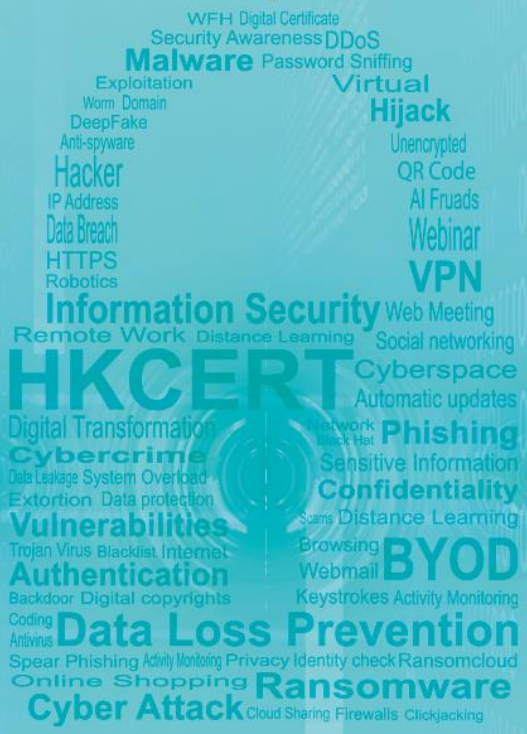
Hong Kong Computer
Emergency Response Team
Coordination Centre
HKCERT 香港電腦保安事故協調中心

Hong Kong Security Watch Report 2023 Q1

Release Date: May 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	2023-04

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

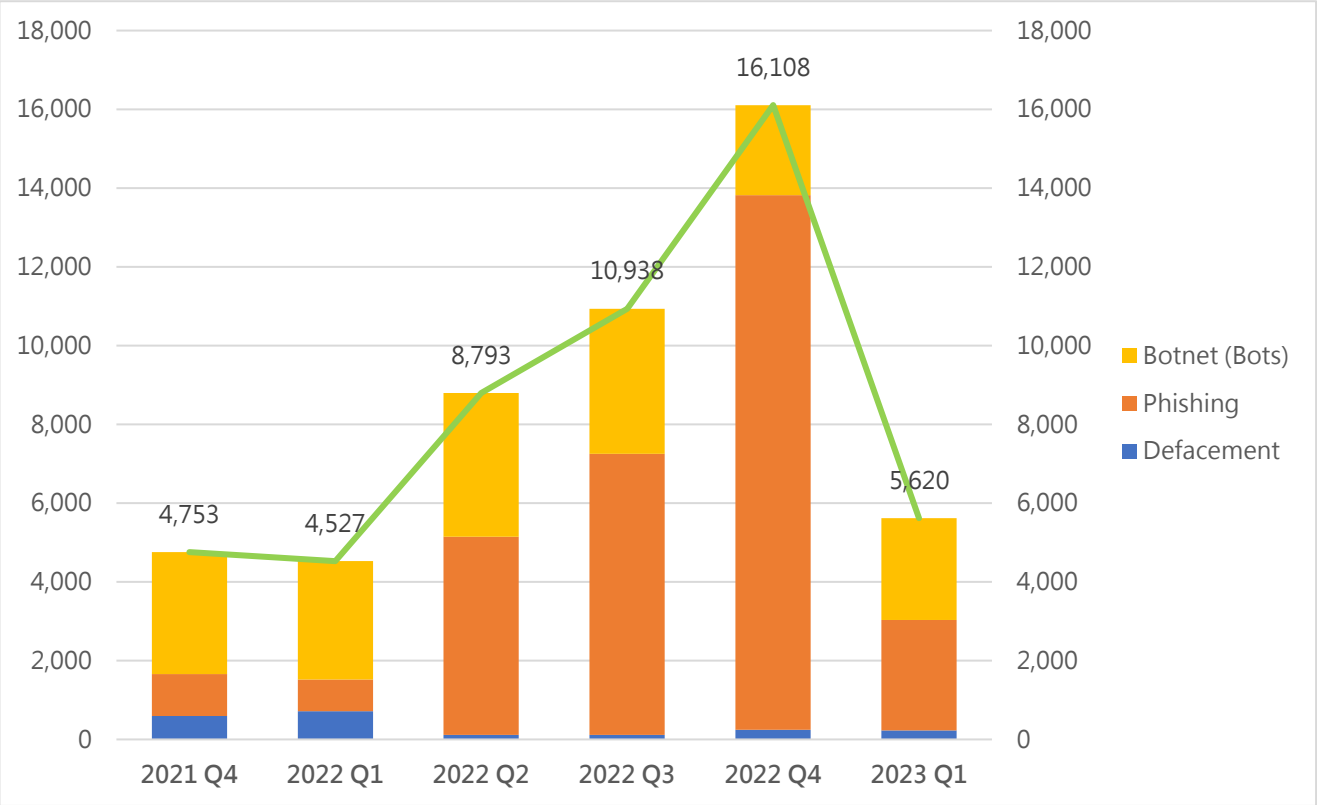
Highlights of the 2023 Q1 Report

Unique security events related to Hong Kong

5,102

Quarter-to-quarter

65%↓



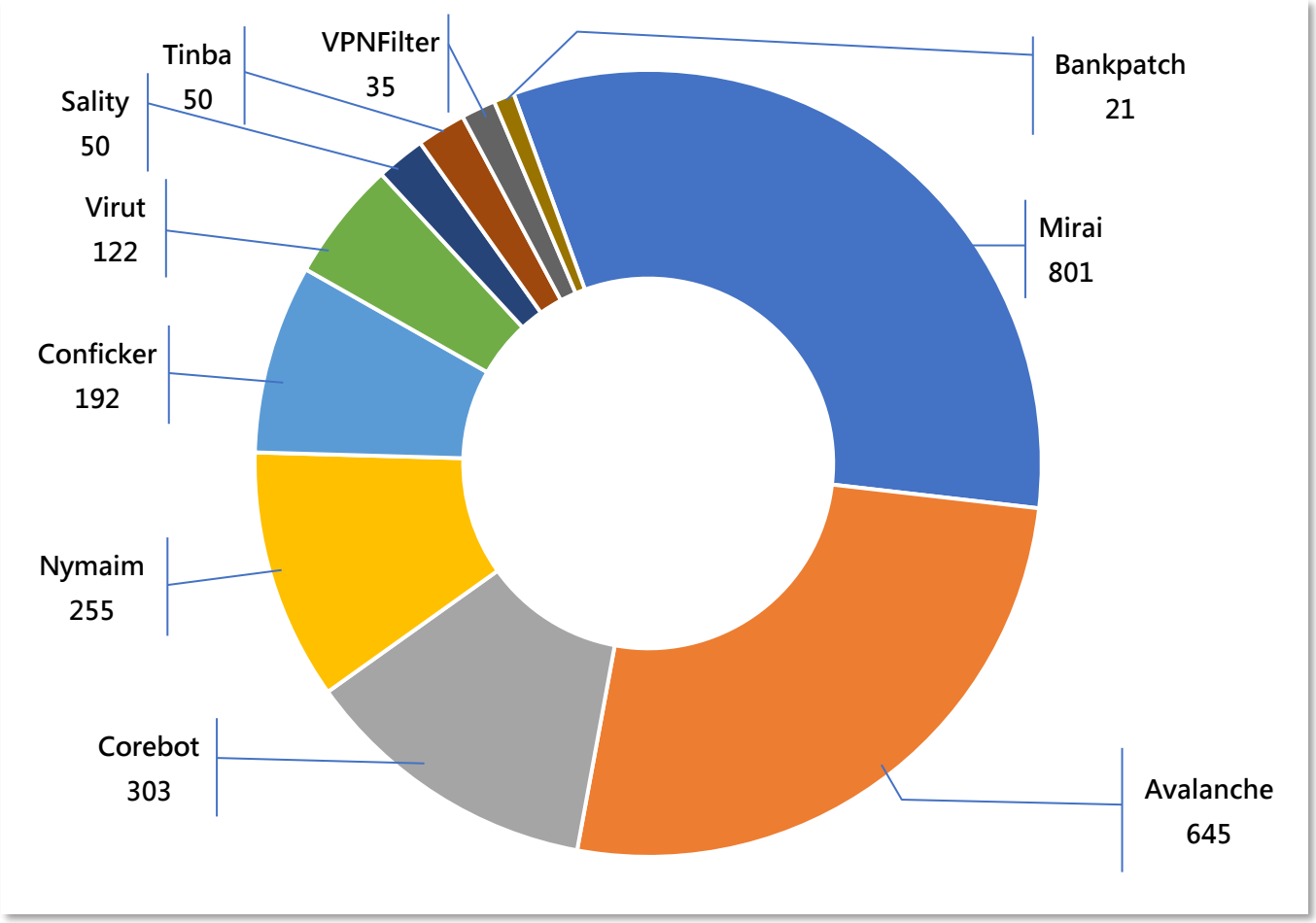
Event Type	2022 Q1	2022 Q2	2022 Q3	2022 Q4	2023 Q1	quarter-to-quarter
Defacement	718	118	113	249	233	-6%
Phishing	806	5,033	7,141	13,574	2,804	-79%
Botnet (Bots)	3,003	3,642	3,684	2,285	2,583	+13%
Total	4,527	8,793	10,938	16,108	5,620	-65%

Major Botnet Families in Hong Kong Network

Mirai
801
↓ 20.0%

Avalanche
645
↑ 51.1%

Corebot	303	+152.5%
Nymaim	255	+54.5%
Conficker	192	-7%
Virut	122	+1425%
Sality	50	+127.3%
Tinba	50	-56.9%
VPNFilter	35	-5.4%
Bankpatch	21	-80%



** 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.*

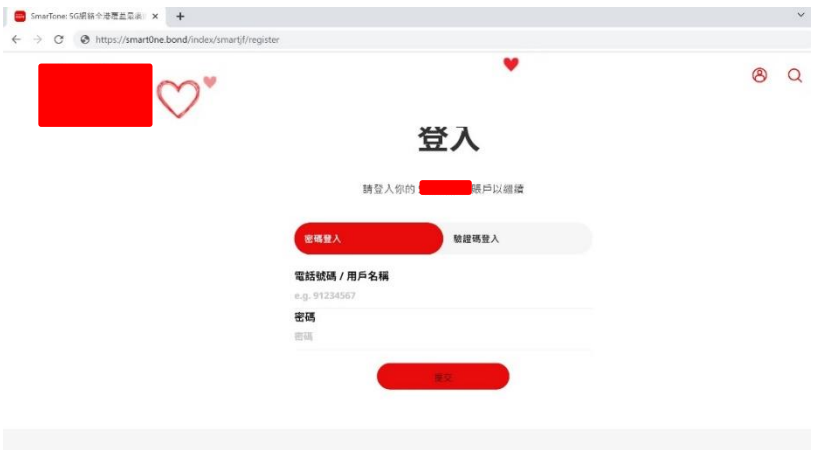
Hong Kong Users Have Reportedly Fallen Victim to Phishing Messages from Alleged Local Shopping Reward Programmes and Telecom

The number of phishing sites involving credit card companies decreased significantly this quarter. The number of phishing events dropped by 79% compared with the previous quarter. However, it is worth noting that the number only reflects the systems involved in phishing activities which are hosted in Hong Kong. In other words, hackers can set up phishing sites in overseas infrastructure systems and target users in Hong Kong. In this quarter, it is reported that several Hong Kong users had fallen victim to phishing attacks and suffered financial loss (Phishing attacks are discussed below), those phishing sites were hosted in overseas systems. It shows that users should stay vigilant against any email or message deemed to be suspicious.

Recent Phishing Attack Targeting Hong Kong Users

Recently, several high-profile phishing cases including a shopping reward programme and a local telecommunications company have been exposed in the news, and the HKCERT also received reports.

In the local telecommunications company case, cybercriminals sent out fake SMS posing as the telecommunications company to customers. The SMS contained a link to a fake website that looked exactly like the company's official website but was designed to steal users' login credentials. The attackers employed a tactic known as "brand hijacking," using a domain name that closely resembled the official company domain, a ploy that could easily deceive unsuspecting users. Once users entered their login credentials on the fake website, the attackers were able to steal their data and use it for fraudulent activities. Such attacks can have serious consequences, including identity theft, financial loss, and damage to the victim's reputation.



Likewise, a well-known reward programme in Hong Kong fell victim to a similar phishing attack. Attackers send fake SMS messages claiming that the points in the user's account are about to expire and need to redeemed by clicking a link to receive a reward. The link leads to a fake website that looks the same as the company's official website but is designed to steal the user's personal information, such as their contact phone number.

To protect the public from phishing attacks, HKCERT also provides some security advice for reference:

1. Be cautious with unknown emails, especially those requesting you to click on links or provide personal information.
2. Carefully check the sender's email address and phone number to ensure it is correct.
3. Before clicking on any links, hover over them to view the full URL and ensure it is not a fake website.
4. Use multiple- or two-factor authentication to reduce the risk of malicious intrusion.
5. Keep your computer and mobile devices up to date with the latest security patches and antivirus software.

"Smart City" Creates the Future, "Be Smart, Spot the Phish" Prevents Fraud

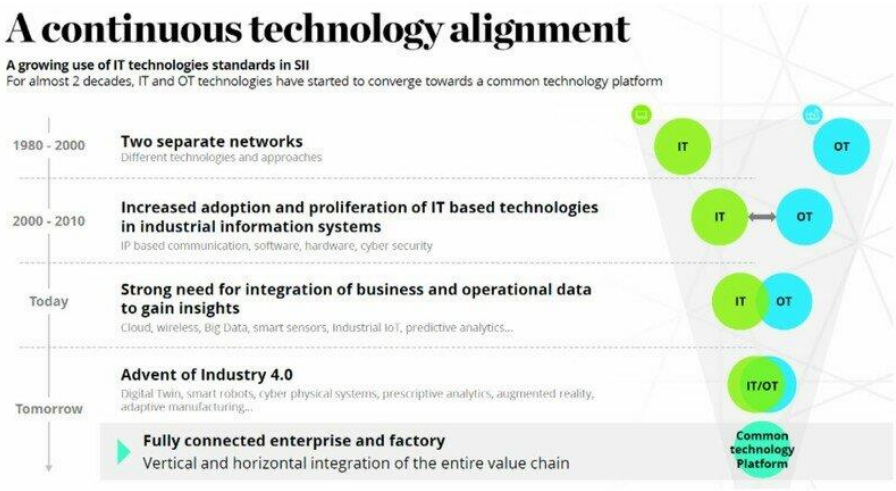
OGCIO (Office of the Government Chief Information Officer) held a smart city event in March this year to promote Hong Kong citizens' awareness and participation in smart city development, and explore how technology and the Internet can be used to create a safer, more convenient, and more liveable city. One of the missions of smart city development is to ensure the cyber security of Internet users. Therefore, HKCERT took part in the event and used mini-games and display boards to raise the security awareness of phishing attacks for local citizens.

Cyber Focus: How to Mitigate New Cyber Security Risks Arising from the Growing Use of Technology in Industrial Operations

In recent years, more enterprises and public utilities are leveraging 5G and Internet of Things (IoT) technologies to connect their industrial operation technology (OT) systems to information technology (IT) systems or the Internet. This enables the operation data of factory machines and critical infrastructure equipment to be sent back to the IT systems instantly, making it more convenient to monitor and analyse their operation in real-time, and even automatically adjust their operation parameters, to improve efficiency and productivity and enhance management.

Investigation

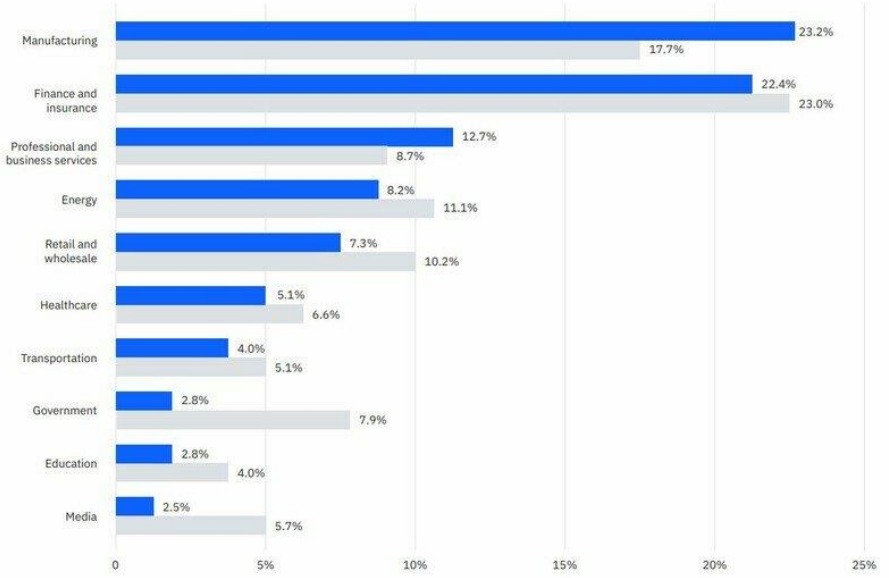
Previously, OT systems and IT systems were in two completely separated networks without any interconnection. OT systems have their communication protocols such as Modbus, which are different from the TCP/IP protocol used in IT systems, making these two systems work independently without interaction. Nowadays, these two systems have gradually adopted the same standardised protocol or used Internet of Things (IoT) devices to connect the two systems and share data. In the future, OT systems and IT systems will be converged to bring automation and intelligence to the industry.

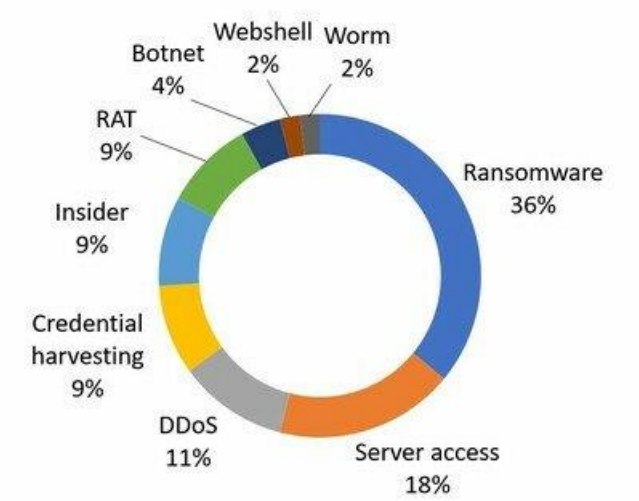


The convergence of OT systems and IT systems brings not only opportunities but also new cyber-security risks. One example is that once the two systems are connected, malware risks that only affect IT systems previously will now extend to OT systems.

Indeed, such risks are already materialising. According to an IBM report, the manufacturing industry suffered the most cyber-attacks in 2021. Ransomware was one of the most common cyber-attacks on OT systems. The reason was that OT systems help generate income. Once hackers use ransomware to paralyse the operations of OT systems, organisations suffer heavy losses directly. The affected organisations are more likely to pay the ransom to resume operations. If the affected organisations are critical infrastructures sector, such as electricity, public utilities, transportation, etc., the impact will extended to the public. Hackers can even coerce the affected organisations to pay a larger amount of ransom. For example, in March 2021, hackers used the remote software TeamViewer to gain access to the computer system of Oldsmar in Florida, United States. They tried to change the concentration of chemicals in the city's water supply facilities, which was enough to harm the human body seriously.

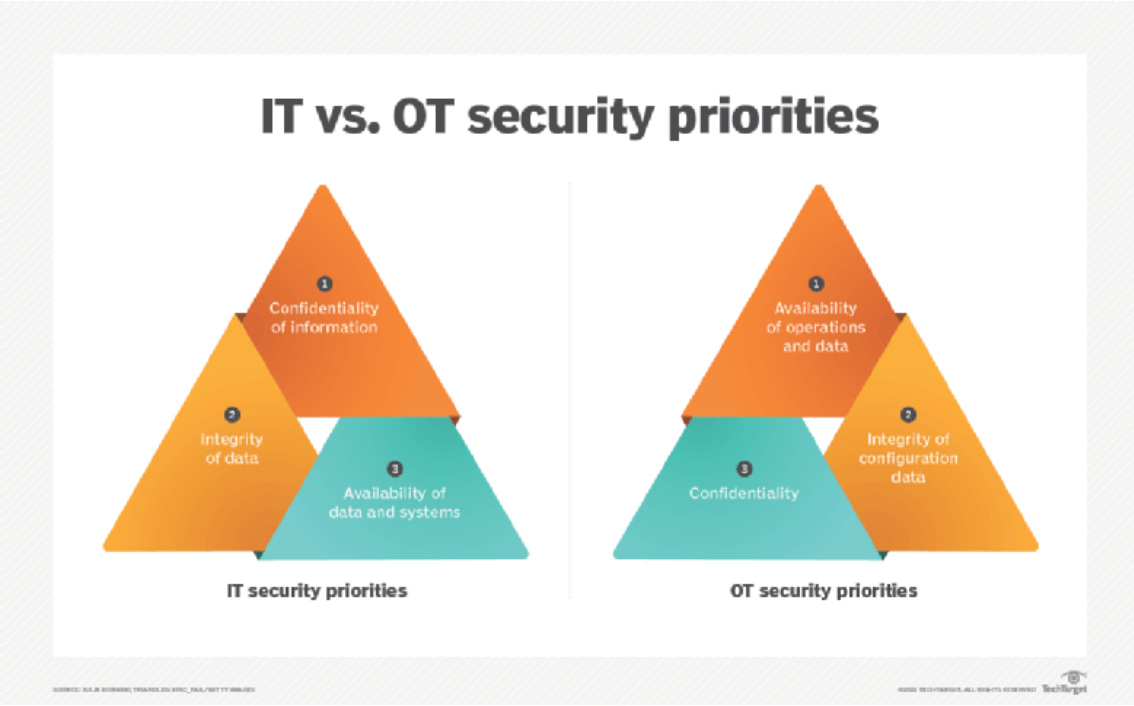
This blog will discuss the security challenges of IT/OT convergence, the preparations before and after the convergence and introduce measures to reduce the risks.





Challenges arisen from IT/OT convergence

A big challenge for i4.0 is the secure connections between OT systems and IT systems (IT/OT Convergence). These two systems have different priorities on security considerations: IT system security focuses on protecting user data and usually uses the concept of CIA (confidentiality, integrity, and availability) to formulate security controls, protecting data against unauthorised access and being tampered with as its goals. On the other hand, OT systems rarely process user data but emphasise more on system availabilities, physical safety of operations of machines and ensuring configuration data is intact.



In addition to the above two main differences, OT systems and IT systems also have the following differences:

- **Lifecycle**

  IT systems generally have a relatively short life cycle of about three to five years. In contrast, OT systems can have a life cycle of more than 20 years. It is not difficult to see legacy OT systems that are still in operation in factories. The companies and the labour market also lack technical professionals who understand these old systems. It is easy to cause technical faults when performing convergence of IT and OT systems.

- **Cyber Security Standards and Operating Systems**

  Information technology systems have been connected to the Internet for a long time. Mature security technologies are in place to prevent hackers' attacks such as data encryption, etc. However, OT systems are generally located in an isolated network environment. Therefore, by design, they have no requirement to use strong encryption or even no encryption for data transmission. In addition, most OT systems run a customised operating system, and any massive changes may affect the operation of different machines, so it is difficult to update the system to fix security vulnerabilities. Furthermore, OT systems have not considered security into consideration during the design phase to prevent cyber-attacks, so there are few protective measures, and the development of related cyber defence is relatively backward, such as measures to detect intrusions, the ability to recover and respond after security incidents, etc.

- **Maintenance Requirements**

  Generally, IT systems are designed with a concept of resilience in mind. Even if the primary system needs to restart during maintenance, the secondary system can continue to serve. It is difficult to implement the resilience in OT systems because the increase in costs means the decline in production efficiency. If an OT system needs to shut down for maintenance, it can take a toll on productivity. Even after maintenance is completed, security testing is required before returning to production. Compared with IT systems, OT systems need to consider more factors during maintenance, resulting in relatively less frequent maintenance, which is likely to leave security risks.

The difference in system design between the two systems will cause different risks.

Preparation before and after IT/OT convergence

Before converging OT systems and IT systems, sufficient preparations are required to reduce the risks. After the convergence, it is necessary to update the company's security, operation and maintenance policies. The Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) has the following suggestions:

- **Conducting Network and Security Assessments**

  Conduct an in-depth assessment of the entire OT systems and IT systems, including network and security assessments. An network assessment is a review of all system assets, network structures and data flows within an organisation. A Security assessment is to analyse the login account, remote access method, system loopholes and network services;

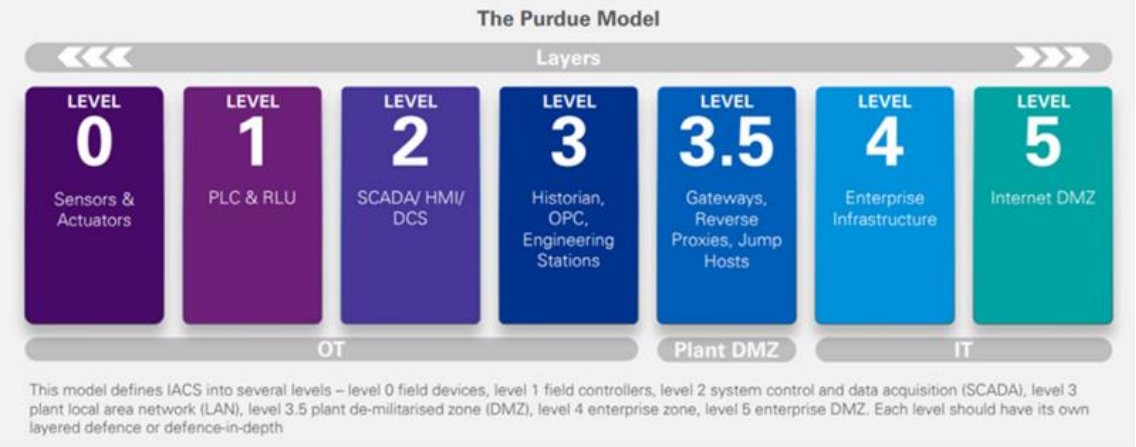
- **Writing a Risk Assessment Report**

  From the perspective of operation and information security, identify and classify risks in operations, processes, and systems. Formulate recommendations and solutions for all risks, and write a comprehensive assessment report.

- **Formulating an Implementation Plan to Follow Strictly**

  Before formulating an implementation plan, clarify the roles and responsibilities of stakeholders. Before the convergence of OT and IT systems, stakeholders should addressed the risks mentioned in the assessment report promptly. Also, they should developed a detailed and clear convergence plan with a feasible timetable. Operators must strictly follow the implementation plan and conduct evaluation tests after the operation is completed. When planning for implementation, one of the common challenges is to design a secure architecture, which involves how different devices should be layered and partitioned. The industry has different standard models for reference, with the Purdue model being one of most frequently referred.

  This computer-integrated-manufacturing model was proposed by scholars of Purdue University, Indiana, United States, back in the 1990s. It is divided into seven layers, each of which has its own functions and related systems. Each layer is also a network segmentation with access being controlled by different security measures to prevent attackers from intruding from one network (e.g. IT network) to another (e.g. OT network). For example, layer level 3.5 is to prevent horizontal lateral threat movement between IT and OT. Generally, security systems such as firewalls and proxies are placed. Users can design an appropriate structure architecture according to the actual situation of the organisation.



Apart from the Purdue reference model, the "Zero Trust" architecture is another security architecture worthy of reference, which promotes the principle of micro-segmentation, data encryption, and authentication and adoption of least-privileged principle for access to any data and system services.

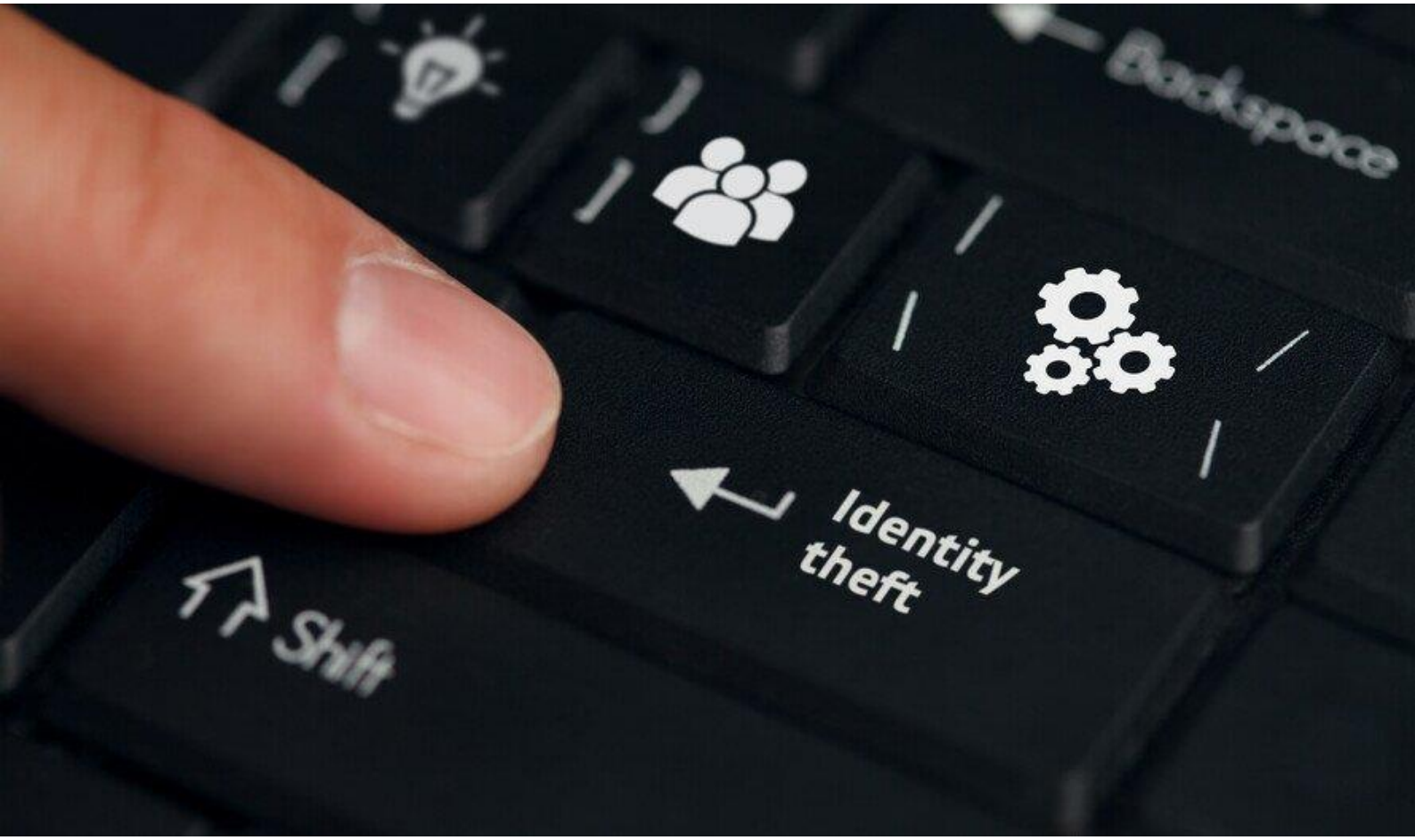
- **Updating Operation Policies**

  After the convergence, the IT and OT teams will interact with each other very often. Organisations can consider reorganising these two teams, or even recruiting experts with both IT and OT skillsets to streamline the operations. In terms of maintenance, since OT systems are connected to IT systems, both teams need to have a unify understanding and standardise information security standards. In addition, unmanaged systems in the past must be immediately controlled to identify any suspicious activities which may be an indication of compromise.

Moreover, as the convergence of IT/OT systems usually requires IoT networks and uses different IoT devices as sensors or data collection, security measures for IoT devices can also be applied. To this end, HKCERT released the “IoT Security Best Practice Guidelines” in 2020 to cover network security issues when using IoT devices. You may refer to the Guidelines as a reference.

For more details, please refer to:
https://www.hkcert.org/blog/how-to-mitigate-new-cyber-security-risks-arising-from-the-growing-use-of-technology-in-industrial-operations

Cyber Analysis: Do you know what is Identity/Credential Theft?



Cyber theft of identity and credentials is not a new phenomenon. However, the COVID-19 pandemic has accelerated people's growing reliance on online services for work and personal tasks, creating more opportunities for cybercriminals to steal our personal information for their gains. As a result, HKCERT has made Identity/Credential Theft one of the top five information security risks for 2023.

What are Identity Authentication and Identity Attack

Identity Authentication refers to the process of validating authorisation to access information or services. It aims to confirm and ensure users have permission to access the information or services. The most common example of identity authentication is the use of a username and password login. Empowered by technology advancements, fingerprints and faces can now be used for identity recognition as well. Although most authentication techniques are trustworthy, they may have limitations that cybercriminals can take advantage of to launch attacks.

As for Identity Attack, as its name implies, it is an attack on identity authentication, using credentials as attack vectors to obtain passwords, keys, session tokens, account information and other personal information to impersonate users' identities. If those high-privileged identity in an organisation is being stolen, it can be used for different malicious acts, such as distributing ransomware or invading the system to steal confidential files, etc., resulting in greater losses.

Trends in identity attacks in recent years

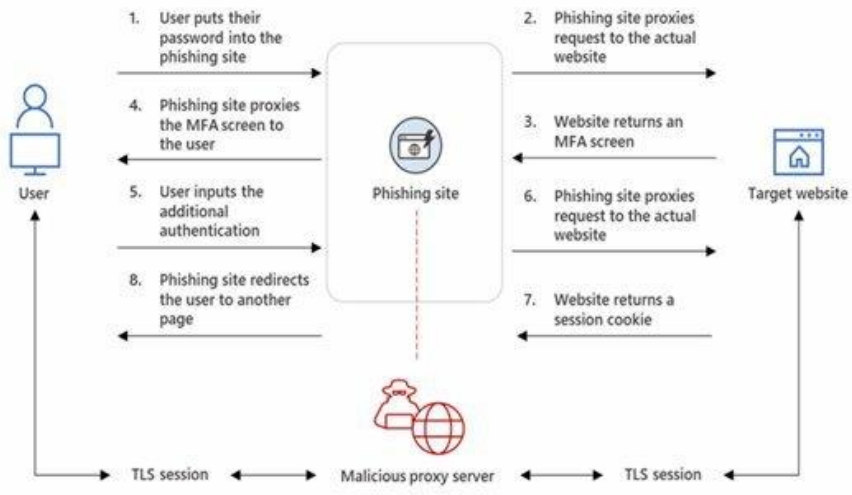
Phishing has been one of the most popular types of identity attacks that have occurred at increased frequency recently. In the latest quarterly report of the Hong Kong Security Watch Report released by HKCERT, local phishing events have exceeded 10,000 for the first time, totalling 13,574 in 2022 Q4, with a quarter-on-quarter increase of 90% and a year-on-year increase of over 11 times. The proliferation of such attacks has attributed to the spread of open-source phishing toolkit such as Evilginx2 which can evade multi-factor authentication (MFA) for session hijacking. Attacks against identity are rife and are expected to remain a major threat to cyber security in the foreseeable future.

Identity attacks in various ways

Attacks against identity come in various forms. Learning more about them could protect you from falling victim to these scams.

- **Adversary-in-the-middle (AiTM) Attack**

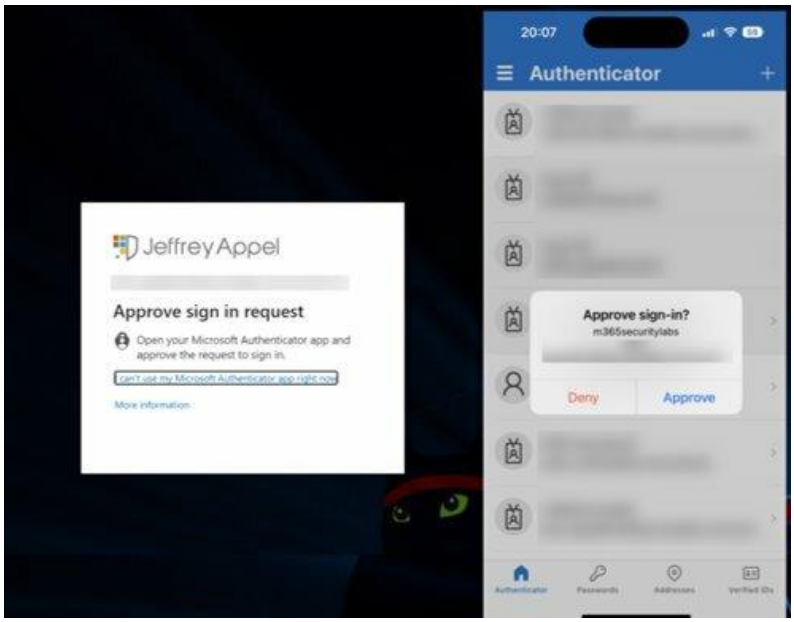
  Cybercriminals will send links to phishing websites that are like the actual website via emails, SMS and other channels to deceive individuals into signing in. The login requests are proxied to and from the actual website, allowing cybercriminals to bypass their victim's multi-factor authentication (MFA). After successful authentication, the victim is sent to the actual website to continue browsing, whereas in the background, cybercriminals have already obtained account information and Session Cookies for use in illicit activities.



- **MFA Fatigue**

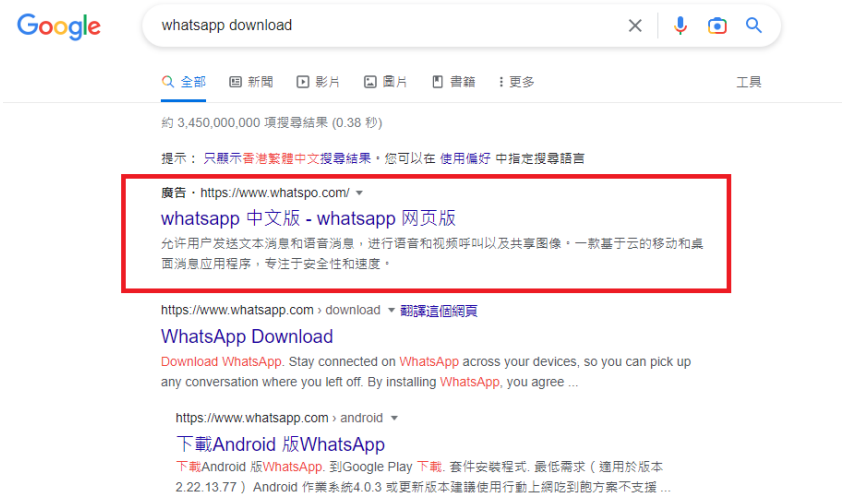
  Cybercriminals will use various means, such as utilising breached data or brute-force attacks, to continuously test possible password combinations to find out account passwords. After that, they will repeatedly bombard their targets with identity verification confirmation prompts until

the requests are accepted.



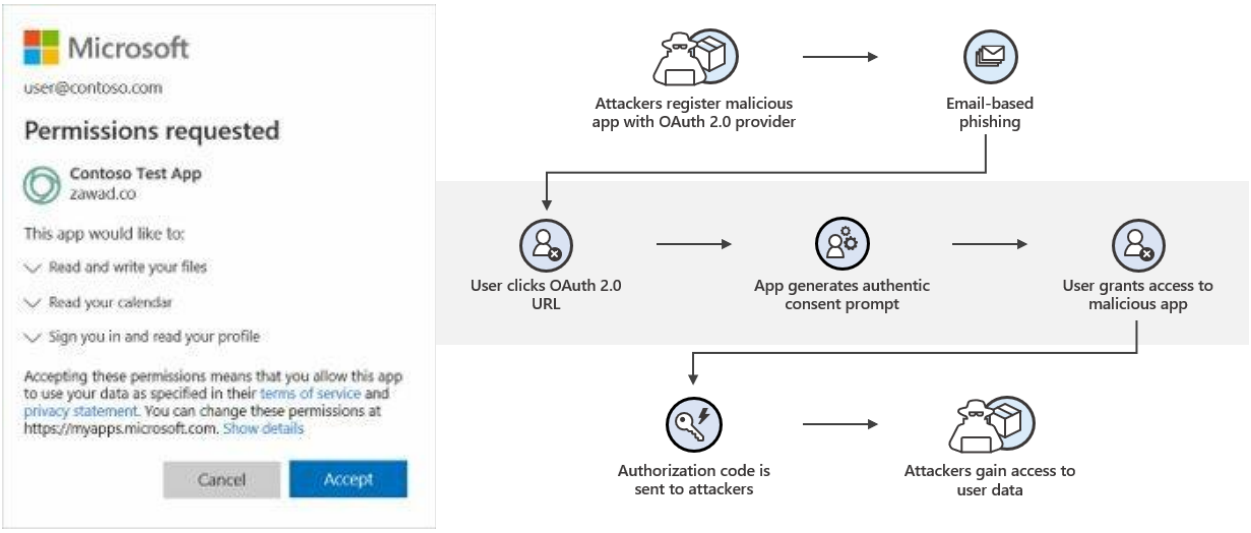
- **Fake Ads**

  Cybercriminals will use Google Ads to push malicious websites to the top of the search result, misleading users to believe as trusted websites. Such malicious websites may entice users to download and install malicious applications or engage in AiTM phishing.



- **OAuth phishing attack**

  Cybercriminals deceive users to grant permissions to malicious applications, allowing them to access account information and perform actions through OAuth 2.0 application. Once the malicious applications obtain the permissions, they can access user data anytime. Microsoft has also cautioned O365 users to be alert about this type of authorisation.

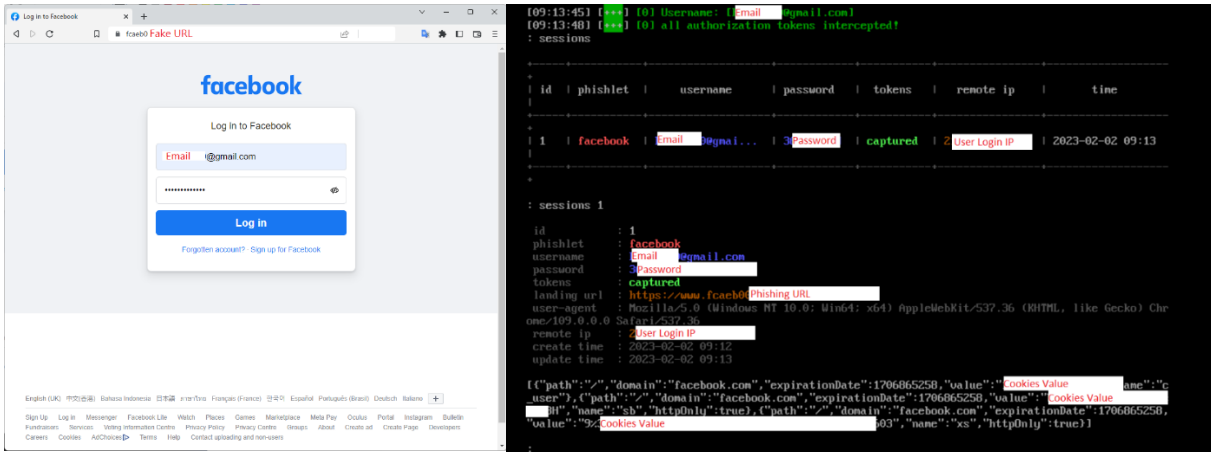


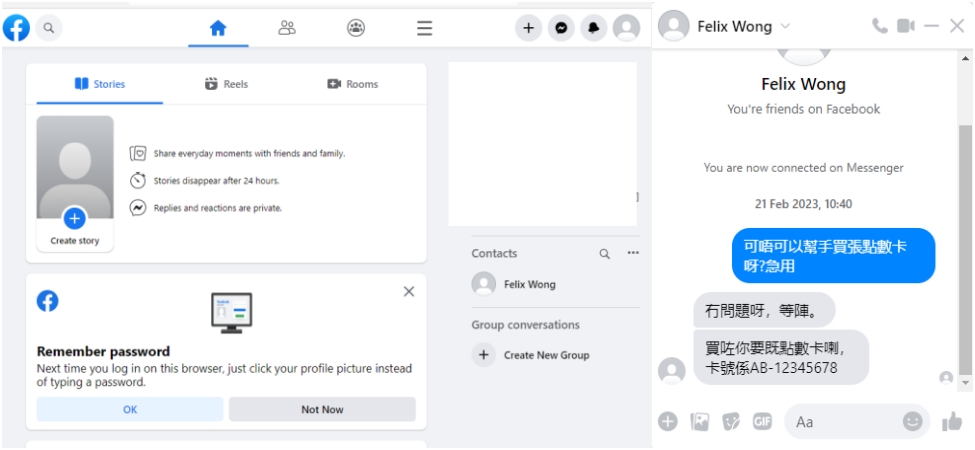
- **Social Engineering Attack**

  Cybercriminals will take advantage of people's empathy to conduct fraud. For example, they may examine the victims' social media posts to learn about their background and then pose as their friends or acquaintance to obtain their victims' personal information for illegal activities.

Example: Adversary-in-the-middle (AiTM) attack Facebook Accounts

Below is an example of the AiTM attack, cybercriminals use open-source tools to reproduce a fake Facebook login page to steal account information. Open-source phishing toolkits and typosquatting are used in the fake login page to provide a more genuine appearance of the page. While users are inputting their account information and completing MFA on the fake page, cybercriminals would obtain their account information and Session Cookies in the backend. Cybercriminals then use the captured information to log in to the victims' accounts and commit fraud against the victims' friends and family.





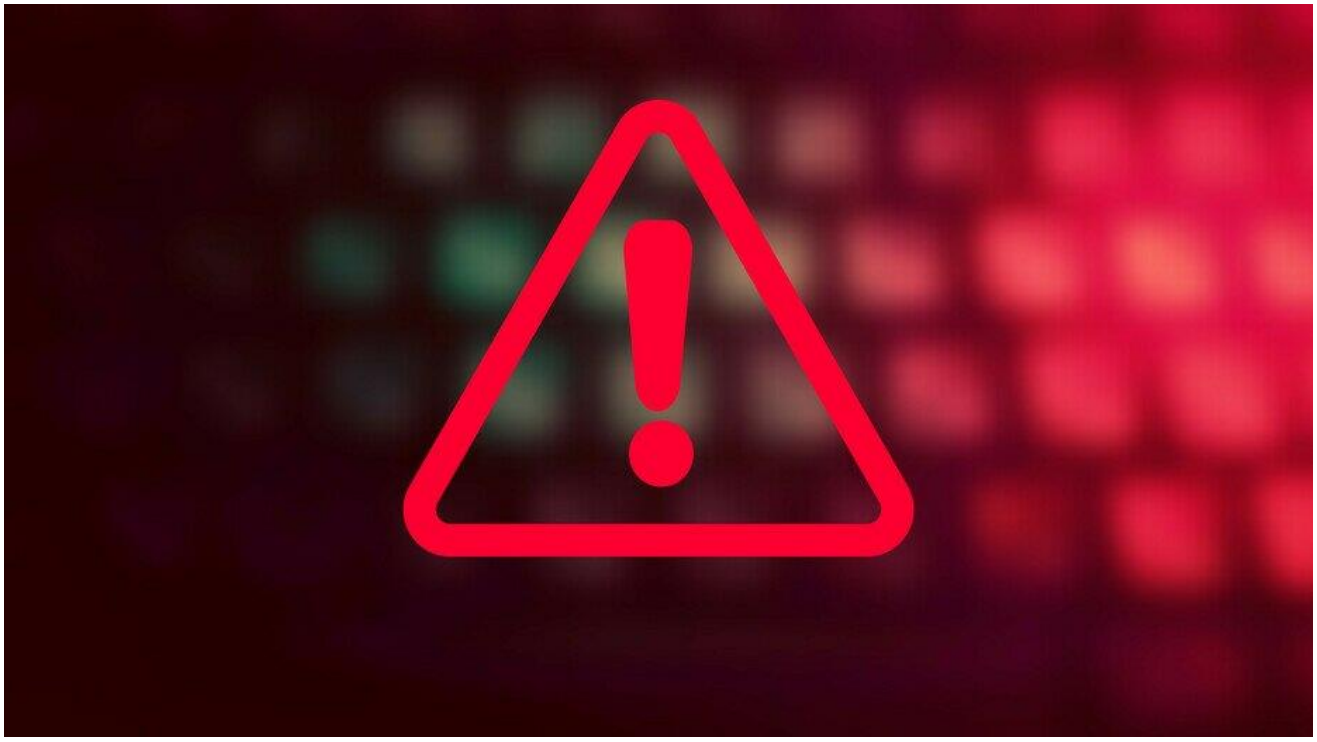
Conclusion and Recommendation

With continued technology advancements, these identity attack methods will become more diverse. To prevent the theft of personal information or accounts, extra vigilance is required when using online services. To this end, HKCERT offers the following security advice:

1. Do not assume websites that use the HTTPS protocol are authentic and credible;
2. Never assume all the search engine results are legitimate;
3. Carefully check the spelling of the URL, and verify the authenticity of the website;
4. Do not open any URLs or attachments from suspicious emails or SMS; use the “Scameter” of Cyberdefender.hk to identify frauds and online pitfalls through email, URL or IP address, etc.
5. Carefully consider before providing personal information to any person or organisation;
6. Use hardware-based FIDO (Fast IDentity Online) password-free login authentication;
7. Avoid using the same account and password for different platforms or services;
8. Logout and close the browser after using the online service.

For more details, please refer to:
https://www.hkcert.org/blog/do-you-know-what-is-identity-credential-theft

HKCERT Security Tips: Beware of Fake ChatGPT Apps and Phishing Websites



The artificial intelligence chatbot, ChatGPT, which gained 100 million users worldwide within just two months of its launch in November 2022, has recently introduced a paid subscription service called ChatGPT Plus. Unfortunately, this has provided an opportunity for hackers to exploit this new measure by offering fake apps or free access to the premium service, to trick users into downloading malware or sharing sensitive information.

According to a recent report from Cyble, a cyber-security intelligence company, hackers have created fake websites, social media pages and mobile apps that resemble the official one to lure users to download malicious files unknowingly. Cyble has discovered over 50 counterfeit and malicious apps that use the ChatGPT logo to execute harmful activities, including SMS fraud, spyware, and billing fraud.

In this regard, HKCERT reminds users to:

- Access ChatGPT only through its official channel (https://chat.openai.com/) once the service becomes available to Hong Kong users;
- Install applications only from official apps stores and from a reputable publisher;
- Verify the social media page by using the social media verification badge function (such as the Blue Badge in Facebook and Instagram);
- Do not open unknown files, web pages and emails; Use the “Scameter” of Cyberdefender.hk to identify frauds and online pitfalls through email, URL or IP address, etc.
- Always keep the system, software, and antivirus software up to date.

For more details, please refer to:
https://www.hkcert.org/blog/hkcert-security-tips-beware-of-fake-chatgpt-apps-and-phishing-websites

- End-

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