GovCERT.HK

Annual Report 2016

1. Highlights of 2016

1.1 Summary of Major Activities

Since its establishment in April 2015, the Government Computer Emergency Response Team Hong Kong, GovCERT.HK, has effectively fulfilled its responsibilities to centrally coordinate incident responses for over 80 departmental Information Security Incident Response Teams (ISIRTs) of the Government of the Hong Kong Special Administrative Region (HKSAR Government) as well as to bolster cyber security capabilities of the territory through proactive collaboration with the industry, critical Internet infrastructures, and the Computer Emergency Response Team (CERT) community for rapid exchange of threat information and coordinated response.

1.2 Achievements and Milestones

To promote the development of cyber security technologies and industry, we organised the first Hong Kong – Mainland Cyber Security Forum in April 2016 for cyber security professionals to share views on emerging cyber risks and counter measures associated with FinTech, cloud computing, and Internet security.

To address the increasing cyber security threats, we are progressively strengthening our capabilities in collating vulnerability information that would have impact on government installations and information and communications technology (ICT) users, assisting the government ISIRTs in contingency planning and incident response communications for both cyber attacks and data breach events.

Inspired by the Information Sharing Working Group and the TSUBAME Working Group, we were developing a cyber risk information sharing platform for internal use to facilitate speedier dissemination of cyber threat intelligence from GovCERT.HK to over 80 government ISIRTs. We would also pilot the use of big data analytics technology to collect and analyse cyber threat intelligence to formulate targeted cyber threat alerts and actionable advice for our stakeholders so that they can take early precautions and reinforce Hong Kong’s cyber security together.

2. About GovCERT.HK

2.1 Introduction

GovCERT.HK is a governmental CERT responsible for coordinating incident response for the HKSAR Government.

Locally, GovCERT.HK works closely with the Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) on sharing threat information and organising public awareness activities. GovCERT.HK focuses on government-related matters while HKCERT provides services related to incident response to all ICT users across the territory, covering public and private sectors as well as individuals.

Globally, GovCERT.HK collaborates with the CERT community in sharing incident information and threat intelligence; participating in training events, workshops and forums; 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 different internal IT security teams within the Office of the Government Chief Information Officer (OGCIO) of the HKSAR Government.

2.3 Resources

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

2.4 Mission and Constituency

Being the governmental CERT, GovCERT.HK will centrally manage incident response within the HKSAR Government and develop CERT-related services to enable government departments to understand the associated risks of information and cyber security, acquire necessary skills and take appropriate actions to protect government information infrastructure and data assets.

3. Activities and Operations

3.1 Scope of Services

GovCERT.HK is the computer emergency response team for the HKSAR Government, providing centrally managed incident response services; providing 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 in the region.

3.2 Incident Handling Reports

In 2016, GovCERT.HK has received and handled various types of information and cyber security incidents that are related to the installations of the HKSAR Government. The issues varied from vulnerable websites, malware infection, web defacement, distributed denial-of-service (DDoS) attacks, fraudulent emails to unauthorised access and loss of computing devices.

3.3 Alerts and Advisories

In 2016, we have published 85 product security alerts associated with computing products widely used in government installations, and one security advisory recommending system administrators to review security configuration of all versions of Microsoft Windows operating systems as well as to mitigate potential risks associated with the Windows PowerShell automation tools.

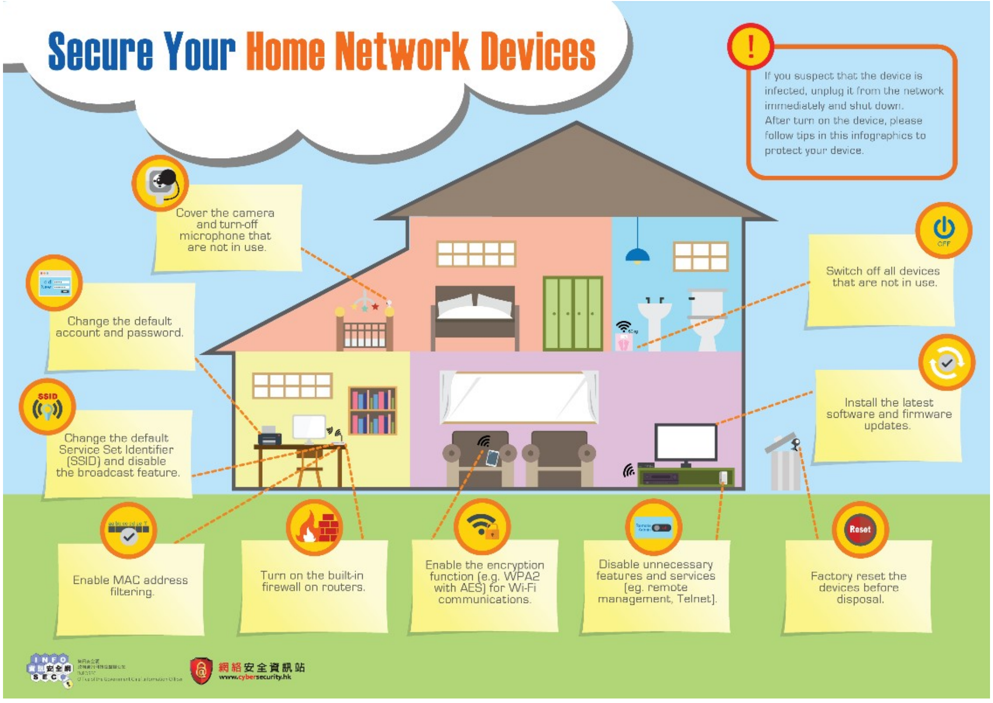
We have also issued 20 security reminders to government departments requesting them to take effective and prompt responsive measures against potential attacks and high-risk malware infection, in particular ransomware. We also reminded all users to regularly use anti-malware software to scan their computer systems and perform data backup, and store the backup copy offline.

3.4 Publications and Mass Media

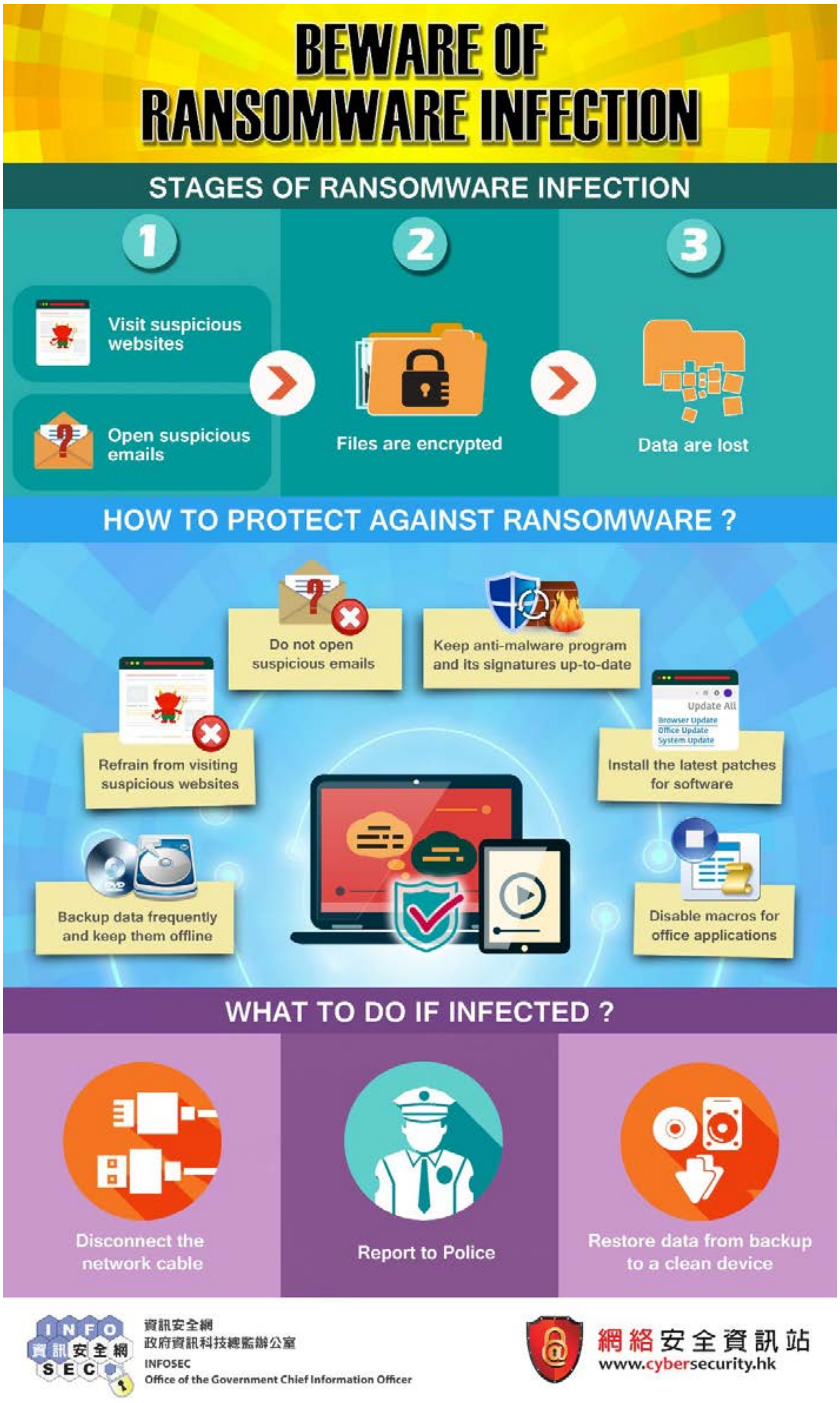
To raise public awareness and knowledge on the importance of information security, we have resorted to different promotion channels to reach out to our target audience and collaborated with industry players during the process.

- Radio episodes entitled "e-World Smart Tips" were broadcast to help the public understand more about information security in various aspects and raise their awareness of information security. The radio episode in each week featured a different theme and offered associated tips having regard to recent security incidents or foreseeable cyber threats. For instance, the radio tips of "Be a Good Netizen" were broadcast in September 2016 to disseminate messages of safe and ethical use of the Internet.

- To provide practical tips and advice for Small and Medium Enterprise (SMEs) and the general public to protect from cyber attacks, we have developed and shared infographics covering popular security topics such as "Secure Your Home Network Devices" to remind the public to take necessary precatory actions for protecting their networking and computing devices.


Secure Your Home Network Devices
If you suspect that the device is infected, unplug it from the network immediately and shut down. After turn on the device, please follow tips in this infographics to protect your device.
Cover the camera and turn-off microphone that are not in use.
Change the default account and password.
Change the default Service Set Identifier (SSID) and disable the broadcast feature.
Switch off all devices that are not in use.
Install the latest software and firmware updates.
Enable MAC address filtering.
Turn on the built-in firewall on routers.
Enable the encryption function (e.g. WPA2 with AES) for Wi-Fi communications.
Disable unnecessary features and services (eg. remote management, Telnet).
Factory reset the devices before disposal.
OFF
Reset
SSID
網絡安全資訊站
www.cybersecurity.hk

- In view of the rising reports of ransomware infection and data loss incidents, we have designed a poster titled “Beware of Ransomware Infection” to advise our stakeholders the importance of data protection and ways to protect themselves against ransomware. The poster was posted in public libraries, government premises and disseminated to schools and SMEs for awareness promotion.



BEWARE OF RANSOMWARE INFECTION

STAGES OF RANSOMWARE INFECTION

1 Visit suspicious websites

Open suspicious emails

2 Files are encrypted

3 Data are lost

HOW TO PROTECT AGAINST RANSOMWARE ?

Do not open suspicious emails

Keep anti-malware program and its signatures up-to-date

Refrain from visiting suspicious websites

Install the latest patches for software

Backup data frequently and keep them offline

Disable macros for office applications

WHAT TO DO IF INFECTED ?

Disconnect the network cable

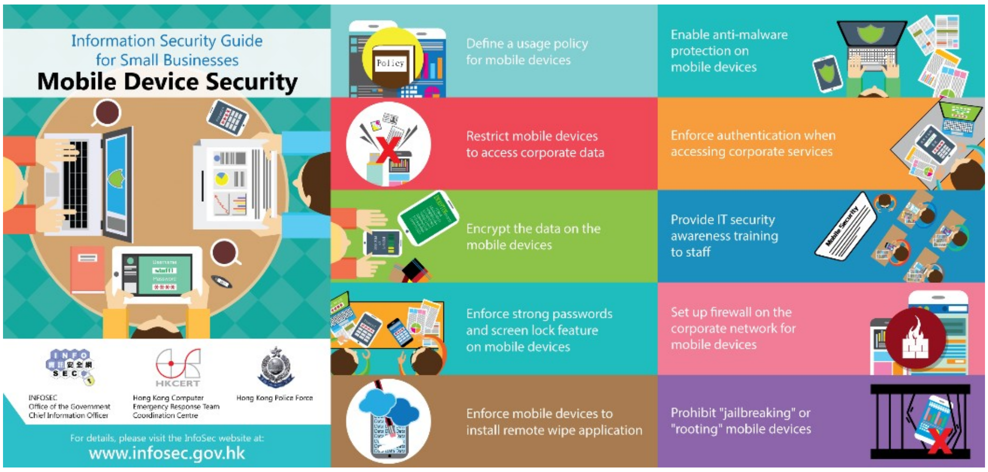
Report to Police

Restore data from backup to a clean device

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

網絡安全資訊站
www.cybersecurity.hk

- A set of practical guidelines with different themes, including “Mobile Device Security”, “Beware of Phishing” and “Defense Against Malware”, were produced to educate SMEs to deploying appropriate security measures in their business environment.



Information Security Guide for Small Businesses

Mobile Device Security

Define a usage policy for mobile devices

Restrict mobile devices to access corporate data

Encrypt the data on the mobile devices

Enforce strong passwords and screen lock feature on mobile devices

Enforce mobile devices to install remote wipe application

Enable anti-malware protection on mobile devices

Enforce authentication when accessing corporate services

Provide IT security awareness training to staff

Set up firewall on the corporate network for mobile devices

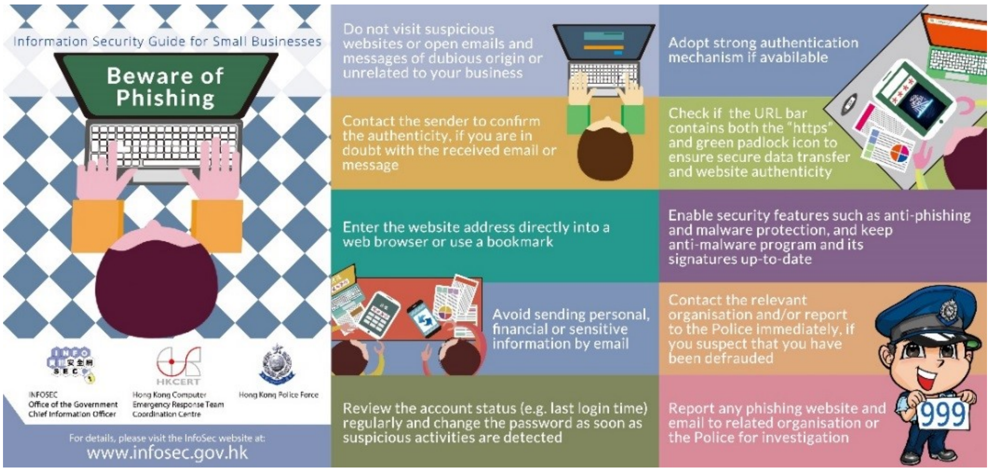
Prohibit "jailbreaking" or "rooting" mobile devices

INFOSEC Office of the Government Chief Information Officer

Hong Kong Computer Emergency Response Team Coordination Centre

Hong Kong Police Force

For details, please visit the InfoSec website at:
www.infosec.gov.hk



Information Security Guide for Small Businesses

Beware of Phishing

Do not visit suspicious websites or open emails and messages of dubious origin or unrelated to your business

Contact the sender to confirm the authenticity, if you are in doubt with the received email or message

Enter the website address directly into a web browser or use a bookmark

Avoid sending personal, financial or sensitive information by email

Review the account status (e.g. last login time) regularly and change the password as soon as suspicious activities are detected

Adopt strong authentication mechanism if avalilable

Check if the URL bar contains both the "https" and green padlock icon to ensure secure data transfer and website authenticity

Enable security features such as anti-phishing and malware protection, and keep anti-malware program and its signatures up-to-date

Contact the relevant organisation and/or report to the Police immediately, if you suspect that you have been defrauded

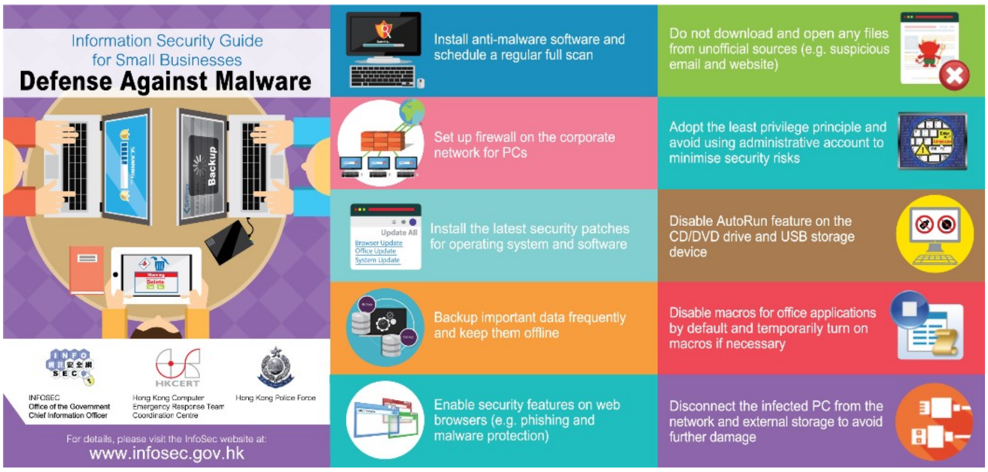
Report any phishing website and email to related organisation or the Police for investigation

INFOSEC Office of the Government Chief Information Officer

Hong Kong Computer Emergency Response Team Coordination Centre

Hong Kong Police Force

For details, please visit the InfoSec website at:
www.infosec.gov.hk



Information Security Guide for Small Businesses

Defense Against Malware

Install anti-malware software and schedule a regular full scan

Set up firewall on the corporate network for PCs

Install the latest security patches for operating system and software

Backup important data frequently and keep them offline

Enable security features on web browsers (e.g. phishing and malware protection)

Do not download and open any files from unofficial sources (e.g. suspicious email and website)

Adopt the least privilege principle and avoid using administrative account to minimise security risks

Disable AutoRun feature on the CD/DVD drive and USB storage device

Disable macros for office applications by default and temporarily turn on macros if necessary

Disconnect the infected PC from the network and external storage to avoid further damage

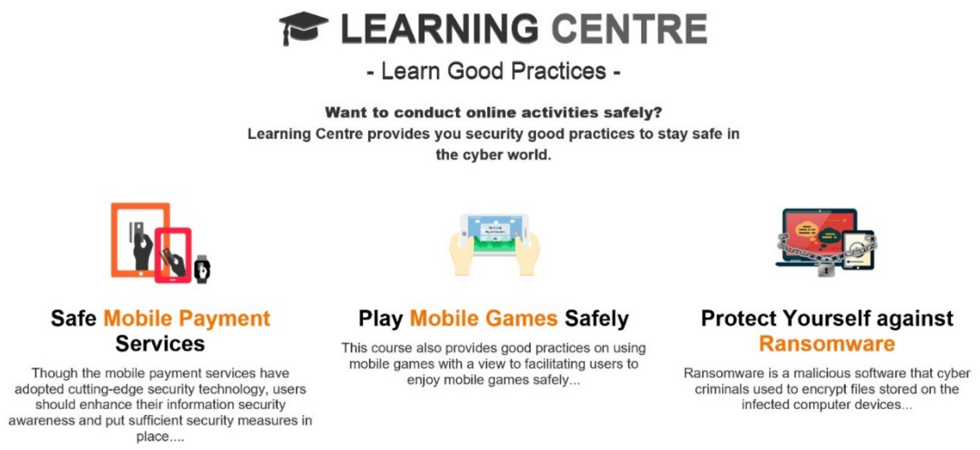
INFOSEC Office of the Government Chief Information Officer

Hong Kong Computer Emergency Response Team Coordination Centre

Hong Kong Police Force

For details, please visit the InfoSec website at:
www.infosec.gov.hk

- Various learning modules were launched on our thematic website in response to high-impact security events. In the light of the surge in ransomware infection cases in 2016, we have developed a learning module on “Protect Yourself against Ransomware”. Other training modules like “Play Mobile Games Safely” and “Safe Mobile Payment Services” were also produced to provide users with good practices to stay safe in the cyber world.



LEARNING CENTRE

- Learn Good Practices -

Want to conduct online activities safely?
Learning Centre provides you security good practices to stay safe in the cyber world.

Safe Mobile Payment Services

Though the mobile payment services have adopted cutting-edge security technology, users should enhance their information security awareness and put sufficient security measures in place....

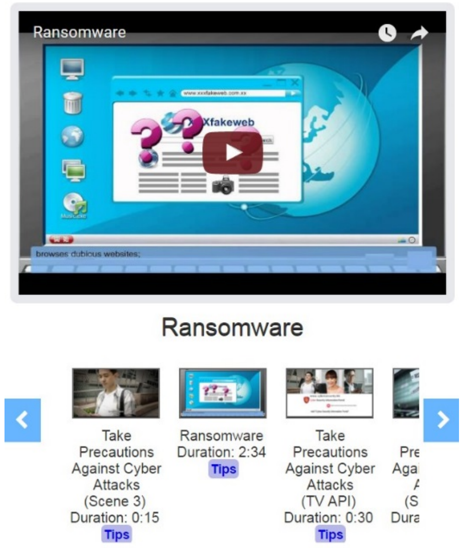
Play Mobile Games Safely

This course also provides good practices on using mobile games with a view to facilitating users to enjoy mobile games safely...

Protect Yourself against Ransomware

Ransomware is a malicious software that cyber criminals used to encrypt files stored on the infected computer devices...

- To actively reach out to the general public, social media like YouTube and Twitter, as well as newspapers, were used to share tips and best practices on information security and attract public to participate in our security seminars and events.



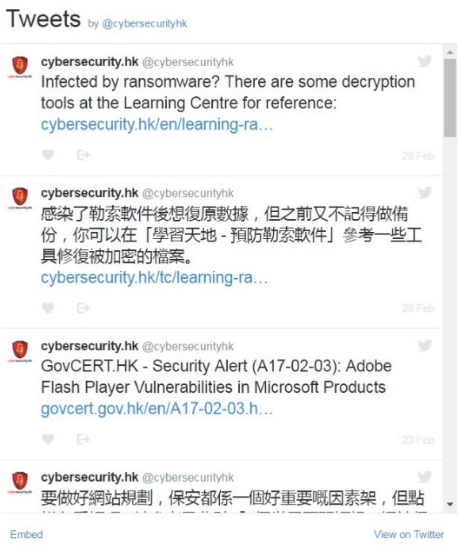
Ransomware

Take Precautions Against Cyber Attacks (Scene 3)
Duration: 0:15
Tips

Ransomware
Duration: 2:34
Tips

Take Precautions Against Cyber Attacks (TV API)
Duration: 0:30
Tips

Pre
Agai
A
(S
Dura



Tweets by @cybersecurityhk

cybersecurity.hk @cybersecurityhk
Infected by ransomware? There are some decryption tools at the Learning Centre for reference:
cybersecurity.hk/en/learning-ra…
28 Feb

cybersecurity.hk @cybersecurityhk
感染了勒索軟件後想復原數據，但之前又不記得做備份，你可以在「學習天地 - 預防勒索軟件」參考一些工具修復被加密的檔案。
cybersecurity.hk/tc/learning-ra…
28 Feb

cybersecurity.hk @cybersecurityhk
GovCERT.HK - Security Alert (A17-02-03): Adobe Flash Player Vulnerabilities in Microsoft Products
govcert.gov.hk/en/A17-02-03.h…
23 Feb

cybersecurity.hk @cybersecurityhk
要做好網站規劃，保安都係一個好重要嘅因素架，但點

Embed
View on Twitter

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 2016, we have organised a total of 14 seminars, workshops and solution showcases for government IT staff and users to enhance their awareness of the latest security vulnerabilities and update their knowledge in information security technologies.

- Seminars and showcases were conducted for government IT staff and users to raise their security awareness and introduce the latest IT security technologies and solutions. The topics included industry best practices, mobile and cyber security, data protection, end-point protection and big data analytics.

- 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.

- Web vulnerability scanning workshops were organised for some 100 government officers to equip them with the necessary skills and knowledge to effectively identify the potential security weaknesses in web applications and remedy the security risks.

4.2 Drills and Exercises

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

In 2016, we conducted eight drill exercises involving different government departments and their respective service contractors. We also conducted an inter-departmental cyber security drill with the participation of some 30 departments to enhance the overall information security incident response capabilities of the Government.

As the Operational member of APCERT, GovCERT.HK participated in the APCERT Drill with the theme of "An Evolving Cyber Threat and Financial Fraud" in March 2016.

4.3 Conferences and Seminars

In 2016, GovCERT.HK adopted the slogan "Protect Data, Secure Transaction" as the key message to government users and the general public. The target audience included businesses especially SMEs, organisations, schools and the general public.

- Two seminars were organised under the "Build a Secure Cyberspace" campaign in May and November 2016, aiming to promote public awareness of information security and the adoption of security best practices. The one-day seminar in November 2016 invited industry associations and experts to share insights on a range of security topics, including the most common cyber security threats nowadays, associated security advice, security challenges faced by website administrators, points-to-note for secure mobile payment and the safe use of public Wi-Fi.
- The Cyber Security Programme was specifically organised this year. The Programme featured a series of activities for public participation, including the "Protect Your Precious Assets in Cyberspace" seminar. Representatives from the Government, industry associations and solution providers spoke on the best practices of information security with regard to a number of hot topics, including online privacy and security measures for mobile platforms.
- 34 seminars were conducted at primary and secondary schools in 2016, reaching out to nearly 11 000 students and teachers for raising their awareness of cyber security and strengthening their knowledge of protecting personal information.

- A mascot design contest with the theme "Protect Data, Secure Transaction" was organised from April 2016 to July 2016. The contest has received overwhelming response with over 2 000 entries. These entries have clearly conveyed the salient points of protecting computing devices from cyber security traps, and accurately highlighted the importance of data protection and online transaction security.

Build a Secure Cyberspace 2016
Protect Data,
Secure Transaction
Seminar cum Mascot Design Contest
Award Presentation Ceremony

- To commend outstanding IT managers and practitioners for their contributions to the industry, the Cyber Security Professionals Awards (CSPA) was organised in September 2016. This event was the first of its kind in Hong Kong to encourage cyber security personnel to exchange experience and insights with the objective of enhancing the industry's capabilities of cyber security protection. The awards presentation ceremony was successfully held in January 2017. [http://www.csprofessionalsawards.net/]

- To promote the development of cyber security technologies and industry in both Hong Kong and the Mainland, the first Hong Kong-Mainland Cyber Security Forum were held in April 2016. The forum attracted some 200 information security professionals from the Government, research institutions, the academia, professional organisations and the information security industry.

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

To raise public awareness, GovCERT.HK collaborated with HKCERT and security service providers to gather information on security vulnerabilities and promptly issue alerts on malicious cyber activities to the public and private sectors.

GovCERT.HK also steered the Internet Infrastructure Liaison Group (IILG) to closely monitor the Internet operation status with a view to alerting related parties to abnormal activities. IILG is comprised of members from Internet infrastructures, including the Hong Kong Internet Exchange and the Hong Kong Internet Registration Corporation Limited, major Internet service providers and stakeholders.

5.2 International Collaboration

To foster the Government's 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.

GovCERT.HK has participated in the following events in 2016:

- CNCERT Annual Conference in May 2016
- FIRST Annual Conference 2016 in June 2016
- NatCSIRT Annual Technical Meeting in June 2016
- 2016 China Cybersecurity Week in September 2016
- APCERT Annual General Meeting and Conference 2016 in October 2016
- Five APCERT on-line training sessions from April to December 2016

6. Future Plans

6.1 Upcoming Projects

Apart from public awareness training and promotion initiatives, GovCERT.HK will support the Inter-university Capture the Flag Contest and work with local universities and the industry to organise a cyber security contest to promote awareness of information security and proper cyber etiquette.

To carry forward the success of the inter-departmental cyber security drill 2016, GovCERT.HK will continue to organise the drill on an even larger scale to enable prompt and efficient response to cyber security incidents.

6.2 Future Operation

GovCERT.HK will continue to forge closer ties and enhance information exchange with the CERT community, as well as streamline and enhance its operations appropriately to cope with the increasing security threats and alleged cyber attacks in the region.

In addition to the events and conferences attended in 2016, GovCERT.HK will also join the Microsoft Digital Crime Consortium to network with the global cyber security communities for knowledge and experience sharing, and to enhance the collaboration with the security industry.

7. Conclusion

GovCERT.HK has made substantial strides towards collaboration and operations with local and global CERTs to meet the ever-increasing challenges on cyber security and yielded well-recognised results in safeguarding the Government and the public against cyber security threats. GovCERT.HK will continue to take forward the cyber security initiatives by joining hands with the industry, professional organisations and various stakeholders to maintain a secure, stable and trustworthy cyber world for people from all walks of life.

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