ANNUAL REPORT 2019

GovCERT.HK

1. Highlights of 2019

1.1 Summary of Major Activities

To enhance the city's overall defensive capability and resilience against cyber attacks, we continue to leverage the first local cross-sector Partnership Programme for Cyber Security Information Sharing named "Cybersec Infohub" and organise a number of seminars and workshops with a view to promoting trusted partnership between local cyber security stakeholders across prominent sectors for sharing cyber security information and providing actionable insights to the community.

Within the Government of the Hong Kong Special Administrative Region of the People's Republic of China (the Government), we organised the annual inter-departmental cyber security drill for government users. To help our government staff familiarise with hands-on analytical skills against cyber security incidents, the drill of this year adopted a model whereby participants were required to analyse a series of log files and recommend actions in response to the simulated cyber attack scenarios. In addition to the inter-departmental cyber security drill, a government-wide phishing drill campaign was also launched to raise awareness of all government users and their capabilities in defending against phishing attacks.

A keen appreciation of the threat landscape could help organisations and individuals to understand better the cyber threat environment so as to adopt early and appropriate mitigation measures. In 2019, we continued publishing threat trends, security alerts and mitigation advice through the Government Computer Emergency Response Team Hong Kong (GovCERT.HK) web portal for reference by the general public. We further tailored specific threat awareness updates for government departments.

We are also committed to promoting information security awareness to various sectors of the community by collaborating with different organisations to regularly hold various cyber security publicity events to raise public awareness and capability development.

1.2 Achievements and Milestones

Cyber Security Information Sharing

With the objective to facilitate cross-sector collaboration for a better visibility of cyber threats globally and locally, Cybersec Infohub serves well as an enabler to nurture culture in sharing cyber security information. The programme has been operating for more than one year and more than 150 public and private organisations have joined the programme, covering a wide range of sectors, including finance and insurance, public utilities, transport, healthcare, telecommunications, innovation and technology, information security, tertiary education institutions, etc. In 2019, we introduced artificial intelligence elements into the collaborative platform of Cybersec Infohub, which facilitated members to easily acquire the required information for timely dissemination of relevant cyber security information to the public. The programme has become an essential reference for organisations in gathering cyber security information and meeting with information security stakeholders to share the latest security trends and best practices.

Cyber Threat Intelligence Management

GovCERT.HK has been monitoring cyber security threat trends and sharing relevant information with our constituents and the community for taking early precautions and together reinforcing Hong Kong's cyber security. We publish monthly Cyber Security Threat Trends Report via the GovCERT.HK web portal to highlight the observations of latest cyber security threat landscape for reference by the public to enhance their situational awareness.

Liaison and Collaboration

We proactively participate in the Asia Pacific Computer Emergency Response Team's (APCERT) activities and work closely with the Computer Emergency Response Team (CERT) community in handling threat information. We have been working closely with the Hong Kong Internet Registration Corporation Limited (HKIRC), one of our local Internet infrastructures stakeholders, to provide them with technical advice in launching a free website scanning service for local small and medium enterprises (SMEs) to assist them to identify and mitigate their information security issues as early as possible.

Capability Development

To facilitate in developing staff capabilities to tackle evolving cyber threats, we have further enriched the services available at the GovCERT.HK Technology Centre. The centre offers government departments relevant tools and network facilities in a controlled environment to enable vulnerability scanning and security testing for potential information security issues of their web applications.

Awareness Building and Public Education

User awareness of information security plays a vital role in coping with cyber threats. In response to the worsening threat of phishing attacks, we launched the "Government-wide Phishing Drill Campaign" in 2019 to raise awareness of government users on phishing and strengthen their capabilities in defending against phishing attacks.

In view of the rising trend of phishing scams and data breaches, GovCERT.HK has produced a series of promotional materials including educational videos and smart tips for the public to protect themselves from and defend against cyber threats.

GovCERT.HK also devotes much attention to public education and capacity building in different business sectors and age groups. In the 2018/2019 school year, we organised more than 40 school visits to reach out to some 10 000 students, parents and teachers.

2. About GovCERT.HK

2.1 Introduction

The Government Computer Emergency Response Team Hong Kong (GovCERT.HK) is a governmental CERT responsible for coordinating incident response for over 80 departmental Information Security Incident Response Teams of the Government of the Hong Kong Special Administrative Region of the People's Republic of China (the Government).

Since its establishment, GovCERT.HK has profoundly shaped the management framework and coordination mechanism of incident handling; and empowered close collaboration with the industry, critical Internet infrastructures, and the CERT community for timely exchange of cyber threat information and coordinated responses. GovCERT.HK also works closely with the Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) and local industry on cyber threat intelligence sharing, capability development, public education, and continuous promotion on cyber security and resilience through social and mass media.

GovCERT.HK also actively collaborates with other governmental and regional CERTs and international organisations in sharing threat intelligence and incident information; participating in training events, workshops, forums and drills; and organising public awareness promotion activities and capability development initiatives.

2.2 Establishment

GovCERT.HK was established on 1 April 2015 through the consolidation of internal IT security teams within the Office of the Government Chief Information Officer (OGCIO) of the Government.

2.3 Resources

GovCERT.HK is an establishment under OGCIO and funded by the Government.

2.4 Mission and Constituency

Being the governmental CERT, GovCERT.HK will centrally manage incident responses within the Government and develop CERT-related services to assist government departments in understanding the associated risks of information and cyber security, implementing appropriate security measures, monitoring potential threats and responding to security events with a view to ensuring government's information infrastructure would be well protected.

3. Activities and Operations

3.1 Scope of Services

GovCERT.HK is the computer emergency response team for the Government, providing centrally managed incident response services and timely security advice; coordinating cyber security drills; promoting public awareness and capabilities; and engaging global CERT community with a view to enhancing information and cyber security locally and in the region.

3.2 Security News Bulletins

In 2019, GovCERT.HK published the following security bulletins to raise the awareness among government users and the general public.

- "Security Vulnerabilities and Patches" information was consolidated on every working day and disseminated to registered subscribers through emails;

- "Security Industry News" was gathered on every working day and top news with wide impact was compiled and disseminated to registered subscribers through emails; and

- "Weekly IT Security News Bulletins" was published on the first working day of each week to highlight top two to three hot security news and summarise vulnerabilities by products for easy reference by security practitioners. These Bulletins were distributed to registered subscribers through emails and posted at the GovCERT.HK website as public information. (www.govcert.gov.hk/en/secbulletins.html)

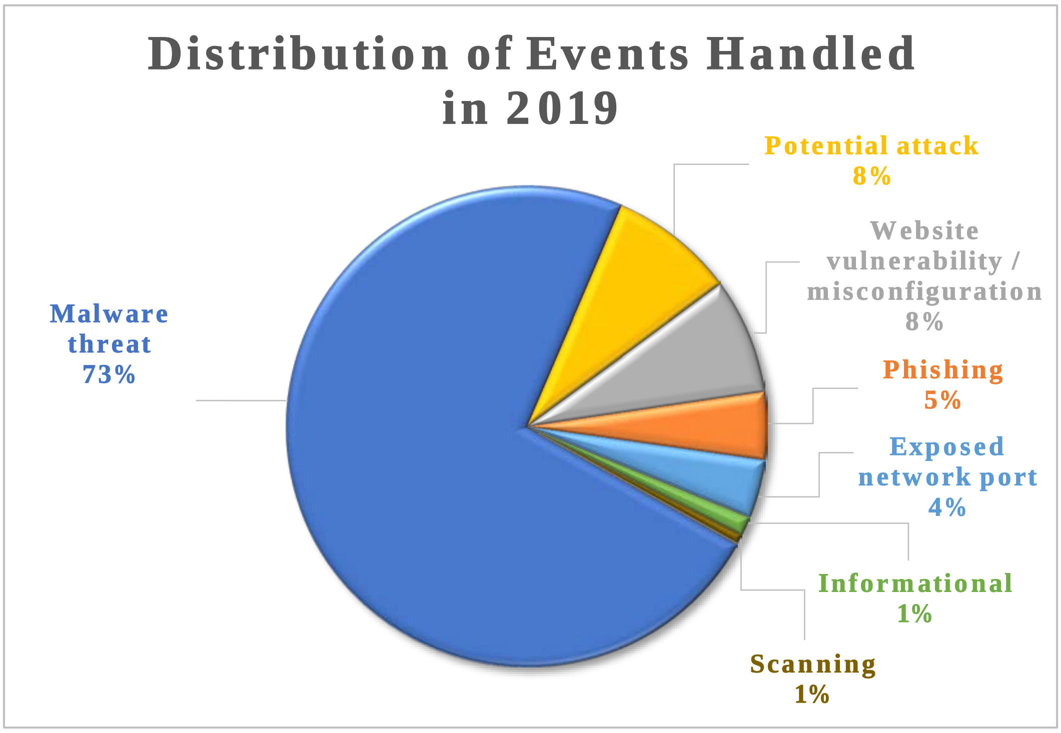
3.3 Alerts and Advisories

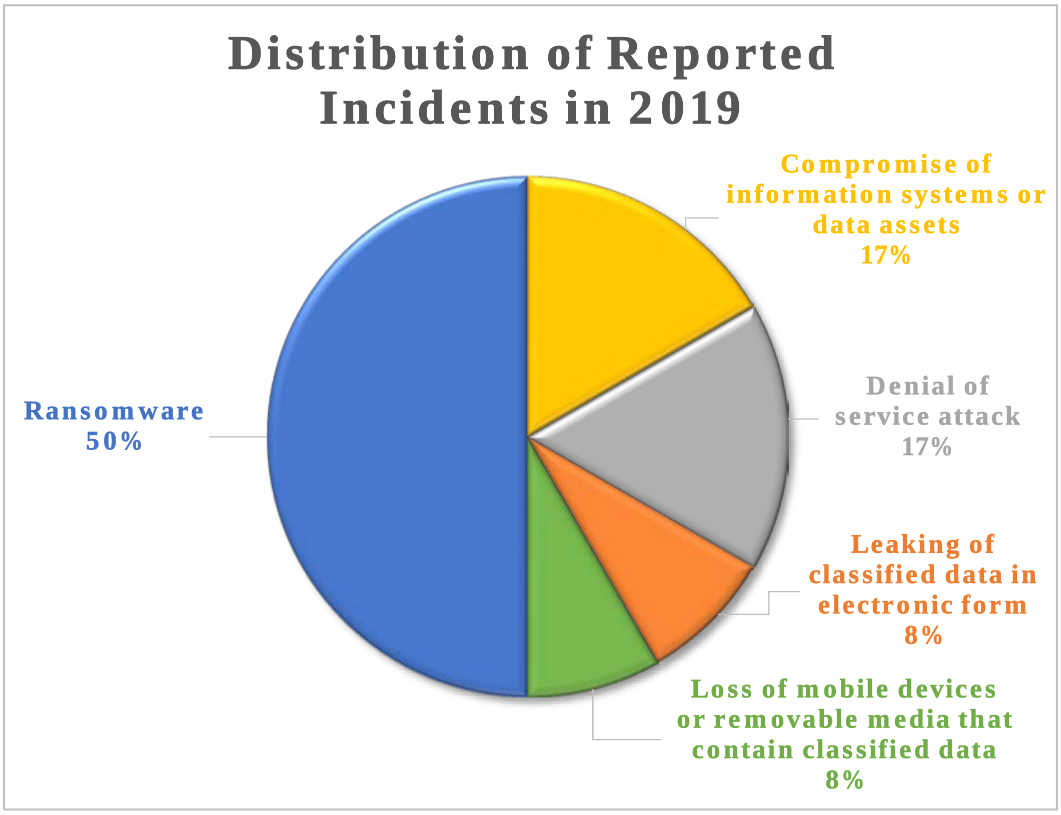
In 2019, GovCERT.HK issued around 90 security alerts associated with computing products widely deployed in government installations. In case the security vulnerabilities were considered highly risky to our environment, we would proactively request government departments to take prompt and appropriate preventive measures against potential information security risks.

We also conducted threat analysis on over 150 security events detected and received from various sources. The threat information was extracted and shared with relevant constituents for appropriate follow-ups.

3.4 Security Events and Incident Handling

Security events indicate possible breaches of information security or failure of security controls. Security incidents, however, are in relation to one or multiple events that can harm information systems and/or data assets or compromise their operations. In 2019, GovCERT.HK dealt with various cyber security events and reported incidents that were related to government installations. The following charts show the distribution of events and reported incidents handled in 2019.



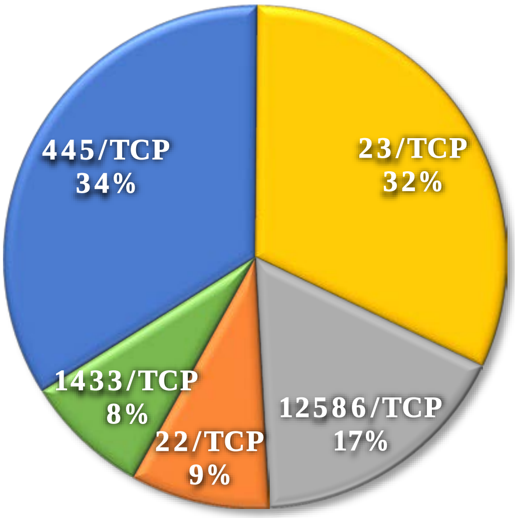


To facilitate the public to access the statistics on information security incidents in the Government, relevant data has been released to the Government's Public Sector Information Portal (www.data.gov.hk/en-data/dataset/hk-ogcio-sec_div_01-information-security-incident).

3.5 Abuse Statistics

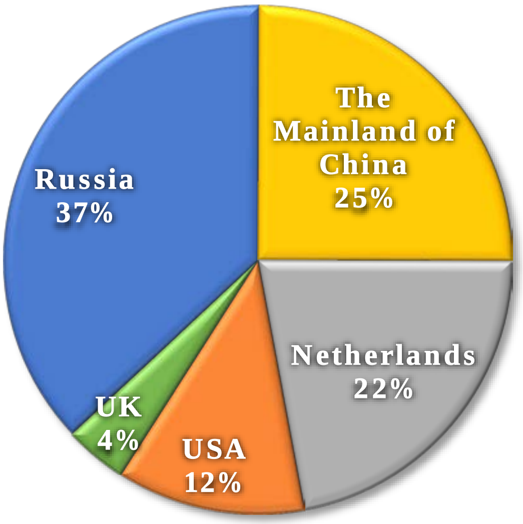
As a member of the TSUBAME project, GovCERT.HK has set up sensors to collect and analyse network scanning activities targeting Hong Kong. The following charts show the top five scanning ports (contributed 19% of all the scanning activities) and the top five source regions (contributed 69% of all the scanning activities) detected by the TSUBAME sensors installed in Hong Kong in 2019.

Top Five Scanning Ports against Hong Kong in 2019



Position in 2019	Port Number	Position in 2018
1	445/TCP	1
2	23/TCP	2
3	12586/TCP	-
4	22/TCP	4
5	1433/TCP	5

Top Five Source Regions of Scanning against Hong Kong in 2019

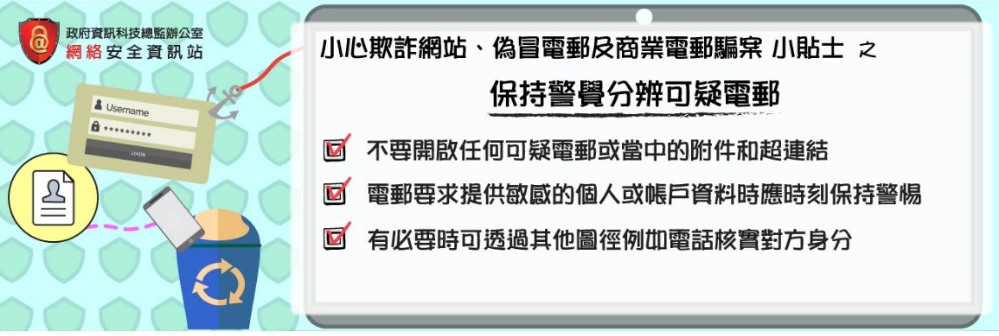


Position in 2019	Source Region	Position in 2018
1	Russia	1
2	The Mainland of China	2
3	Netherlands	4
4	USA	3
5	UK	-

3.6 Publications and Mass Media

As cyber attacks continue to increase in number and sophistication, members of the public face cyber security risks when using different technologies, such as mobile devices, cloud services and social networking applications. We have made use of different promotion channels to reach out to our target audience and collaborated with industry players during the process.

- We broadcasted radio episodes entitled “e-World Smart Tips” to help the public understand more about information security in various aspects and raise their awareness of information security. The radio episode in each month featured a specific theme and offered associated tips on mitigating the risks of cyber threats through daily life examples and in a lively and interesting way. In 2019, we covered a wide range of topics including data security, password management, phishing attacks, endpoint security, and more. (www.cybersecurity.hk/en/media.php#Radio)



小心欺詐網站、偽冒電郵及商業電郵騙案 小貼士 之

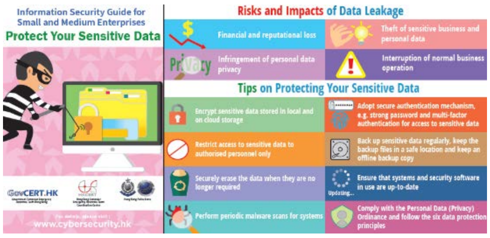
保持警覺分辨可疑電郵

☑ 不要開啟任何可疑電郵或當中的附件和超連結

☑ 電郵要求提供敏感的個人或帳戶資料時應時刻保持警惕

☑ 有必要時可透過其他圖徑例如電話核實對方身分

- A series of handy guidelines with different themes were developed to provide practical tips and advice for SMEs and the general public to defend against cyber threats. (www.cybersecurity.hk/en/resources.php#leaflets)



Information Security Guide for Small and Medium Enterprises

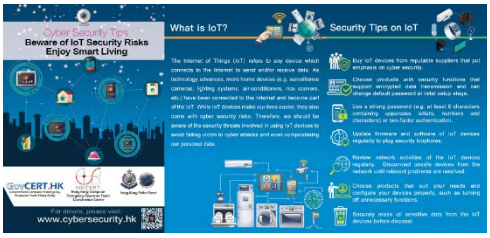
Protect Your Sensitive Data

Risks and Impacts of Data Leakage

- Financial and reputational loss
- Theft of sensitive business and personal data
- Infringement of personal data privacy
- Interruption of normal business operation

Tips on Protecting Your Sensitive Data

- Encrypt sensitive data stored in local and on cloud storage
- Adopt secure authentication mechanism, e.g. strong password and multi-factor authentication for access to sensitive data
- Restrict access to sensitive data to authorised personnel only
- Back up sensitive data regularly, keep the backup files in a safe location and keep an offline backup copy
- Securely erase the data when they are no longer required
- Ensure that systems and security software in use are up-to-date
- Perform periodic malware scans for systems
- Comply with the Personal Data (Privacy) Ordinance and follow the six data protection principles



Cyber Security Tips

Beware of IoT Security Risks Enjoy Smart Living

GovCERT.HK
HKCERT
Hong Kong Computer Emergency Response Team Coordination Centre
Hong Kong Police Force
For details, please visit:
www.cybersecurity.hk

What is IoT?

The Internet of Things (IoT) refers to any device which connects to the Internet to send and/or receive data. As technology advances, more home devices (e.g. surveillance cameras, lighting systems, air-conditioners, rice cookers, etc.) have been connected to the internet and become part of the IoT. While IoT devices make our lives easier, they also come with cyber security risks. Therefore, we should be aware of the security threats involved in using IoT devices to avoid falling victim to cyber attacks and even compromising our personal data.

Security Tips on IoT

- Buy IoT devices from reputable suppliers that put emphasis on cyber security.
- Choose products with security functions that support encrypted data transmission and can change default password at initial setup stage.
- Use a strong password (e.g. at least 8 characters containing uppercase letters, numbers and characters) or two-factor authentication.
- Update firmware and software of IoT devices regularly to plug security loopholes.
- Review network activities of the IoT devices regularly. Disconnect unsafe devices from the network until relevant problems are resolved.
- Choose products that suit your needs and configure your devices properly, such as turning off unnecessary functions.
- Securely erase all sensitive data from the IoT devices before disposal.

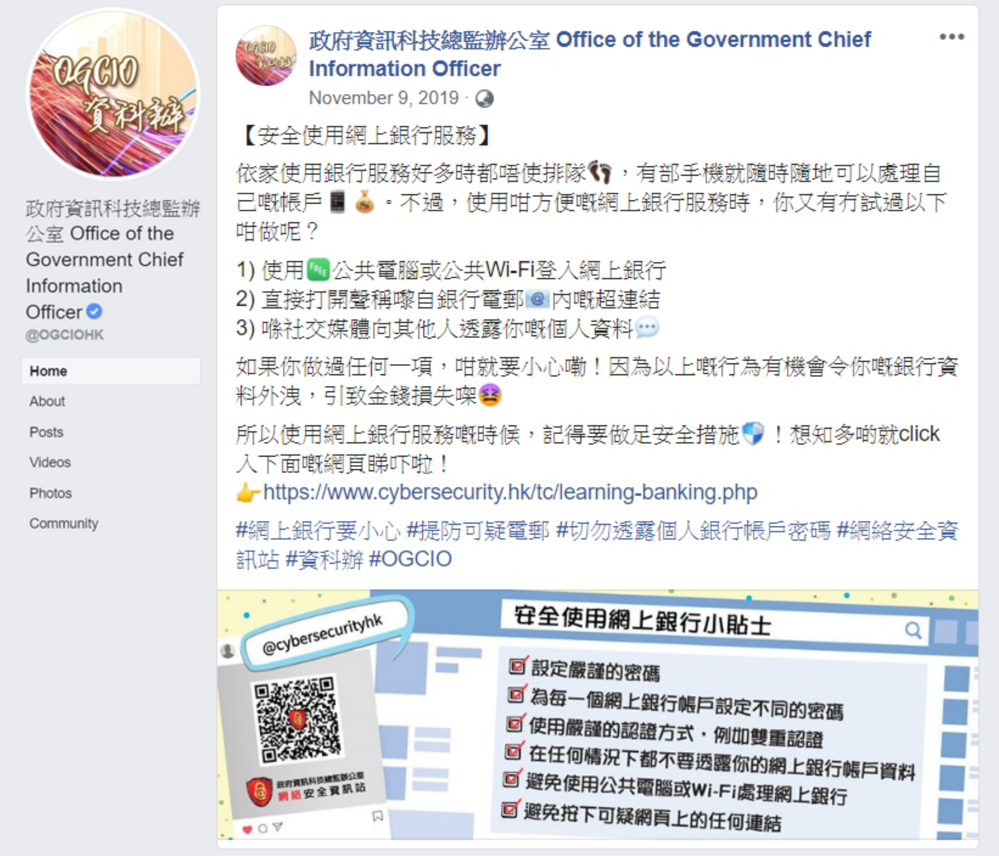
- To encourage the public to adopt data protection best practices, enhance their awareness of cyber security and draw their attention to the importance of information security, we organised the "We Together! Secure Data!" poster design contest in 2019. Participants fully demonstrated their creativity to get across data protection message to the public and the industry in a creative manner. The winning and shortlisted entries have been published to the Cyber Security Information Portal website for public reference as well.

(www.cybersecurity.hk/en/contest-2019.php)

Winning Entries

網絡攻擊花樣多
保護數據靠你我
掃描連結
立即報告
不要點擊
SPAM
更新軟件
更改密碼
保安程式
網絡森林
進攻贏比賽
防守贏冠軍
網絡攻擊花樣多
網絡數據齊守護

- Leveraging the OGCIO Facebook page as newly launched in 2019, we have published a series of posts with infographics and videos to reach out to the general public with timely updates and tips on cyber security topics such as identifying phishing websites and safe use of online banking. This is an effective social media channel for engaging the community in enhancing their security awareness. (www.facebook.com/ogciohk)



政府資訊科技總監辦公室 Office of the Government Chief Information Officer

November 9, 2019 ·

【安全使用網上銀行服務】

依家使用銀行服務好多時都唔使排隊👣，有部手機就隨時隨地可以處理自己嘅帳戶📱💰。不過，使用咁方便嘅網上銀行服務時，你又有冇試過以下咁做呢？

1) 使用🆓公共電腦或公共Wi-Fi登入網上銀行
2) 直接打開聲稱嚟自銀行電郵📧內嘅超連結
3) 喺社交媒體向其他人透露你嘅個人資料💬

如果你做過任何一項，咁就要小心嘞！因為以上嘅行為有機會令你嘅銀行資料外洩，引致金錢損失㗎😩

所以使用網上銀行服務嘅時候，記得要做足安全措施🛡！想知多啲就click入下面嘅網頁睇吓啦！
👉https://www.cybersecurity.hk/tc/learning-banking.php

#網上銀行要小心 #提防可疑電郵 #切勿透露個人銀行帳戶密碼 #網絡安全資訊站 #資科辦 #OGCIO

安全使用網上銀行小貼士

☑ 設定嚴謹的密碼
☑ 為每一個網上銀行帳戶設定不同的密碼
☑ 使用嚴謹的認證方式，例如雙重認證
☑ 在任何情況下都不要透露你的網上銀行帳戶資料
☑ 避免使用公共電腦或Wi-Fi處理網上銀行
☑ 避免按下可疑網頁上的任何連結

3.7 GovCERT.HK Technology Centre

To facilitate the Government in developing staff capabilities on more specialised knowledge and skills to tackle evolving cyber threats, we established the GovCERT.HK Technology Centre. The centre offers government departments a controlled environment with relevant facilities and equipment to enable vulnerability scanning and security testing for potential security issues of their web applications. This year, we enhanced the capability of the centre with more services offered, such as the dynamic application security testing service to facilitate users in examining their web applications. Users can benefit by making use of the tools to identify web vulnerabilities, misconfigurations, compromised passwords, etc.

Web vulnerability scan

Dynamic application security testing

Penetration test platform

Malware analysis corner

Password checker

GovCERT.HK Technology Centre

4. Events Organised/Hosted

GovCERT.HK regularly organises awareness training and solution workshops to share the latest knowledge on security measures, best practices, skills and security solutions with various levels of government users to continuously strengthen their knowledge on cyber attacks and enhance their information security skills, thereby strengthening their capabilities in guarding against cyber attacks.

4.1 Training

In 2019, we organised a total of 16 seminars, trainings and solution showcases for government IT staff and users to raise their awareness of the latest security vulnerabilities and update their knowledge in information security technologies. More than 1 800 government staff participated in these events to understand the latest cyber security trends and preventive measures.

- Seminars, trainings and showcases were conducted for government IT staff and users to raise their security awareness and introduce the latest IT security technologies and solutions. Topics included industry best practices on the security of mobile and Internet of Things (IoT) devices, defence against phishing, promotion of various security solutions, etc.

- Seminars were organised for departmental IT security officers to refresh their security knowledge and update them on the Government's latest requirements and approaches in dealing with cyber security threats and adopting mitigation measures.

4.2 Drills and Exercises

Inter-departmental Cyber Security Drill of the Government

GovCERT.HK has coordinated government departments to conduct cyber security drills to assess the participants' capabilities of incident analysis and test their incident response procedures with a view to enhancing the overall incident response capability.

With the ever-changing cyber threat landscape, it is imperative to enhance the competencies in mitigating cyber threats. This year, we continued to organise the annual inter-departmental cyber security drill with some 45 departments participated to strengthen the readiness and capabilities of departments to respond to cyber security incidents. The drill adopted a model whereby participants were required to analyse a series of log files in order to strengthen their technical and analytical skills in handling cyber security incidents. In form of table-top exercises, participants discussed and presented their way of responding to any data breach and malware infection arouse in the simulated cyber attack scenarios.

Government-wide Phishing Drill Campaign

In defending against the ever-growing phishing attacks, this year we launched the "Government-wide Phishing Drill Campaign" to raise government users' awareness of phishing. All government users under the drill would receive simulated phishing emails and immediate feedback explaining the proper way to handle emails if the users clicked the hyperlinks in these emails. We also organised seminars, thematic websites, education videos and quizzes to introduce different ways to identify phishing emails in order to raise their awareness of phishing and strengthen their capabilities in defending against potential phishing attacks.

APCERT Drill

As an Operational Member of the APCERT, GovCERT.HK participated in the APCERT Drill with the theme of "Catastrophic Silent Draining in Enterprise Network" in July 2019. GovCERT.HK played the role of Exercise Controller in addition to Player and Observer in the drill.

4.3 Conferences and Seminars

Build a Secure Cyberspace Promotional Campaign

To promote public awareness of information security, especially data protection, GovCERT.HK adopted the slogan “We Together! Secure Data!” as the theme in 2019. A series of promotional activities were organised for businesses, organisations, schools and the public to raise their awareness of adopting security measures proactively to better protect their digital assets.

- Two seminars were organised under the “Build a Secure Cyberspace” promotional campaign in May and September 2019, aiming to promote public awareness of information security and adoption of security best practices, in particular the risks of phishing scams and strategies in protecting data assets.

- More than 40 school visits were conducted at primary and secondary schools in the 2018/19 school year, reaching out to some 10 000 students, parents and teachers for raising their awareness of cyber security and encouraging the proper attitude in using the Internet.

Cybersec Infohub – Partnership Programme for Cyber Security Information Sharing

To encourage trust building and promote closer collaboration among different sectors under the Cybersec Infohub programme, activities ranging from sector-specific face-to-face meetings, closed group meetings, professional workshops and webinars were arranged in 2019 with positive response from participants.

5. Local and International Collaboration

GovCERT.HK has been working closely with HKCERT and other regional and global CERTs for coordinating threat information sharing and incident response.

5.1 Local Collaboration

GovCERT.HK is keen on fostering exchanges and experience sharing among the local information security industry. We continue to leverage the Cybersec Infohub programme to promote closer collaboration among local information security stakeholders across different sectors. Under the programme, we have provided a community-driven collaborative platform (Cybersechub.hk) and organised various industry events to facilitate the exchange of cyber security information. As of 2019, more than 150 public and private organisations across various sectors have joined the programme. (www.cybersechub.hk)

To celebrate Cybersec Infohub's anniversary since its launch, we held the first anniversary celebration-cum-professional workshop in November 2019 to recognise the positive contributions and cyber security experts.

The Internet is critical to communications, conduct of e-business and access to e-services. GovCERT.HK has been acting as a supportive role in the Internet Infrastructure Liaison Group (IILG) established and led by OGCIO. The key roles of the IILG are to maintain close liaison with Internet infrastructure stakeholders and strive in collaboration with the stakeholders for the healthy operation of the Internet infrastructure of Hong Kong. In 2019, the IILG collaboration mechanism was activated ten times to strengthen monitoring of cyber security of large-scale events and provide support events to protect the local Internet infrastructure against alleged cyber attacks. Particularly in January and March 2019, local Internet stakeholders were reminded through the IILG collaboration mechanism to monitor the healthiness of their DNS resolvers regarding the revocation and removal of the Old Key Signing Key (KSK-2010) of DNSSEC Root Zone.

SMEs are generally less adequately allocated with IT and security resources to enhance their cyber security protections. We have been working closely with HKIRC to provide them with technical advice in launching a free website scanning service to assist SMEs to identify and mitigate their information security issues as early as possible. Apart from scanning malware in the system and providing information security improvement solutions, a number of seminars and workshops have also been arranged with overwhelming response from the community.

5.2 International Collaboration

To foster closer collaboration with international security experts for sharing experience in information security and strengthening the knowledge of emerging cyber threats, vulnerabilities and appropriate mitigation solutions, GovCERT.HK strives to learn from the CERT community on global trends in international standards development, global information security and data privacy policies, cyber crime initiatives and technological researches.

In November 2019, GovCERT.HK officials, along with representatives of HKCERT, received a visit from delegates of the National Center of Incident Readiness and Strategy for Cybersecurity (NISC) of Cabinet Secretariat, the Government of Japan and the Consulate General of Japan in Hong Kong. There was an in-depth exchange of experiences and views on cyber security policy and security incident response strategies.

GovCERT.HK participated in the following events in 2019:

- FIRST Annual Conference
- Annual Technical Meeting for CSIRTs with National Responsibility
- CNCERT/CC Annual Conference
- 2019 China Cybersecurity Week
- APCERT Annual General Meeting and Conference
- APCERT Drill
- Five APCERT on-line training sessions

6. Future Plans

6.1 Upcoming Projects

The accelerated development of emerging technologies is spurring continuous innovation, however, it could also bring along different cyber security threats. GovCERT.HK will continue to stay vigilant in defending against potential cyber attacks. In particular to the rapid development of technology such as artificial intelligence, big data and Internet of Things, we are conducting a new round of review on the "Government IT Security Policy and Guidelines", covering the latest areas of information and cyber security as well as smart city development with reference to the latest international standards and industry best practices.

To enhance the capability of cyber threat intelligence management, we would continue to enhance our Cyber Risk Information Sharing Platform (CRisP) with integration of a Malware Information Sharing Platform (MISP) instance to enable sharing, storing and correlation of Indicators of Compromise.

We are also revamping our existing Information Security (InfoSec) Website to provide a more lively design for better user experience and facilitate dissemination of information security related tips and advices to the public.

6.2 Future Operations

In view of the positive response from the participating organisations of Cybersec Infohub and industries, we would regularise the programme and partner with HKIRC to promote the participation of more public and private organisations and sharing of cyber security information. This would also facilitate enterprises including SMEs to gather cyber security information and defend against cyber threats.

7. Conclusion

Cyber security attacks are increasingly targeted and sophisticated, with the forms they take becoming more diversified. GovCERT.HK has been proactively collaborating with local and global CERTs, making timely responses and enhancing appropriate defensive measures to the inevitable cyber security threats. In facilitating Hong Kong to become a secure smart city, GovCERT.HK will continue to foster all stakeholders to take forward communication and exchange of cyber security information so as to keep abreast of the fast-evolving cyber security landscape and be more vigilant to take prompt and appropriate measures to protect their information systems and data assets, with a view to continuously enhancing the cyber security resilience capability of the community.

Contact:	cert@govcert.gov.hk
Websites:	www.govcert.gov.hk
	www.cybersecurity.hk
	www.cybersechub.hk
	www.infosec.gov.hk