

Information Security in Schools— Recommended Practice (September 2019)

IT in Education Section
Education Bureau
25 September 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 (last updated version issued in January 2019).
- Under the principle of school-based management, schools are responsible for taking appropriate IT security measures to protect the IT systems and data of their schools, and they may determine their own requirements to adopt the practice where applicable to their own environment and operational needs.
- Schools could adopt different technical solutions.

School satisfaction of current IT security situation



89.2%

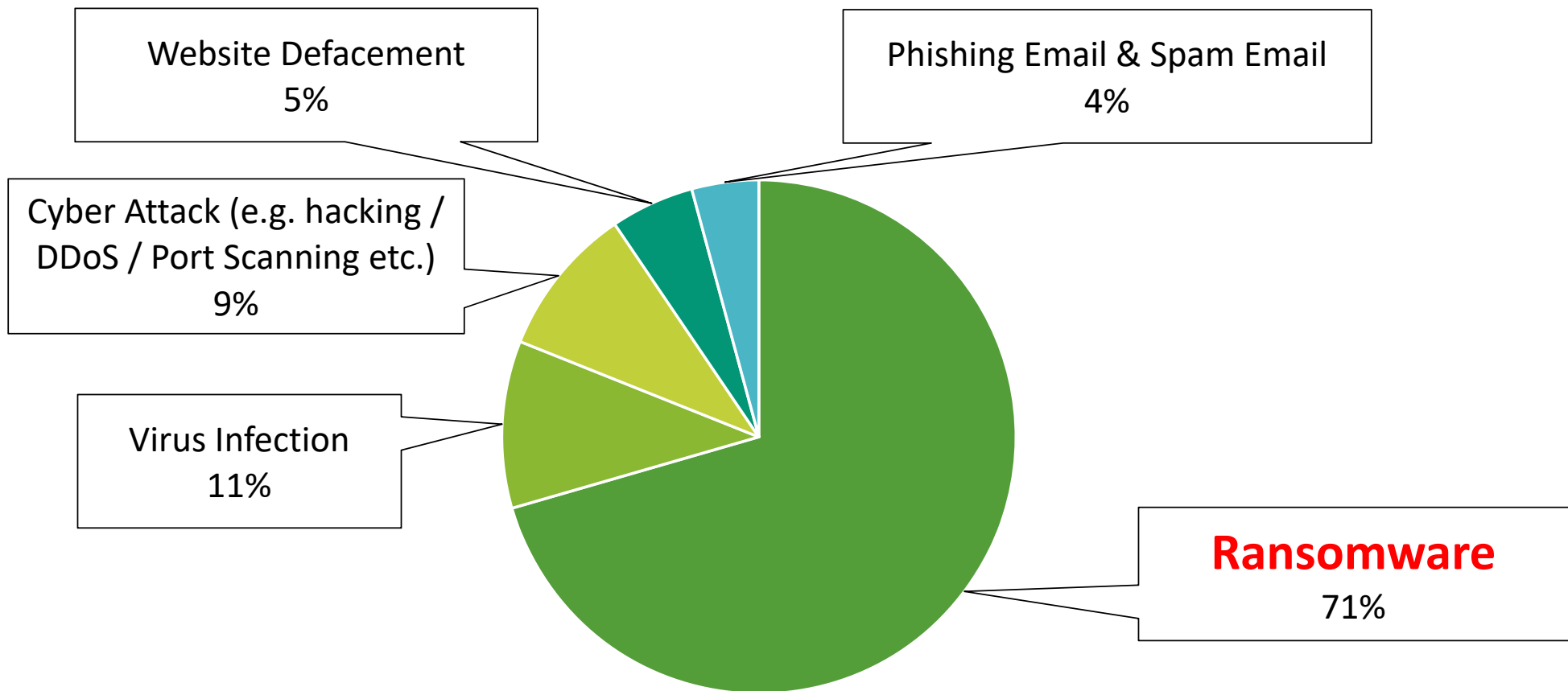


10.8%

Suggested improvement by schools:

- (a) ↑ Network security e.g. firewall setting and update
- (b) ↑ Cloud backup
- (c) ↑ Data privacy
- (d) ↑ Teachers and students consciousness on IT security
- (e) ↑ Technical support on IT security

Security Threats in Schools



Source: ITE Annual Survey 2018/19 School Year

Information Security in Schools – Recommended Practice (September 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>



Introduction

This document is written for schools' reference in protecting their information and IT assets when implementing e-learning. Schools are responsible for taking 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 and adopt the practices 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 Chapter 12 "Resources of Reference on IT Security" 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	Network and Communication Security
Chapter 8	Website & Web Application Security
Chapter 9	Mobile Device and Mobile Application Protection
Chapter 10	Malware Protection
Chapter 11	Cloud Service
Chapter 12	Resources of Reference on IT Security

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	NETWORK AND COMMUNICATION SECURITY
CHAPTER 8	WEBSITE AND WEB APPLICATION SECURITY
CHAPTER 9	MOBILE DEVICE AND MOBILE APPLICATION PROTECTION
CHAPTER 10	MALWARE PROTECTION
CHAPTER 11	CLOUD SERVICE
CHAPTER 12	RESOURCES OF REFERENCE ON IT SECURITY

Information Security in Schools
Recommended Practice

Education Bureau
The Government of the HKSAR

Revised in September 2019

Major Updates

2019 January 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 AND 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

2019 September Version

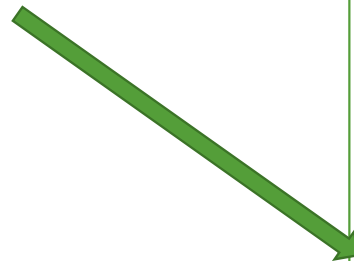
CHAPTER 1 ABOUT THIS DOCUMENT
CHAPTER 2 SECURITY MANAGEMENT (Updated)
CHAPTER 3 SECURITY INCIDENT HANDLING (Updated)
CHAPTER 4 PHYSICAL SECURITY (Updated)
CHAPTER 5 ACCESS CONTROL (Updated)
CHAPTER 6 DATA SECURITY (Updated)
CHAPTER 7 NETWORK AND COMMUNICATION SECURITY
CHAPTER 8 WEBSITE AND WEB APPLICATION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

*Those chapters/items highlighted in green are with substantial revisions.

Major Updates – Chapter 2 SECURITY MANAGEMENT

2019 January Version

- Information Security Objectives
- Security Policy
- Security Personnel
- IT Security Functions



2019 September Version

- Introduction to Information Security
- Security Management Cycle
- Assessing Security Risks
- Implementing and Maintaining a Secure Framework
 - *Set up and Implement a Security Policy*
 - *Set up and Implement Management and Administrative Processes*
 - *Select and Implement Technological Measures*
- Monitoring and Recording
- Reviewing and Improving
 - *Security assessment*
 - *Security audit*

Major Updates – Chapter 2

SECURITY MANAGEMENT

- Introduction to Information Security
- Security Management Cycle
- Assessing Security Risks
- Implementing and Maintaining a Secure Framework
- Monitoring and Recording
- Reviewing and Improving

Major Updates – Chapter 3

SECURITY INCIDENT HANDLING

2019 January Version

- Checklist
 - *Establish an IT Security Incident Response Team*
 - *Escalation procedure*
 - *Security incident response procedure*
 - *Reporting procedure*
 - *Training and education*

2019 September Version

- What is an Information Security Incident?
- Objectives of Security Incident Handling
- Steps for Security Incident Handling
- Training and Education

Major Updates – Chapter 3

SECURITY INCIDENT HANDLING

- What is an information security incident?
- Objectives of Security Incident Handling
- Steps for Security Incident Handling
- Training and Education
 - School-based policy and guidelines
 - EDB professional training programmes / seminars
e.g. Training programmes by ITE Section
<https://www.edb.gov.hk/en/edu-system/primary-secondary/applicable-to-primary-secondary/it-in-edu/pdp-ited.html>
 - EDB website / email notifications
e.g. Information Security in Schools by ITE Section
<https://www.edb.gov.hk/ited/i-security>
 - HKCERT news / notifications / alerts
 - Security reports



Major Updates – Chapter 4

PHYSICAL SECURITY

2019 January Version

- Hardware and Software Asset Protection
 - *Recommended practices for server room protection*
 - *Recommended practices to secure mobile devices*
 - *Recommended practices to handle software copies and backup device / media*
 - *Recommended practices for performing property marking and inventory taking*

2019 September Version

- **Meaning of Physical Security**
- **Site Preparation in School**
- Computer Hardware and Software Assets Protection
 - *Workstation / Computer Room Protection*
 - *Server and Network Device Protection*
 - *Mobile Device Protection*
 - *Software Copies, Storage and Backup Media*

Major Updates – Chapter 4

PHYSICAL SECURITY

- Meaning of Physical Security
- Site Preparation in School
- Computer Hardware and Software Assets Protection

Major Updates – Chapter 5

ACCESS CONTROL

2019 January Version

- Access Control
 - *Recommended practices for the authentication and authorisation to prevent unauthorised access*
 - *Recommended practices or administration of user accounts including (Third Party)*
 - *Recommended practices for performing user and access rights assignment*

2019 September Version

- **Significance of Access Control**
- Requirements of Access Control
- User Access Management
- **User Responsibilities**
- **System and Application Access Control**
- **Mobile Computing and Remote Access**



Major Updates – Chapter 5

ACCESS CONTROL

- Significance of Access Control
- Requirements of Access Control
- User Access Management
- User Responsibilities
- System and Application Access Control
- Mobile Computing and Remote Access

Major Updates – Chapter 6

DATA SECURITY

2019 January Version

- Data Security
 - *Some general data backup and recovery practices*
 - *Recommended practices for protecting sensitive data*
 - *Disposing old computer equipment or media containing non-volatile data*
 - *Personal Data (Privacy) Ordinance*

2019 September Version

- Information Classification
- Cryptography
- Backup
- Personal Data (Privacy)
- Information Erasure
- Promotion of Security Awareness of the Data Security Requirements

Major Updates – Chapter 6

DATA SECURITY

- Information Classification
- Cryptography
- Backup
- Personal Data (Privacy)
- Information Erasure
- Promotion of Security Awareness of the Data Security Requirements

Some Security Tips

- Schools should incorporate security management in the school policy.
- Schools are recommended to develop school-based security policy and assign roles and responsibilities to stakeholders. Also, the security policy should be reviewed annually.
- Schools should define school-based security incident handling procedures and disseminate to all stakeholders.
- Schools should provide training and sharing on the latest security trends to all stakeholders.
- Schools should disable the port 3389 (RDP) to prevent unauthorised attack.
- There are security vulnerability in WPA2, schools are recommended to deploy network device with WPA3 when upgrading the Wi-Fi network.

For schools adopting the Integration Mode of WiFi networks

- It is recommended to build the WiFi network completely separated from schools' existing network with separate broadband line to reduce security risk in the coming WiFi services contract renewal exercise.
- 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.

(Please refer to Section 7.2.4 of Chapter 7 for details)

IT Security Measures to address the Security Concerns on Integrating the 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

(Please refer to Section 7.2.5 of Chapter 7 for details)

Related Promotion and Support by EDB

- Webpage of Information Security in Schools

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



- Email Message on IT Security Alert



- Information Security in Schools – Recommended Practice

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

- Co-organise with professional bodies and schools to provide IT security related seminars / workshops (6 events planned for 2019/20 s.y. and this seminar will also be rerun)
- Promote IT security related events / activities through school circular memorandum
- Professional development programmes (PDP) in Information Literacy
<https://www.edb.gov.hk/il/eng>
- Grants



Overview of Various ITE Grants

Recurrent

Composite IT Grant (CITG)

\$209,367 – 720,089 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 \$317,338

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

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
- 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

<https://www.cybersecurity.hk/tc/contest-2019.php>

共建安全網絡2019
網絡攻擊花樣多
保護數據靠你我
海報設計比賽

詳情及報名方法請瀏覽：
www.cybersecurity.hk/campaign.php
2788 5617 event@hkcrt.org

截止報名日期
2019年7月16日

公開組	中學組及小學組	網上最有人氣獎
冠軍 11吋 iPad Pro (MR 256GB) (約值港幣7,500元)	冠軍 獎品 + 港幣1,500元禮券	港幣500元現金券
亞軍 Apple Watch Series 4 (約值港幣4,000元)	亞軍 獎品 + 港幣1,000元禮券	
季軍 亞馬遜 Oasis 電子書閱讀器 (約值港幣2,800元)	季軍 獎品 + 港幣500元禮券	
總獎獎 亞馬遜 Alexa Echo Plus (約值港幣1,900元)	總獎獎 港幣300元禮券	

電子組

- 冠軍 DJI Mavic Air 航拍機 (約值港幣6,300元)
- 亞軍 任天堂Switch 遊戲機套裝 (約值港幣2,800元)
- 季軍 Garmin vivoactive HR 智慧運動錶 (約值港幣2,100元)
- 總獎獎 TransSoy 人工智能即時雙內網譯機 (約值港幣1,900元)

最積極參與學校獎

- 冠軍 獎品
- 亞軍 獎品
- 季軍 獎品

主辦機構: 資訊安全網, GovCERT.HK, 香港電腦緊急應變中心
協辦機構: 香港警察, 香港電腦緊急應變中心
贊助機構: 香港電腦緊急應變中心, 香港電腦緊急應變中心
教育局: Education Bureau, Deloitte, 香港電腦緊急應變中心

Education Bureau Circular Memorandum No. 71/2019

From : Secretary for Education To : Heads of Primary and Secondary Schools
Ref : EDB(EID/ITE)/IT/PRO/189
Date : 8 April 2019

Build a Secure Cyberspace 2019
“We Together! Secure Data!” Poster Design Contest

Summary

The purpose of this circular memorandum is to inform heads of primary and secondary schools of the Build a Secure Cyberspace 2019 “We Together! Secure Data!” Poster Design Contest. All students and teachers of the schools are invited to participate in the captioned activity.

Details

2. The above contest is jointly organised by the Office of the Government Chief Information Officer (OGCIO), the Hong Kong Police Force (HKPF) and the Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) and supported by the Education Bureau. It aims at raising public awareness of cyber security and encouraging the adoption of the best practices in data protection. The deadline of submission is 15 July 2019. For details, please refer to the webpages at <https://www.cybersecurity.hk/en/contest-2019.php>.

3. Two posters in Chinese will be distributed to schools for promotion of the activity. The softcopy of the poster has also been uploaded to the above webpages.

Enquiry

4. For enquiries, please contact the HKCERT at 2788 5617 or by email (event@hkcrt.org).

Dr WC HO
for Secretary for Education

c.c. Heads of Sections – for information

Thank you