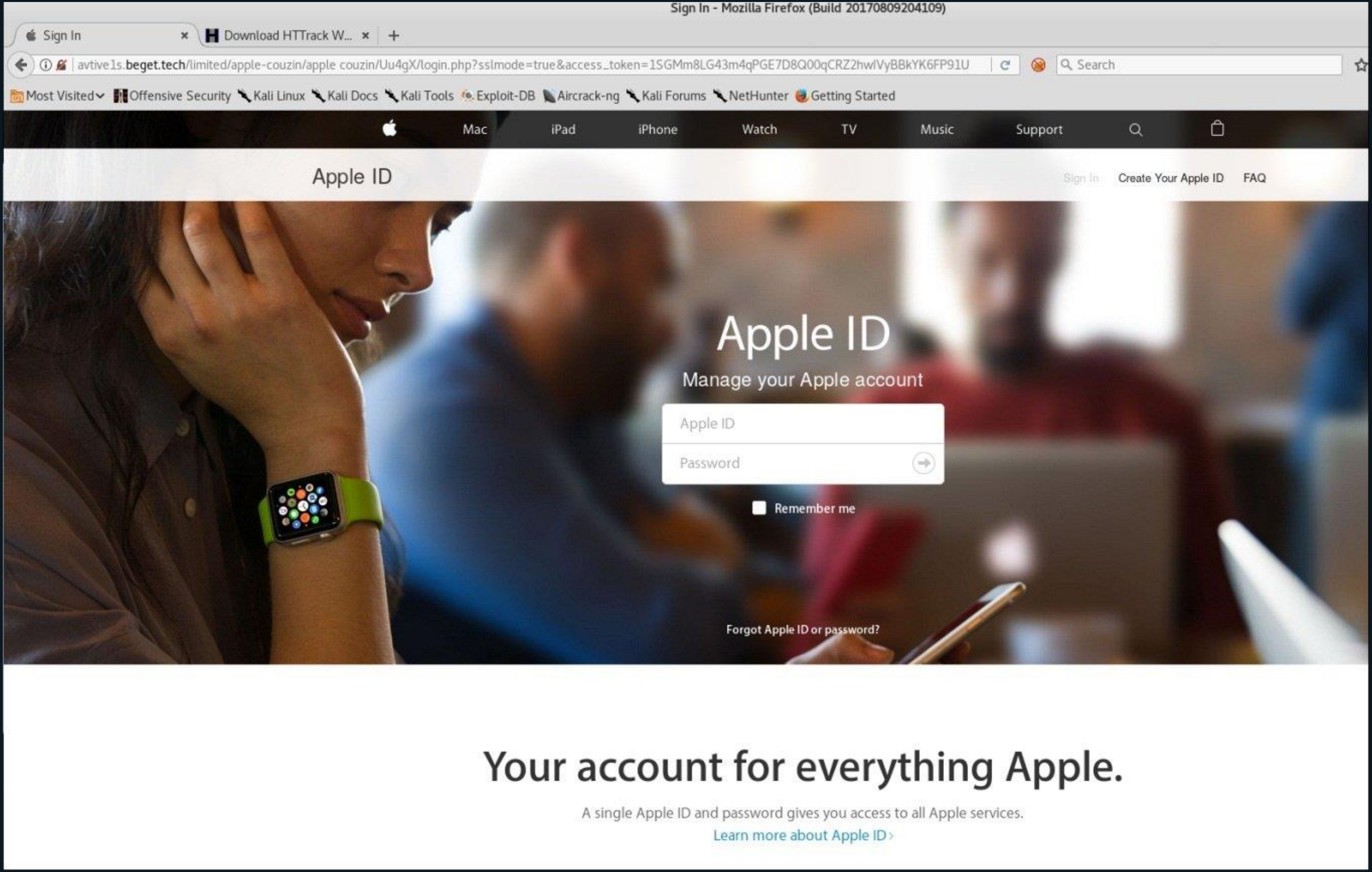
Regards.
Microsoft Outlook

Phishing SMS



HSBC:You will not be able to use your account. You have to activate the new web security system from: https://butyl.co/5ro2

Example of Phishing



Sign In - Mozilla Firefox (Build 20170809204109)

avtive1s.beget.tech/limited/apple-couzin/apple couzin/Uu4gX/login.php?sslmode=true&access_token=1SGMm8LG43m4qPGE7D8Q00qCRZ2hwlVyBBkYK6FP91U

Apple ID

Manage your Apple account

Your account for everything Apple.

A single Apple ID and password gives you access to all Apple services.

Learn more about Apple ID ›

How to Preventing Phishing?

- ✓ **Be skeptical** of unsolicited messages that request personal information.
- ✓ **Verify the sender's identity** through official channels instead of clicking links.
- ✓ **Check URLs** by hovering over links to see their actual destination. , and ensure that websites are secure (look for HTTPS) before entering sensitive information.
- ✓ **Enable two-factor authentication (2FA)** for added security

Password Security and Management

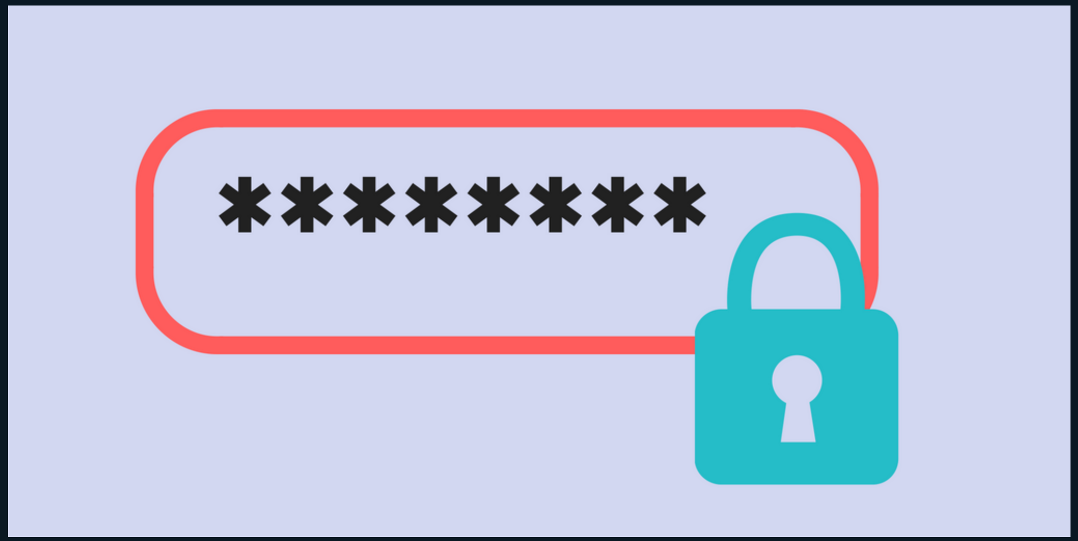
Digital Security
Progress. Protected.

What Makes a Strong Password?

- A secret string of characters used to authenticate a user’s identity.

- Its effectiveness depends on its **complexity and uniqueness.**

- A Strong password should combine **uppercase and lowercase letters, numbers, and special characters.**



Risk of using Weak Passwords

- Increase the risk **of hacking and unauthorized access.**

- Make **identity theft** more likely.

- **Reusing passwords** across multiple accounts creates major vulnerabilities.

- Using weak passwords may lead to legal and compliance issues.

12345678
PxH1#n!8

2025’s worst passwords

Rank	Password	Time to crake it
1	123456	< 1 Second
2	password	< 1 Second
3	123456789	< 1 Second
4	qwerty	<1 Second
5	abc123	< 1 Second
6	111111	< 1 Second
7	12345678	< 1 Second
8	letmein	< 1 Second
9	admin	<1 Second
10	welcome	< 1 Second

Source: NordPass

Characteristics of Weak Passwords

- Based on personal information: Passwords that include your name, pet's name, birthdate, or a family member's name are easy to guess. For example, "john1985" is a weak password.

- Short length: Passwords that are fewer than 8-12 characters long are easier for hackers to crack using automated tools.

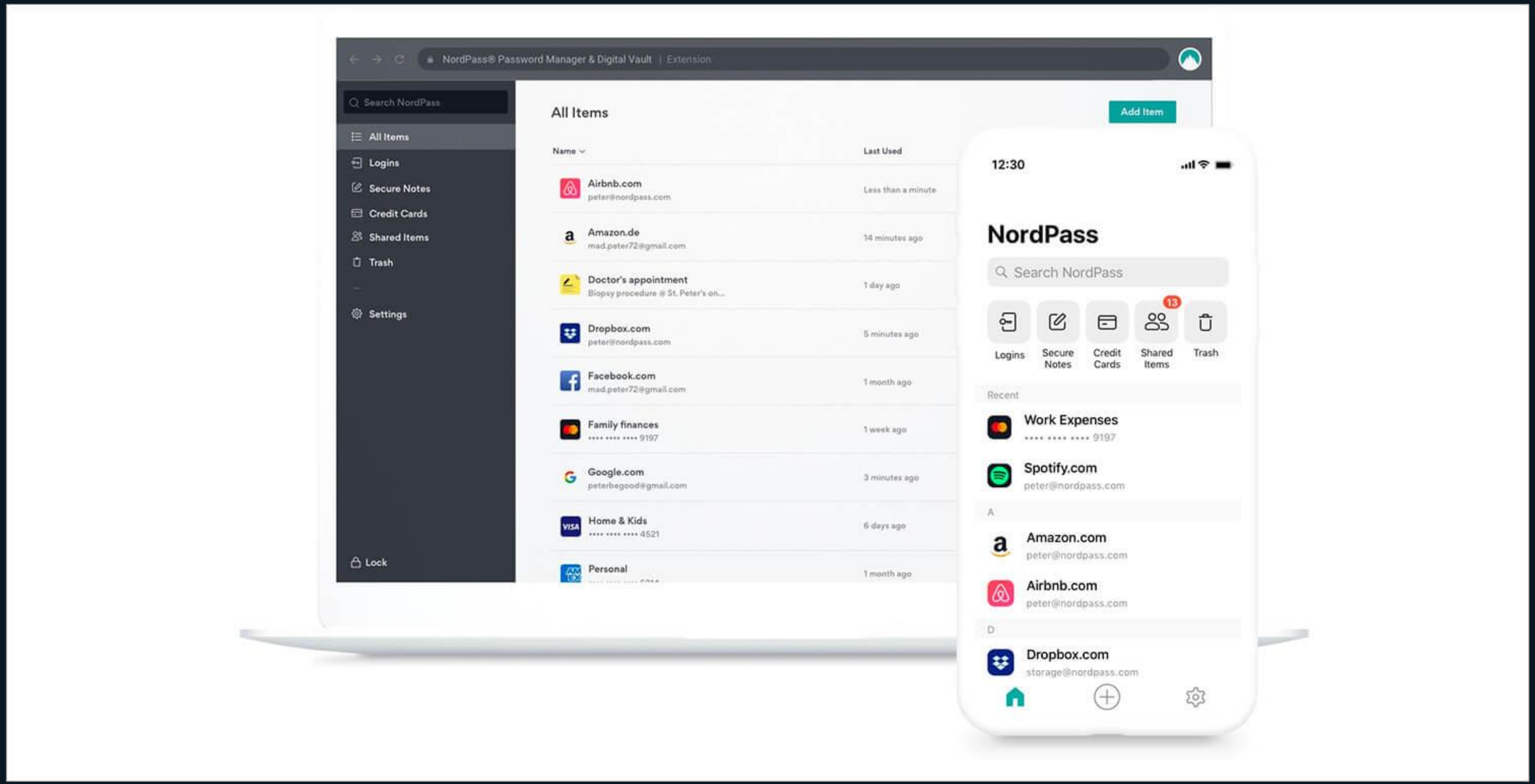
- Use of common words: Dictionary words, common phrases, or the name of a fictional character are predictable. Examples include "password," "qwerty," or "superman.“

- Simple patterns: Using simple number or keyboard patterns like "12345678" or "asdfghjkl" makes a password very easy to guess.

- Reused passwords: Using the same password across multiple websites or services is a major security risk. If one account is compromised, all of your accounts are vulnerable.

How To manage Password?

- **Password Managers:** Use tools to securely store, generate, and manage your passwords. They create **strong, random passwords** for each account.



All Items

Name	Last Used
Airbnb.com peter@nordpass.com	Less than a minute
Amazon.de mad.peter72@gmail.com	14 minutes ago
Doctor's appointment Biopsy procedure @ St. Peter's on...	1 day ago
Dropbox.com peter@nordpass.com	5 minutes ago
Facebook.com mad.peter72@gmail.com	1 month ago
Family finances •••• •••• •••• 9197	1 week ago
Google.com peterbegood@gmail.com	3 minutes ago
Home & Kids •••• •••• •••• 4521	6 days ago
Personal	1 month ago

Recent

Work Expenses
•••• •••• •••• 9197

Spotify.com
peter@nordpass.com

A

Amazon.com
peter@nordpass.com

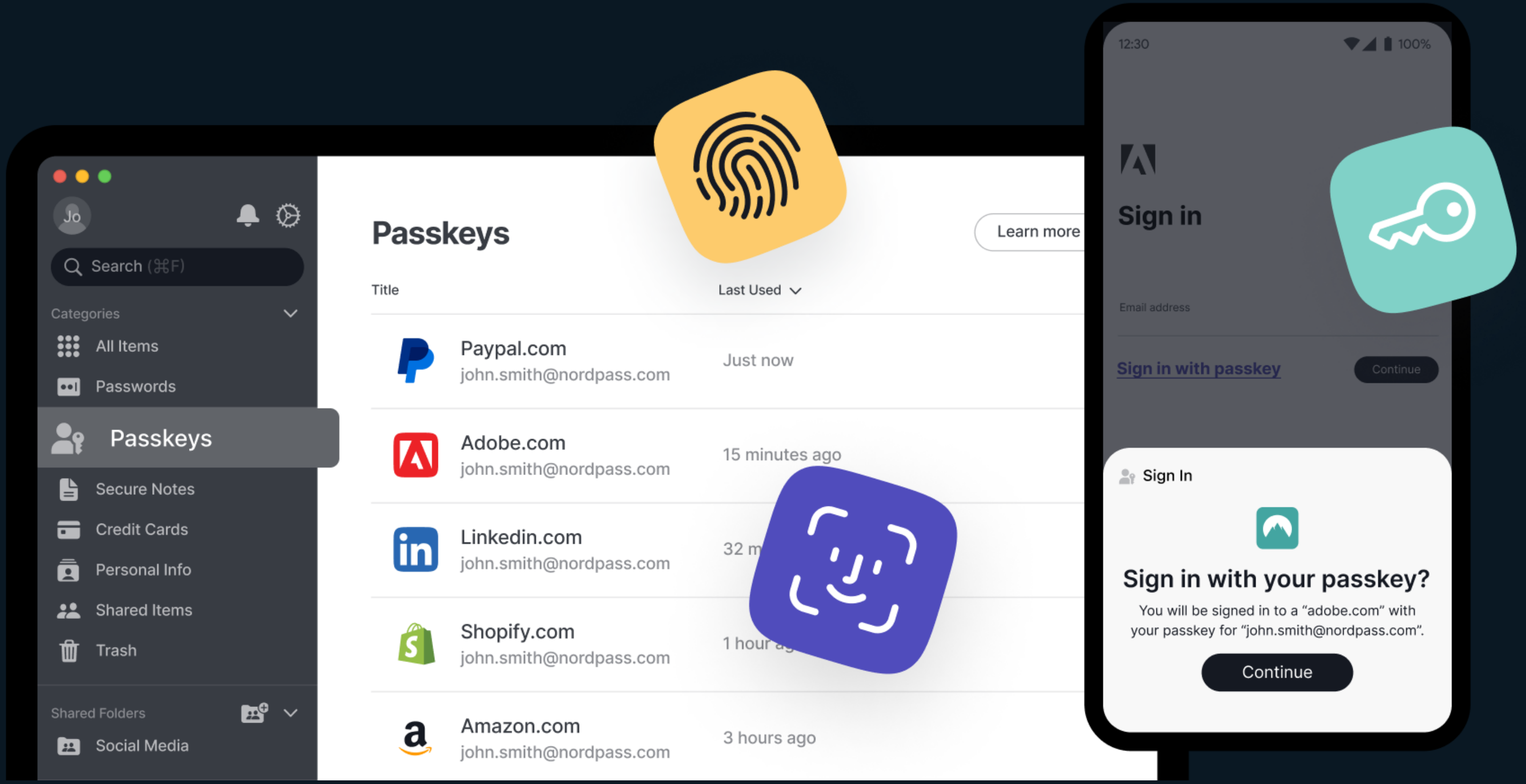
Airbnb.com
peter@nordpass.com

D

Dropbox.com
storage@nordpass.com

Passkey – Beyond Password

- **Passkeys:** This is a technology that goes **beyond passwords**, using secure cryptographic authentication that is resistant to phishing.



Paypal.com john.smith@nordpass.com Just now

Adobe.com john.smith@nordpass.com 15 minutes ago

Linkedin.com john.smith@nordpass.com 32 m

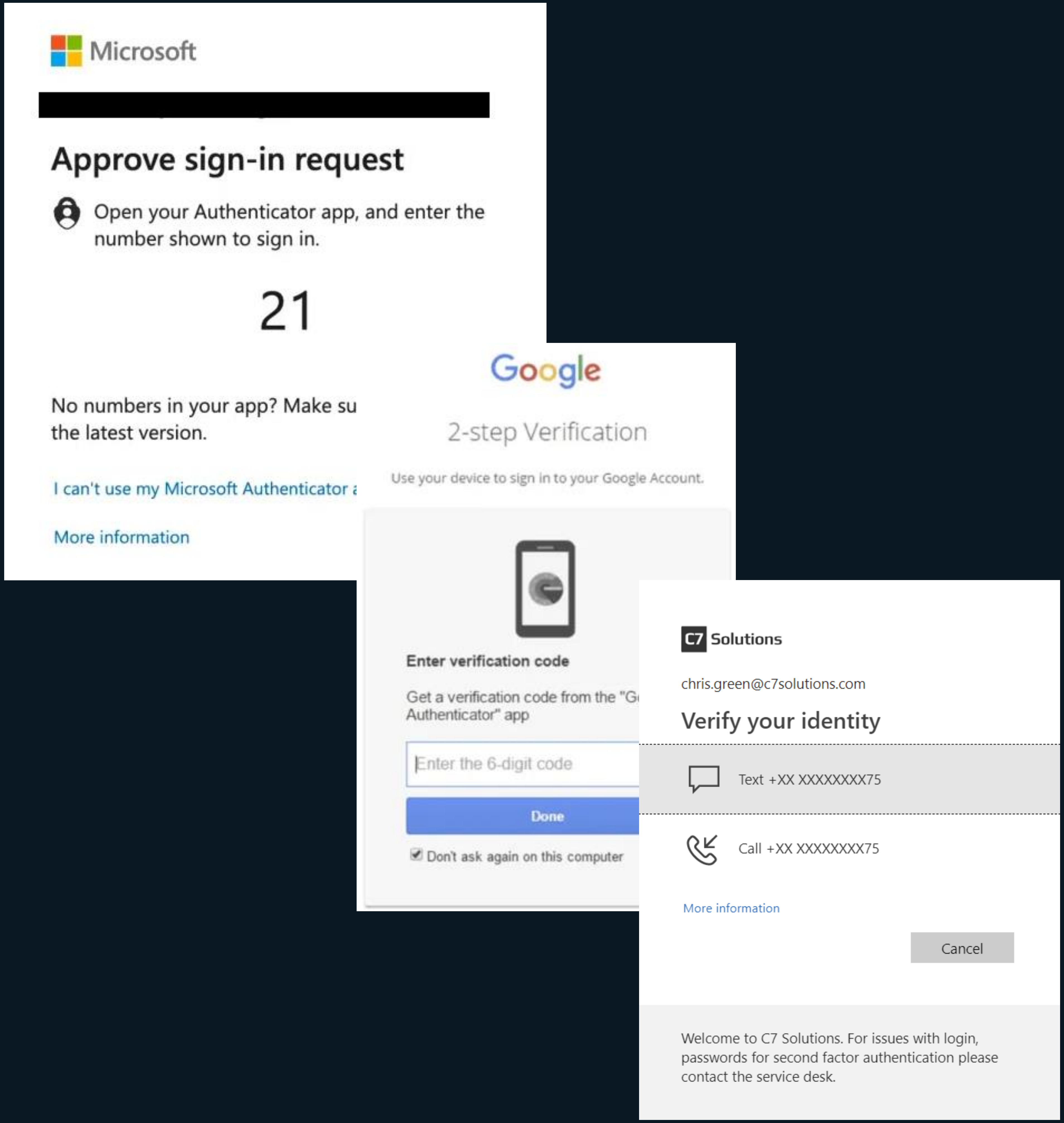
Shopify.com john.smith@nordpass.com 1 hour a

Amazon.com john.smith@nordpass.com 3 hours ago

Sign in with your passkey?

You will be signed in to a "adobe.com" with your passkey for "john.smith@nordpass.com".

- **Multi-Factor Authentication (MFA):** Always enable MFA as an **essential extra layer of security**. It requires additional verification, like a one-time code or biometric scan.



[redacted]

Approve sign-in request

Open your Authenticator app, and enter the number shown to sign in.

21

No numbers in your app? Make su the latest version.

I can't use my Microsoft Authenticator a

More information

2-step Verification

Use your device to sign in to your Google Account.

Enter verification code

Get a verification code from the "G Authenticator" app

Enter the 6-digit code

☑ Don't ask again on this computer

chris.green@c7solutions.com

Verify your identity

Text +XX XXXXXXXX75

Call +XX XXXXXXXX75

More information

Welcome to C7 Solutions. For issues with login, passwords for second factor authentication please contact the service desk.

Mobile Devices

and Security

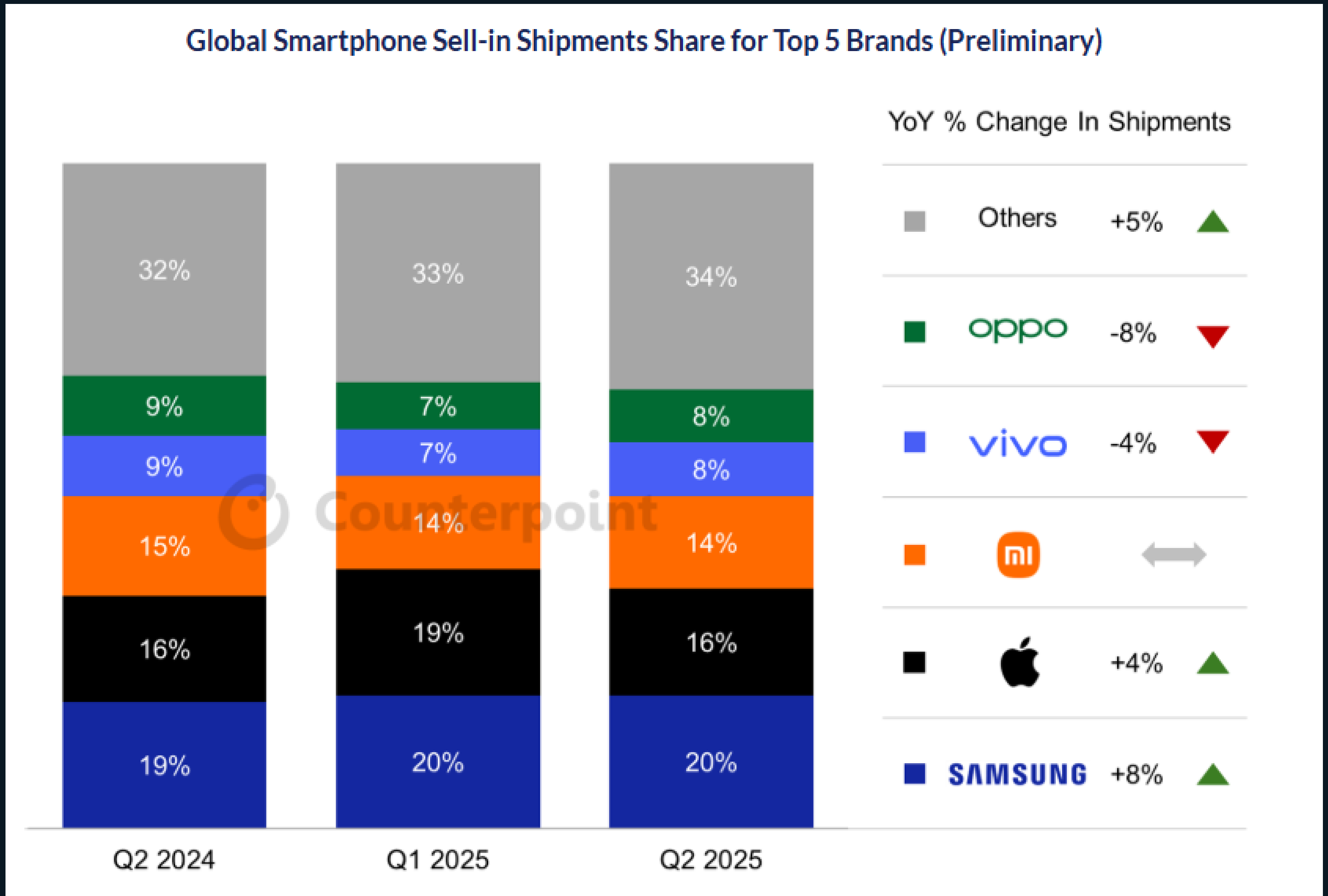
Digital Security
Progress. Protected.

The story of smart devices

Smartphones began in the late 1990s with devices like BlackBerry and Palm Treo, offering basic internet and email features.

The 2007 launch of the iPhone revolutionized the market with its touchscreen interface and app ecosystem, leading to widespread innovation and transforming how we communicate and access information.

The trends of smart device



One of the study from 2025 shown that the Global smartphone shipments by vendor.

In this report, we may found the grow of the mobile device:

Samsung: Expected to remain a leading vendor with a significant market share.

Apple: Anticipated to maintain strong sales, particularly in premium segments.

Xiaomi: Expected to grow, capturing a larger share in emerging markets.

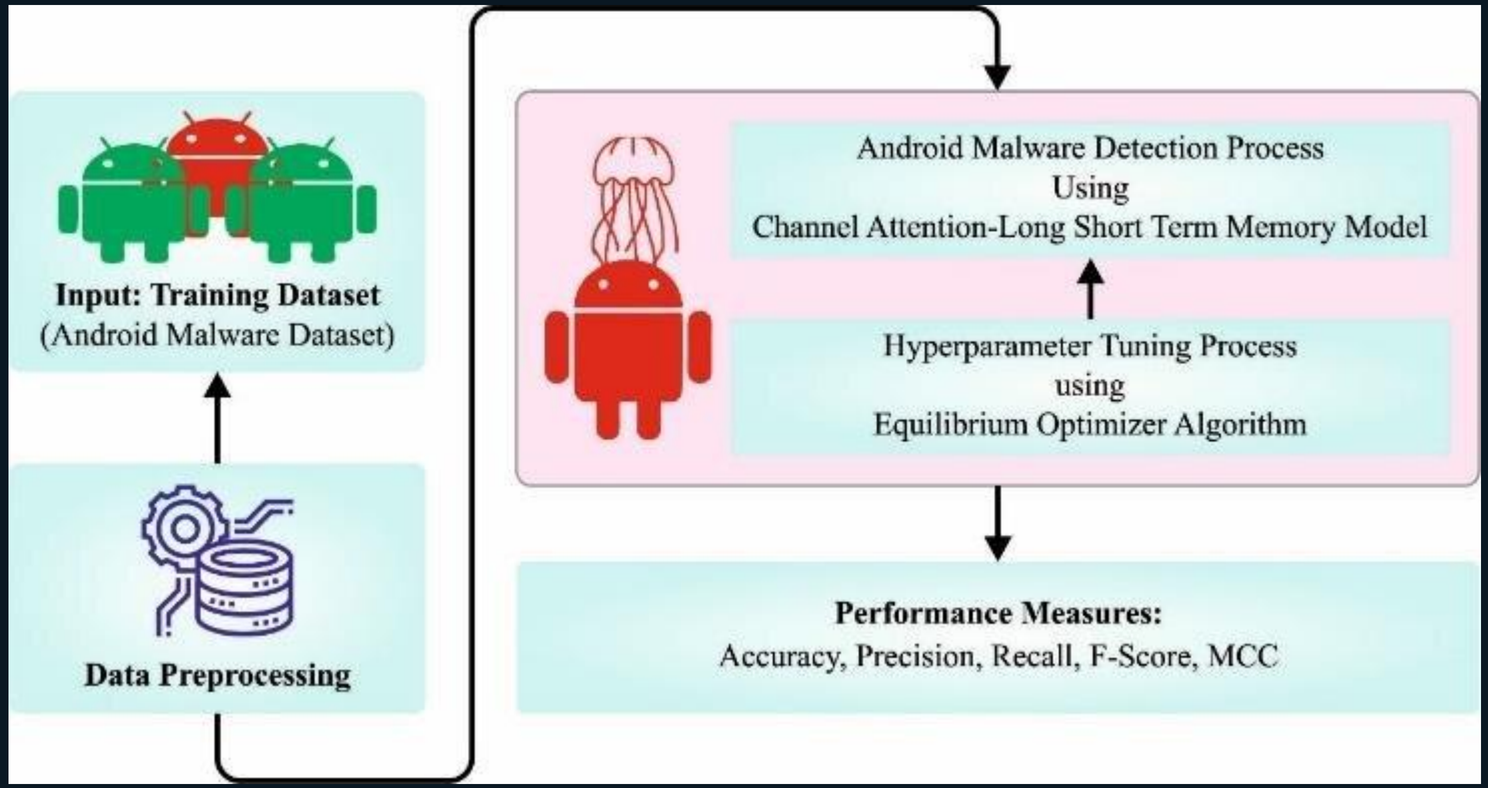
Source: https://www.counterpointresearch.com/insight/global-smartphone-market-q2-2025

What is the threat on the smart device?

- Smart devices face risks like **malware, phishing attacks, and unauthorized access.**

- Attackers can exploit vulnerabilities to **steal sensitive personal data** like contacts, photos, and financial information.

- **Public Wi-Fi networks** are risky because they can be easily intercepted by hackers



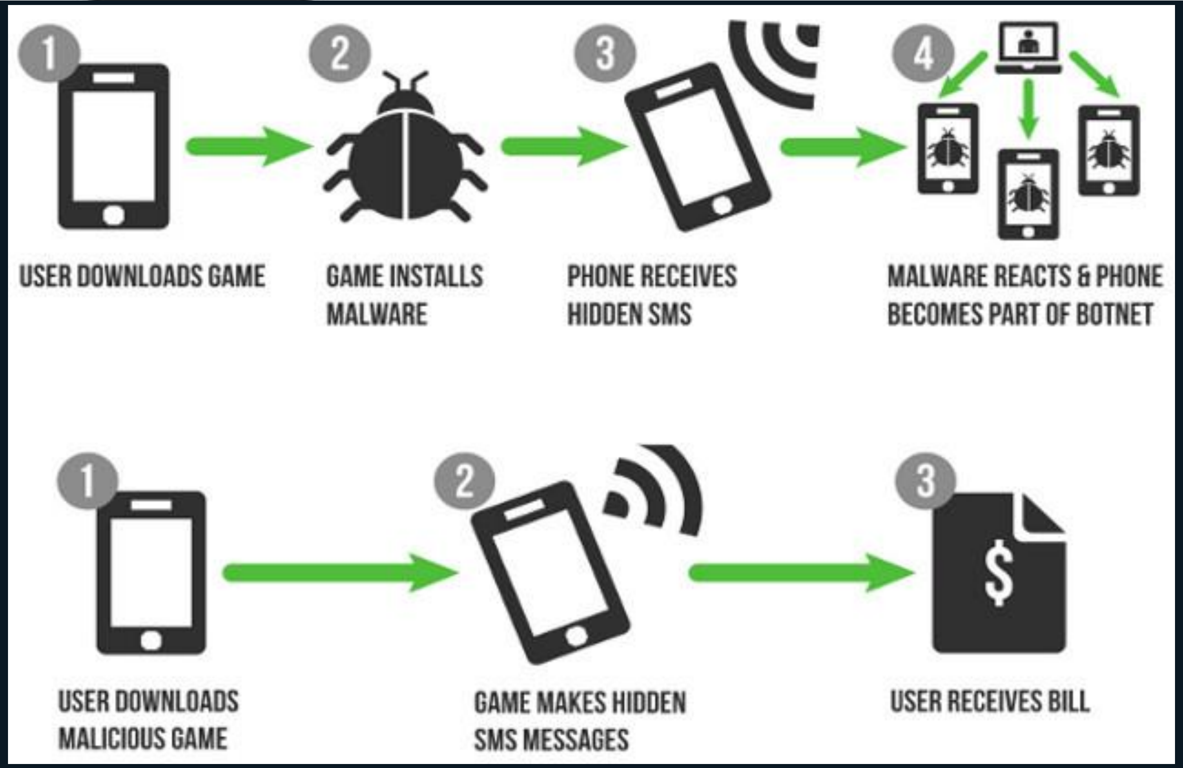
Input: Training Dataset
(Android Malware Dataset)

Data Preprocessing

Android Malware Detection Process
Using
Channel Attention-Long Short Term Memory Model

Hyperparameter Tuning Process
using
Equilibrium Optimizer Algorithm

Performance Measures:
Accuracy, Precision, Recall, F-Score, MCC



1 USER DOWNLOADS GAME

2 GAME INSTALLS MALWARE

3 PHONE RECEIVES HIDDEN SMS

4 MALWARE REACTS & PHONE BECOMES PART OF BOTNET

1 USER DOWNLOADS MALICIOUS GAME

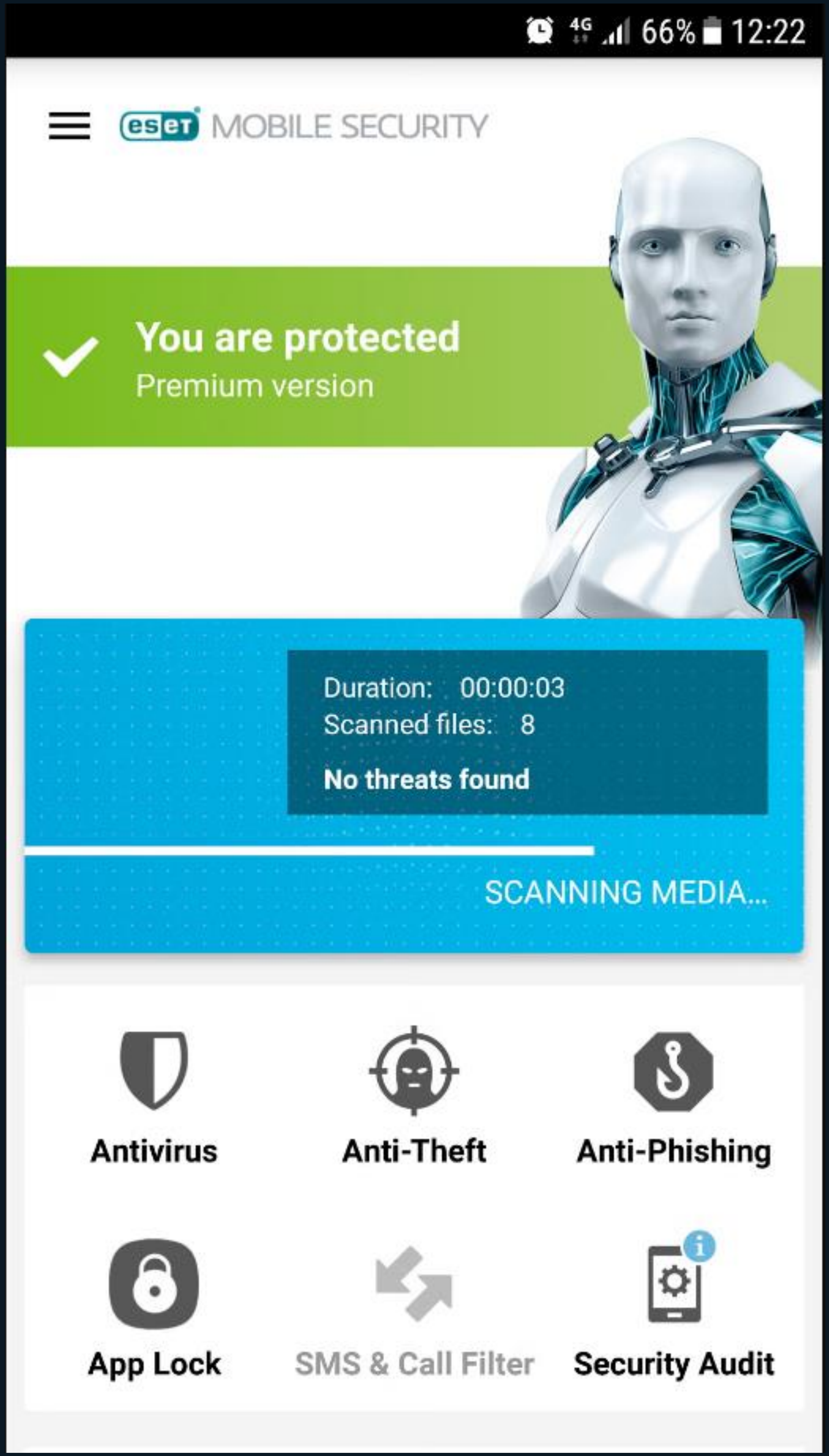
2 GAME MAKES HIDDEN SMS MESSAGES

3 USER RECEIVES BILL

How Can I Prevent The Threats On Smart Devices

- **Device Security**: Use **strong passwords** and enable **biometric authentication** (fingerprint or face ID).

- **Regular Updates:** Keep your **operating system and apps updated** to patch security vulnerabilities



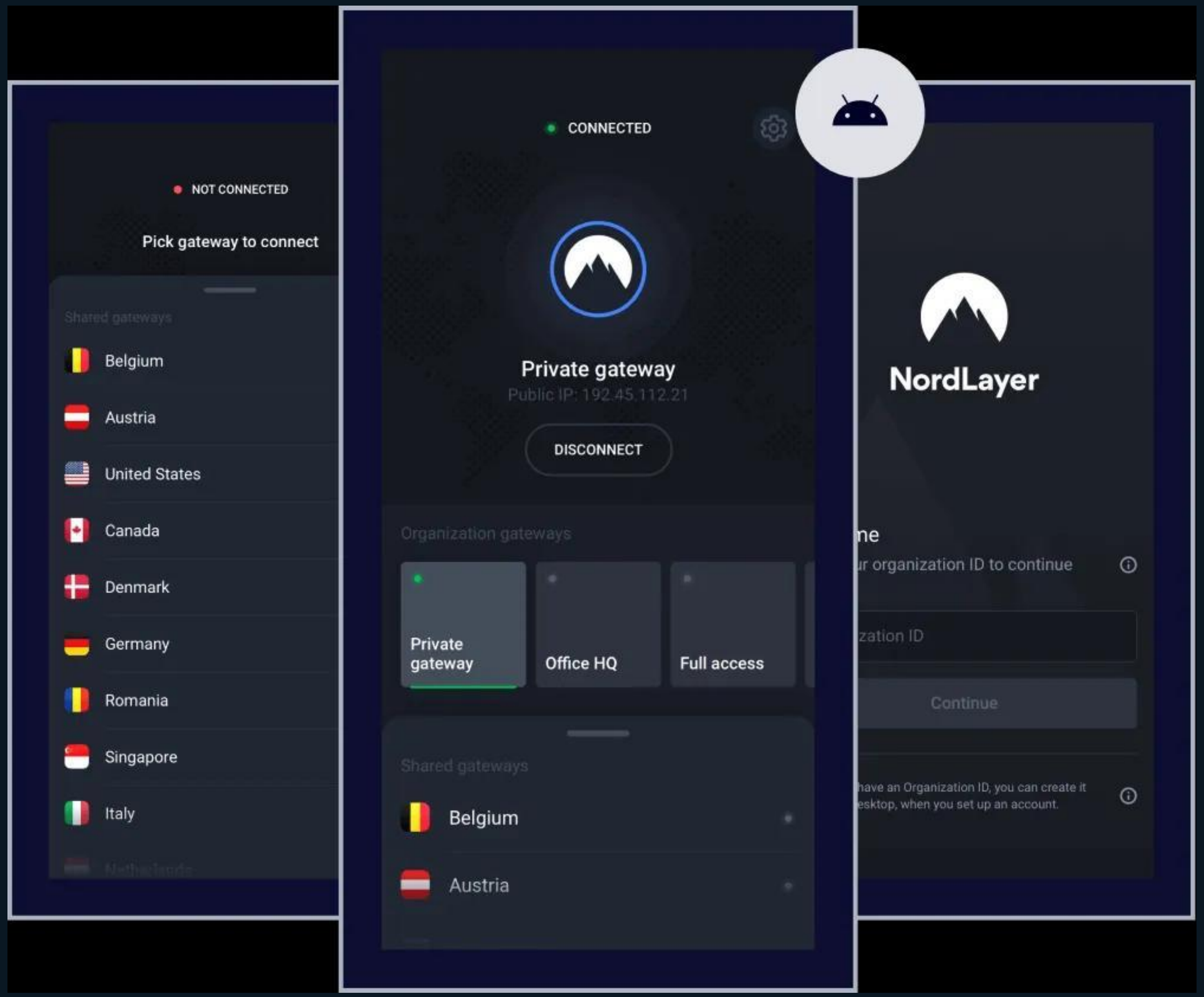
You are protected
Premium version

Duration: 00:00:03
Scanned files: 8
No threats found

SCANNING MEDIA...

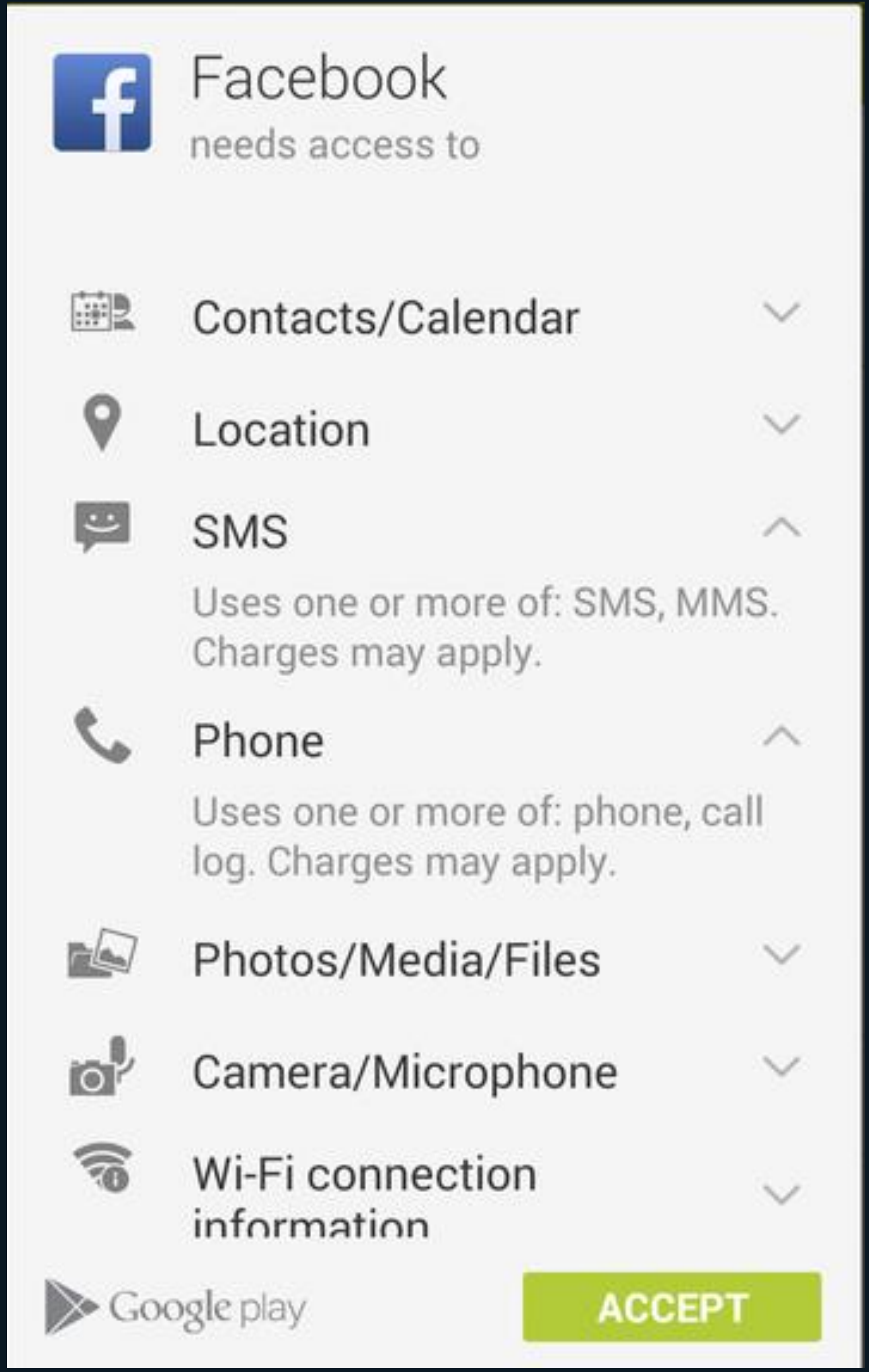
- **Network Security:** Avoid using **public Wi-Fi** for sensitive transactions and consider using a **VPN.**

- Also avoid to access **suspicious WIFI connection**, for example, a WIFI connection without password protection.



- Check the **privacy requirement** before installing or updating an app. If the privacy requirement is non-reasonable, for example, a PDF viewer tool requiring full access to the contact list, phone access, location access, Etc.

- Only install apps from official stores and **check privacy permissions** before installing.



Facebook
needs access to

Contacts/Calendar

Location

SMS

Uses one or more of: SMS, MMS. Charges may apply.

Phone

Uses one or more of: phone, call log. Charges may apply.

Photos/Media/Files

Camera/Microphone

Wi-Fi connection information

Internet of Things (IoT) Security

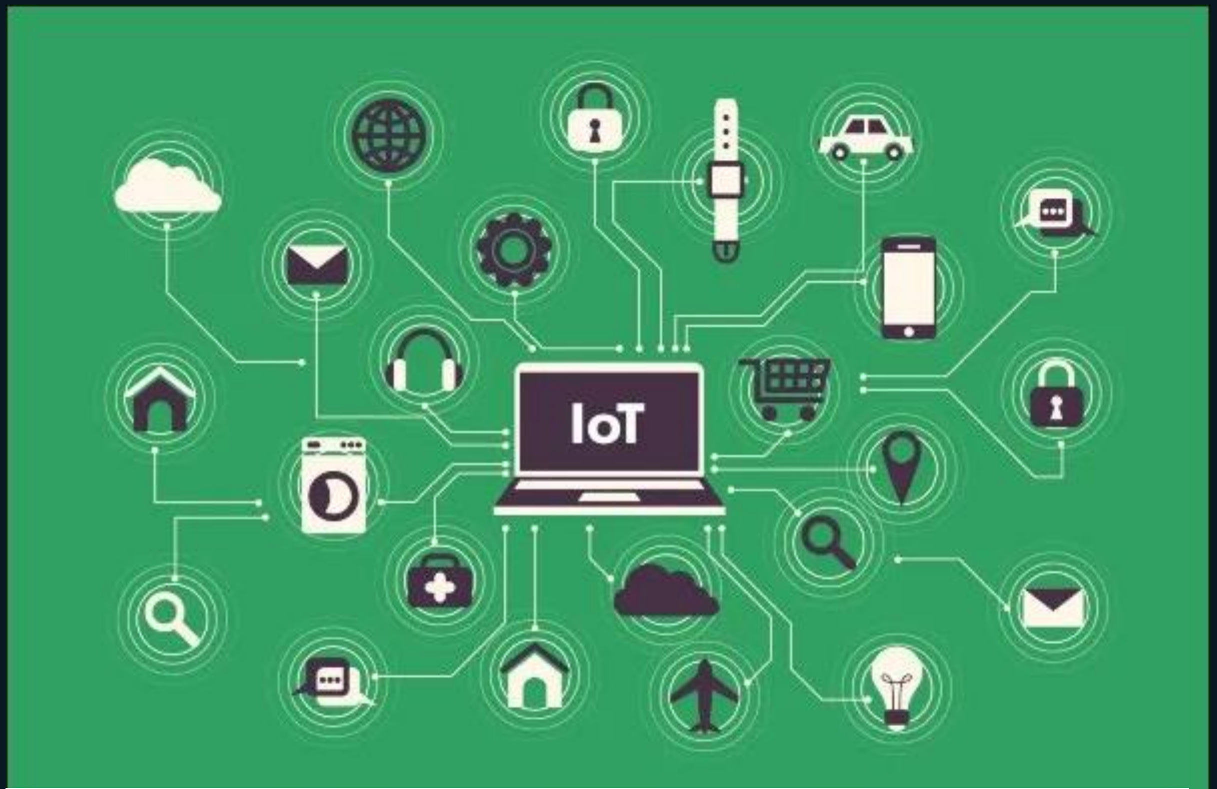
Digital Security
Progress. Protected.

IoT Security.
What is the Internet of Things (IoT)?

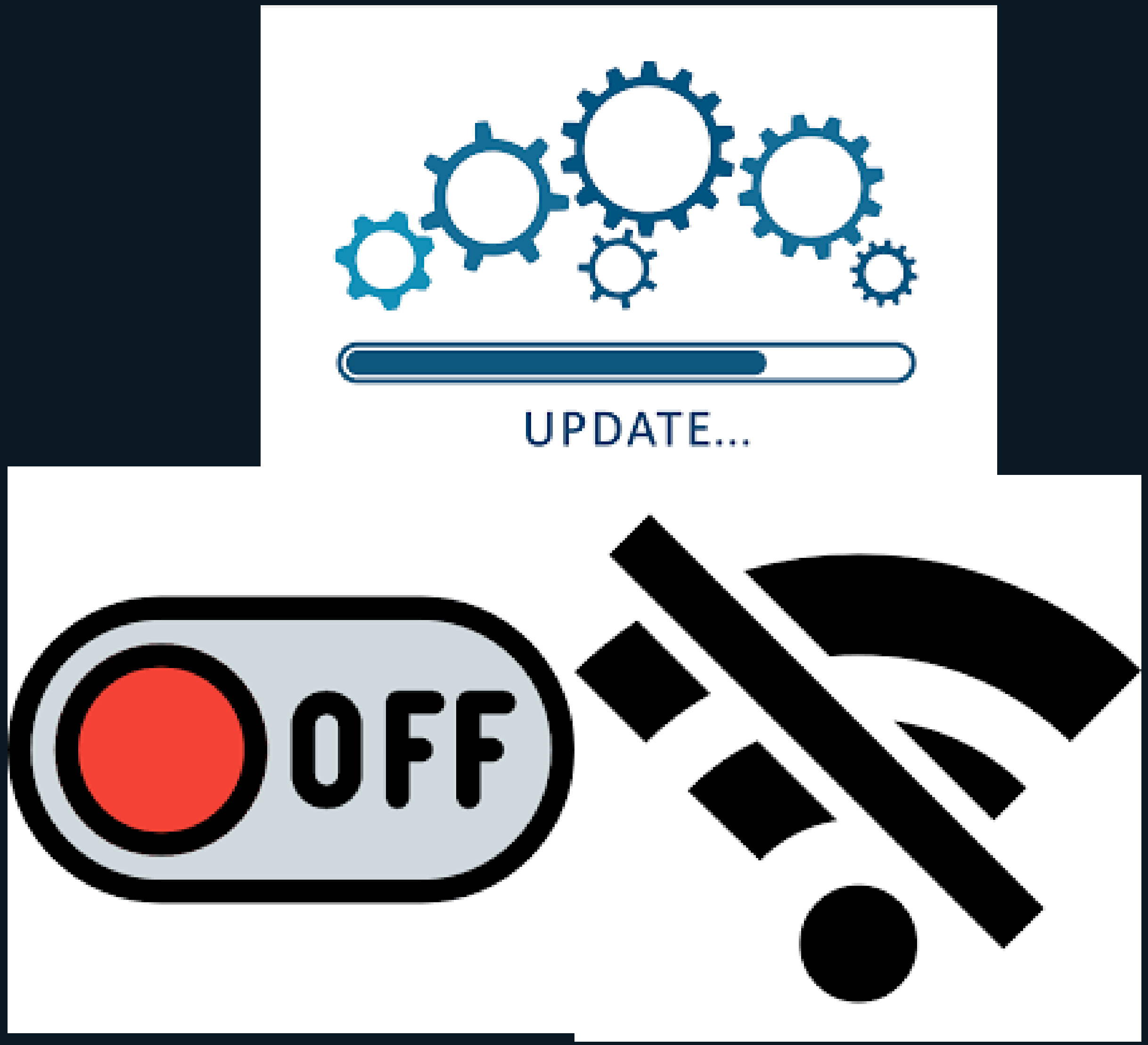
- A network of **interconnected devices,** from smart home appliances to industrial sensors, that exchange data over the internet.

- Unlike mobile phones, many IoT devices operate **autonomously** without direct user intervention.

.



How to Protect IoT Devices

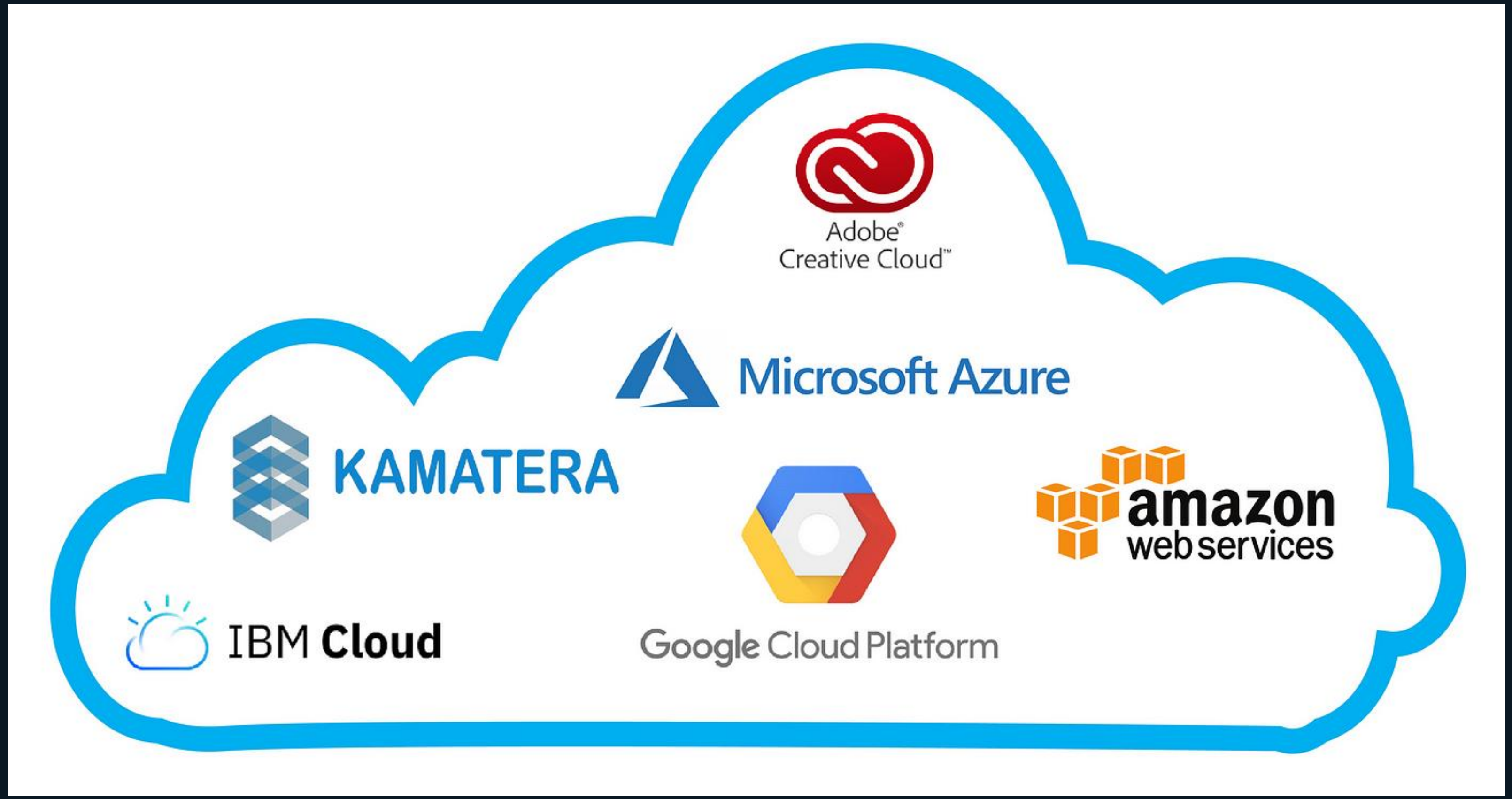


- **Change default passwords** to strong, unique ones.
- Enable **two-factor authentication (2FA)** where available.
- **Regularly update** the device firmware to patch vulnerabilities.
- **Disable unnecessary features** to reduce potential attack surfaces.

Cloud Service and Security

Digital Security
Progress. Protected.

What are the Risks?



- Cloud services pose risks such as **data breaches**, **unauthorized access**, and potential **loss of control** over your information.

What are the Risks?

- Vulnerabilities in **shared environments** can lead to data exposure.

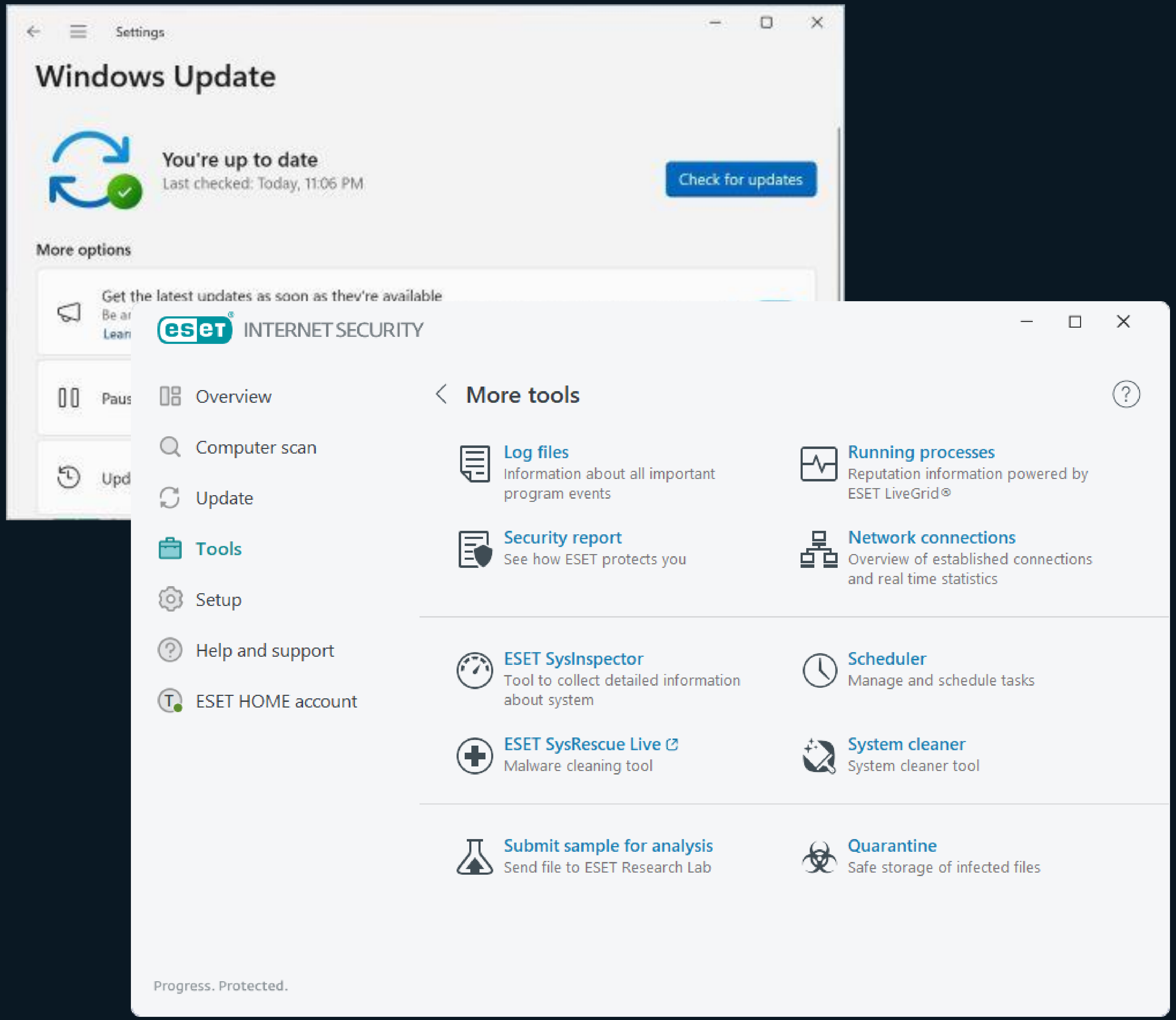
How To Improve Cloud Security?

- Implement **strong authentication,** such as Multi-Factor Authentication (MFA).

- **Encrypt data** both when it is stored and when it is being transmitted.

- **Regularly update and patch** systems to prevent vulnerabilities.

- Conduct frequent **security audits and employee training.**



Settings

Windows Update

You're up to date
Last checked: Today, 11:06 PM

More options

Get the latest updates as soon as they're available

ESET INTERNET SECURITY

More tools

Log files
Information about all important program events

Running processes
Reputation information powered by ESET LiveGrid®

Security report
See how ESET protects you

Network connections
Overview of established connections and real time statistics

ESET SysInspector
Tool to collect detailed information about system

Scheduler
Manage and schedule tasks

ESET SysRescue Live
Malware cleaning tool

System cleaner
System cleaner tool

Submit sample for analysis
Send file to ESET Research Lab

Quarantine
Safe storage of infected files

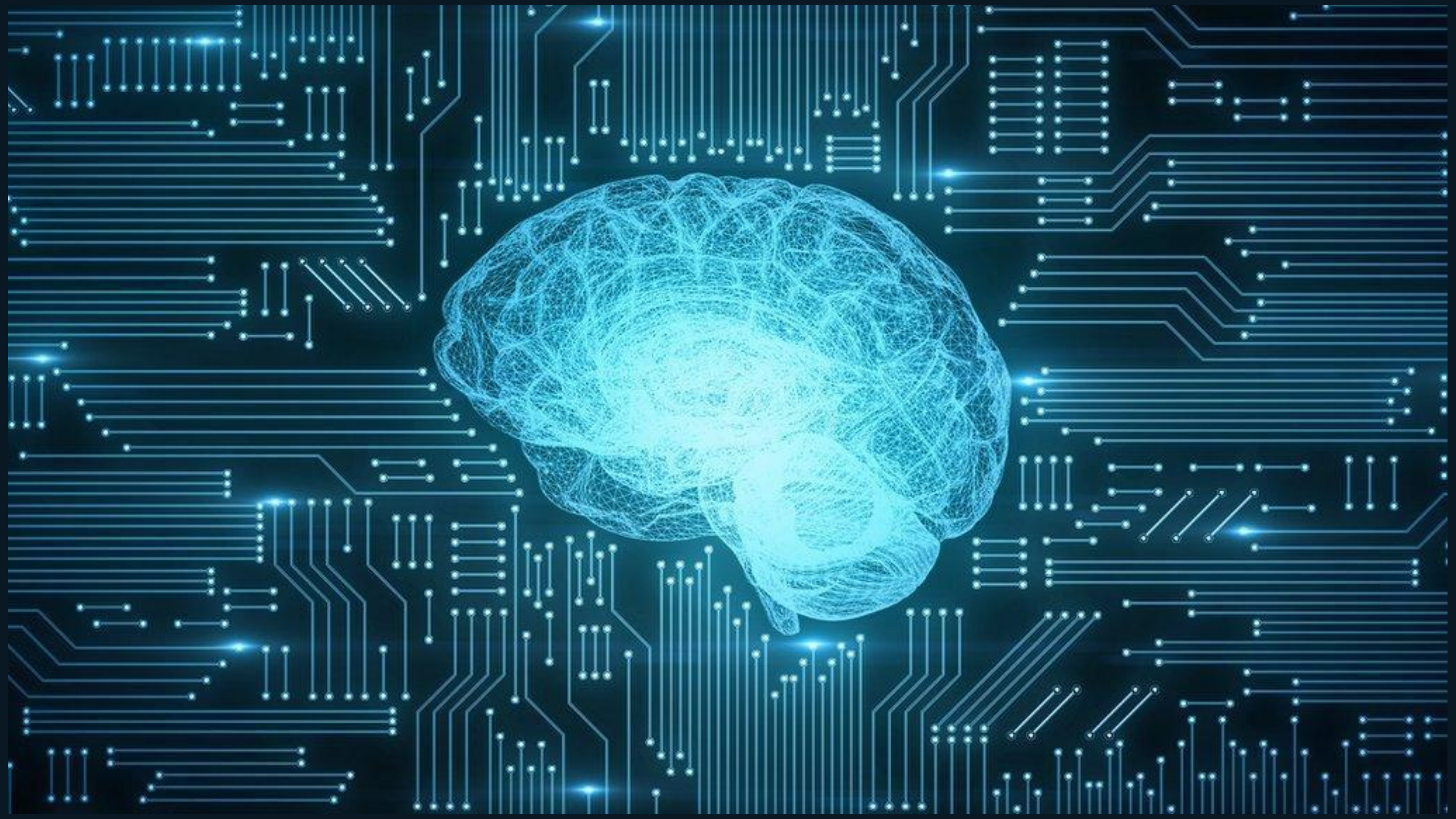
Progress. Protected.

Security Impact of Artificial intelligence (AI)

Digital Security
Progress. Protected.

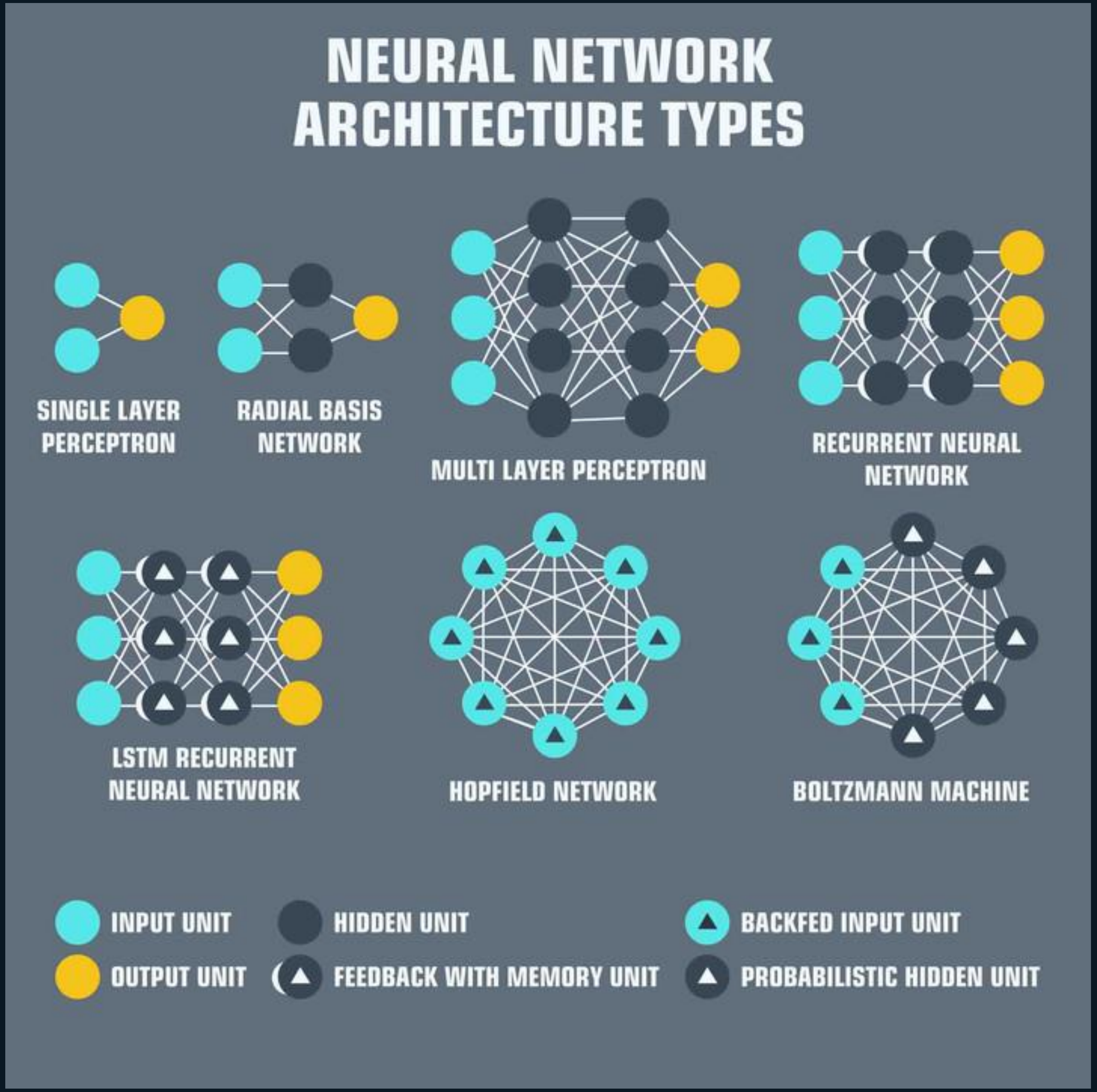
What is Artificial intelligence (AI)?

- The **simulation of human intelligence** in machines, allowing them to perform tasks like learning, reasoning, and problem-solving.



What is Artificial intelligence?

- Today, AI powers a wide range of tasks, from **chatbots** and **virtual assistants** to complex **data analysis**.



How AI Impacts Security

- **Positive:** AI enhances security by improving **threat detection**, automating responses, and analyzing data for anomalies.

- **Negative:** It also introduces risks, such as sophisticated **AI-driven cyberattacks**.

How to Handle AI-Related Risks

- keep your devices **updated** with the latest software and security patches.

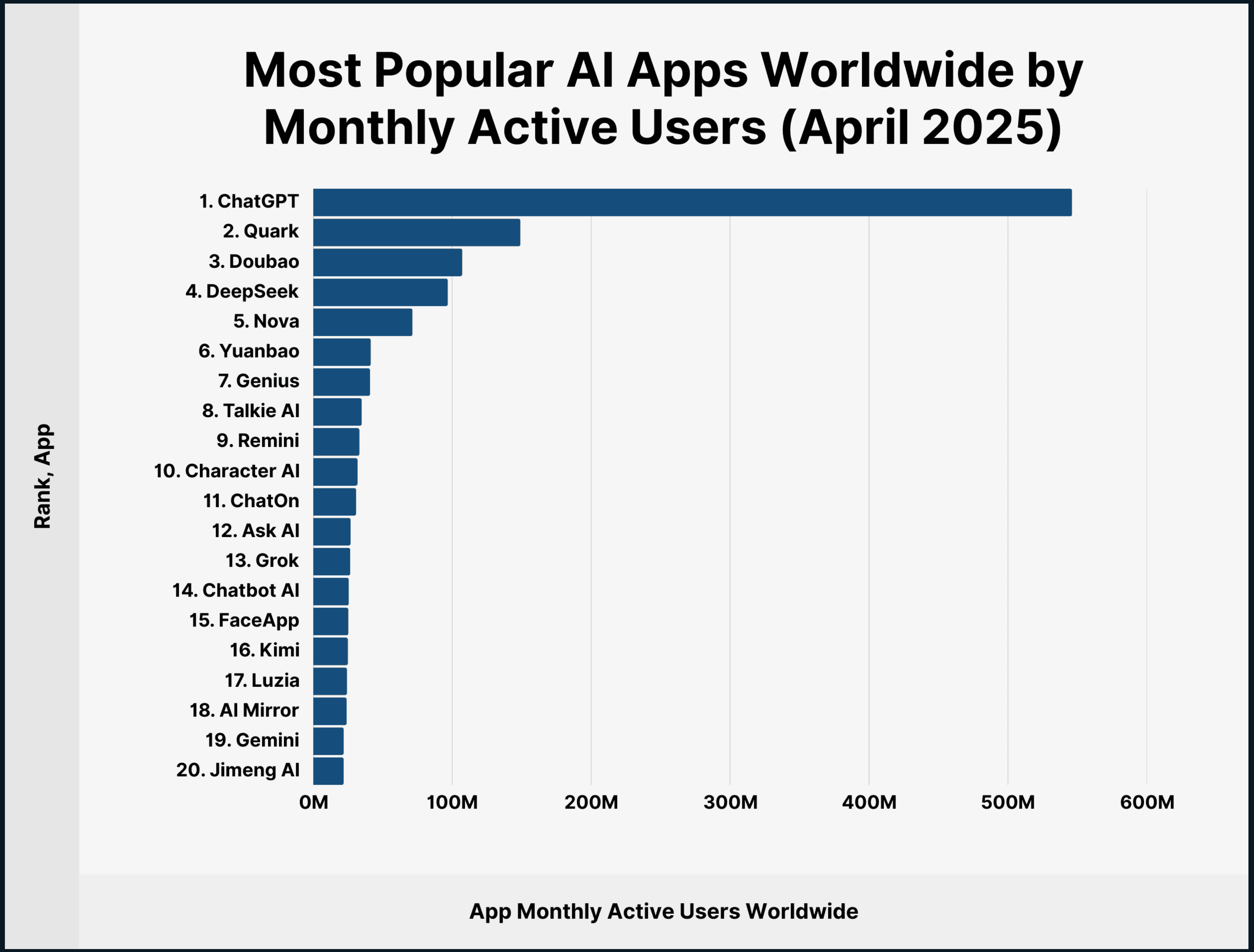
- Use **strong, unique passwords** and **enable two-factor authentication.**

- Be **cautious about the data you share** with AI applications and regularly review your privacy settings.

The Most Popular AI Applications In 2025 First Half

1. ChatGPT by OpenAI (US)
2. Quark by Alibaba (China)
3. Doubao by ByteDance (China)
4. DeepSeek by DeepSeek (China)
5. Nova by HubX (Turkey)

https://backlinko.com/most-popular-ai-apps



Want to know more?

Digital Security
Progress. Protected.