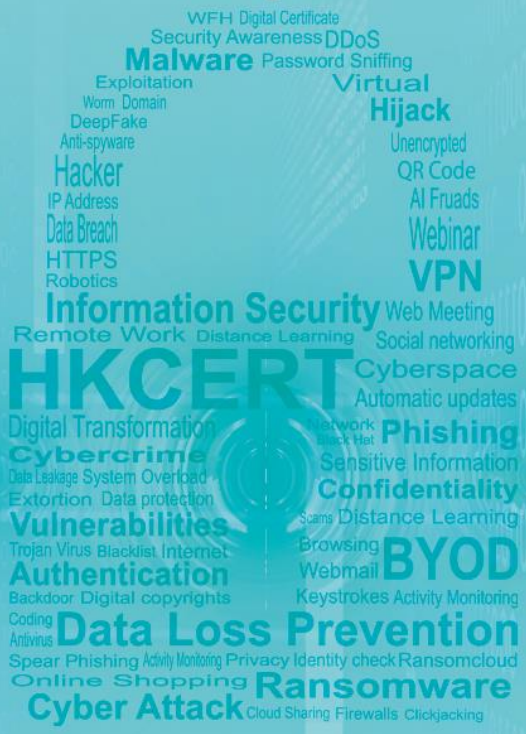
Hong Kong Computer
Emergency Response Team
Coordination Centre
HKCERT 香港電腦保安事故協調中心

# Hong Kong Security Watch Report 2023 Q3

Release Date: Nov 2023



# Foreword

## Better Security Decision with Situational Awareness

Nowadays, many networked digital devices, such as computers, smartphones, tablets, are being compromised without the user's knowledge. The data on them may be mined and exposed every day, and even be used for various criminal activities.

The Hong Kong Security Watch Report aims to raise public awareness of the problem of compromised systems in Hong Kong, enabling them to make better decision in information security. The data in this quarterly report focuses on the activities of compromised systems in Hong Kong which suffer from, or have participated in various types of cyber-attacks, including web defacement, phishing and botnets. "Computers in Hong Kong" refer to those whose network geolocation is Hong Kong, or the top-level domain of their host name is ".hk". Also, this report will review major security incidents and explore hot security topics with easy-to-adopt security advice with an aim to improve public's information security posture and enhance their security resilience capabilities.

## Capitalising on the Power of Global Intelligence

This report is the result of collaboration between the Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) and global security researchers. Many security researchers could detect attacks against their own or clients' networks. Some will provide the collected information of IP addresses of attack source or web links of malicious activities to other information security organisations with an aim to collectively improve the overall security of the cyberspace. They have good practice in sanitizing personal identifiable data before sharing the information.

HKCERT collects and aggregates such data about Hong Kong from multiple information sources for analysis with the Information Feed Analysis System (IFAS), a system developed by HKCERT. The information sources are very diverse and reliable, providing a balanced reflection of the security status of Hong Kong.

HKCERT removes duplicated events reported by multiple sources and uses the following metrics for measurement to assure the quality of the statistics.

| Type of Attack | Metric used |
|---|---|
| Defacement, Phishing | Security events on unique URLs within the reporting period |
| Botnet (Bots) | Maximum daily count of security events on unique IP addresses within the reporting period |

**Sources of information in IFAS:**

| Event Type | Source | First introduced |
|---|---|---|
| **Defacement** | Zone – H | 2013-04 |
| **Phishing** | CleanMX – Phishing | 2013-04 |
| **Phishing** | Phishtank | 2013-04 |
| **Botnet (Bots)** | Shadowserver - microsoft_sinkhole_events | 2021-06 |
| **Botnet (Bots)** | Shadowserver - microsoft_sinkhole_http_events | 2021-06 |
| **Botnet (Bots)** | Shadowserver - sinkhole_http_events | 2021-06 |
| **Botnet (Bots)** | Shadowserver - sinkhole_events | 2021-06 |
| **Botnet (Bots)** | Shadowserver - honeypot_darknet_events | 2021-06 |

**Geolocation identification methods in IFAS**

| Method | First introduced | Last update |
|---|---|---|
| Maxmind | 2013-04 | 2023-11 |

## Better information better service

HKCERT will continue to enhance this report with more valuable information sources and more in-depth analysis and explore how to make best use of the data to enhance our services. Please send your feedback via email (hkcert@hkcert.org).

## Limitations

Data collected for this report come from multiple sources with different collection periods, presentation formats and their own limitations. The statistics from the report should be used as a reference only and should neither be compared directly nor be regarded as a full picture of the reality.

## Disclaimer

Data may be subject to update and correction without notice. We shall not have any liability, duty or obligation for or relating to the content and data contained herein, any errors, inaccuracies, omissions or delays in the content and data, or for any actions taken in reliance thereon. In no event shall we be liable for any special, incidental or consequential damages, arising out of the use of the content and data.

## License

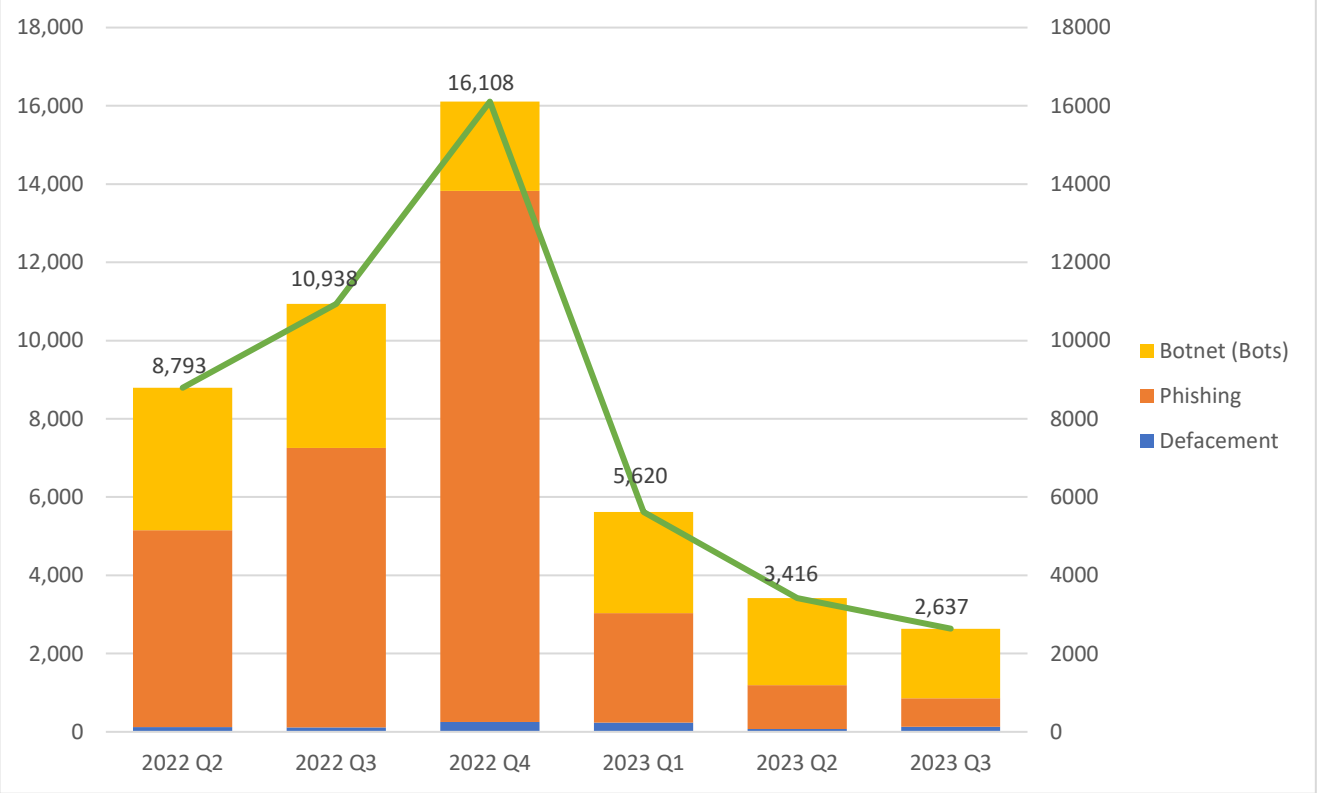
# Highlights of the 2023 Q3 Report

**Unique security events related to Hong Kong**

**2,637**

**Quarter-to-quarter**

**22.8%↓**



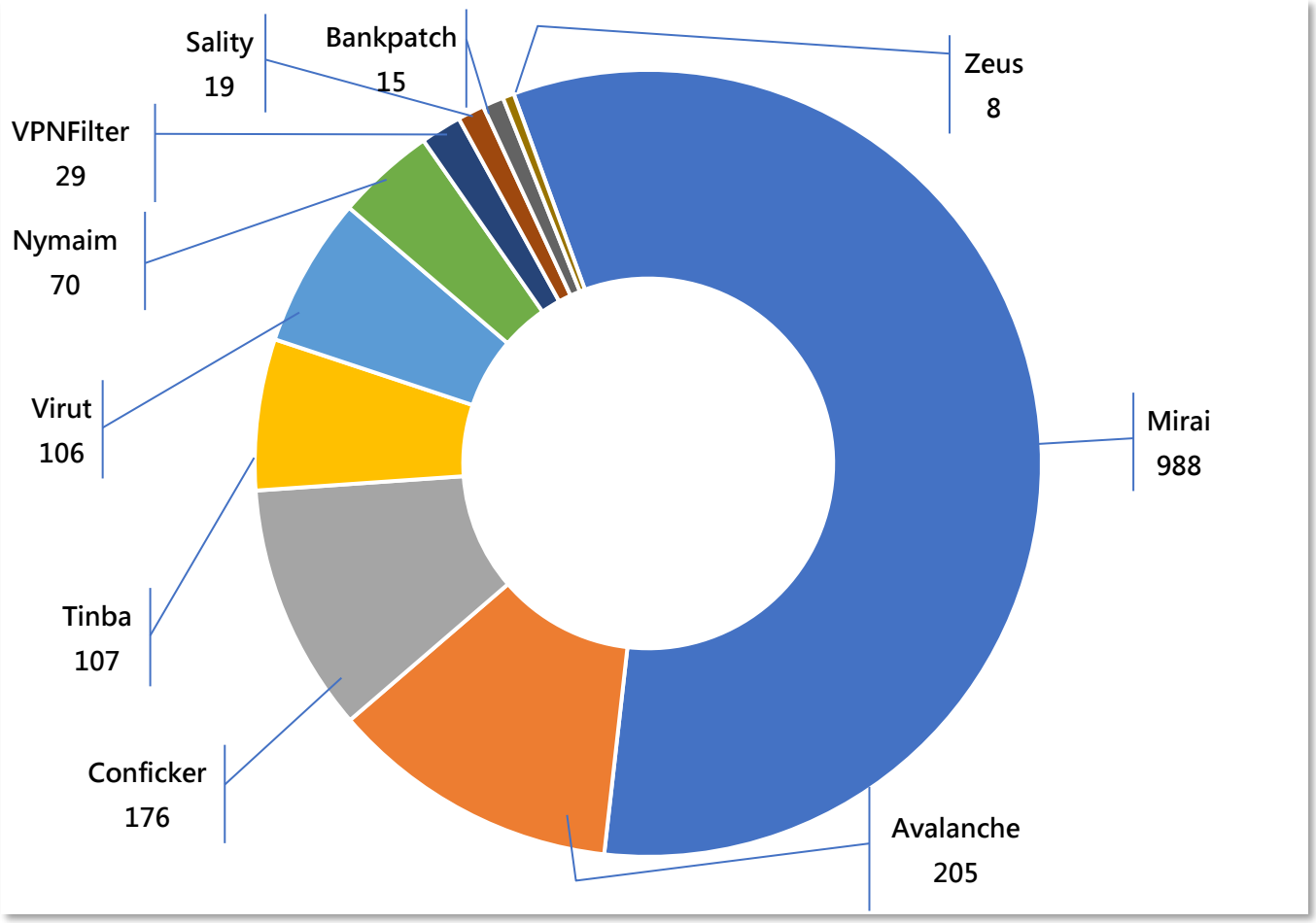

| Event Type | 2022 Q3 | 2022 Q4 | 2023 Q1 | 2023 Q2 | 2023 Q3 | quarter-to-quarter |
|---|---|---|---|---|---|---|
| Defacement | 113 | 249 | 233 | 69 | 132 | +91.3% |
| Phishing | 7,141 | 13,574 | 2,804 | 1,120 | 722 | -35.5% |
| Botnet (Bots) | 3,684 | 2,285 | 2,583 | 2,227 | 1,783 | -19.9% |
| Total | 10,938 | 16,108 | 5,620 | 3,416 | 2,637 | -22.8% |

# Major Botnet Families in Hong Kong Network

**Mirai**
988
19.8%

**Avalanche**
205
17.7%

| | | |
|---|---|---|
| Conficker | 176 | -16.6% |
| Tinba | 107 | -7.8% |
| Virut | 106 | -0.9% |
| Nymaim | 70 | -9.1% |
| VPNFilter | 29 | -56.1% |
| Sality | 19 | -38.7% |
| Bankpatch | 15 | -50.0% |
| Zeus | 8 | -73.3% |




** Individual botnet's size is calculated from the maximum of the daily counts of unique IP address attempting to connect to the botnet in the reporting period. In other words, the real botnet size should be larger than in the report because not all bots are activated on the same day.*

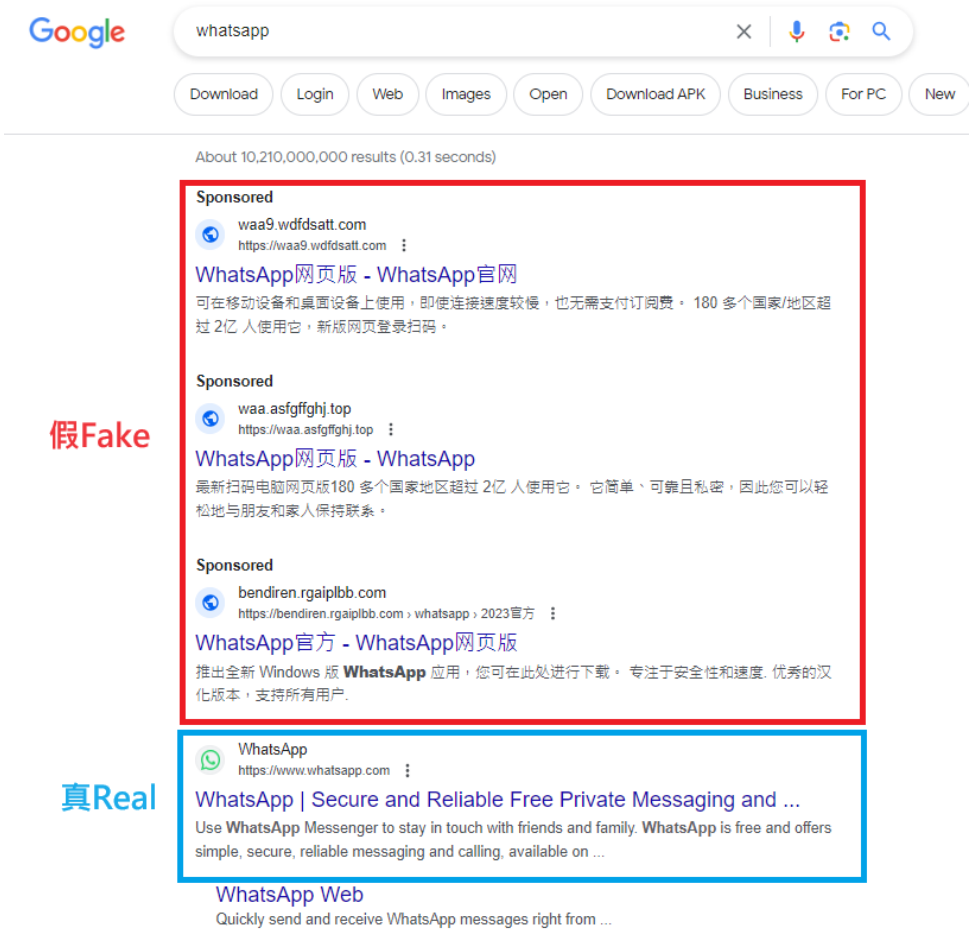
# Focus：Protect Your WhatsApp Account & Be Cautious Of Scams Targeting Hong Kong WhatsApp Users

***Recently, there have been a series of scams in Hong Kong involving the theft of WhatsApp accounts, posing a serious threat to the public's personal privacy and information security. In order to protect the interests of citizens, the Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) specifically advises everyone to strengthen the protection of their WhatsApp accounts. The following will introduce the operation methods of these scams and provide some preventive measures to help citizens increase their awareness and protect their personal information.***

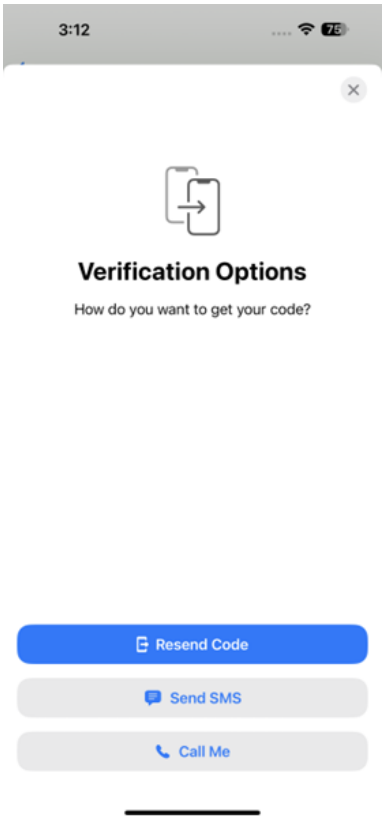

The purpose of these scammers is mainly financial gain. They use social engineering and technical means to deceive victims into scanning the QR codes of fake WhatsApp websites (phishing websites) or stealing the one-time verification codes (OTP) of victims' accounts, thus gaining control of their WhatsApp accounts. Once they have control of the account, scammers can impersonate the victim and send fraudulent messages to their contacts, and even further deceive others.

Recently, HKCERT has noticed that scammers are even using advertising or Search Engine Optimization (SEO) techniques to promote their carefully designed phishing websites, increasing the chances of users clicking on them and falling into the scam.

In the next chapter, HKCERT has compiled the most frequently asked questions by citizens and provided answers and security recommendations.




## Can the account owner regain control immediately after it has been stolen?

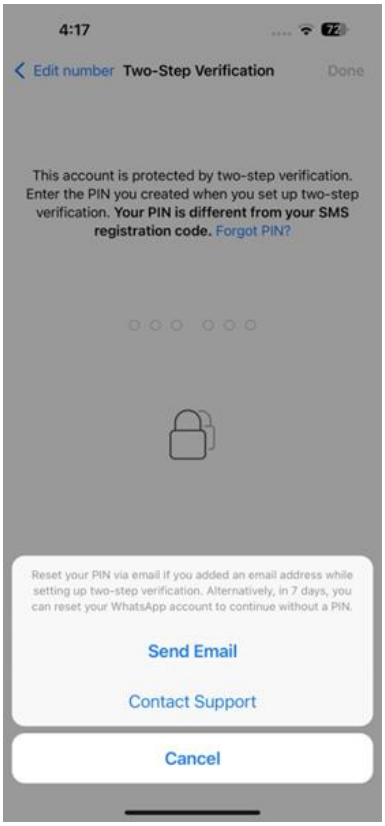



Once the hackers obtain the registration code for the victim's WhatsApp account, they can log into and hijack the victim's account. Meanwhile, the victim will be forcefully logged out of their own account, and WhatsApp will display a screen requesting the input of the phone number. If the victim immediately logs in with their registered phone number at this point, they can regain control of their account.

The steps are as follows: Once the victim enters their phone number to log in again, WhatsApp will request a one-time registration code. At this point, the user can wait and choose to receive and enter the registration code through SMS or phone call. After completing this process, they can regain control of their account.

When the victim logs in to their account again, they will be prompted to enter the registration code for their WhatsApp account. User should choose to receive the verification code via SMS or phone call.

## Can enabling two-step verification to provide effective protection for the account?




Enabling two-step verification can effectively prevent hackers from logging into and hijacking user accounts.

After enabling two-step verification, users are required to set a 6-digit PIN code. Once set, even if a fraudster manages to obtain the user's login registration code and successfully accesses the user's account, the fraudster will still be prompted to enter the user's pre-set two-step verification PIN code in order to use the user's WhatsApp account. In other words, after setting up the PIN, hackers cannot take over the user's WhatsApp account.

Hackers cannot use the user's WhatsApp account if they do not have the user's two-step verification PIN code.

## If the original account does not have two-step verification enabled and the fraudster enables it after gaining access, would it be impossible to regain control of the account?

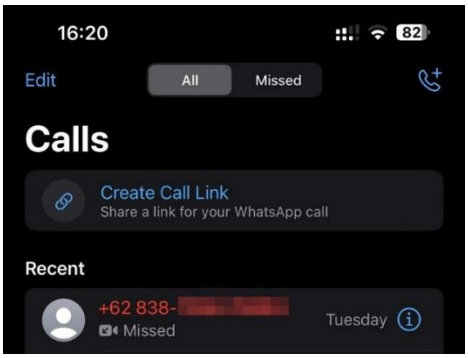
No. If a fraudster manages to hijack a user's account and enables two-step verification, the user can still regain control.

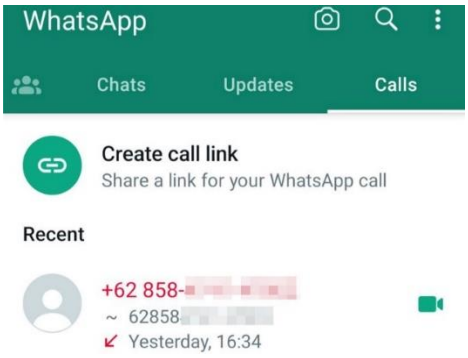
When the user logs into the account again, WhatsApp will require the user to enter the two-step verification PIN set by the scammer. User could not use WhatsApp without the PIN. However, according to WhatsApp's guidelines, it would allow the user to reset the PIN after seven days. Besides, it also allows the user to reset the PIN by email, which the user has provided to WhatsApp, if any.

Nonetheless, regardless of whether you possess the PIN or not, if the user enters the SMS registration code, the other party will be forced to log out and be unable to use the WhatsApp account anymore.

# Frequent occurrences of unfamiliar video calls on WhatsApp.

In addition, some citizens have contacted our center to inquire about receiving suspicious WhatsApp video calls from unknown individuals, using unfamiliar numbers such as +62 and +44. The callers claim to be from law enforcement or banking institutions and can mention the names of the recipients.







## Why Attackers Initiate Video Calls than Voice Calls?

- **Personal Identity:** Attackers may capture the appearance of citizens through video calls and relating the video or image capture to an identifiable individual through Internet search from Google, social media posts or online photo albums. Also, it can observe personal details in targets' backgrounds or appearances that can aid future social engineering or identity theft attacks.

- **Obtain Facial Information for Deepfake:** Attackers may obtain the appearance and voice of citizens through video calls to create a highly realistic deepfake, which may be used in other fraudulent activities to your family members or friends.

- **Identity Impersonation for Illegal Activities:** With both video and voice of the attackers is visible, it is easier for attackers to create an illusion with fake scene, background or costume, pretending to be from organizations like law enforcement or banks to sound legitimate and intimidating for financial scam.

- **Sense of Urgency:** A video call makes the targets feel they need to respond quickly, leaving less time for critical thinking. This helps attackers maintain control of the interaction for scam.

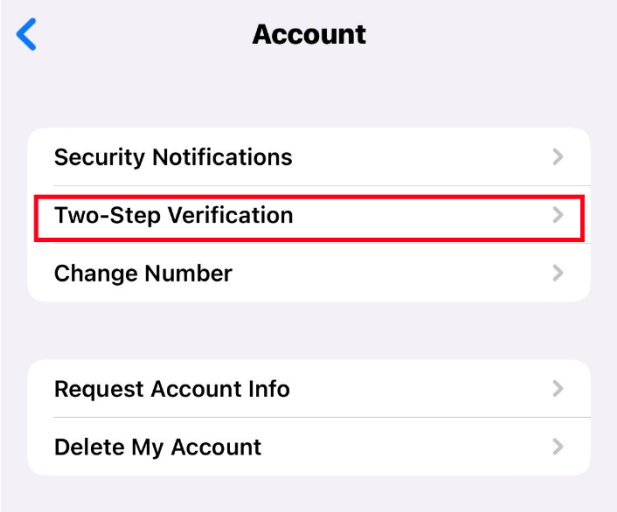
## What Are the Risks of Unknown Video Calls?

- **Scams:** Attackers may attempt to engage in fraudulent activities through video calls, such as impersonating police officers or bank staff to obtain your personal information or money.

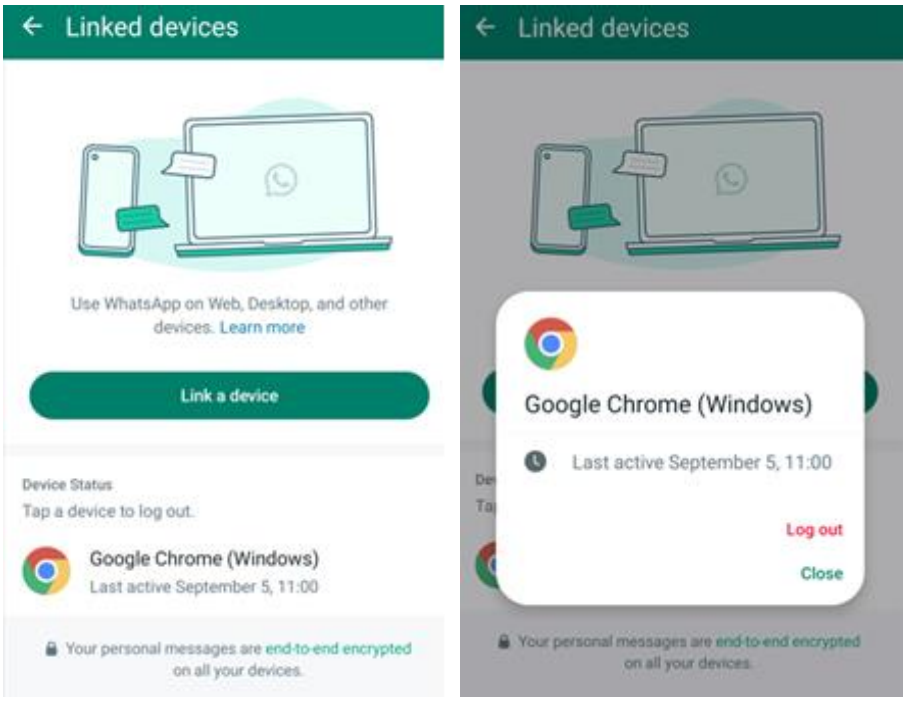
- **Privacy Breach:** Strangers may use video calls to invade your privacy by secretly recording videos or taking photos for improper use or dissemination. In addition, careless use of the screen sharing function in WhatsApp increases the risk of data leakage (Right Image). For example, the user is using banking service or typing a password.

# Preventive Measures

1. **Strengthen Account Security:**
   - Set a PIN code and change it regularly: Avoid using the same PIN code across different accounts and consider adding an email address for PIN code resets.
   - Enable two-step verification: Activate the two-step verification feature in your WhatsApp settings. This adds an extra layer of security to your account, requiring a PIN code for login.

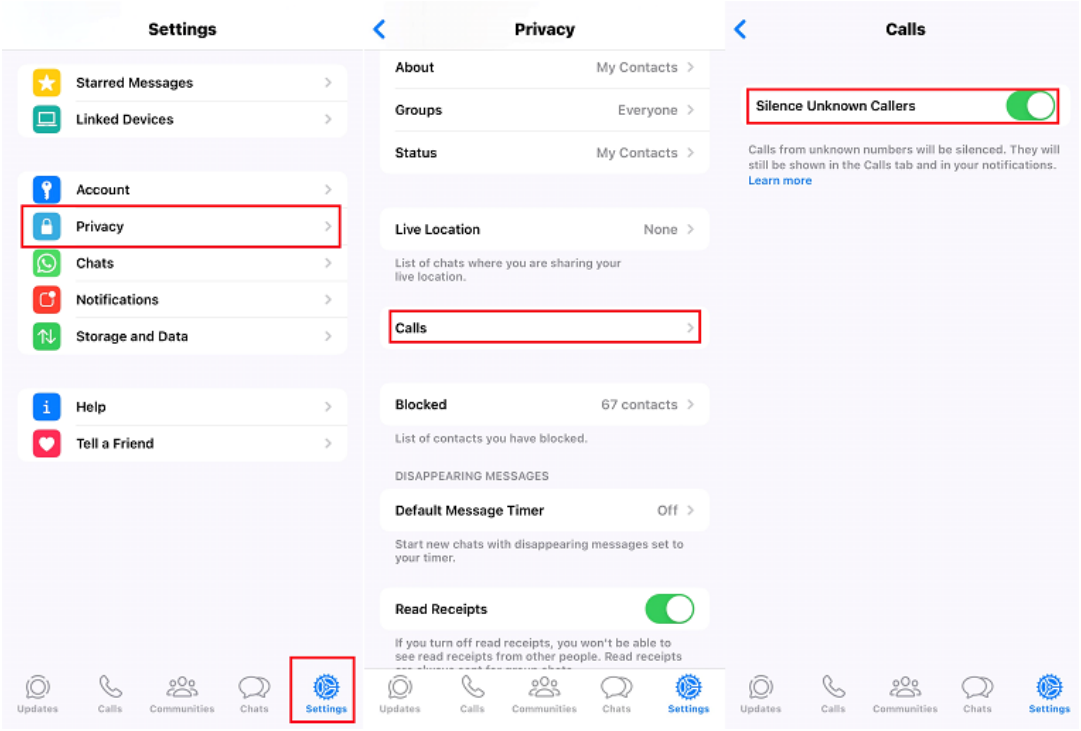



   - Do not share verification codes: Do not share any received verification codes with anyone, including family and friends. Scammers may attempt to gain control of your account by asking for verification codes.
   - Regularly check linked devices in WhatsApp settings: Log out of any devices that are no longer in use.




If you discover any unfamiliar devices in the "Settings -> Linked Devices" list, you should immediately log out of those devices.

- **Configure Privacy Settings:** Check the privacy options of your devices and applications to ensure that only authorized individuals can initiate video calls with you, or you can mute unknown callers (Open WhatsApp “Setting” > “Privacy” > “Calls” > enable “Silence Unknown Callers”).



2. **Be cautious of social engineering attacks:**
    - **Verify the identity:** When receiving messages involving money or emergency situations, try to verify the sender's identity through alternative channels. You can confirm the person's real identity through voice or video calls.
    - **Exercise caution when clicking on links:** Avoid clicking on unfamiliar links, especially when receiving unusual or suspicious messages. These links may contain malicious software or phishing websites that can compromise your account security.

3. **Regularly update and secure your devices:**
    - **Update applications:** Ensure that your WhatsApp application and device operating system are up to date to benefit from the latest security patches and features.
    - **Install official software:** Install trusted security software on your mobile phone or device to detect and block attacks from malicious software.

4. **Increase awareness:**
    - **Learn about scam techniques:** Familiarize yourself with different types of scams and common scam patterns. This will help you identify and avoid scams more effectively.
    - **Communicate with family and friends:** Share information about these scams with your family and friends, reminding them to stay vigilant and cautioning against easily trusting suspicious messages.

Protecting personal information and privacy is the responsibility of each individual. In light of recent cases of WhatsApp account theft in Hong Kong, it is crucial to enhance account protection, increase awareness, and strictly follow security measures. By using strong passwords, enabling two-step verification, being cautious of social engineering attacks, regularly updating and securing devices, and increasing awareness, we can better protect our WhatsApp accounts from scam threats.

**For more details, please refer to:**
https://www.hkcert.org/blog/hkcert-alerts-the-public-on-preventive-measures-against-whatsapp-account-theft

# Ransomware Trends Q2 2023: Surge in Attacks Across Asia-Pacific, Persistent Multiple Extortion, and Evolving Threat Landscape


*The evolution of ransomware has significantly affected businesses in recent years. Current trends indicate that ransomware developers are increasingly inclined to employ multiple extortion strategies. Furthermore, they have expanded their focus to platforms that previously received less scrutiny, such as the macOS operating system. Employing diverse technical methods to evade detection and exploit vulnerabilities across various products, they have made the detection and prevention of ransomware attacks more challenging.*

## Significant Increase in Ransomware Attacks in the Asia-Pacific Region

**There has been a significant increase in ransomware attacks targeting the Asia-Pacific region. According to research by cyber security firm Check Point, the second quarter of 2023 witnessed a ransomware attack on one in every 44 organisations worldwide. Comparatively, the number of attacks in the Asia-Pacific region saw a 29 percent increase compared to the same period in 2022, indicating an upward trend in ransomware attacks. Among the sectors affected, government/military, healthcare and education/research sectors suffered the highest number of ransomware attacks. In addition, utilities, insurance/legal and consulting organisations have witnessed a rise in ransomware attacks. Recently, a hospital chain in California had to suspend most of its IT services due to ransomware attacks, affecting 17 hospitals and 166 clinics. Consequently, it is crucial for relevant industries and organisations to fortify their cybersecurity measures to safeguard against such threats.**

Recently, there have been incidents in Hong Kong where data leaks occurred due to ransomware attacks. Institutions such as Cyberport, Consumer Council, and Hong Kong Ballet have become victims of such incidents. These events serve as a reminder of the importance of personal data and the necessity of protecting oneself from ransomware attacks. This article aims to provide the public with relevant knowledge about ransomware and emphasize the importance of safeguarding personal data, in order to help raise awareness and take appropriate preventive measures.

## Threat of Ransomware

Ransomware is a type of malicious software that can invade your computer system and encrypt your files. Subsequently, the attackers will demand a ransom payment (usually in the form of cryptocurrency) to decrypt your files. This type of attack causes significant losses for individuals and organizations, including data loss, financial damages, and reputational harm.


## Impact of Data Leaks

The incidents of data leaks at institutions such as Cyberport, Consumer Council, and Hong Kong Ballet have garnered significant attention. These events highlight the serious consequences of personal data leaks, including infringements on personal privacy, identity theft, and financial fraud, among others. These incidents serve as a reminder to the public that protecting personal data is an urgent task, irrespective of whether it pertains to individuals or organizations.

## Multiple Extortion Continues

Based on research conducted by cybersecurity firm Palo Alto Networks Unit 42, it was found that as of late 2022, data theft occurred in an average of 70% of ransomware cases. This represents a significant increase compared to mid-2021, data theft occurred in only around 40% of ransomware cases on average. Additionally, research conducted by cybersecurity firm Cisco Talos revealed a substantial 25% increase in the number of data theft extortion cases during the second quarter of 2023, as compared to the first quarter. These findings indicate a continuing and escalating trend of multiple extortion and data theft. In such attacks, ransomware gangs coerce victim organizations by threatening to leak stolen data on the dark web if the ransom is not paid.

Recently, Hawaii Community College even paid a ransom to ransomware gangs to prevent data leakage. Although the ransomware gangs have removed the relevant organisations entries from the data leakage website after receiving the ransom, but it cannot be ruled out that they may continue to ransom the victims or leak the data in the future.

## Ransomware Keeps Evolving

Recently, the well-known ransomware gang and service provider LockBit introduced a new variant specifically targeting Apple macOS devices. In addition, according to research by cyber security firm Uptycs revealed that ransomware service provider Cyclops has developed ransomware that can infect all three major operating systems (Windows, Linux, and macOS). This indicates an increasing trend among ransomware gangs to target various systems. Furthermore, there is a new ransomware Cactus, which exploits vulnerabilities in VPN devices to gain initial access to the victim organisation network and infect the victim organisation devices. The difference between Cactus and other

ransomware is that it encrypts the ransomware itself. By encrypting itself, it can bypass detection by antivirus software and network monitoring tools, enabling it to carry out malicious activities undetected.

According to research by cyber security firm Cisco Talos and Vmware, two new ransomware activities emerged in the second quarter of 2023, namely 8Base and MoneyMessage. 8Base was first discovered in March 2022, but its activity increased dramatically from June 2023 onwards. 8Base uses customised Phobos ransomware to conduct data theft and file encryption, and Phobos ransomware is sold in the underground market as ransomware-as-a-service (RaaS). MoneyMessage ransomware activity was first discovered in March 2023, and similar to 8Base it uses the same double extortion model. Considering the increasing ransomware activity, it is crucial to take immediate action and proactive measures must be implemented to mitigate the risks posed by ransomware attacks.

## Exploiting Product Vulnerabilities to Conduct Attacks

Numerous ransomware gangs are actively exploiting product vulnerabilities in various products to execute data theft. For example, Bl00dy, Clop, and LockBit ransomware have been identified targeting product vulnerabilities such as PaperCut, GoAnywhere MFT, and MOVEit Transfer. These vulnerabilities serve as entry points for data theft and facilitate lateral movement within compromised systems. PaperCut is a widely adopted printer and document management solution utilised by enterprises and educational instiutions, while GoAnywhere MFT and MOVEit Transfer are enterprise-level file transfer and collaboration platforms designed to provide secure file sharing and transfer capabilities.

## Measures to Strengthen Defence

The evolution of ransomware persists, with attackers expanding their focus beyond operating systems and actively developing novel techniques to evade detection and amplify the impact of their attacks. This presents a substantial challenge for cyber security and data protection efforts, underscoring the critical need for organisations and individuals alike to heighten their security awareness and implement robust protective measures. Urgency and importance lie in strengthening defences against these evolving threats.

HKCERT advises users and system administrators to stay alert and take appropriate protection measures:

**General User:**

1. Regular update and upgrade of systems and applications, include operating systems and anti-virus software;
2. Change your password regularly, and use Multi-Factor Authentication (MFA) to increase the security of your account;
3. Backup important files and data regularly and store the backups offline and in an encrypted location;
4. Conduct regular cyber security training to keep abreast of the latest cyber threats and enhance staff ability to recognise cyber-attacks.
5. Use public Wi-Fi networks with caution and avoid accessing sensitive information or conducting financial transactions. Use a virtual private network (VPN) to encrypt your

internet connection and protect your data from interception.

6. Exercise caution when dealing with emails and attachments. Avoid opening emails or attachments from unknown sources to prevent triggering malicious software or ransomware.

**System Administrator:**

1. Minimise the number of users with privileged access (e.g., domain administrative rights) to confine the scope and impacts in case of an attack and use general account in day-to-day operation.
2. Harden the network infrastructure and minimise the points of exposure to the Internet.
3. Implement endpoint security protection solutions to inspect emails and web content for malicious payloads, detect and quarantine malicious programs to prevent malware infection.
4. Build cyber threat intelligence capability to keep track with most recent threats, and exchange information with peer organisations to pre-empt emerging attacks.
5. Ensure network monitoring and security detection are in place and ready to carry out immediate incident response if any abnormal network activities are detected.

In summary, the recent ransomware incidents in Hong Kong serve as a reminder of the importance of protecting personal data. We should enhance our awareness of ransomware and take appropriate preventive measures, such as keeping our systems updated, exercising caution with emails and attachments, creating strong passwords, being cautious when using public Wi-Fi, and regularly backing up important data. Safeguarding personal data is not only crucial for personal privacy but also for financial security and reputation protection. Let us work together to raise awareness and protect our personal data from the threat of ransomware.

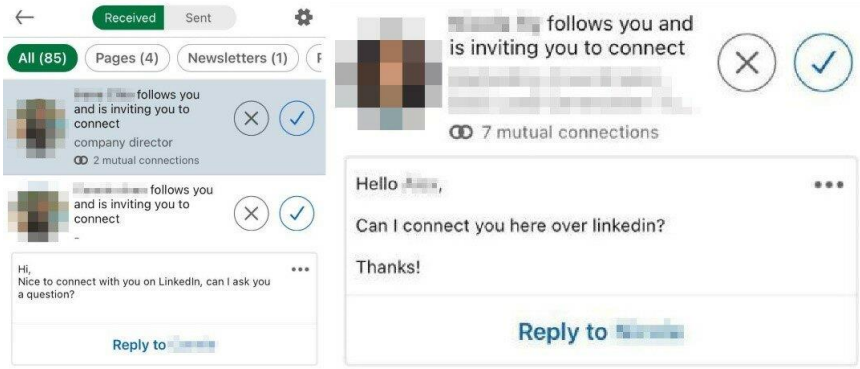
For more details or security advice, please refer to the security blog "Unmasking Cybercrime-as-a-Service: The Dark Side of Digital Convenience" or "Incident Response Guideline for SMEs".

**For more details, please refer to:**
https://www.hkcert.org/blog/ransomware-trends-q2-2023-surge-in-attacks-across-asia-pacific-persistent-multiple-extortion-and-evolving-threat-landscape

# Comprehensive Guide to Social Media Scams: Setting up Defense to Safeguard Your Personal Information


***Social media has become a necessary part of people's daily lives, but it has also attracted the attention of unscrupulous individuals. The Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) reminds the public to be cautious of social media scams and to always remain vigilant. In this regard, we will delve into how to enhance the awareness of social media users, thereby more effectively curbing online fraudulent activities. Additionally, later in the article, we will provide some social media settings for securing Facebook and LinkedIn accounts to reduce the opportunities for others to access users' personal information.***

Although the development of science and technology has brought convenience to the public, it has also increased the channels for criminals to attack. Users have a responsibility to protect their own accounts and personal information. Here are several suggestions to prevent social media scams:

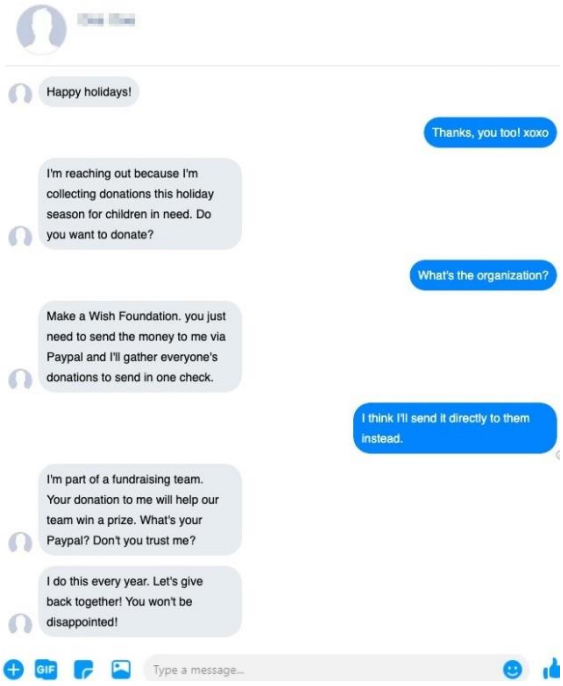



## Be cautious when dealing with strangers

There is always a risk when interacting with strangers online. Review the personal information of unknown individuals and determine their trustworthiness before considering whether to respond to them.

## Avoid sharing personal sensitive information

Do not disclose sensitive information such as your full name, address, phone number, bank details, or passwords to strangers.


## Pay attention to suspicious “signs”

If a stranger appears overly eager, offers unrealistic benefits, or request a user’s donation, they may have fraudulent intentions.

## Strengthen account protection

Enhance the security of your social media accounts through measures like strong passwords, multi-factor authentication, and SMS verification codes. At the same time, some social media site will set up a cyber security guideline page to provide the related settings for the public reference.

## Regularly review account privacy and security settings

Ensure the privacy settings of the social media accounts are properly configured, which is crucial to keeping the information uploaded only visible to designated users.

## Report suspicious behaviour

If you suspect any fraudulent activity, immediately report it to the relevant social media platforms and law enforcement agencies.

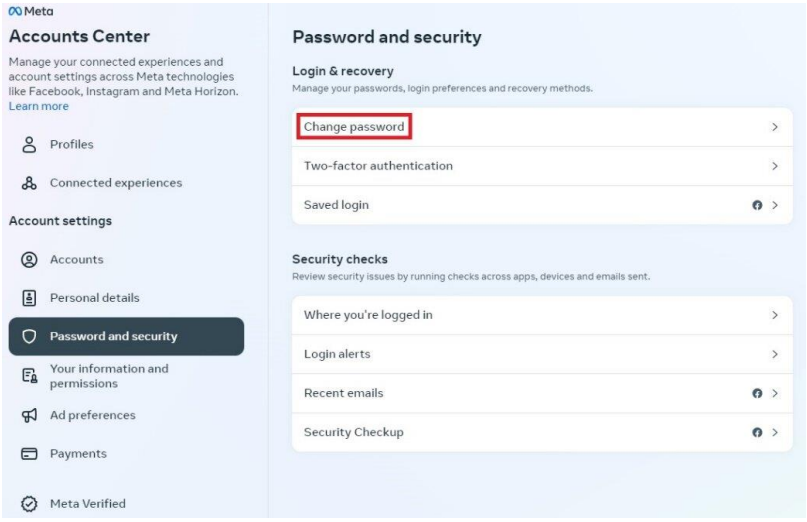
Social media provides many conveniences, but it also comes with risks. Users must learn to increase our awareness, handle all contacts with strangers carefully, and always remain cautious of suspicious signs. Then, we could enjoy the benefits of social media while being safe from online scams.

Facebook and LinkedIn offer various security settings for users to choose from.
Here are some examples:

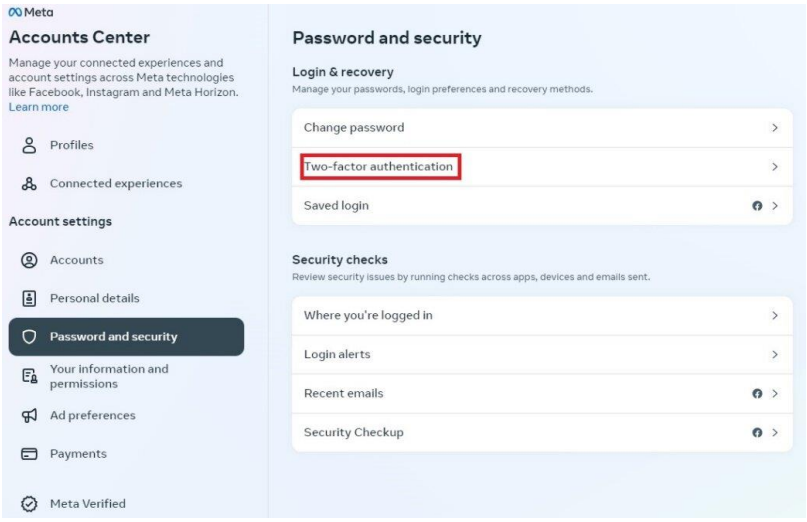
## Facebook Security Setting (Recommended)

For any other questions about Facebook, please refer to https://www.facebook.com/help

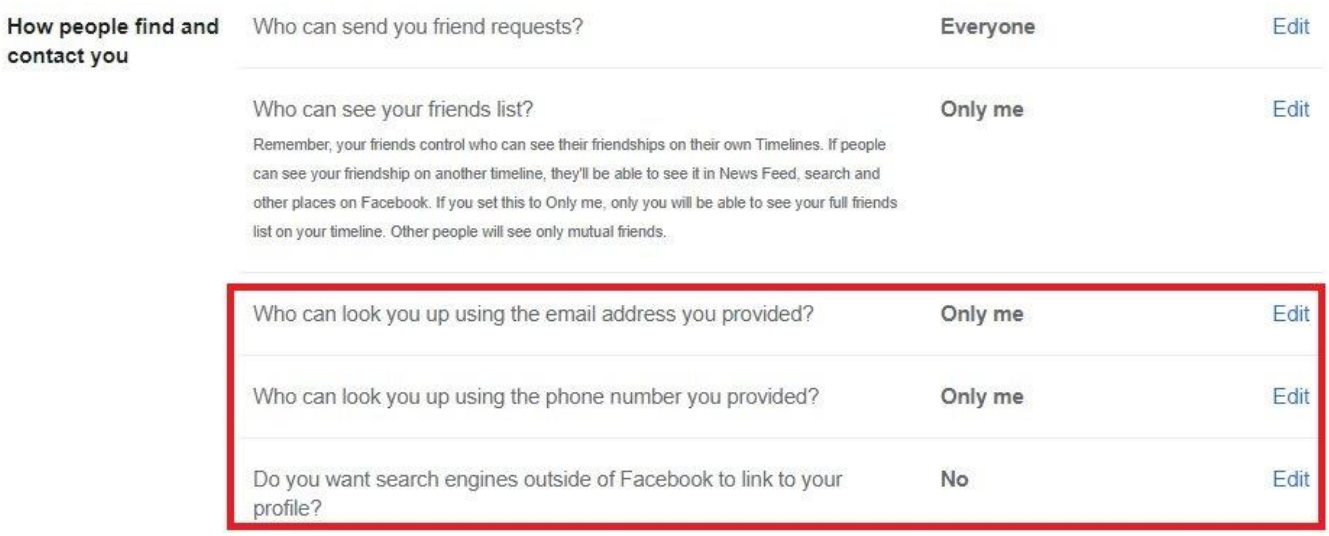
- Regularly change passwords (Develop the habit of regularly changing passwords. In case of any security concerns, promptly change the password.)



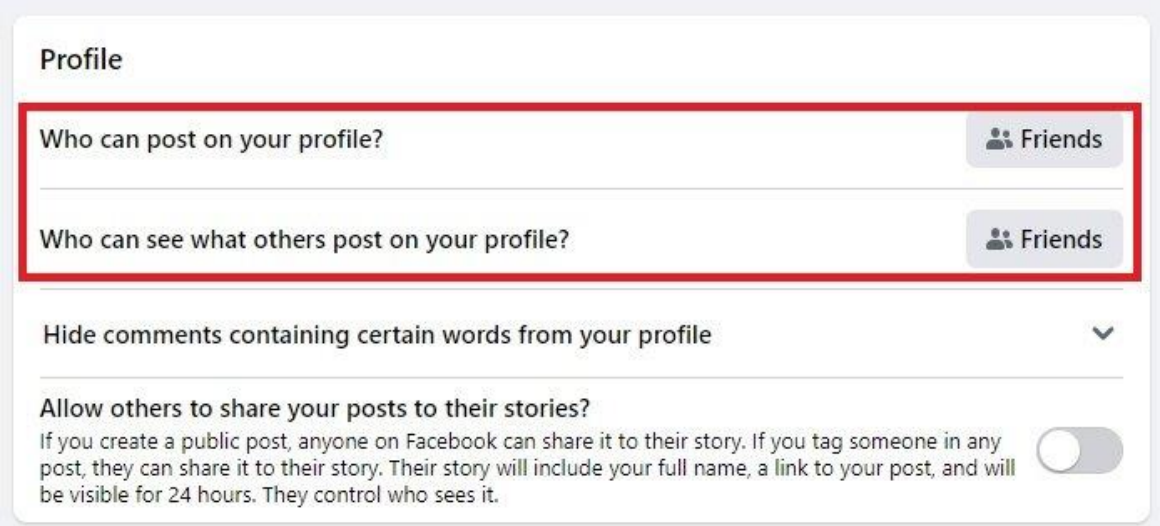

- Enable two-factor authentication (After enabling this feature, in addition to the login password, users will need to provide an additional verification method to verify their identity, reducing the chances of being hacked. This can include verification apps, SMS codes, or security keys.)




- Restrict others from finding you through alternative means (Users can limit others from finding you through phone numbers, email addresses, or search engines other than Facebook.)

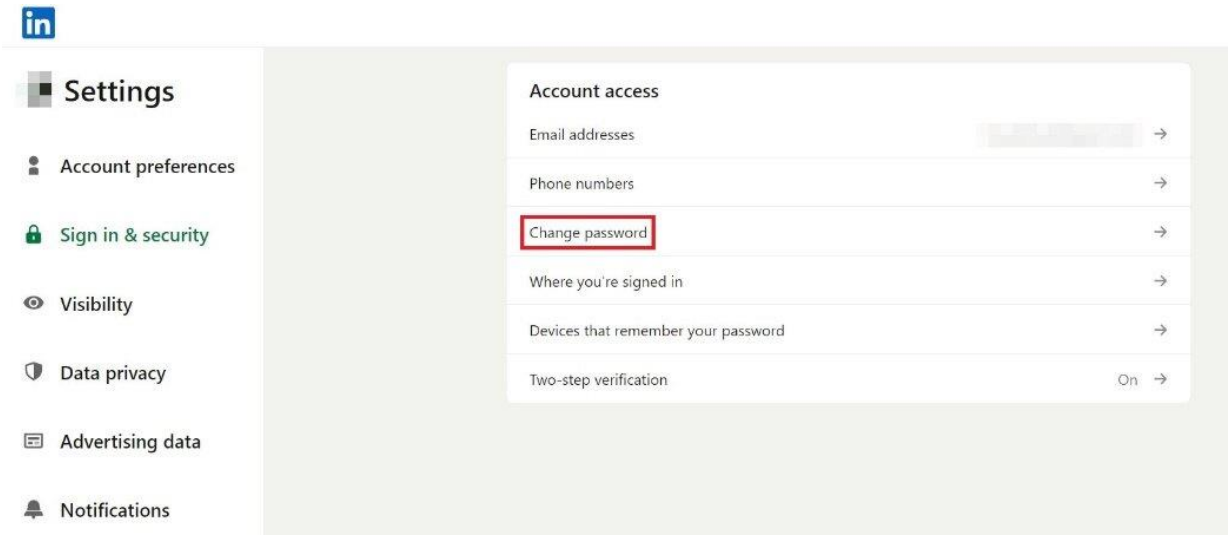



- Restrict everyone from seeing your profile posts (This can reduce the risk of further personal data exposure.)

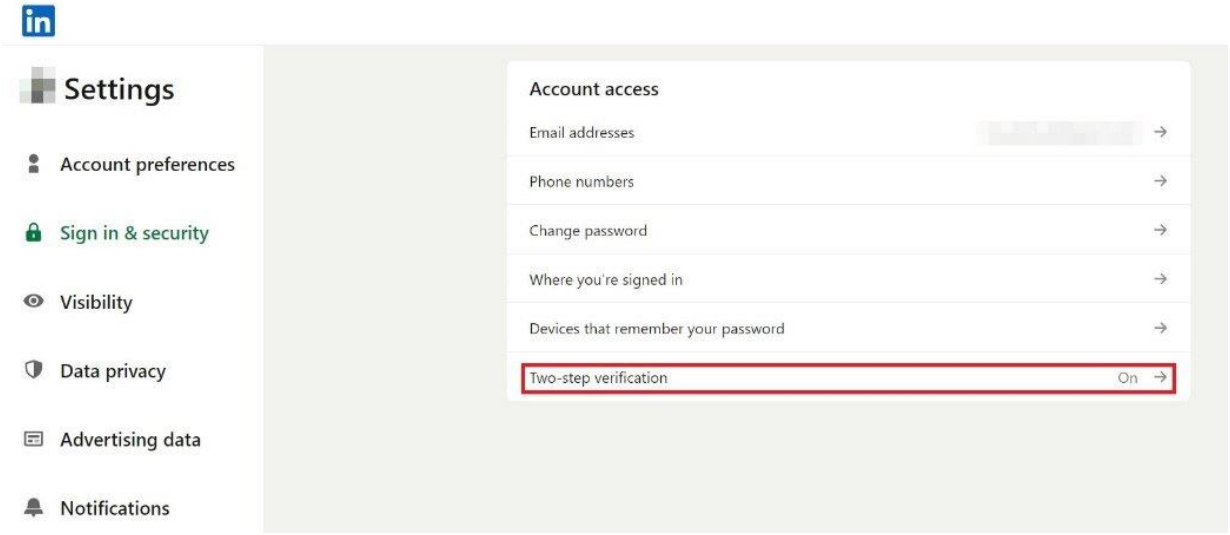



LinkedIn Security Setting (Recommended)
For any other questions about LinkedIn, please refer to https://www.linkedin.com/help/linkedin?lang=en

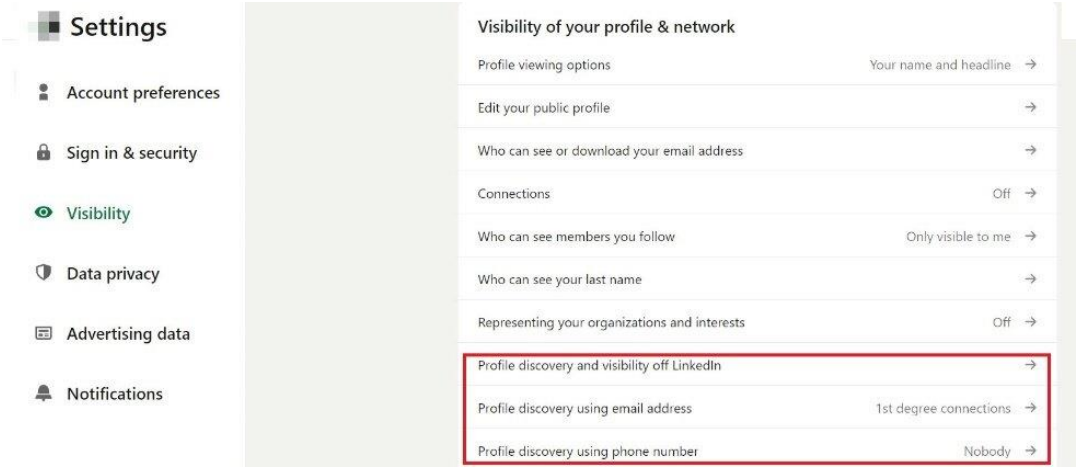
- Regularly change passwords (Develop a habit of regularly changing passwords. In case of any security concerns, promptly change the password.)



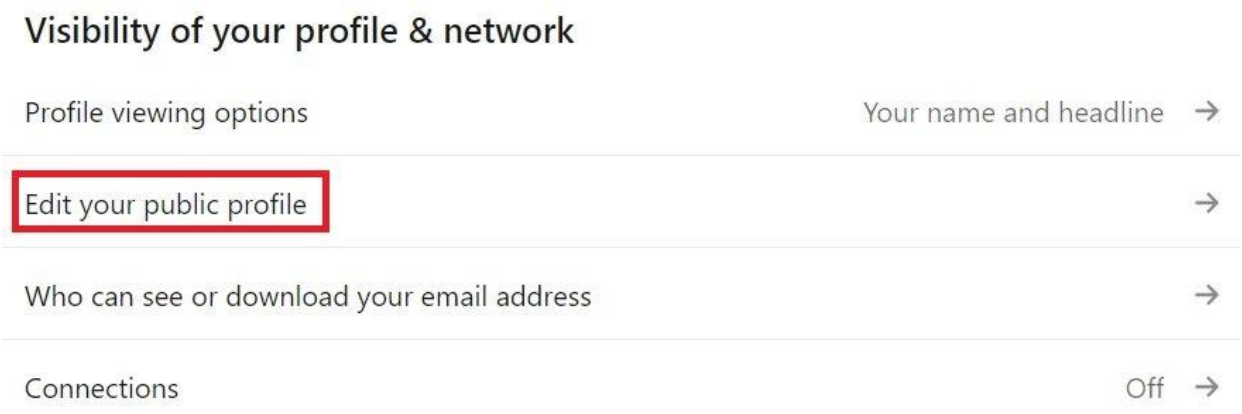

- Enable two-factor authentication (After enabling this feature, in addition to the login password, users will need to provide an additional verification method to verify their identity, reducing the chances of being hacked. This can include verification apps or SMS codes.)




- Restrict others from finding you through alternative means (Users can limit others from finding you through phone numbers, email addresses, or search engines other than LinkedIn.)




- Restrict everyone from viewing your profile posts (This can reduce the risk of further personal data exposure.)




The above suggestions are provided for user reference. Users can independently choose the security settings based on their preferences and needs. It is hoped that this article can provide the public with more ways to enhance awareness and effectively counter social media scams.

**For more details, please refer to:**
https://www.hkcert.org/blog/comprehensive-guide-to-social-media-scams-setting-up-defense-to-safeguard-your-personal-information

**-End-**

Hong Kong Computer Emergency Response Team Coordination Centre
Tel.: 8105 6060
Email: hkcert@hkcert.org