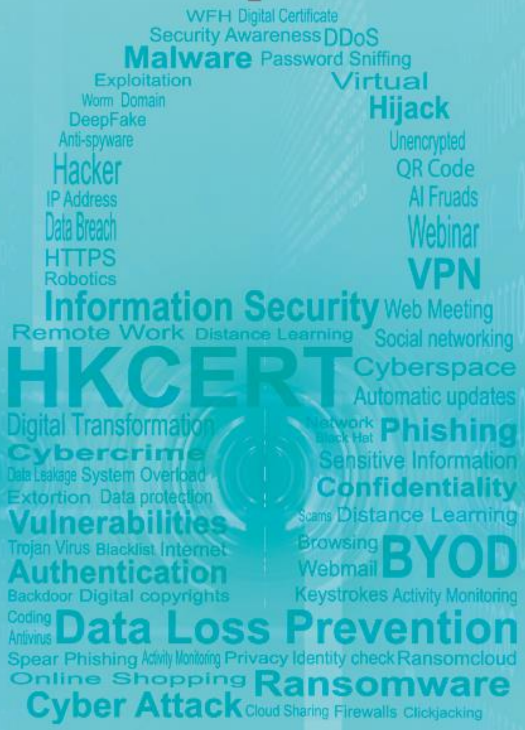
Hong Kong Computer
Emergency Response Team
Coordination Centre
HKCERT 香港電腦保安事故協調中心

Hong Kong Security Watch Report

2024 Q1

Release Date: May 2024



WFH Digital Certificate
Security Awareness DDoS
Malware Password Sniffing
Exploitation Virtual
Worm Domain Hijack
DeepFake
Anti-spyware Unencrypted
Hacker QR Code
IP Address AI Fruads
Data Breach Webinar
HTTPS
Robotics VPN
Information Security Web Meeting
Remote Work Distance Learning Social networking
HKCERT Cyberspace
Automatic updates
Digital Transformation Network Black Hat Phishing
Cybercrime Sensitive Information
Data Leakage System Overload Confidentiality
Extortion Data protection
Vulnerabilities Scams Distance Learning
Trojan Virus Blacklist Internet Browsing
Authentication Webmail BYOD
Backdoor Digital copyrights Keystrokes Activity Monitoring
Coding
Antivirus Data Loss Prevention
Spear Phishing Activity Monitoring Privacy Identity check Ransomcloud
Online Shopping Ransomware
Cyber Attack Cloud Sharing Firewalls Clickjacking

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	2024-04

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

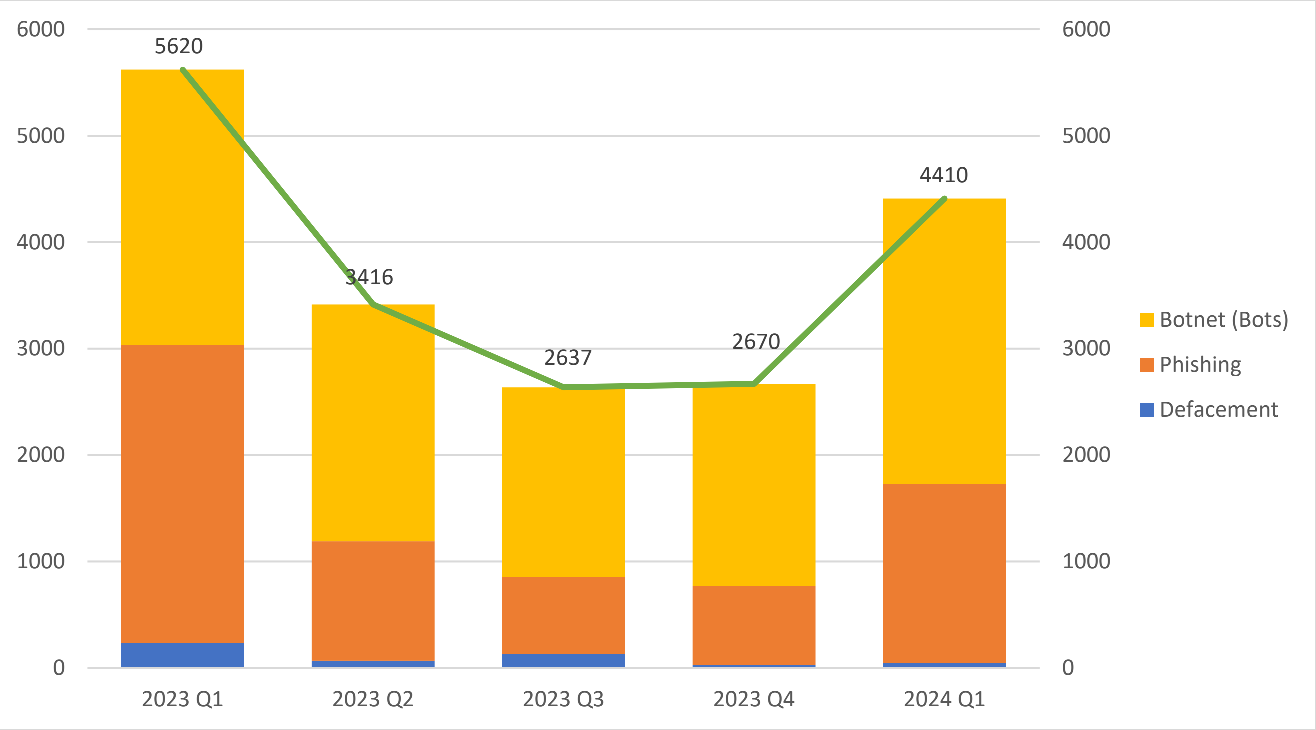
Highlights of the 2024 Q1 Report

Unique security events related to Hong Kong

4,410

Quarter-to-quarter

65.2%↑



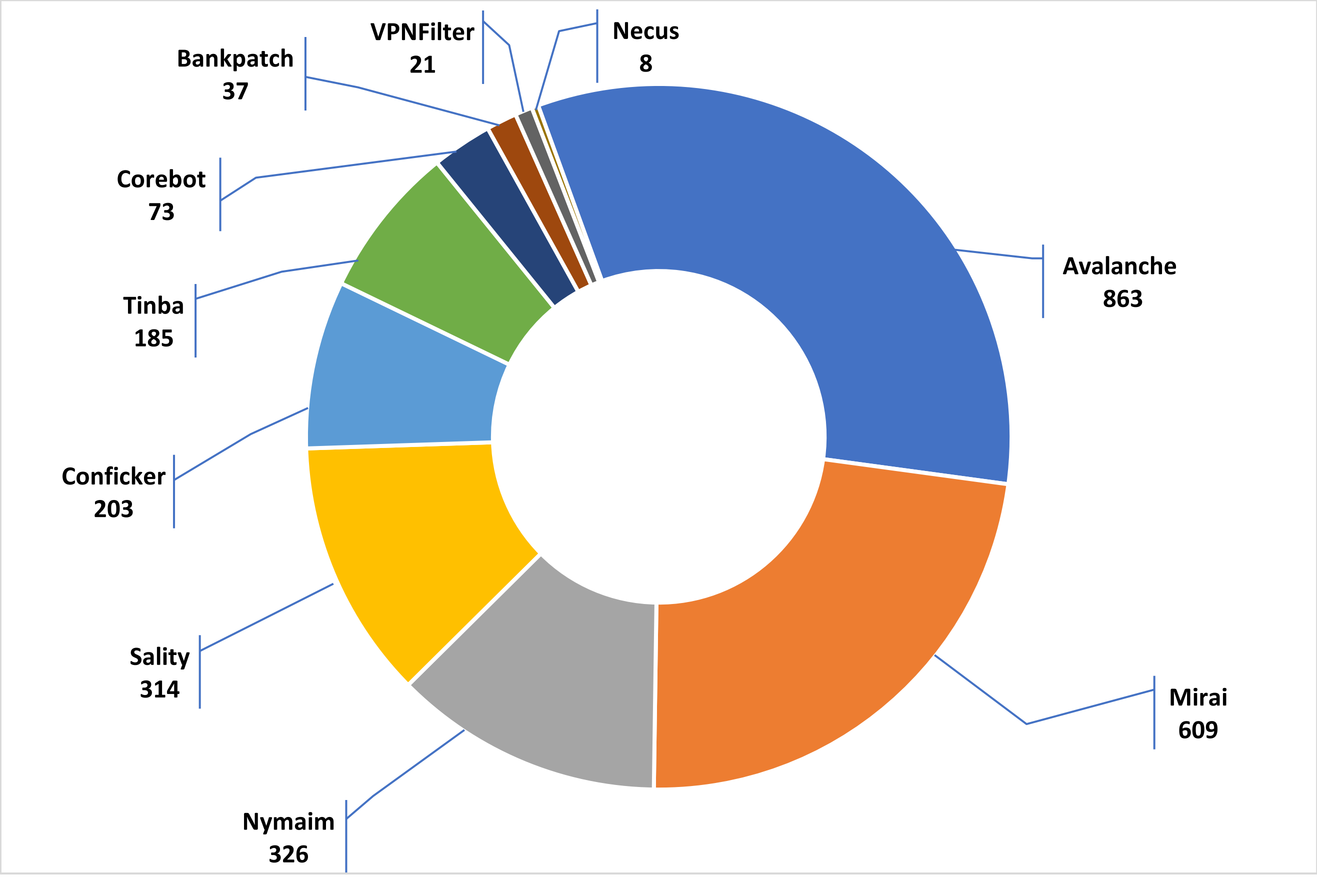
Event Type	2023 Q1	2023 Q2	2023 Q3	2023 Q4	2024 Q1	quarter-to-quarter
Defacement	233	69	132	31	46	+32.6%
Phishing	2,804	1,120	722	742	1,682	+126.7%
Botnet (Bots)	2,583	2,227	1,783	1,897	2,682	+41.4%
Total	5,620	3,416	2,637	2,670	4,410	+65.2%

Major Botnet Families in Hong Kong Network

Avalanche
863
↑ 99.3%

Mirai
609
↓ 17.7%

Nymaim	326	+176.3%
Sality	314	+1644%
Conficker	203	+13.4%
Tinba	185	+50.4%
Corebot	73	+564.6%
Bankpatch	37	-15.6 %
VPNFilter	21	-25%
Necus	8	-38.5%



** 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.*

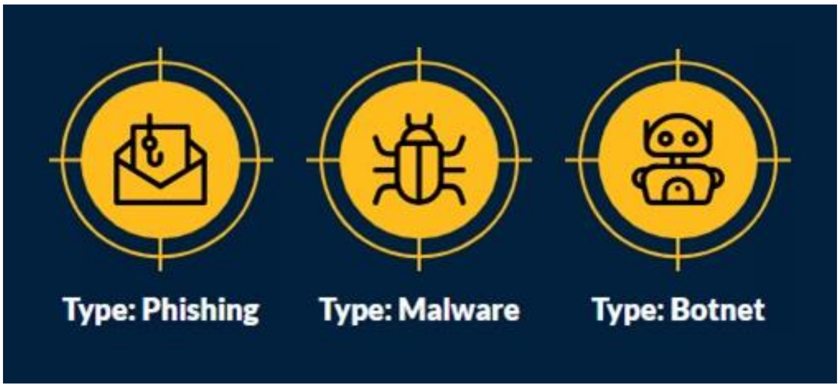
Cyber Security Risk Standing High, Prompt Reminders to Take Actions Will Be the Element

The figures for security incidents in the first quarter of 2024 were officially released. Defacement, phishing and botnet recorded significant growth in this quarter, with quarter-on-quarter increases of 32.6%, 126.7% and 41.4% respectively. Almost 40% of phishing URLs contained the string “usps” or “usops”. It is believed that hackers were pretending the portal service of United States after the holiday shopping season to increase the likelihood of clicking.

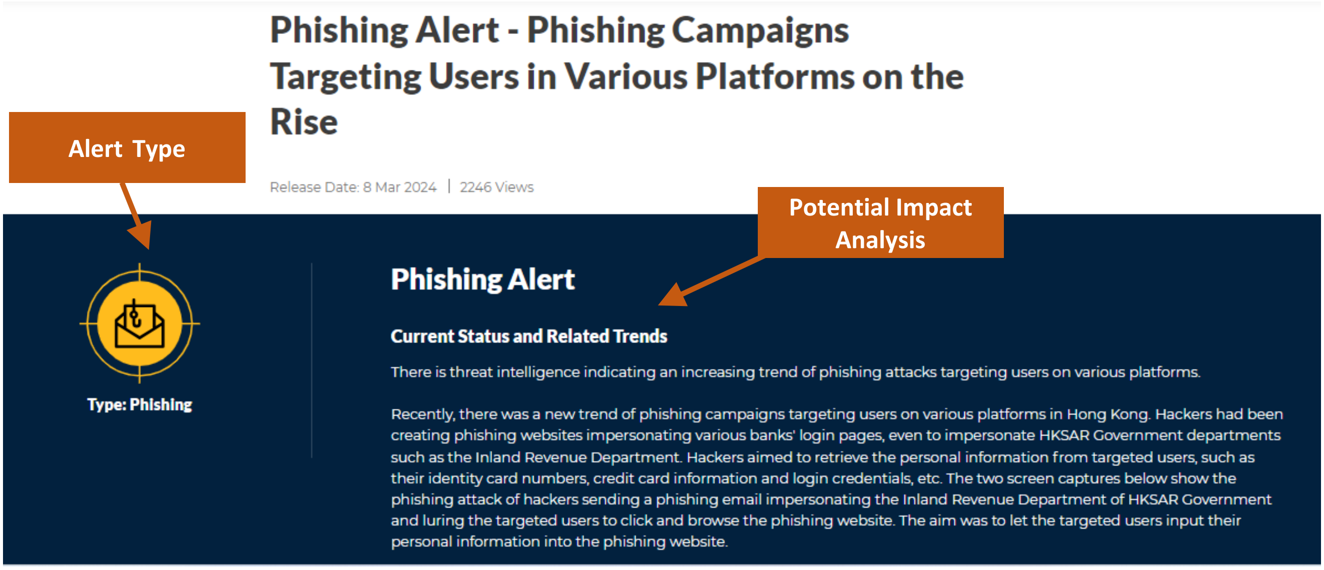
The figure of botnet Avalanche increased a fold compared to previous quarter. The botnet involved in the banking fraud and acted as downloader of other malware.

However, the relevant figures only reflected attacks originating in Hong Kong and did not include overseas. In other words, hackers may host the attack sources on overseas servers but target Hong Kong users. These types of cyber attacks were not reflected in the numbers. The actual numbers were much higher. The increasing trend of security events indicating that cyber attacks were frequent and the public requires to take precautions.

In response to the increasing cyber security risks, HKCERT added a new function, Security Alert, to the website in February 2024. HKCERT collects threat intelligence around the world for analysis and evaluation. If it is discovered that cyber attacks trend to be more active, HKCERT will publish an alert on the website to remind the public to respond to potential cyber attacks. Alerts include alert type, current situation and trend analysis, security advise and intelligence sources. There are three types of alerts. They are Phishing, Malware and Botnet.



Types of alerts



Phishing Alert - Phishing Campaigns Targeting Users in Various Platforms on the Rise

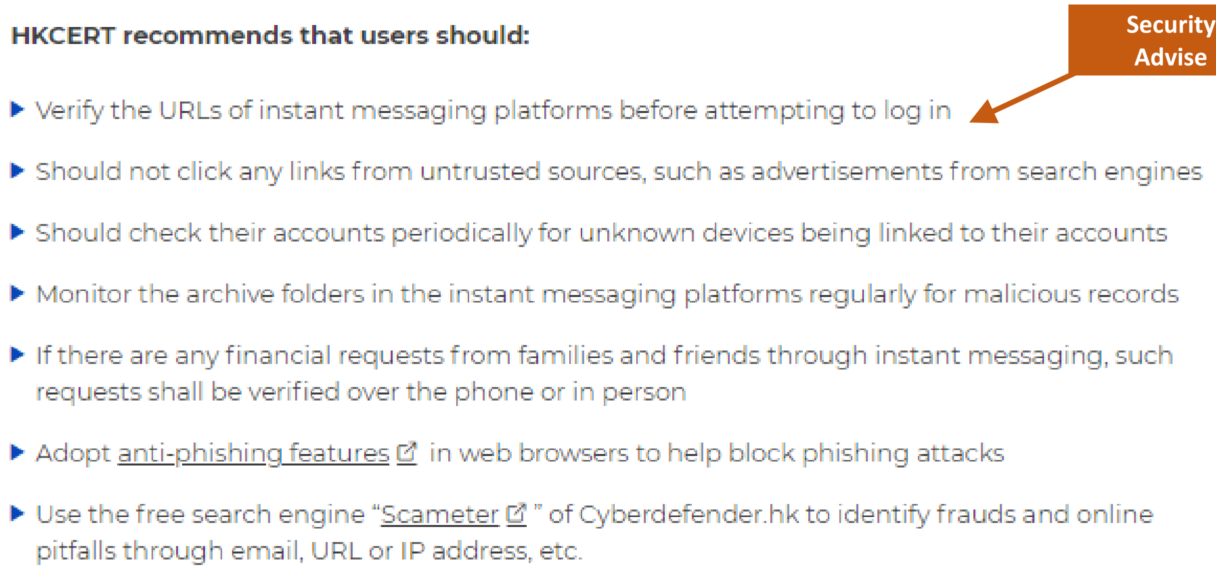
Release Date: 8 Mar 2024 | 2246 Views

Phishing Alert

Current Status and Related Trends

There is threat intelligence indicating an increasing trend of phishing attacks targeting users on various platforms.

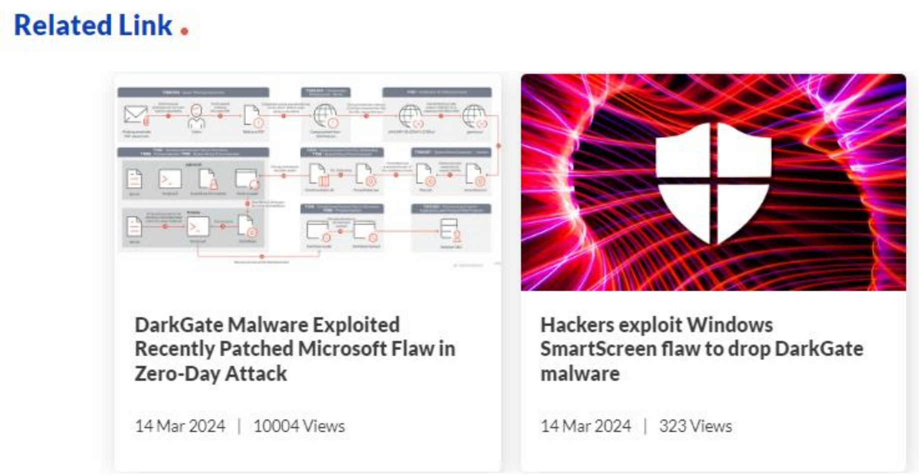
Recently, there was a new trend of phishing campaigns targeting users on various platforms in Hong Kong. Hackers had been creating phishing websites impersonating various banks' login pages, even to impersonate HKSAR Government departments such as the Inland Revenue Department. Hackers aimed to retrieve the personal information from targeted users, such as their identity card numbers, credit card information and login credentials, etc. The two screen captures below show the phishing attack of hackers sending a phishing email impersonating the Inland Revenue Department of HKSAR Government and luring the targeted users to click and browse the phishing website. The aim was to let the targeted users input their personal information into the phishing website.



HKCERT recommends that users should:

- Verify the URLs of instant messaging platforms before attempting to log in
- Should not click any links from untrusted sources, such as advertisements from search engines
- Should check their accounts periodically for unknown devices being linked to their accounts
- Monitor the archive folders in the instant messaging platforms regularly for malicious records
- If there are any financial requests from families and friends through instant messaging, such requests shall be verified over the phone or in person
- Adopt anti-phishing features in web browsers to help block phishing attacks
- Use the free search engine "Scameter " of Cyberdefender.hk to identify frauds and online pitfalls through email, URL or IP address, etc.

Security Advise



Related Link

DarkGate Malware Exploited Recently Patched Microsoft Flaw in Zero-Day Attack

14 Mar 2024 | 10004 Views

Hackers exploit Windows SmartScreen flaw to drop DarkGate malware

14 Mar 2024 | 323 Views

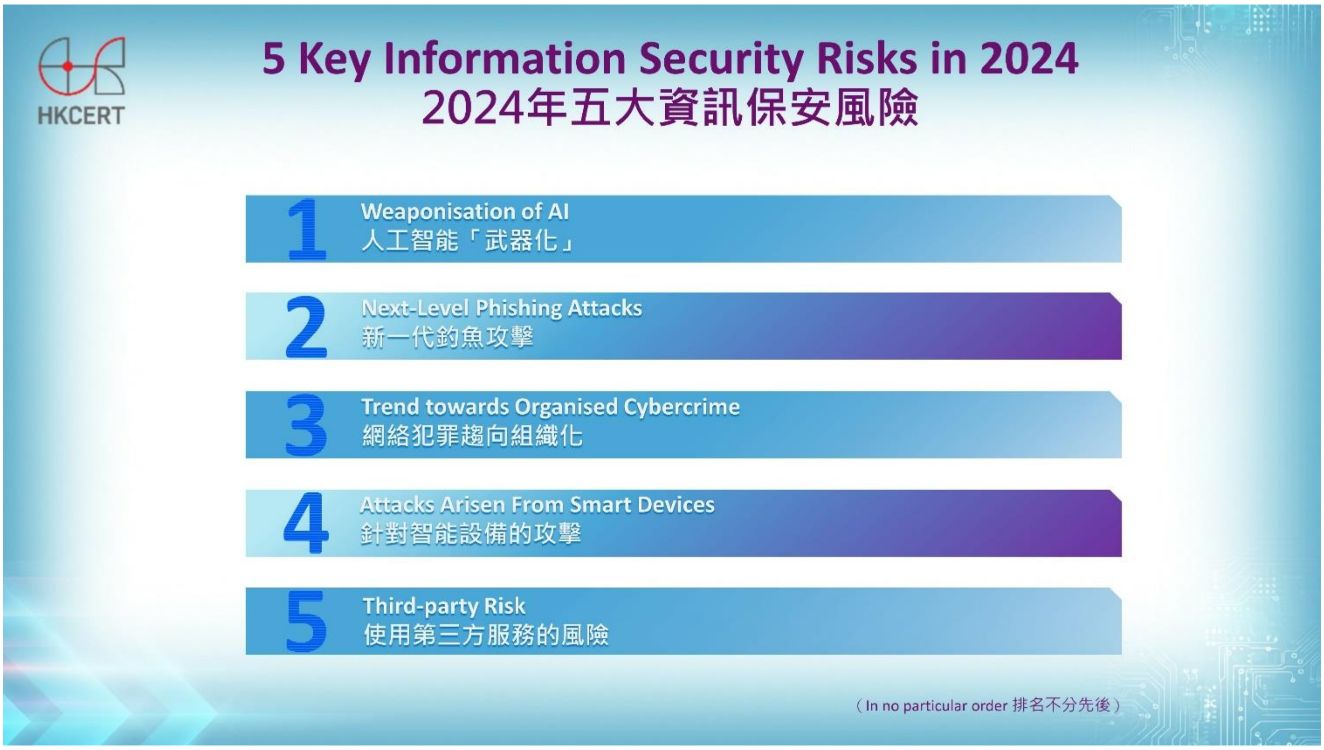
Intelligence sources

Until March, HKCERT has published phishing alerts and malware alerts to remind the public to prevent the latest phishing techniques and malware attacks. The public can search for relevant alerts at the top of the HKCERT website or in the Security Bulletin.

(Past alerts issued by HKCERT: https://www.hkcert.org/en/tag?q=Risk%20Alert)

5 Key Information Security Risk in 2024

Also, HKCERT summarised the cyber security situation in Hong Kong in 2023 and released a security outlook for 2024. Emerging technologies, such as artificial intelligence (AI), can bring additional benefits to businesses. However, with the development of these technologies, cyber attacks come one after another, and cyber threats become more complicated. Organisations and citizens must not underestimate them. It is important for organisations and citizens to have a better understanding of cyber security and to enhance their ability to respond to cyber security risks.



HKCERT

5 Key Information Security Risks in 2024
2024年五大資訊保安風險

1 Weaponisation of AI
人工智能「武器化」

2 Next-Level Phishing Attacks
新一代釣魚攻擊

3 Trend towards Organised Cybercrime
網絡犯罪趨向組織化

4 Attacks Arisen From Smart Devices
針對智能設備的攻擊

5 Third-party Risk
使用第三方服務的風險

（In no particular order 排名不分先後）

1. **"Weaponisation" of AI:** Hackers use generative AI to issue instructions for generating malicious code, dominating cyber attacks. Additionally, hackers can use AI to generate disinformation that affects the output of other AI, bypassing cyber security measures. Hackers also use AI to create fake videos to deceive for personal gain.

2. **Next-Level Phishing Attacks:** In addition to using traditional methods such as emails and text messages to conduct phishing attacks, hackers also use fake videos to impersonate someone’s identity. Phishing attacks also extend to social media platforms, impersonating some brand pages. At the same time, hackers use search engine optimisation (SEO) techniques to make phishing websites appear at the top of search results, deceiving more victims.

3. **Trend towards Organised Cybercrime:** In 2023, Hong Kong experienced several ransomware attacks targeting local organisations, resulting in large amounts of ransom being extorted and sensitive data being exposed. Citizens also faced threats from malicious apps and phishing. Globally, the number of ransomware attacks and vulnerabilities reached a new high in 2023, indicating an increasingly serious trend of organised and systematic cybercrimes.

4. **Attacks Arisen from Smart Devices:** Electronic products nowadays are most equipped with network connectivity, allowing them to connect to other devices or the internet. These products have varying cyber security standards and are susceptible to intrusion and malicious manipulation. Some products cannot patch security vulnerabilities, making them difficult to block cyber attacks.

5. **Third-party Risk:** Most companies use IT services provided by third-party, such as software and IT personnel, but this gives rise to IT supply chain attacks and insider threats, leading to data breaches, ransomware attacks, and other consequences. Additionally, research suggests that generative AI may produce incorrect information, such as code with security vulnerabilities or false information. If organisations adopt such information without verification, it brings risks to their operations.

Defacement Attacks: Understanding and Prevention

What is Defacement Attacks?

Defacement attacks occur when malicious actors infiltrate a website online or a digital advertising panel device hardware, and replace its content with their own messages. These messages can range from political or religious statements to offensive language or embarrassing content.

Here are some common causes of defacement attacks:

1. **Unauthorized Access:** Attackers gain unauthorized entry to the content management console of websites or digital advertising display panel devices, altering its appearance and content.
2. **SQL Injection:** Exploiting vulnerabilities in the website's database or device storage to manipulate content. Some of the digital advertising display panel devices are also based on web protocols.
3. **DNS Hijacking:** Redirecting users to a different server by falsifying DNS responses.
4. **Malware Infection:** Malicious software modifies website content or infects the operating systems to take control of digital advertising display panel devices.
5. **Cloud Resources Attack:** Attackers compromise cloud services' account credentials and take control of the cloud resources, in which to alter, delete or replace the website storage or cloud managed devices with malicious contents.

Real-World Examples of Defacement Attacks:

1. **Smart Billboards in Israel Defacement Attack Incident (2023):**
   - The hacker managed to hijack the smart billboards that switched commercials to anti-Israel, pro-Hamas footage.
   - Investigation shows the network of the smart billboard was opened to public for only few minutes, the hackers had immediately hijacked the devices.
2. **Ukrainian Government Websites Defacement Attack Incident (2022):**
   - The hacker managed to hijack a number of Ukrainian government websites and display posted provocative messages on the main pages.
   - Ukrainian CERT claimed that the attackers may have exploited the vulnerability in Laravel-based October CMS.
3. **Georgia's Largest Cyber Attack Incident (2019):**
   - 15,000 Georgian websites were defaced and knocked offline.
   - Government sites, banks, and media outlets were targeted.
4. **NHS Defacement Attack Incident (2018):**
   - The UK National Health Service (NHS) website was defaced by hackers, raising concerns about medical data safety.
   - The defacement message was removed, but the damage to the NHS's reputation persisted.
5. **Google.ro and PayPal.ro Defacement Attack Incident (2012):**
   - DNS hijacking led users to a defaced webpage instead of Google Romania's website.
   - The same attack affected the domain paypal.ro.

Impact of Defacement Attacks

1. **Loss of Credibility:** Defacement undermines a website's trustworthiness, affecting the company's or organisation's reputation.
2. **Data Breach Risk:** Vulnerabilities exploited during defacement attacks may lead to unauthorized access and data breaches.
3. **Service Interruption:** Defacement causes the website or digital advertising display services not functioning normally and thus affecting the online services and interrupt the normal operation.

Preventing Website Defacement

1. **Principle of Least Privilege**
   - Limit user permissions to the minimum necessary for their tasks
   - Regularly review and revoke unnecessary privileges
2. **Regular Vulnerability Scans**
   - Scan your website for vulnerabilities frequently
   - Address identified issues promptly
3. **Secure Coding Practices**
   - Follow secure coding guidelines to prevent common vulnerabilities
   - Validate user input and sanitize data
   - Develop with trusted coding libraries, avoid to end-of-support libraries.
4. **Web Application Firewall (WAF)**
   - Implement a WAF to filter out malicious traffic
   - Block suspicious requests and protect against attacks
5. **Perform Software Update**
   - Deploy latest software patch update to fix vulnerabilities

- Schedule to check software updates regularly

Securing Digital Advertising Display Panel Devices

1. **Physical Security**
    - Install panels in secure locations
    - Use tamper-resistant enclosures
    - Restrict physical access to administrative connection ports
2. **Network Security**
    - Isolate display panels from internal or corporate networks
    - Allow only corporate IPs to access the management panel
3. **Authentication and Authorization**
    - Restrict access to allow only authorized personnel
    - Use strong passwords and two-factor authentication
4. **Monitoring and Alerts**
    - Monitor display panels for anomalies
    - Set up alerts for unauthorized changes
5. **Perform Firmware and Software Update**
    - Deploy latest software patch update to fix vulnerabilities
    - Schedule to check software updates regularly

Organisations should take a proactive approach to cyber security to mitigate the risks associate with public materials, explicitly focusing on mitigating defacement attacks. HKCERT urges any organisations to stay vigilant to such cyber attacks and adopt the above security best practices.

For more details, please refer to:
https://www.hkcert.org/blog/defacement-attacks-understanding-and-prevention

Deepfake: Where Images Don't Always Speak Truth

> "Deepfake" is the combination of "Deep learning" and "Fake". It utilizes deep learning techniques to train on vast amounts of data, including facial images, voices, and videos. This data is used to mimic and learn the characteristics, movements, and sounds of different individuals. Then, artificial intelligence (AI) technology is employed to create fake content, including fake images, voices, and videos, thus enabling functions like AI Face Swapping and Voice Cloning.

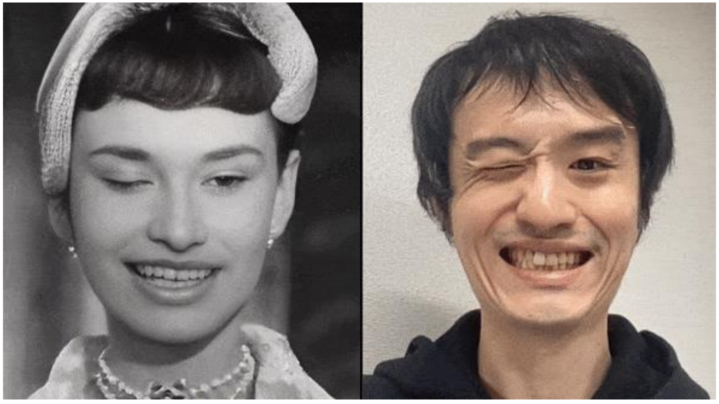
AI Face Swapping

AI Face Swapping is a technique that swaps a person's face with another person's face. This technology executes face swapping through facial recognition and facial capture. Nowadays the face swapping process can be easily done using a single image of the person's frontal face. AI can track the position and orientation of user's face and seamlessly fit it with the swapped face, even if the user's head is in motion. There are currently three main forms of AI face swapping:

1. **Replace your face with the face in a photo:** Replacing the face of a person in front of the camera with the face in a photo.

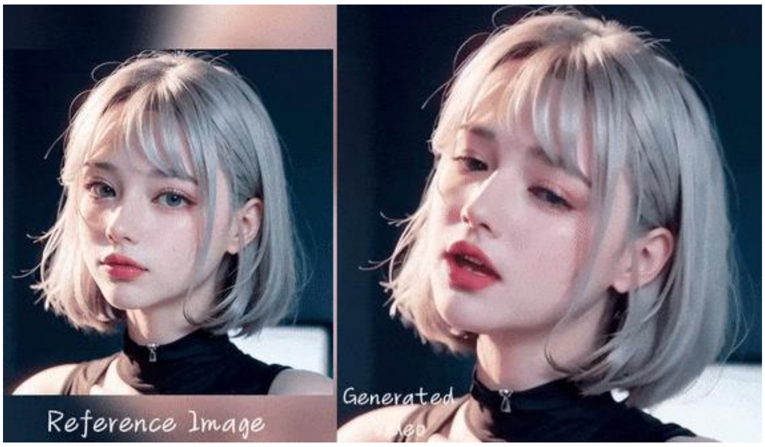
Source: HKCERT YouTube Channel

2. **Apply your expression to a photo:** Capturing the expression changes of a person in front of the camera, including the expression movements of lips, eyes, eyebrows, cheeks, and head, and reflecting these expressions onto another person's face in a photo. In this way, the viewer will feel as if he or she is communicating with the real person in the photo.



Source: Xpression Camera Demo

3. **Generate facial expression from audio:** Generating facial expressions and head movements of people in a photo based on recorded or real-time voice input, and converting the photo into a video that looks as if the person in the photo is speaking the voice input by the user. However, this technology is still in the research stage and has many limitations.



Source: Emote Portrait Alive (EMO) demo

The effectiveness of AI Face Swapping technology varies depending on the context of its application. In addition to editing prerecorded videos, some tools can even swap faces in real-time meetings. Generally, this technology produces realistic swapping effects that are difficult to distinguish from reality.

Voice Cloning

Voice cloning is a technology that uses AI to replicate voices. The cloned voice would sound like the original's person voice in real life, including the speed, pitch, accent, and style. There are two types of implementations for voice cloning:

1. **Text to Speech:** User inputs text, and the AI system reads it out using the replicated voice.
2. **Speech to Speech:** User inputs their own voice, and the original voice is replaced with the replicated voice.

Voice cloning requires large amounts of training data (usually more than 10 hours of recording of the target's voice to be cloned) and long training time (usually more than 10 hours, depending on the hardware) to obtain a high-quality voice replication.

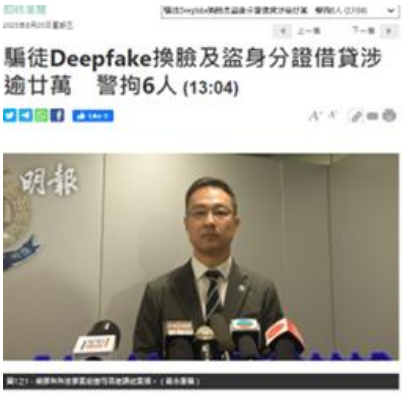
Through AI Face Swapping and Voice Cloning, combined with massive data training, we can create lifelike replicas of anyone in the AI system. These replicas have both visual and auditory effects that are extremely realistic, achieving a seamless integration.

New Threats to Cyber Security

Despite the positive applications of deepfake technology in entertainment and healthcare, such as digitally recreating the images of deceased actors or reproducing the voices of people who have lost their voices due to illness or accidents, the most widely known usage of deepfake is to create fake videos or audios of celebrities to disseminate false or misleading information. Other abusive usages involve sexual imagery and fraud. Therefore, the danger of deepfake technology cannot be ignored, and this danger has been fully demonstrated in some real cases.

Examples of Recent Incidents

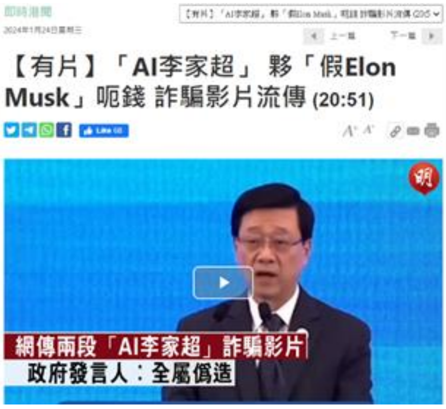
1. In August 2023, A criminal group was arrested for using deepfake to fake their identities to apply for loans.



騙徒Deepfake換臉及盜身分證借貸涉逾廿萬　警拘6人 (13:04)

Source (Chinese only): Ming Pao

2. In January 2024, a fake video surfaced featuring Hong Kong Chief Executive John Lee selling investment products, where the criminal used deepfake software to generate a fake voice of John Lee to make the video appear more authentic.



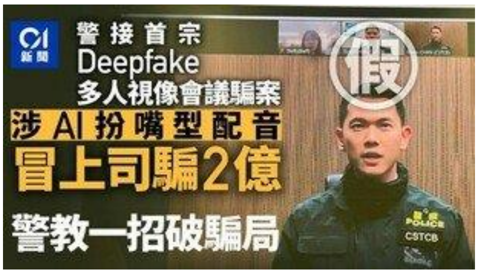
即時港聞

2024年1月24日星期三

【有片】「AI李家超」夥「假Elon Musk」呃錢 詐騙影片流傳 (20:51)

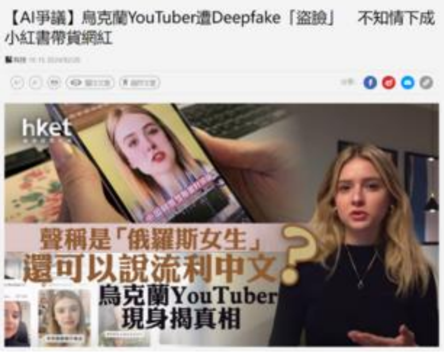
Source (Chinese only): Ming Pao

3. In February 2024, Hong Kong police reported a case where a multinational company's financial officer was deceived in a video conference. The criminals used deepfake technology to impersonate the company's chief financial officer, thereby defrauding the company of 200 million Hong Kong dollars.



Source (Chinese only): HK01

4. In February 2024, a Ukraine YouTuber discovered that her voice and face was stolen and being used in internet celebrity of selling good in Chinese social media using deepfake.



【AI爭議】烏克蘭YouTuber遭Deepfake「盜臉」　不知情下成小紅書帶貨網紅

Source (Chinese only): HKET

Impact of Abusive Deepfake

Numerous deepfake software applications are available on today's Internet, providing user-friendly interfaces for operation. Criminals can easily use this software to generate deepfake content even through cloud services. This accessibility makes it easy to create and spread deepfake content on the internet.

What is even more concerning is that deepfake technology may even bypass biometric security systems (such as facial or voice recognition), further increasing the risk of cyber security. In addition, the misuse of deepfake technology may induce more phishing and internet frauds, false and misleading information, as well as bring trust and reputation crisis.

Phishing and Internet Fraud

Cases originating from Hong Kong and globally are concerning. Deepfake technology enables criminals to create more sophisticated phishing attacks. In the past, phishing attacks primarily relied on written messages. However, with the aid of deepfake technology, criminals increasingly use this technology to impersonate others and engage in fraudulent activities towards victims' relatives or colleagues. Particularly in an era where video calls and video-based communication are commonplace, fraudsters are further incentivized to produce more deepfake videos to deceive victims.

False and misleading information

Criminals produce deepfake videos impersonating celebrities, politicians, officials, etc., to disseminate false or misleading information, such as fake investment advice, false shares or statements, misleading victims' decision-making, and even creating social conflicts.

Trust and Reputation Crisis

Deepfake content has the potential to create a climate of distrust on the internet. As Deepfake can be challenging to distinguish, if there is a plethora of such videos online, genuine information will also be affected. Since people cannot easily discern whether the information they receive is mixed with deepfake content, ultimately leading to distrust in any information to prevent being deceived. Additionally, deepfake content will replace the traditional fake videos, such as creating indecent, vulgar, or violent videos, leading viewers to believe that the victims are involved in certain activities, even if they are skeptical, it will damage the victim's reputation.

How to Spot Deepfake?

Identifying deepfake technology is quite challenging. Although there are online tools which claim to be able to detect the use of Deepfake in video, the key to distinguishing authenticity still lies in public awareness of security. Especially in a real time video scenario, such as in a video call or online conference, so we need to always remain vigilant.
If you receive a suspicious video call, you can take the following measures:

Interfering with Deepfake Recognition Function

1. Ask the person to slowly cover their face with their hand. The original face may be revealed because the facial recognition algorithm in the deepfake software may fail to recognise a covered human face.

2. Request the person to move the camera around to capture another person. Deepfake software may misidentify the person to be replaced, leading to instant changes in the faces of both parties, being repeatedly replaced.

Paying Attention to the Detail of the Person’s Face

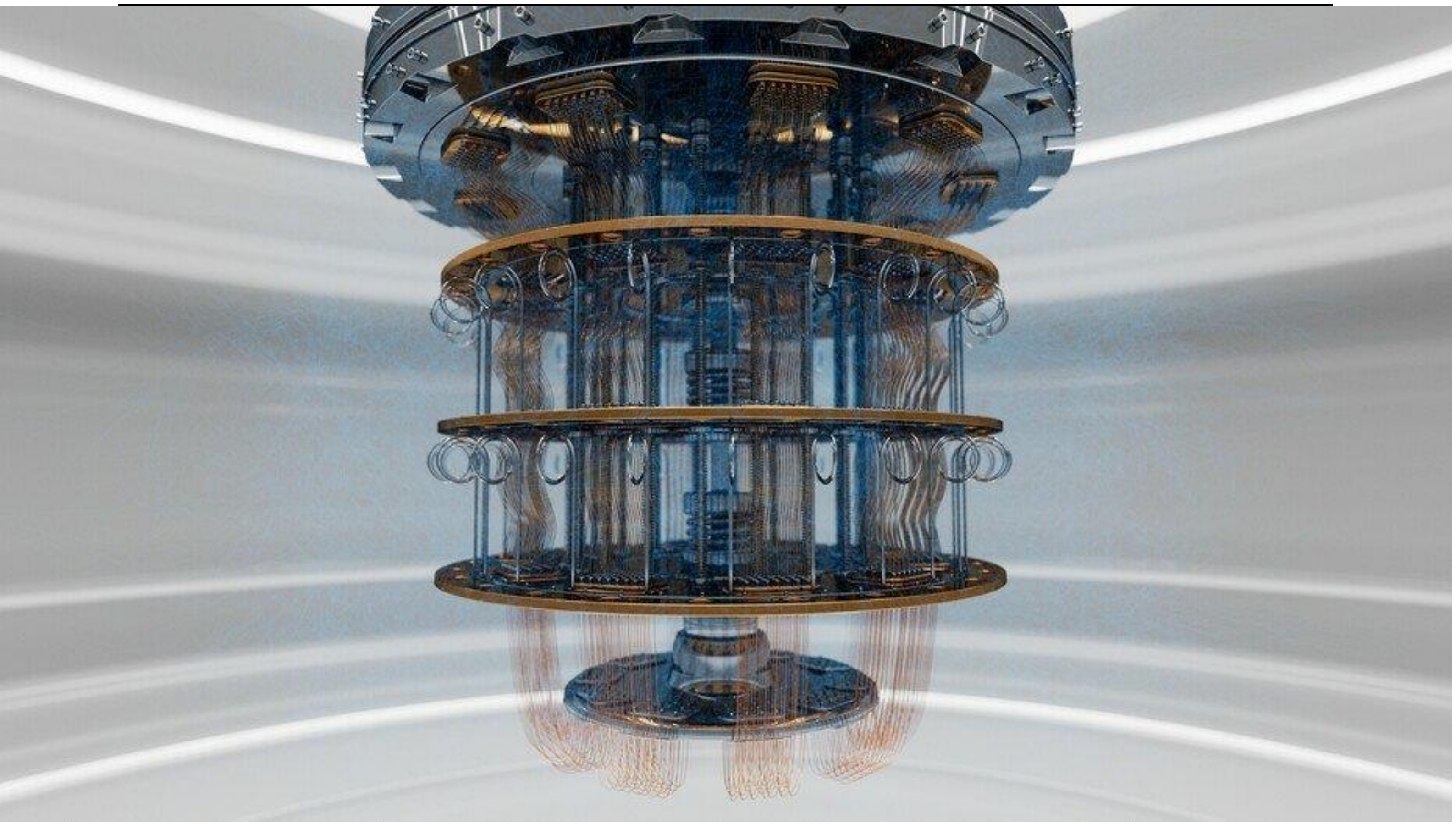
3. Observe the facial details of the person to identify any abnormalities when moving their head.
4. Check the skin colour, as facial color may differ from other parts of the body (e.g., neck, shoulders).
5. Pay attention to the person's skin texture, checking for excessive smoothness or too many wrinkles.
6. Focus on facial features for any unnatural features. For example:
    - l Whether the beard and hairstyle look authentic;
    - l Whether the person’s eyes appear natural;
    - l Whether facial expressions are too stiff;
    - l Whether there is any unreasonable expression when speaking, e.g. a serious expression on a relaxed face.
7. Observe whether the body below the head or background objects remain fixed.

Test the Person’s Reaction or Response

8. Ask questions about the fact that is known only between you and other person in order to verify his/her identity.

For more details, please refer to:
https://www.hkcert.org/blog/deepfake-where-images-don-t-always-speak-truth

How To Protect Your Data in Quantum Age



A quantum computer represents a groundbreaking paradigm shift in computing, leveraging the intricate principles of quantum mechanics to execute certain computations exponentially faster than their classical counterparts.

While classical computers rely on binary units known as classical bits, denoted as 0 or 1, quantum computers operate on an entirely different mechanism. They use quantum bits, or qubits, which possess the unique ability to exist in a superposition of states, simultaneously representing both 0 and 1. This property empowers quantum computers to explore multiple states concurrently. Moreover, qubits can become entangled, signifying that the state of one qubit can be intricately linked to another, even when separated by vast distances.

Quantum algorithms harness these characteristics to perform complex calculations with superior efficiency compared to classical computers for specific tasks, such as quantum world simulation, algorithm speedup, and artificial intelligence.

Apart from running quantum algorithms, quantum computers also can execute classical algorithms. However, due to the running environment and error correction of quantum computers, it is more efficient and cost-effective to execute day-to-day processing tasks such as word processing and spreadsheet calculation on classical computers. Therefore, it is believed that quantum computers would not replace classical computers, they would operate on different tasks instead.

Quantum Algorithm: A Potential Threats to Data Encryption

In contemporary digital communication, encryption stands as the vanguard of data security, ensuring the confidentiality and privacy of sensitive information. There are two major methods in modern encryption: symmetric and asymmetric encryption. The former, known as "symmetric," refers to a method where the sender and receiver share a single secret key generated from pseudorandom number. The key can be used for both encryption and decryption. Due to its efficiency, symmetric encryption is widely used in data transmission and storage encryption.

Asymmetric encryption, on the other hand, requires the use of different keys for encryption and decryption. A public key is used for encryption, while its corresponding private key is used for decryption. When generating the keys, two random prime numbers are multiplied together to generate a very large integer, which becomes part of both the public and private keys. For hackers, cracking the key requires finding the prime factors of that integer, a process known as prime factorisation (for example, the integer 3233 can be factored into the primes 61 and 53). However, this process takes the hacker a lot of time. Even though prime factorisation may be relatively easy for small numbers, there is no known fast algorithm that can solve this problem efficiently for large numbers. For example, given a 1000 digits number which is the product of two very large prime numbers, it may take billions of attempts to find the combination of these two large prime numbers. It requires a lot of computational time and resources, and makes cracking the encrypted message very difficult.

Therefore, prime factorisation plays a critical role in asymmetric encryption algorithms, ensuring its security by making it infeasible for hackers to crack encrypted messages.

Breaking Cryptography

Against the backdrop of the rise of quantum computing, Grover's algorithm proposed by Lov Kumar Grover poses a certain degree of threat to symmetric encryption, but it can only shorten the time to crack symmetric keys to some extent, which has a relatively small impact.

In contrast, Shor's algorithm proposed by Peter Shor could revolutionise today's asymmetric encryption. The algorithm leverages the superposition and quantum entanglement properties of quanta to drastically reduce the computation time for prime factorisation. For example, if we use the RSA encryption with 2048 bits RSA key, it may take a conventional computer 30 billion years to crack it. But if we use a quantum computer and apply the Shor’s algorithm, theoretically a hacker can crack the key within just 8 hours using a quantum computer of 20 million qubits. This breakthrough demonstrates the vulnerability of modern cryptography to the challenge of quantum computers.

Although current quantum technology has not yet been able to implement the Shor’s algorithm to break asymmetric encryption, with the advancement of technology and the invention of the new factorisation method, it is not impossible to break any existing encryption method swiftly, and people have even named the future day that quantum computers can be truly applied to break asymmetric encryption as Q-Day.

In addition, many people are concerned that hackers may collect existing encrypted data and decrypt it once quantum computers become powerful enough, which could pose a serious threat to data security.

Current Quantum Computers Pose a Relatively Low Threat to Data Encryption

At present, quantum computer development is less likely to pose an immediate threat to current data encryption application for several compelling reasons.

- Firstly, large-scale quantum computers capable of breaking widely-used encryption algorithms remain in the theoretical and experimental phase and are not yet readily accessible.
- Secondly, until now, there is no empirical evidence on running Shor’s algorithm to break the modern suggested encryption standard RSA-2048 (i.e. factoring a 617-digits natural number) because it requires capabilities beyond the current technology.
- Thirdly, the security level of both techniques depends on the length of the key, i.e. the longer the key is, the longer it takes to crack it, If the key size of symmetric encryption is large enough, there is no quantum algorithm to break it in a short time.
- Fourthly the establishment and maintenance of stable, error-corrected quantum computers pose formidable technological challenges.
- Furthermore, even if such quantum computers were to be realized, they would necessitate substantial resources and infrastructure.

Post-quantum cryptographic algorithms and their challenges

Although current quantum computing development cannot directly threaten modern encryption, concerns persist regarding the vulnerability of existing encrypted data when practical quantum computers become available. To address this concern, computer scientists and cryptographers are actively working on post-quantum cryptographic algorithms designed to protect data from quantum computers. These post-quantum cryptographic algorithms involve complex mathematical problems, approaches including Lattice-based cryptography and Hash-based Cryptography, etc., which are believed to be computational hard for both quantum and classical computer.

National Institute of Standards and Technology (NIST) of the United States selected 4 algorithms and is standardising them. Those 4 algorithms are CRYSTALS-Kyber (used in data encryption), CRYTRALS-Dilithium, SPHINCS+ and FALCON (used in digital signature). Two noteworthy applications include instant messaging application Signal’s 'PQXDH Protocol' (based on CRYTRALS-Kyber) and the 'FIDO2 security key' (based on CRYTRALS-Dilithium) introduced by Google. NIST would continue to evaluate different post-quantum cryptographic algorithms and may publish more in the future.

However, it's essential to note that even these post-quantum cryptography methods may face challenges, as demonstrated by the recent vulnerability discovered on CRYSTALS-Kyber public-key encryption. The research team used recursive training AI to break it by running deep learning analysis on measurable information such as timing and power consumption of devices using this encryption method. This highlights the need for ongoing research and adaptability in safeguarding our data against quantum threats.

Given that many post-quantum cryptographic algorithms are still in the early stages of development, one approach is hybrid cryptography to protect the data. This approach uses both classical encryption and post-quantum cryptography methods to encrypt data, ensuring data protection without relying solely on post-quantum cryptography.

Conclusion

Quantum computing is a fascinating technology which represent the new page of computing. While quantum computers excel in specific tasks, they also pose challenges to traditional data encryption techniques. Despite the current technological limitations, the proactive development of post-quantum cryptography methods opens up new possibilities for data security in a quantum-enabled future. However, these methods are not without challenges, and ongoing research and adaptability will be essential to stay ahead of evolving quantum threats. As we navigate this complex landscape, hybrid cryptography provides a promising approach to secure our data effectively, leveraging both classical and post-quantum cryptography techniques.

In the future digital era, with the development of quantum technology, it will become more crucial to protect the data security of individuals and organizations. In order to cope with quantum threats, HKCERT recommends everyone to pay attention to the development of post-quantum encryption methods and adopt hybrid encryption technology to ensure data security. It is also essential to pay more attention to data security, such as data classification, access control, key management, segregation of data storage and backup, data loss prevention, etc.. Only through continuous vigilance we can enhance the data security of individuals and organizations, and build a secure network environment for the future.

For more details, please refer to:
https://www.hkcert.org/blog/how-to-protect-your-data-in-quantum-age

- End -

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