Information Security in Schools– Recommended Practice (September 2019)

IT in Education Section
Education Bureau
9 December 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

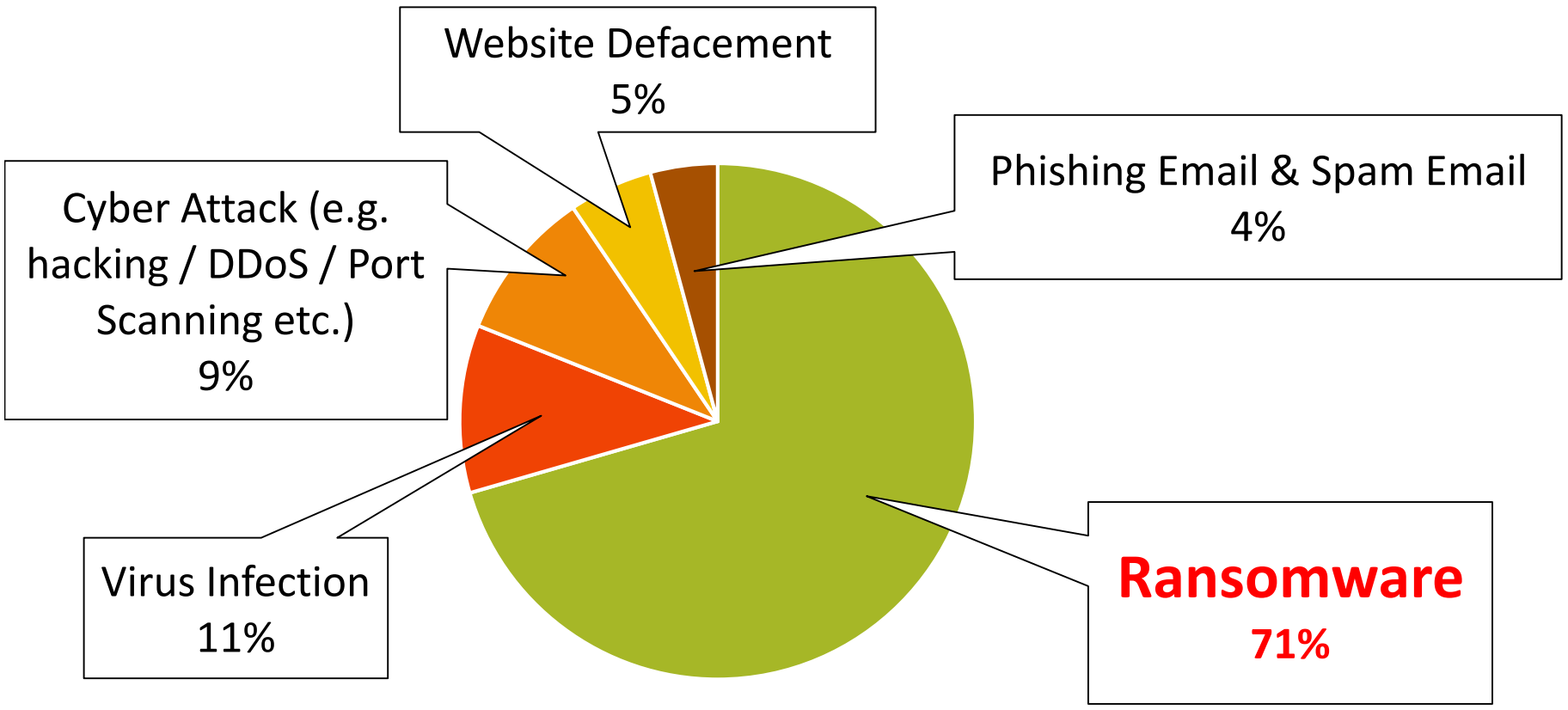
89.2%

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

Source: ITE Annual Survey 2018/19 School Year

Security Threats in Schools



Source: ITE Annual Survey 2018/19 School Year

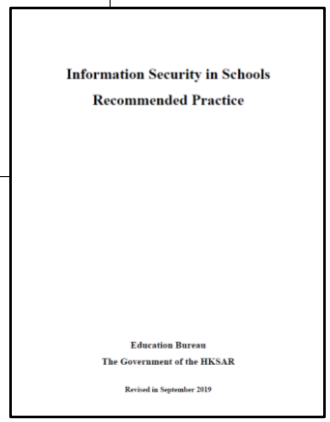
Information Security in Schools – Recommended Practice (September 2019)

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.

TABLE OF CONTENT



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.

Some Security Tips (1)

- Develop school-based security policy and assign roles and responsibilities to stakeholders. Also, the security policy should be reviewed annually.
- Define school-based security incident handling procedures and disseminate to all stakeholders.
- Provide training and sharing on the latest security trends to all stakeholders.
- Have careful site preparation of the server room or computer room and appropriate security measures should be adopted.
- Keep an updated inventory list of computer hardware facilities and software licences.
- Uninstall all programs and erase all data, if applicable, before disposing any piece of hardware.

Some Security Tips (2)

- Determine appropriate access control rules, access rights and restrictions for specific user roles on their information. Access to information should not be allowed unless authorised by the relevant information owners. The rules should be reviewed from time to time and at least annually.
- Carry out backups at regular intervals and should establish and implement backup and recovery policies for their information systems. It is advisable to store backup copies offline at a safe and secure location remote from the site of the systems.
- Disable the port 3389 (RDP) to prevent unauthorised attack.
- Deploy network device with WPA3 when upgrading the Wi-Fi network as there are security vulnerability in WPA2.
- Apply latest approved security patches to any software (especially the operating system) and avoid using the end of supported components. Ensure the hardware and software are properly maintained and patched.

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

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

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@hkcert.org).

Dr W C HO
for Secretary for Education

c.c. Heads of Sections – for information

The School Visit Programme began in 2007 as part of our commitment to promote cyber security awareness and cyber etiquette to our community. The programme was joined by our industry partners as volunteers to visit primary, secondary schools and tertiary institutions. From Sep 2007 to Oct 2019, we have held 273 school visits and relayed information security message to over 79 780 participants, including students, teachers and parents.

For details, please refer to https://www.cybersecurity.hk/en/school-visit.php

Cyber Security Information Portal
www.cybersecurity.hk

Thank you