

Information Security in Schools— Recommended Practice (January 2019)

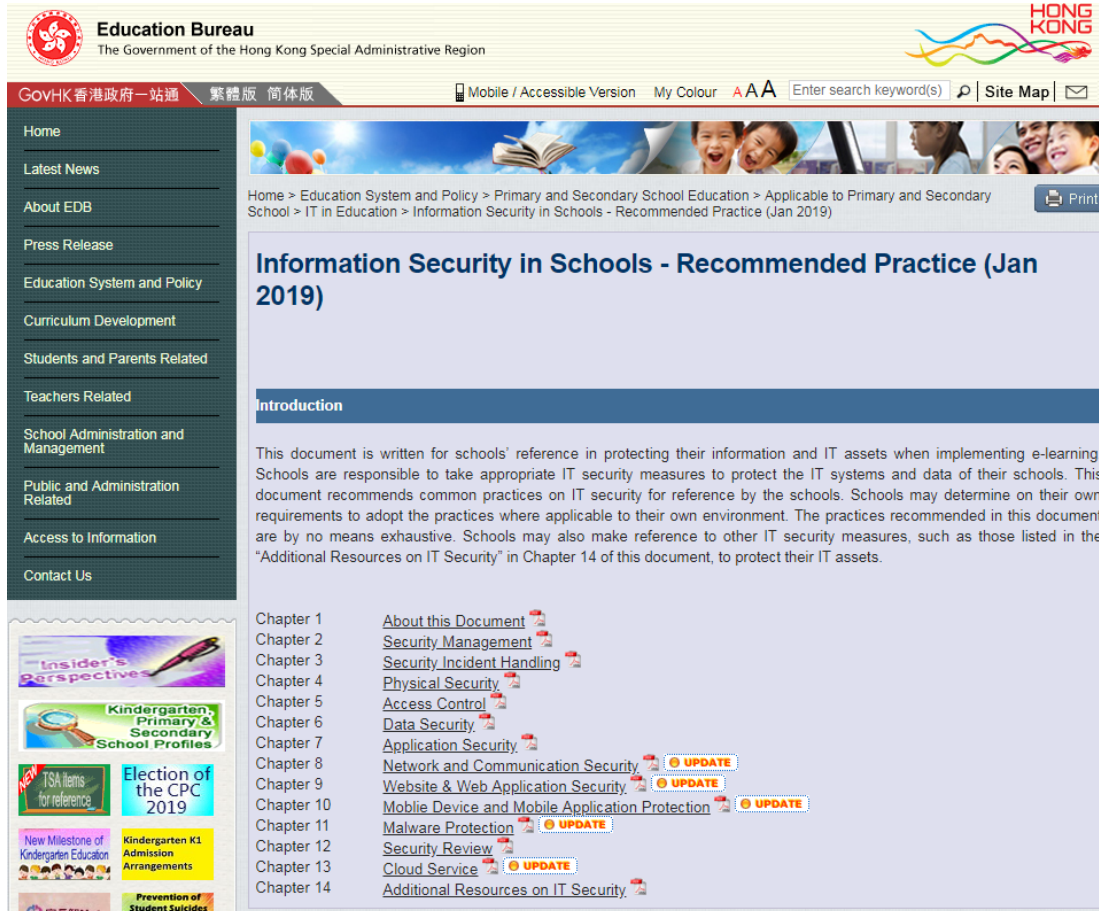
IT in Education Section
Education Bureau
15 January 2019

Information Security in Schools – Recommended Practice

- Since 2002, the EDB has been providing recommended practice on IT security to assist schools in formulating IT security policies and promoting related good practices.
- The EDB updates the document from time to time.

Information Security in Schools – Recommended Practice (January 2019)

<https://www.edb.gov.hk/en/edu-system/primary-secondary/applicable-to-primary-secondary/it-in-edu/Information-Security/information-security-in-school.html>



Education Bureau
The Government of the Hong Kong Special Administrative Region

GovHK 香港政府一站通 繁體版 簡體版 Mobile / Accessible Version My Colour A A Enter search keyword(s) Site Map

Home
Latest News
About EDB
Press Release
Education System and Policy
Curriculum Development
Students and Parents Related
Teachers Related
School Administration and Management
Public and Administration Related
Access to Information
Contact Us

Home > Education System and Policy > Primary and Secondary School Education > Applicable to Primary and Secondary School > IT in Education > Information Security in Schools - Recommended Practice (Jan 2019)

Information Security in Schools - Recommended Practice (Jan 2019)

Introduction

This document is written for schools' reference in protecting their information and IT assets when implementing e-learning. Schools are responsible to take appropriate IT security measures to protect the IT systems and data of their schools. This document recommends common practices on IT security for reference by the schools. Schools may determine on their own requirements to adopt the practices where applicable to their own environment. The practices recommended in this document are by no means exhaustive. Schools may also make reference to other IT security measures, such as those listed in the "Additional Resources on IT Security" in Chapter 14 of this document, to protect their IT assets.

Chapter 1 [About this Document](#)
Chapter 2 [Security Management](#)
Chapter 3 [Security Incident Handling](#)
Chapter 4 [Physical Security](#)
Chapter 5 [Access Control](#)
Chapter 6 [Data Security](#)
Chapter 7 [Application Security](#)
Chapter 8 [Network and Communication Security](#) **UPDATE**
Chapter 9 [Website & Web Application Security](#) **UPDATE**
Chapter 10 [Mobile Device and Mobile Application Protection](#) **UPDATE**
Chapter 11 [Malware Protection](#) **UPDATE**
Chapter 12 [Security Review](#) **UPDATE**
Chapter 13 [Cloud Service](#) **UPDATE**
Chapter 14 [Additional Resources on IT Security](#)

Insider's Perspectives
Kindergarten, Primary & Secondary School Profiles
TSA Items for reference
Election of the CPC 2019
New Milestone of Kindergarten Education
Kindergarten K1 Admission Arrangements
Prevention of Student Suicides



TABLE OF CONTENT	
CHAPTER 1	ABOUT THIS DOCUMENT
CHAPTER 2	SECURITY MANAGEMENT
CHAPTER 3	SECURITY INCIDENT HANDLING
CHAPTER 4	PHYSICAL SECURITY
CHAPTER 5	ACCESS CONTROL
CHAPTER 6	DATA SECURITY
CHAPTER 7	APPLICATION SECURITY
CHAPTER 8	NETWORK AND COMMUNICATION SECURITY
CHAPTER 9	WEBSITE & WEB APPLICATION SECURITY
CHAPTER 10	MOBILE DEVICE AND MOBILE APPLICATION PROTECTION
CHAPTER 11	MALWARE PROTECTION
CHAPTER 12	SECURITY REVIEW
CHAPTER 13	CLOUD SERVICE
CHAPTER 14	ADDITIONAL RESOURCES ON IT SECURITY

Information Security in Schools Recommended Practice

Education Bureau
The Government of the HKSAR

Revised in January 2019

Major Updates

2016 Version

PART 1 ABOUT THIS DOCUMENT
PART 2 SECURITY MANAGEMENT
PART 3 SECURITY INCIDENT HANDLING
PART 4 PHYSICAL SECURITY
PART 5 ACCESS CONTROL
PART 6 DATA SECURITY
PART 7 APPLICATION SECURITY
PART 8 NETWORK AND COMMUNICATION SECURITY
PART 9 WEB APPLICATION SECURITY
PART 10 SECURITY ISSUES OF MOBILE APPLICATIONS
PART 11 COMPUTER VIRUS PROTECTION
PART 12 SECURITY REVIEW
PART 13 CLOUD SERVICE
~~PART 14 WI-FI SECURITY QUICK REFERENCE~~
PART 15 ADDITIONAL RESOURCES ON IT SECURITY

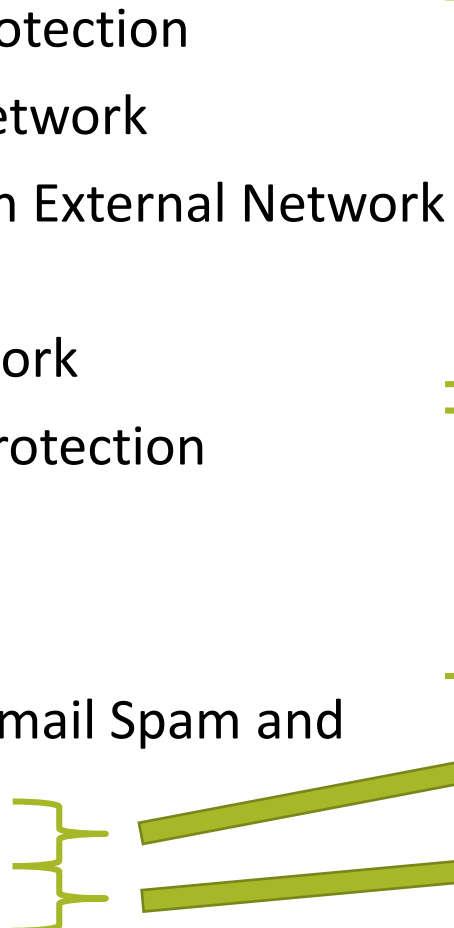
2019 Version

CHAPTER 1 ABOUT THIS DOCUMENT
CHAPTER 2 SECURITY MANAGEMENT
CHAPTER 3 SECURITY INCIDENT HANDLING
CHAPTER 4 PHYSICAL SECURITY
CHAPTER 5 ACCESS CONTROL
CHAPTER 6 DATA SECURITY
CHAPTER 7 APPLICATION SECURITY
CHAPTER 8 NETWORK AND COMMUNICATION SECURITY
CHAPTER 9 WEBSITE & WEB APPLICATION SECURITY
CHAPTER 10 MOBILE DEVICE AND MOBILE APPLICATION PROTECTION
CHAPTER 11 MALWARE PROTECTION
CHAPTER 12 SECURITY REVIEW
CHAPTER 13 CLOUD SERVICE
CHAPTER 14 ADDITIONAL RESOURCES ON IT SECURITY

Major Updates – Chapter 8

Network and Communication Security

2016 Version

- General Network Protection
 - Building a Secure Network
 - Communication with External Network
 - Remote Access
 - Virtual Private Network
 - Wireless Network Protection
 - Management Control
 - Technical Control
 - End-user Control
 - Protection against Email Spam and Malicious code
 - System Prospective
 - End-user Prospective
 - ~~Prevent Malicious Code (Merge to Chapter 11)~~
- 

2019 Version

- Network Security Management (Revised)
 - Recommendations for schools on building a secure network
 - Remote Access
 - Virtual Private Network
- **Wireless Network Build Up Security Concerns (New)**
 - Security Risks
 - Recommendations for schools on wireless network deployment
 - Network Mode (Separate / Integrate)
- Security Controls to Protect WLAN (Revised)
 - Management Control
 - Technical Control
 - End-user Control
- Mail Gateway Security and Email Handling
 - Mail Server Protection (Revised)
 - **Tips for protecting schools from email bombing, spamming and spoofing (New)**
 - Reduce the amount of incoming spam (Revised)
 - **Protection against Email Scam (New)**

Major Updates – Chapter 8

Network and Communication Security

- Security concerns on the communication with the external network and access privilege.
- Protection against the system and end-user strengthened.
- Email Bombing, Spamming & Spoofing and Email Scam.
- Security concerns on the network modes (Separate / Integrate) adopted by schools.

Separate or Integrate?

- It is recommended to build the WiFi network completely separated from schools' existing network with separate broadband line to reduce security risk
- Due to the nature of wireless technology, wireless networks are relatively hard to contain within a building and it is generally considered to be an un-trusted network.
- As a best practice, wireless networks and wired networks should not be directly connected to each other.

IT Security Measures to address the Security Concerns on Integrating the Networks

- For schools adopting the integration mode of WiFi networks, schools' IT personnel needs to assess, understand and eliminate the security issues and risks to school existing network when the WiFi network is integrated or connected to schools' existing network.
- Schools adopting the integration mode of WiFi networks are recommended to apply the "Defence-in-Depth" approach.
- Possible measures that can be employed to build multiple layers of defense:
 - ◆ *Separation of wireless and wired network segments*
 - ◆ *Use of strong device and user authentication methods*
 - ◆ *Application of network filtering based on addresses and protocols*
 - ◆ *Deployment of intrusion detection systems on the wireless and wired networks*

Major Updates – Chapter 9

Website & Web Application Security

2016 Version

WEB APPLICATION SECURITY

- Adopt Web Application Security Architecture
 - *Architecture*
 - *Web Server Security*

2019 Version

WEBSITE & WEB APPLICATION SECURITY

- Website & Web Application Security Architecture
- Web Server Security (Revised)
- **Web Server Monitoring and Incident Handling (New)**
- **Web Application Security (New)**
- **Keep Your School's Website Safe (New)**
- **Secure Website with HTTPS Protocol (New)**
- **Anti-DDoS Protection (New)**

Major Updates – Chapter 9

Website & Web Application Security

- Important of web server security such as account management, web server application management, ports management, patch management, security monitoring, backup.
- Web application security and data protection.
- HTTPS issue.
- How to prevent DDoS / Botnet attack.
- For better security incidents handling, schools are recommended to:
 - *Follow the security incident handling procedure to handle the security incident until it is mitigated; and*
 - *Report the case to Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) and Hong Kong Police Force (HKPF).*

Major Updates – Chapter 10

Mobile Device and Mobile Application Protection

2016 Version

SECURITY ISSUES OF MOBILE APPLICATIONS

- Protecting Mobile Devices
 - *Configuration Mobile Device*
 - *Precautions of Using Mobile Applications*

2019 Version

MOBILE DEVICE AND MOBILE APPLICATION PROTECTION (New)

- Security Concerns of Mobile Devices
- Information Security Policy for Mobile Devices
- Data Communication and Storage for Mobile Devices
- User and Device Authentication for Mobile Devices
- Security Control for Mobile Device Application
- Mobile Device Management (MDM) Solution

Major Updates – Chapter 10

Mobile Device and Mobile Application Protection

- Schools should establish a mobile device security policy to specify the operation and security requirements for mobile devices access.
- A formal usage policy and procedures should be in place, and appropriate security measures should be adopted to protect against the risks of using mobile computing and communication facilities.
- Schools are recommended to install security control tools such as MDM, anti-malware software.

Major Updates – Chapter 11

Malware Protection

2016 Version

COMPUTER VIRUS PROTECTION

- Anti-Virus Software
- Legal and Authorised Use of Software and Hardware
- Prevention from Doubtful File Resources

2019 Version

MALWARE PROTECTION (New)

- **Protection against Malware by Schools**
- **Protection against Malware by Users**
- **Malware Incident Handling and Recovery**
- **Protection against Ransomware**
- **Ransomware Incident Handling and Recovery**

Major Updates – Chapter 11

Malware Protection

- Malware can cause different level of security risks to computer assets, such as disrupt computer operations, gather sensitive information, etc.
- Schools are advised to adopt the precaution measures against ransomware.
- Ransomware Incident Handling:
 - a) *Disconnect* the network cable of the computer to avoid affecting network drives and other computers.
 - b) *Power off* the computer to stop the ransomware encrypting more files.
 - c) *Jot down* what have been accessed (such as programs, files, emails and websites) before discovering the issue.
 - d) *Report* to the HKCERT and HKPF the criminal offence if necessary.
 - e) *Recover* the data from backup to a clean computing device.

Major Updates – Chapter 13

Cloud Service

2016 Version

CLOUD SERVICE

- Cloud computing security considerations

2019 Version

CLOUD SERVICE (New)

- **Cloud Security Overview**
- **Cloud Service Security Consideration**
 - *Checklist on selecting cloud service provider*
 - *On using cloud services*

Updates – Chapter 13

Cloud Service

- A checklist on selecting cloud service provider was provided to schools for reference.
- Using encryption to protect stored data.
- Think twice when you want to store sensitive data in the cloud and assess the impact if the data concerned is exposed.
- Perform a regular backup of the data stored in the cloud service and maintain a local backup copy of important data so that this data can still be available when the service provider is out of service.

Security Tips

- TSS or IT Head should harden the firewall regularly including update firmware, review policy and check event log.
- Cyber attack are become more advance and unpredictable. Schools are recommended to deploy security device with the latest technology to secure the school's network.
- Many schools were infected ransomware by opening attachments in suspicious email. Schools are recommended to purchase the latest anti-malware software with signature to filter the malicious attachment.
- There were security vulnerability in WPA2, schools are recommended to deploy network device with WPA3 when upgrading the Wi-Fi network.
- Apply latest approved security patches to any software (especially the operating system) and avoid using the end of supported components.

Related Promotion and Support by EDB

- Information Security in Schools webpage
- Email Message on IT Security Alert
- Information Security in Schools – Recommended Practice
- Co-organise with professional bodies to provide IT security related seminars
- Promote IT security related events / activities through school circular memorandum
- Grants

Overview of Various ITE Grants

Recurrent

Composite IT Grant (CITG)

\$202,679 – 697,086 dependent on school type and size

Operational needs for e-learning, such as -

- IT-related consumables
- Digital resource materials
- Technical Support Staff (TSS)
- Maintenance of IT facilities, etc.

Funding for ITE4

\$70,000 on average

- WiFi services fee
- Maintenance/ replacement of mobile devices

ITSSG

Flat rate of \$307,200

Recruitment of TSS through contract or services procurement

One-off

ITE4 (\$100,000 on average)

- Mobile devices

Extra One-off IT Grant (\$200,000 on average)

- Mobile devices
- Recruitment of TSS
- E-resource/platform

Information Security in Schools webpage

<https://www.edb.gov.hk/ited/i-security>

The screenshot shows the Education Bureau (EDB) website. The header includes the EDB logo and the text 'Education Bureau The Government of the Hong Kong Special Administrative Region'. Below the header is a navigation bar with links for 'Home', 'Latest News', 'About EDB', 'Press Release', 'Education System and Policy', 'Curriculum Development', 'Students and Parents Related', 'Teachers Related', 'School Administration and Management', 'Public and Administration Related', 'Access to Information', and 'Contact Us'. The main content area is titled 'Information Security in Schools' and features a banner for a seminar on 15 Jan 2019. Below the banner, there is a section for the seminar details, including the date, time, venue, and a link to the application form. The sidebar on the left contains various links and resources, including 'Insider's Perspectives', 'School Management Committee', 'TSA Items for reference', 'New Milestone of Kindergarten Education', 'Kindergarten K1 Admission Arrangements', '家長智Net Smart Parent Net', 'Prevention of Student Suicides', 'The Chief Executive's 2018 Policy Address', and '2018 Policy Address Policy Initiatives of Education Bureau'.

(02/06/2018) IT in Education e-Safety Series: School Websites Secure Sockets Layer (SSL) Protection, Security Risk and Cyber Security Seminar on 2 June 2018 [EI0020180236]

This seminar aims to arouse the schools' awareness and knowledge on information and cyber security issues. Information of the seminar are as follows:

Date : 2 June 2018 (Sat)

Time : 9:30 am - 12:30 pm

Venue : Lecture Theatre, 4/F, West Block, Kowloon Tong Education Services Centre, 19 Suffolk Road, Kowloon Tong

Speaker's presentation slides are as follows:

- [Presentation by EDB ITE Section](#)
- [Presentation by PISA](#)
- [Presentation by HKCERT](#)
- [Presentation by HKPF*](#)
- [Presentation by WebOrganic](#)
- [Presentation by HKITF*](#)

*Remark: Presentation slides by HKPF & HKITF could not be provided.



Information Literacy

<https://www.edb.gov.hk/il/eng>



The screenshot shows the Education Bureau website. The header includes the Education Bureau logo, the text "Education Bureau The Government of the Hong Kong Special Administrative Region", and a "HONG KONG" logo. Below the header is a navigation bar with links for "GOVHK 香港政府一站通", "繁體版", "简体版", "Mobile / Accessible Version", "My Colour", "AA", a search bar, "Site Map", and an email icon. A left sidebar contains a list of links: Home, Latest News, About EDB, Press Release, Education System and Policy, Curriculum Development, Students and Parents Related, Teachers Related, School Administration and Management, Public and Administration Related, Access to Information, and Contact Us. The main content area features a banner with colorful balloons and a book. Below the banner is a breadcrumb trail: Home > Education System and Policy > Primary and Secondary School Education > Applicable to Primary and Secondary School > IT in Education > Information Literacy for Hong Kong Students. A "Print" button is located to the right of the breadcrumb trail. The main heading is "Information Literacy for Hong Kong Students". Below the heading are links for "Introduction", "Related Documents", "On-going Support", and "Related Links". The "Introduction" section contains two paragraphs. The first paragraph states that information technology (IT) is a powerful tool to unleash the learning capability of students, and that strategies for information literacy (IL) are formulated at various stages to enable students to learn and excel through realising the potential of IT in enhancing interactive learning and teaching experiences. The second paragraph states that as an important competency, IT helps students identify the need for information, locate, evaluate, extract, organise and present information, create new ideas, cope with the dynamics in our information world, use information ethically as well as refrain from immoral practices such as cyber bullying and infringing intellectual property rights. IL could be developed through the application of the generic skills (see Section 2.3.1 and Appendix 1 of this booklet) in the context of handling information in different media in our information world. This also involves various knowledge contexts and has close linkage with the KLAs. A third paragraph states that schools can make reference to the "Information Literacy for Hong Kong Students" for suggestions on how to develop students' knowledge, skills and attitudes to use information and information technology ethically and effectively as responsible citizens and lifelong learners. Incorporation of IL in the whole-school curriculum will provide authentic contexts for students to apply the skills and benefit their learning in relevant KLAs. At the bottom left, there is a small image of a book titled "Insider's Perspectives" and a link to "Kindergarten".

Education Bureau
The Government of the Hong Kong Special Administrative Region

GOVHK 香港政府一站通 繁體版 简体版 Mobile / Accessible Version My Colour AA Enter search keyword(s) Site Map

Home > Education System and Policy > Primary and Secondary School Education > Applicable to Primary and Secondary School > IT in Education > Information Literacy for Hong Kong Students

Information Literacy for Hong Kong Students

[Introduction](#) | [Related Documents](#) | [On-going Support](#) | [Related Links](#)

Introduction

Information technology (IT) is a powerful tool to unleash the learning capability of students. With the advancement of technology and its application through innovative pedagogies in all KLAs, students' capability in information literacy (IL), self-directed learning and other 21st century skills such as creativity, problem solving skills, collaboration skills and computational thinking skills are enhanced. Strategies on IT in Education are formulated at various stages to enable students to learn and excel through realising the potential of IT in enhancing interactive learning and teaching experiences.

As an important competency, IT helps students identify the need for information; locate, evaluate, extract, organise and present information; create new ideas; cope with the dynamics in our information world; use information ethically as well as refrain from immoral practices such as cyber bullying and infringing intellectual property rights. IL could be developed through the application of the generic skills (see Section 2.3.1 and Appendix 1 of this booklet) in the context of handling information in different media in our information world. This also involves various knowledge contexts and has close linkage with the KLAs.

Schools can make reference to the "Information Literacy for Hong Kong Students" for suggestions on how to develop students' knowledge, skills and attitudes to use information and information technology ethically and effectively as responsible citizens and lifelong learners. Incorporation of IL in the whole-school curriculum will provide authentic contexts for students to apply the skills and benefit their learning in relevant KLAs.

Insider's Perspectives Kindergarten



Promote IT security related events / activities through school circular memorandum

<https://www.cybersecurity.hk/en/resources.php>

BEWARE OF RANSOMWARE INFECTION

STAGES OF RANSOMWARE INFECTION

- 1 Visit suspicious websites
- 2 Open suspicious emails
- 3 Files are encrypted
- 4 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
- Update All: Browser, Office, System, Software
- 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

EDBCM No.164/2018 Cyber Security Campaign – Smart Devices Security

Education Bureau Circular Memorandum No. 164/2018

From : Secretary for Education To: Heads of Primary and Secondary Schools
Ref : EDB(EID/ITE)/IT/PRO/189
Date : 24 September 2018

Cyber Security Campaign – Smart Devices Security

Summary

The purpose of this circular memorandum is to inform heads of schools about the launch of the "Cyber Security Campaign – Smart Devices Security" organised by the Cyber Security and Technology Crime Bureau (CSTCB) of Hong Kong Police Force (HKPF), and the distribution of the relevant posters and leaflets on the Campaign.

Details

2. To enhance the public awareness on cyber security and their understanding on the security threats imposed by botnets, the Cyber Security and Technology Crime Bureau (CSTCB) launched the "Cyber Security Campaign" (the Campaign) in 2017.
3. In view of the increasing popularity of mobile smart devices and their wide applications in daily life, the CSTCB kicked off the "Cyber Security Campaign – Smart Devices Security" in August 2018, which aims at educating the general public on the security threats associated with the use of smart devices and how to use the devices in a responsible manner and adopting effective defensive measures. On top of the malicious codes cleaning tools, the anti-virus software companies are providing smart device scanning tools for both Android and iOS operating systems for the public to download. For details, please visit the website of the campaign at <http://www.cybersecuritycampaign.com.hk>.
4. Relevant posters and leaflets will be distributed to schools for promotion of the Campaign. School Heads are requested to complete the collection form enclosed and make arrangement to collect the posters and leaflets at the respective Regional Education Offices from **2 October to 2 November 2018**. The softcopies of the posters and leaflets have also been uploaded to the above website.

Enquiry

5. For enquiries on collection of posters and leaflets, please contact the respective Regional Education Offices. For enquiries on the Campaign, please contact Mr Alan CHUNG, Sergeant of Police at 2860 2569 or email cybersecuritycampaign@police.gov.hk.

Dr W C HO
for Secretary for Education

c.c. Heads of Sections – for information

<https://www.cybersecuritycampaign.com.hk/>

CYBER SECURITY CAMPAIGN

Is Your Smart Phone Safe?

Be a Smart Netizen

Be Prudent With Your Smart Devices

Hong Kong Police Force
www.police.gov.hk

Cyber Security Campaign
www.cybersecuritycampaign.com.hk

Supporting Organisation:

- Bitdefender
- eset
- KASPERSKY
- Microsoft
- Symantec
- TREND
- 珠海學院 CHU HAI COLLEGE
- 港電 HK Electric
- HKT
- IVE
- PCCW
- Singtel
- 香港中文大學 The Chinese University of Hong Kong
- 香港中文大學電腦科學系 Department of Computer Science

Thank you