香港電腦教育學會
The Hong Kong Association for Computer Education

# 學校網絡和網站保安漏洞及相關保安措施分享會

金偉明校長
簡偉鴻校長

# Why are schools being targeted?

- Schools are typically vulnerable and unprepared for these types of attacks
- Schools rely on technology for day-to-day operations.
- Teachers and students are increasingly bringing their own laptops, phones, and other personal devices to campus and connecting to the campus network, bringing in increased risks for cyberattacks.
- Students may be interested in carrying out these attacks.

# 近日發生的大型資安事件

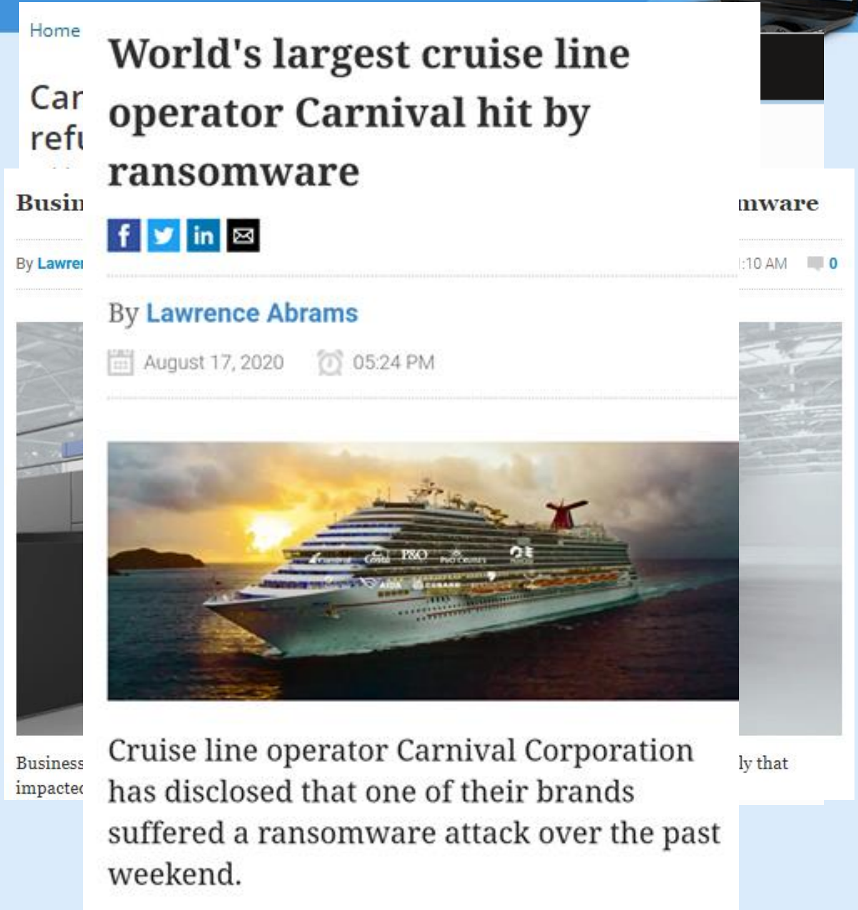
Garmin受勒索軟件攻擊致服務停頓數天

Canon 資料被盜取及加密，不願支付贖金資料被公開

Konica Minolta 被勒索軟件攻擊服務停頓

世界最大遊輪集團Carnival Cruise部份IT系統被加密、資料可能被盜

**特點: 高針對性 / 人手操作的長時間攻擊**



## World's largest cruise line operator Carnival hit by ransomware

By Lawrence Abrams

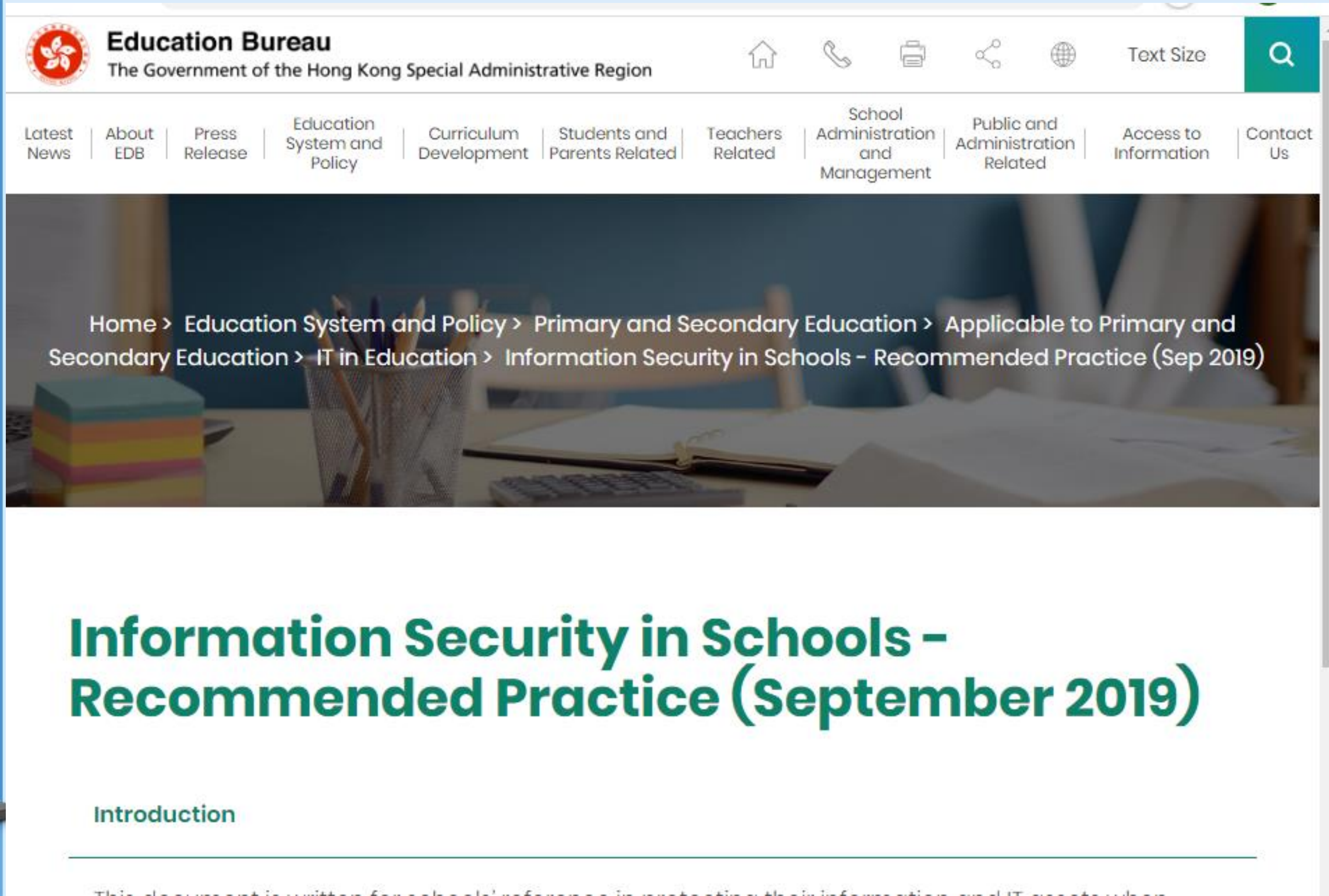
August 17, 2020 05:24 PM

Cruise line operator Carnival Corporation has disclosed that one of their brands suffered a ransomware attack over the past weekend.

# Cybersecurity incidents can lead to trouble

## Here are the top outcomes to avoid:

- Unauthorized Disclosure and Theft of Student, Teacher and Parent Info
- Breaches and Hacks Affecting School Operations and Student Data
- Phishing and Credential Misuse
- Corruption of School Technology and Security Systems
- Ransomware for the Purposes of Extortion


Education Bureau
The Government of the Hong Kong Special Administrative Region
Text Size
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 Education > Applicable to Primary and Secondary Education > IT in Education > Information Security in Schools - Recommended Practice (Sep 2019)

# Information Security in Schools - Recommended Practice (September 2019)

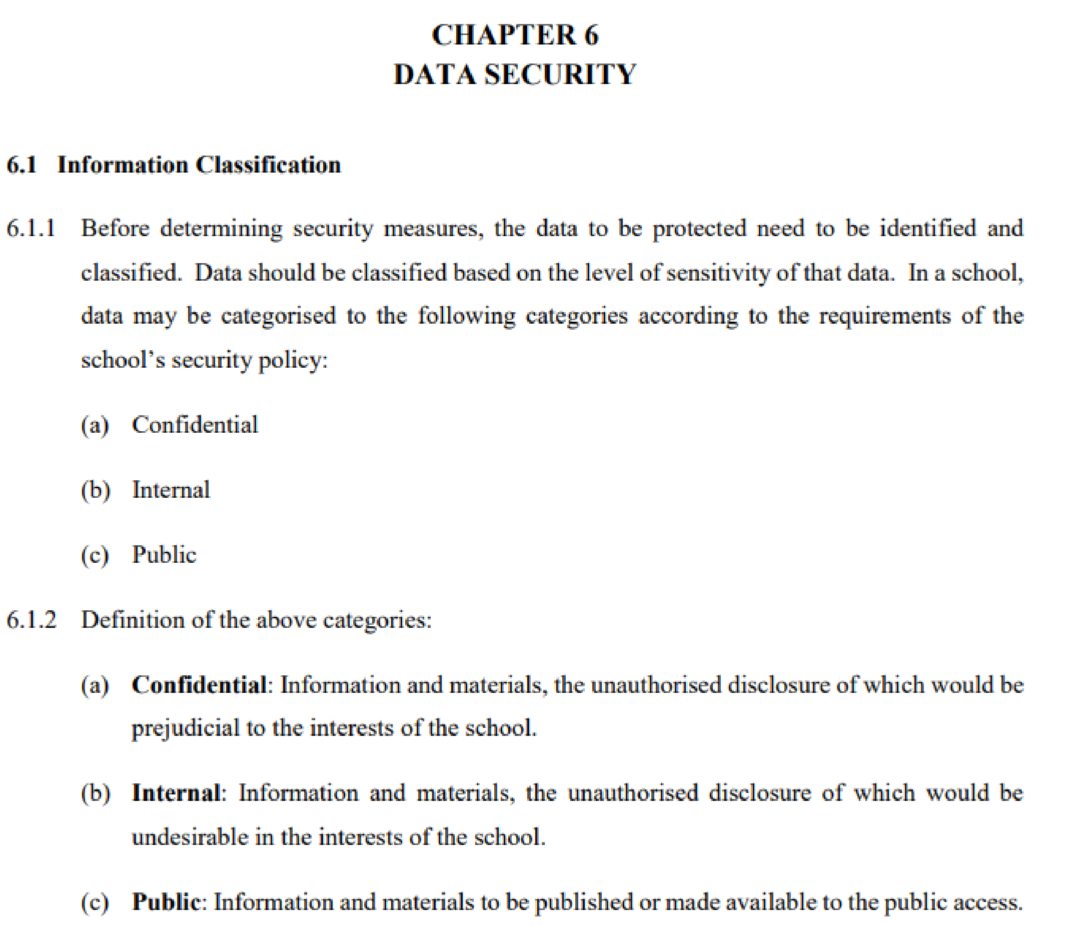
## Introduction

This document is written for schools' reference in protecting their information and IT assets when

# Information Security in Schools - Recommended Practice (September 2019)

| | |
|---|---|
| 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 |

# Chapter 6 Data Security



## CHAPTER 6
## DATA SECURITY

### 6.1 Information Classification

6.1.1 Before determining security measures, the data to be protected need to be identified and classified. Data should be classified based on the level of sensitivity of that data. In a school, data may be categorised to the following categories according to the requirements of the school's security policy:

(a) Confidential

(b) Internal

(c) Public

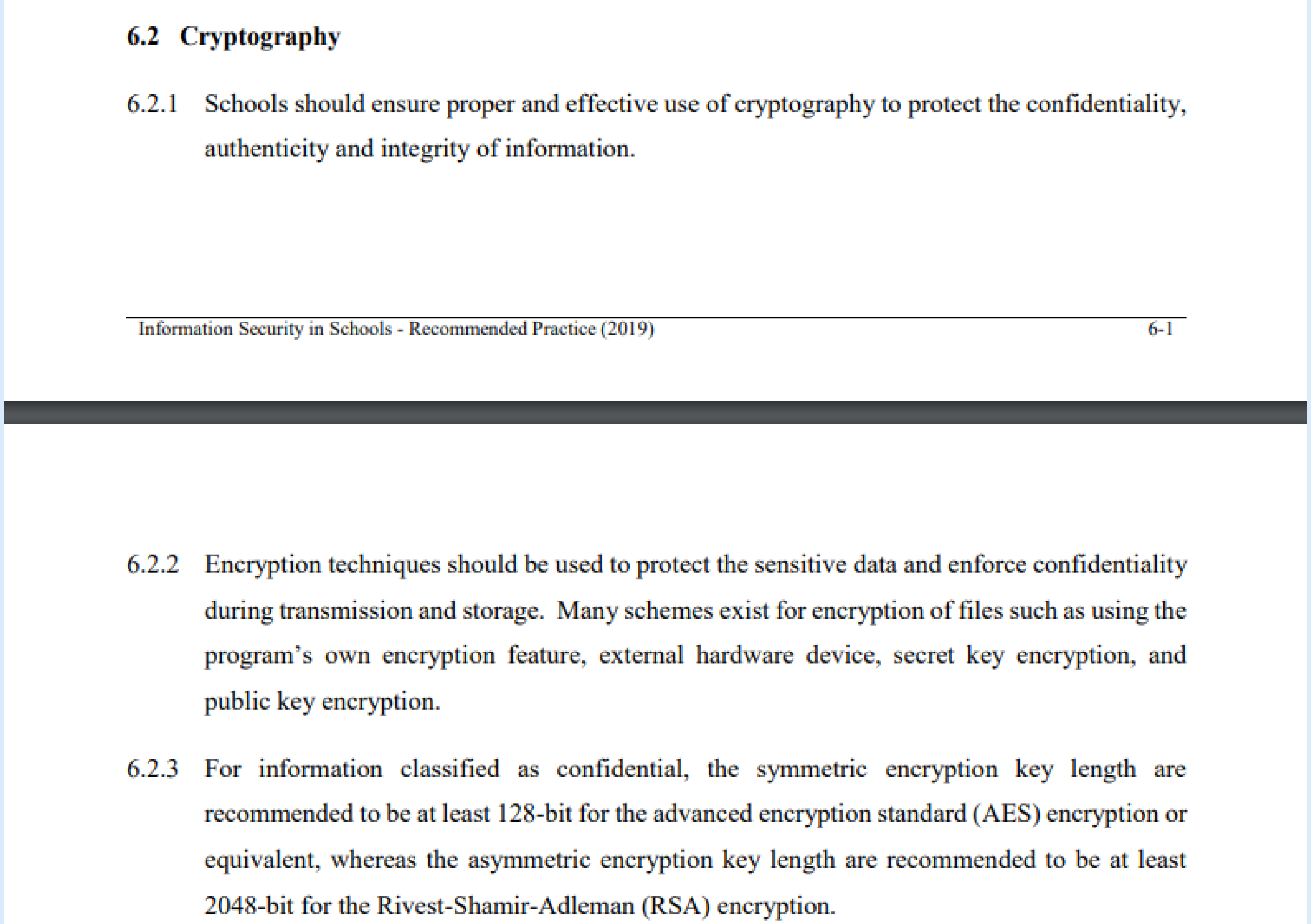
6.1.2 Definition of the above categories:

(a) **Confidential**: Information and materials, the unauthorised disclosure of which would be prejudicial to the interests of the school.

(b) **Internal**: Information and materials, the unauthorised disclosure of which would be undesirable in the interests of the school.

(c) **Public**: Information and materials to be published or made available to the public access.

# Chapter 6 Data Security



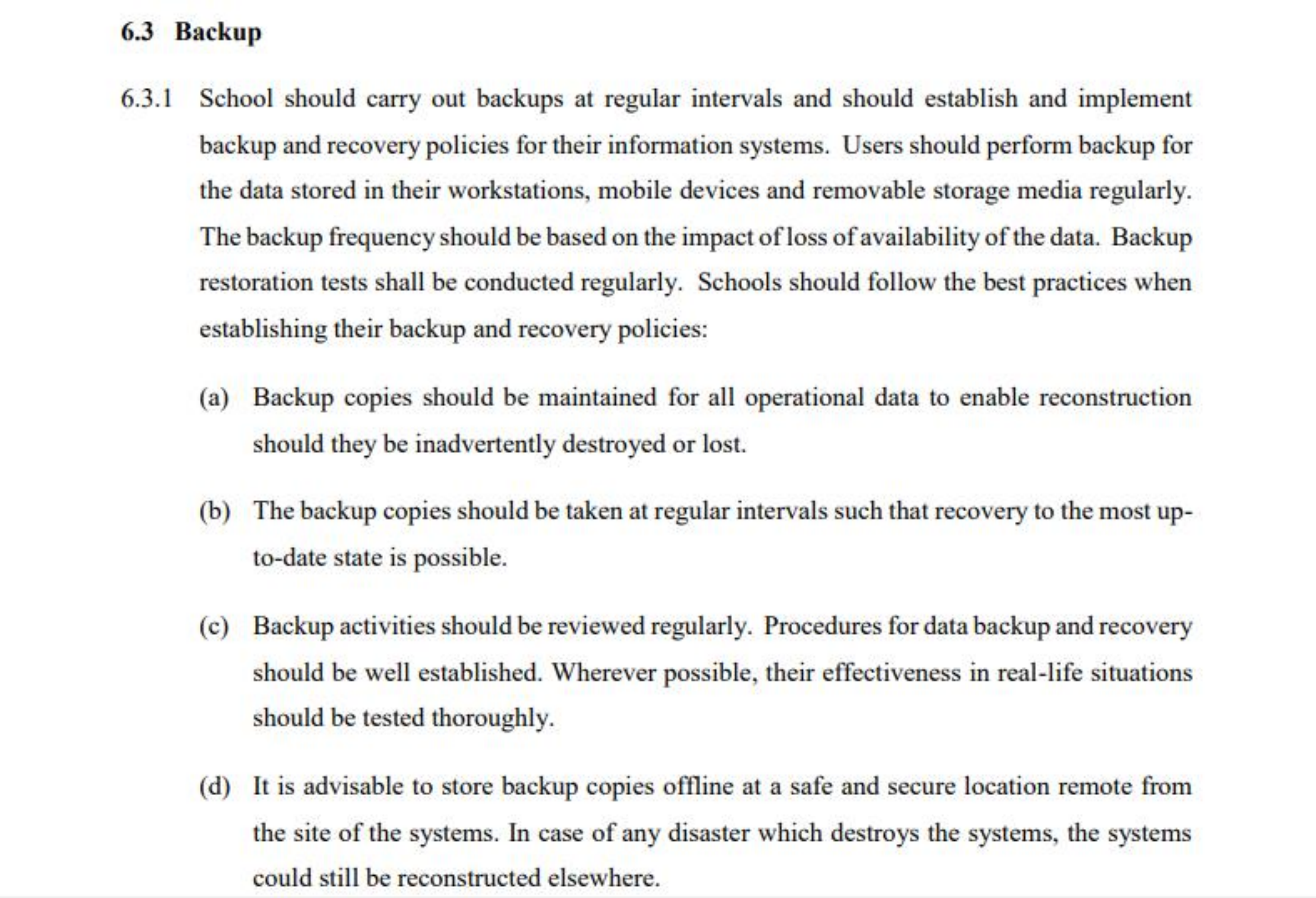
## 6.2 Cryptography

6.2.1 Schools should ensure proper and effective use of cryptography to protect the confidentiality, authenticity and integrity of information.

6.2.2 Encryption techniques should be used to protect the sensitive data and enforce confidentiality during transmission and storage. Many schemes exist for encryption of files such as using the program's own encryption feature, external hardware device, secret key encryption, and public key encryption.

6.2.3 For information classified as confidential, the symmetric encryption key length are recommended to be at least 128-bit for the advanced encryption standard (AES) encryption or equivalent, whereas the asymmetric encryption key length are recommended to be at least 2048-bit for the Rivest-Shamir-Adleman (RSA) encryption.

# Chapter 6 Data Security



### 6.3 Backup

6.3.1 School should carry out backups at regular intervals and should establish and implement backup and recovery policies for their information systems. Users should perform backup for the data stored in their workstations, mobile devices and removable storage media regularly. The backup frequency should be based on the impact of loss of availability of the data. Backup restoration tests shall be conducted regularly. Schools should follow the best practices when establishing their backup and recovery policies:

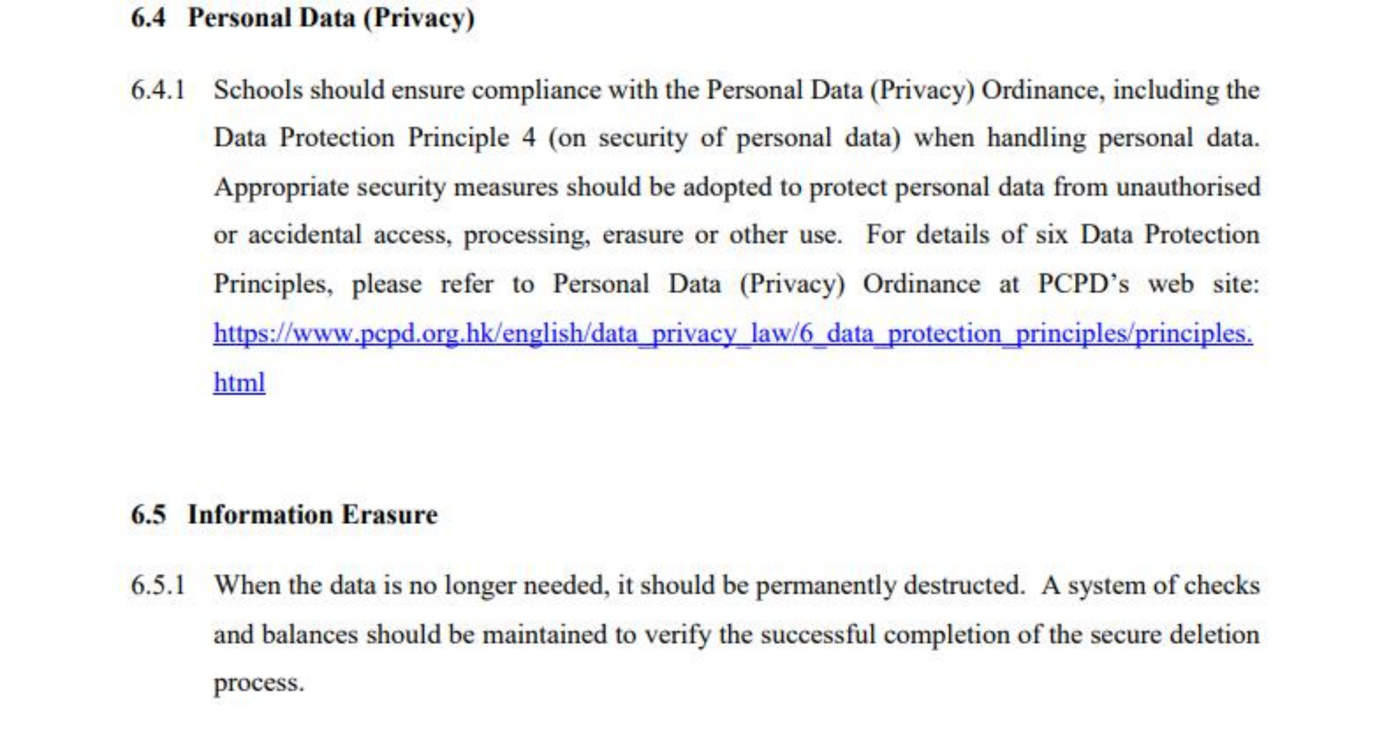
(a) Backup copies should be maintained for all operational data to enable reconstruction should they be inadvertently destroyed or lost.

(b) The backup copies should be taken at regular intervals such that recovery to the most up-to-date state is possible.

(c) Backup activities should be reviewed regularly. Procedures for data backup and recovery should be well established. Wherever possible, their effectiveness in real-life situations should be tested thoroughly.

(d) It is advisable to store backup copies offline at a safe and secure location remote from the site of the systems. In case of any disaster which destroys the systems, the systems could still be reconstructed elsewhere.

# Chapter 6 Data Security



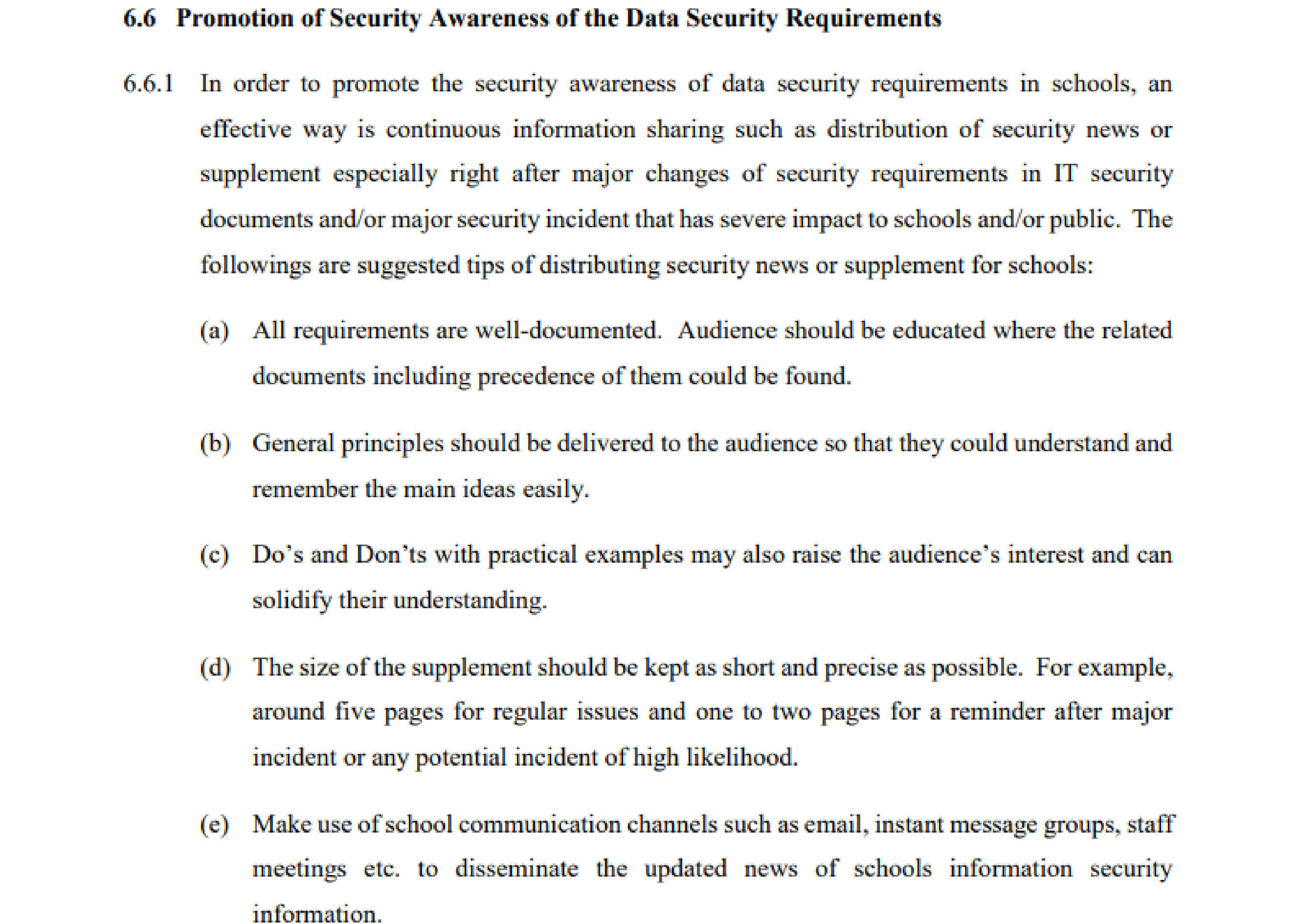
### 6.4 Personal Data (Privacy)

6.4.1 Schools should ensure compliance with the Personal Data (Privacy) Ordinance, including the Data Protection Principle 4 (on security of personal data) when handling personal data. Appropriate security measures should be adopted to protect personal data from unauthorised or accidental access, processing, erasure or other use. For details of six Data Protection Principles, please refer to Personal Data (Privacy) Ordinance at PCPD's web site: https://www.pcpd.org.hk/english/data_privacy_law/6_data_protection_principles/principles.html

### 6.5 Information Erasure

6.5.1 When the data is no longer needed, it should be permanently destructed. A system of checks and balances should be maintained to verify the successful completion of the secure deletion process.

# Chapter 6 Data Security



### 6.6 Promotion of Security Awareness of the Data Security Requirements

6.6.1 In order to promote the security awareness of data security requirements in schools, an effective way is continuous information sharing such as distribution of security news or supplement especially right after major changes of security requirements in IT security documents and/or major security incident that has severe impact to schools and/or public. The followings are suggested tips of distributing security news or supplement for schools:

(a) All requirements are well-documented. Audience should be educated where the related documents including precedence of them could be found.

(b) General principles should be delivered to the audience so that they could understand and remember the main ideas easily.

(c) Do’s and Don’ts with practical examples may also raise the audience’s interest and can solidify their understanding.

(d) The size of the supplement should be kept as short and precise as possible. For example, around five pages for regular issues and one to two pages for a reminder after major incident or any potential incident of high likelihood.

(e) Make use of school communication channels such as email, instant message groups, staff meetings etc. to disseminate the updated news of schools information security information.

# School e-Security Checklist

- 10 steps to protect your school’s network

https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security/introduction-to-cyber-security/executive-summary

- 20 CIS Controls

https://learn.cisecurity.org/cis-controls-download

National Cyber Security Centre

# 10 Steps to Cyber Security

Defining and communicating your Board's Information Risk Regime is central to your organisation's overall cyber security strategy. The National Cyber Security Centre recommends you review this regime – together with the nine associated security areas described below, in order to protect your business against the majority of cyber attacks.

## Network Security

Protect your networks from attack. Defend the network perimeter, filter out unauthorised access and malicious content. Monitor and test security controls.

## User education and awareness

Produce user security policies covering acceptable and secure use of your systems. Include in staff training. Maintain awareness of cyber risks.

## Malware prevention

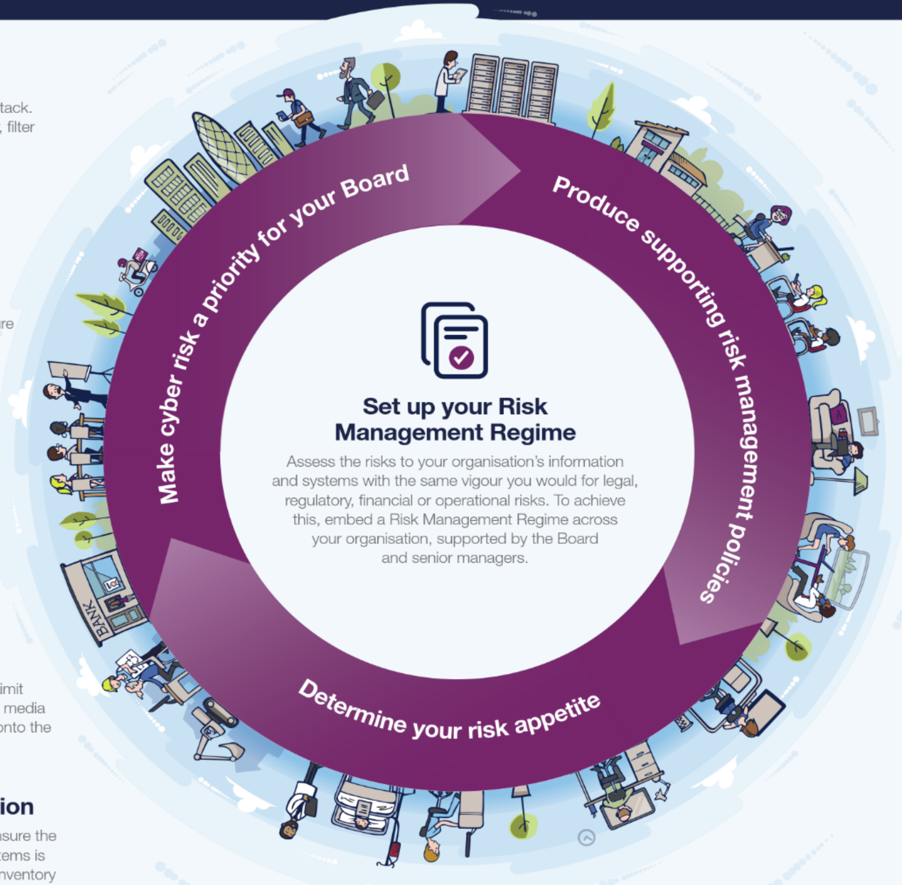
Produce relevant policies and establish anti-malware defences across your organisation.

## Removable media controls

Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing onto the corporate system.

## Secure configuration

Apply security patches and ensure the secure configuration of all systems is maintained. Create a system inventory and define a baseline build for all devices.



Make cyber risk a priority for your Board

Produce supporting risk management policies

Determine your risk appetite

## Set up your Risk Management Regime

Assess the risks to your organisation's information and systems with the same vigour you would for legal, regulatory, financial or operational risks. To achieve this, embed a Risk Management Regime across your organisation, supported by the Board and senior managers.

## Managing user privileges

Establish effective management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.

## Incident management

Establish an incident response and disaster recovery capability. Test your incident management plans. Provide specialist training. Report criminal incidents to law enforcement.

## Monitoring

Establish a monitoring strategy and produce supporting policies. Continuously monitor all systems and networks. Analyse logs for unusual activity that could indicate an attack.

## Home and mobile working

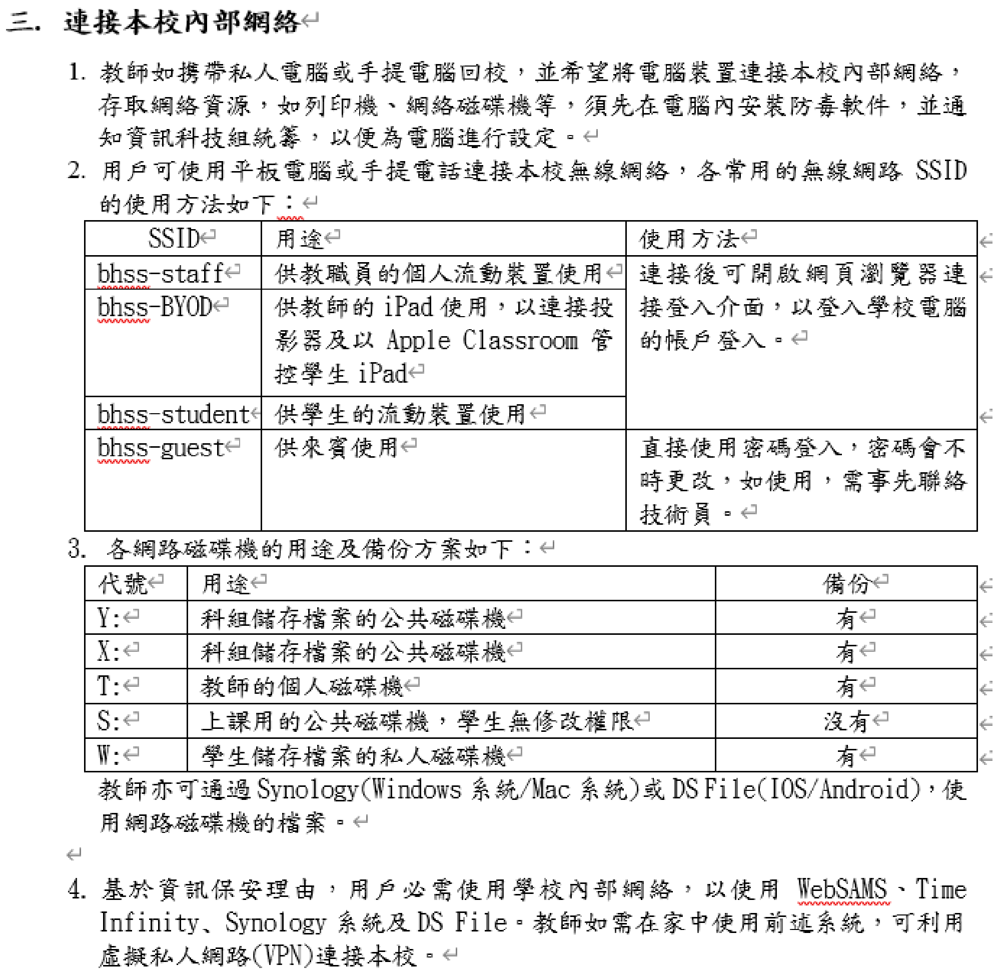
Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline and build to all devices. Protect data both in transit and at rest.

For more information go to 🖳 www.ncsc.gov.uk @ncsc

# CIS Essential Cybersecurity Practices

1 – Inventory and Control of Hardware Assets
2 – Inventory and Control of Software Assets
3 – Continuous Vulnerability Management
4 – Controlled Use of Administrative Privileges
5 – Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
6 – Maintenance, Monitoring, and Analysis of Audit Logs
7 – Email and Web Browser Protections
8 – Malware Defenses
9 – Limitation and Control of Network Ports, Protocols, and Services
10 – Data Recovery Capabilities
11 – Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches
12 – Boundary Defense
13 – Data Protection
14 – Controlled Access Based on the Need to Know
15 – Wireless Access Control
16 – Account Monitoring and Control
17 – Implement a Security Awareness and Training Program
18 – Application Software Security
19 – Incident Response and Management
20 – Penetration Tests and Red Team Exercises

# School Cyber Security Policies



## 三. 連接本校內部網絡

1. 教師如携帶私人電腦或手提電腦回校，並希望將電腦裝置連接本校內部網絡，存取網絡資源，如列印機、網絡磁碟機等，須先在電腦內安裝防毒軟件，並通知資訊科技組統籌，以便為電腦進行設定。
2. 用戶可使用平板電腦或手提電話連接本校無線網絡，各常用的無線網路 SSID 的使用方法如下：

| SSID | 用途 | 使用方法 |
|---|---|---|
| bhss-staff | 供教職員的個人流動裝置使用 | 連接後可開啟網頁瀏覽器連接登入介面，以登入學校電腦的帳戶登入。 |
| bhss-BYOD | 供教師的 iPad 使用，以連接投影器及以 Apple Classroom 管控學生 iPad | |
| bhss-student | 供學生的流動裝置使用 | |
| bhss-guest | 供來賓使用 | 直接使用密碼登入，密碼會不時更改，如使用，需事先聯絡技術員。 |

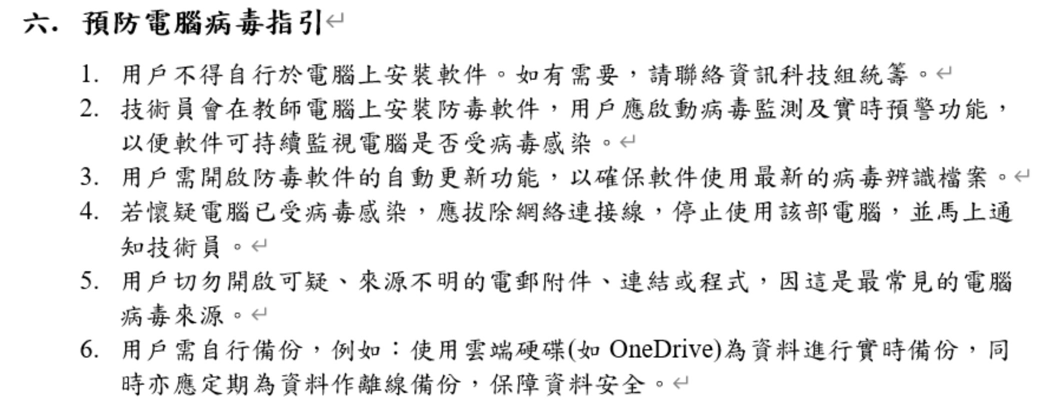
3. 各網路磁碟機的用途及備份方案如下：

| 代號 | 用途 | 備份 |
|---|---|---|
| Y: | 科組儲存檔案的公共磁碟機 | 有 |
| X: | 科組儲存檔案的公共磁碟機 | 有 |
| T: | 教師的個人磁碟機 | 有 |
| S: | 上課用的公共磁碟機，學生無修改權限 | 沒有 |
| W: | 學生儲存檔案的私人磁碟機 | 有 |

教師亦可通過 Synology(Windows 系統/Mac 系統)或 DS File(IOS/Android)，使用網路磁碟機的檔案。

4. 基於資訊保安理由，用戶必需使用學校內部網絡，以使用 WebSAMS、Time Infinity、Synology 系統及 DS File。教師如需在家中使用前述系統，可利用虛擬私人網路(VPN)連接本校。

# School Cyber Security Policies



## 六. 預防電腦病毒指引

1. 用戶不得自行於電腦上安裝軟件。如有需要，請聯絡資訊科技組統籌。
2. 技術員會在教師電腦上安裝防毒軟件，用戶應啟動病毒監測及實時預警功能，以便軟件可持續監視電腦是否受病毒感染。
3. 用戶需開啟防毒軟件的自動更新功能，以確保軟件使用最新的病毒辨識檔案。
4. 若懷疑電腦已受病毒感染，應拔除網絡連接線，停止使用該部電腦，並馬上通知技術員。
5. 用戶切勿開啟可疑、來源不明的電郵附件、連結或程式，因這是最常見的電腦病毒來源。
6. 用戶需自行備份，例如：使用雲端硬碟(如 OneDrive)為資料進行實時備份，同時亦應定期為資料作離線備份，保障資料安全。

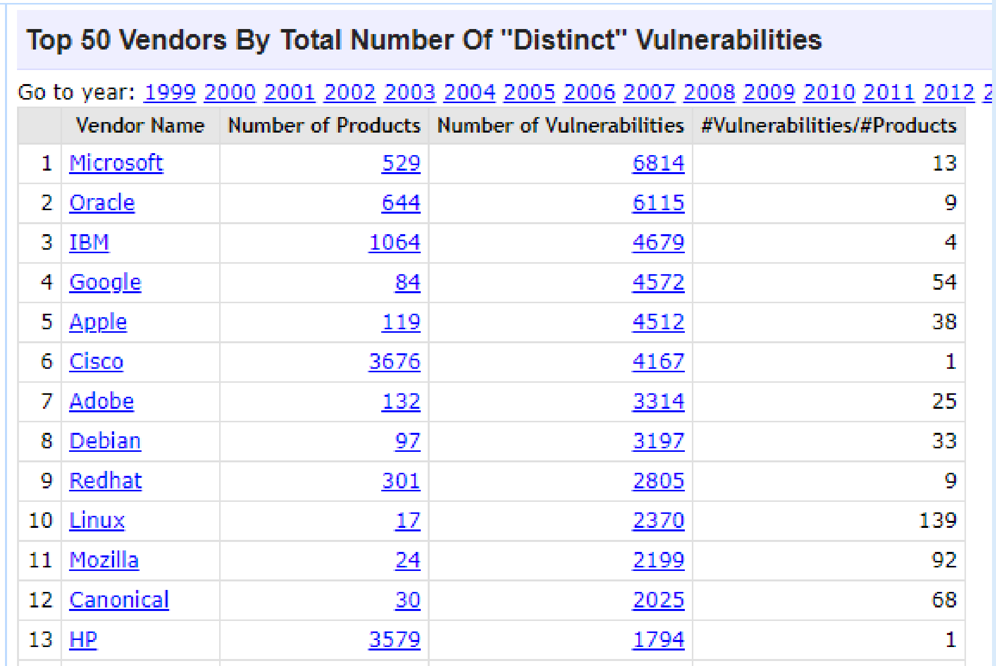
# Patch Management

*只安裝防毒軟件並不足夠 – 黑客採用高針對性、人手操作的精密攻擊*

## 事件共通點

- 應用程式安全漏洞 (Vulnerabilities)
- 帳戶被盜 取得管理員權限

學校使用的作業系統、應用程式如Microsoft Windows、Office、Adobe等每年釋出大量安全更新堵塞安全漏洞，學校有及時安裝嗎？



### Top 50 Vendors By Total Number Of "Distinct" Vulnerabilities

Go to year: 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2

| | Vendor Name | Number of Products | Number of Vulnerabilities | #Vulnerabilities/#Products |
|---|---|---|---|---|
| 1 | Microsoft | 529 | 6814 | 13 |
| 2 | Oracle | 644 | 6115 | 9 |
| 3 | IBM | 1064 | 4679 | 4 |
| 4 | Google | 84 | 4572 | 54 |
| 5 | Apple | 119 | 4512 | 38 |
| 6 | Cisco | 3676 | 4167 | 1 |
| 7 | Adobe | 132 | 3314 | 25 |
| 8 | Debian | 97 | 3197 | 33 |
| 9 | Redhat | 301 | 2805 | 9 |
| 10 | Linux | 17 | 2370 | 139 |
| 11 | Mozilla | 24 | 2199 | 92 |
| 12 | Canonical | 30 | 2025 | 68 |
| 13 | HP | 3579 | 1794 | 1 |

# Patch Management

✓ 定時為全校電腦安裝安全更新 (Patch)

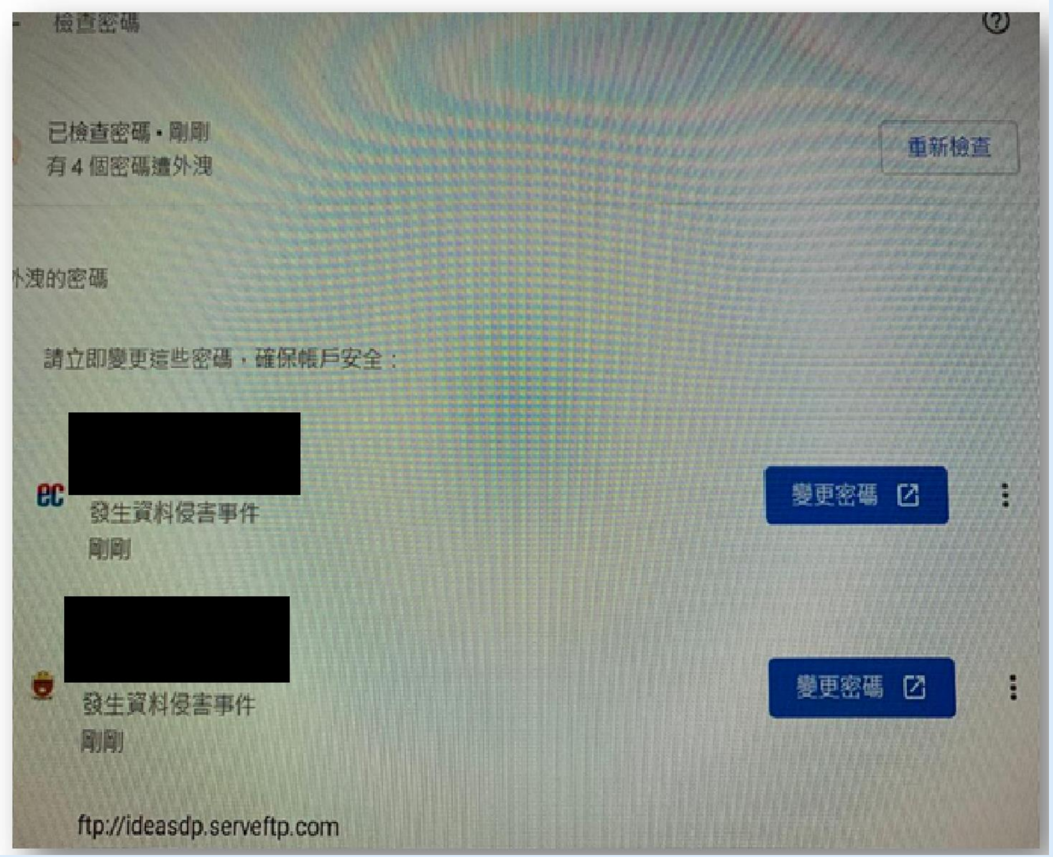
學校電腦數量多，人手安裝更新需時

市場上Patch Management軟件可協助進行安全更新

如Microsoft SCCM、Kaspersky Patch Management等

可自動下載、測試及自動為網絡內電腦安裝作業系統及應用程式的更新

# Password Setting



檢查密碼

已檢查密碼 • 剛剛
有 4 個密碼遭外洩

外洩的密碼

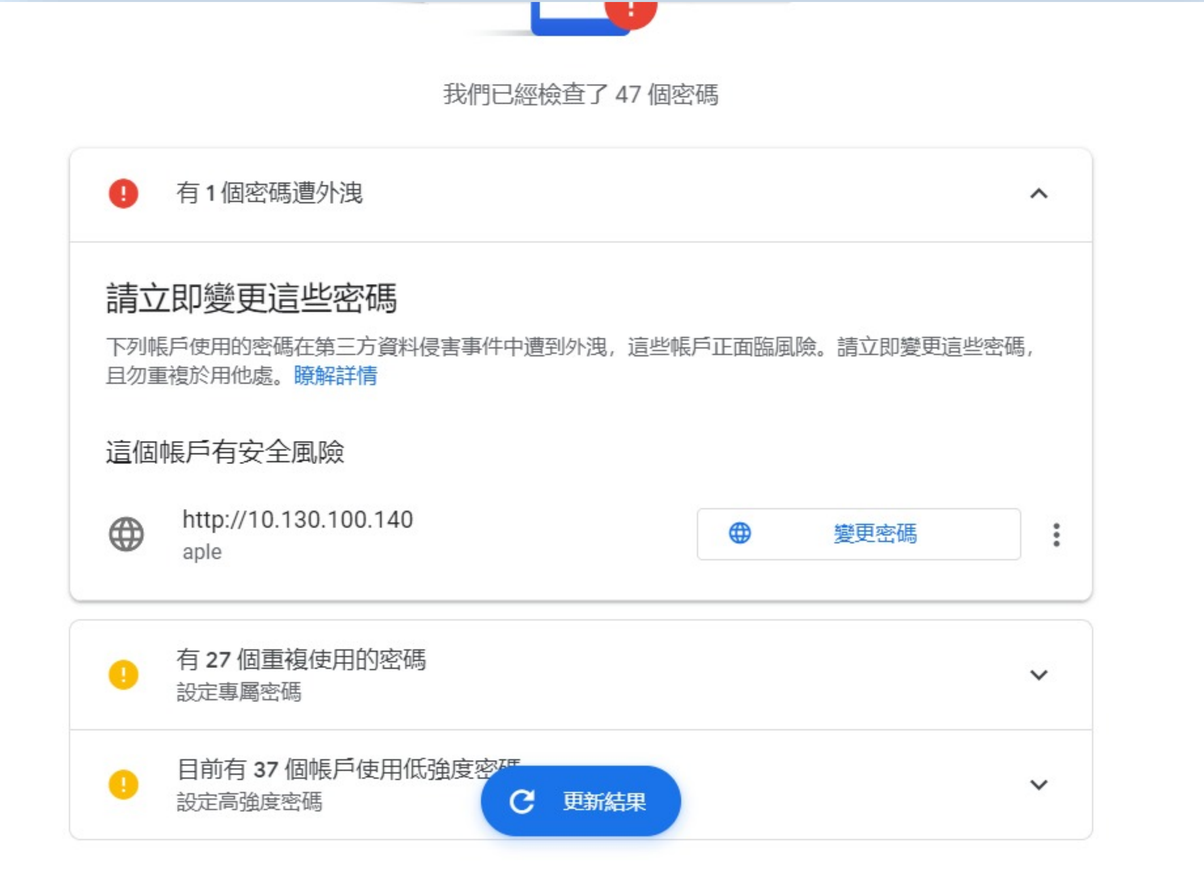
請立即變更這些密碼，確保帳戶安全：

[redacted]
發生資料侵害事件
剛剛

[redacted]
發生資料侵害事件
剛剛

ftp://ideasdp.serveftp.com

# Password Setting



我們已經檢查了 47 個密碼

有 1 個密碼遭外洩

## 請立即變更這些密碼

下列帳戶使用的密碼在第三方資料侵害事件中遭到外洩，這些帳戶正面臨風險。請立即變更這些密碼，且勿重複於用他處。瞭解詳情

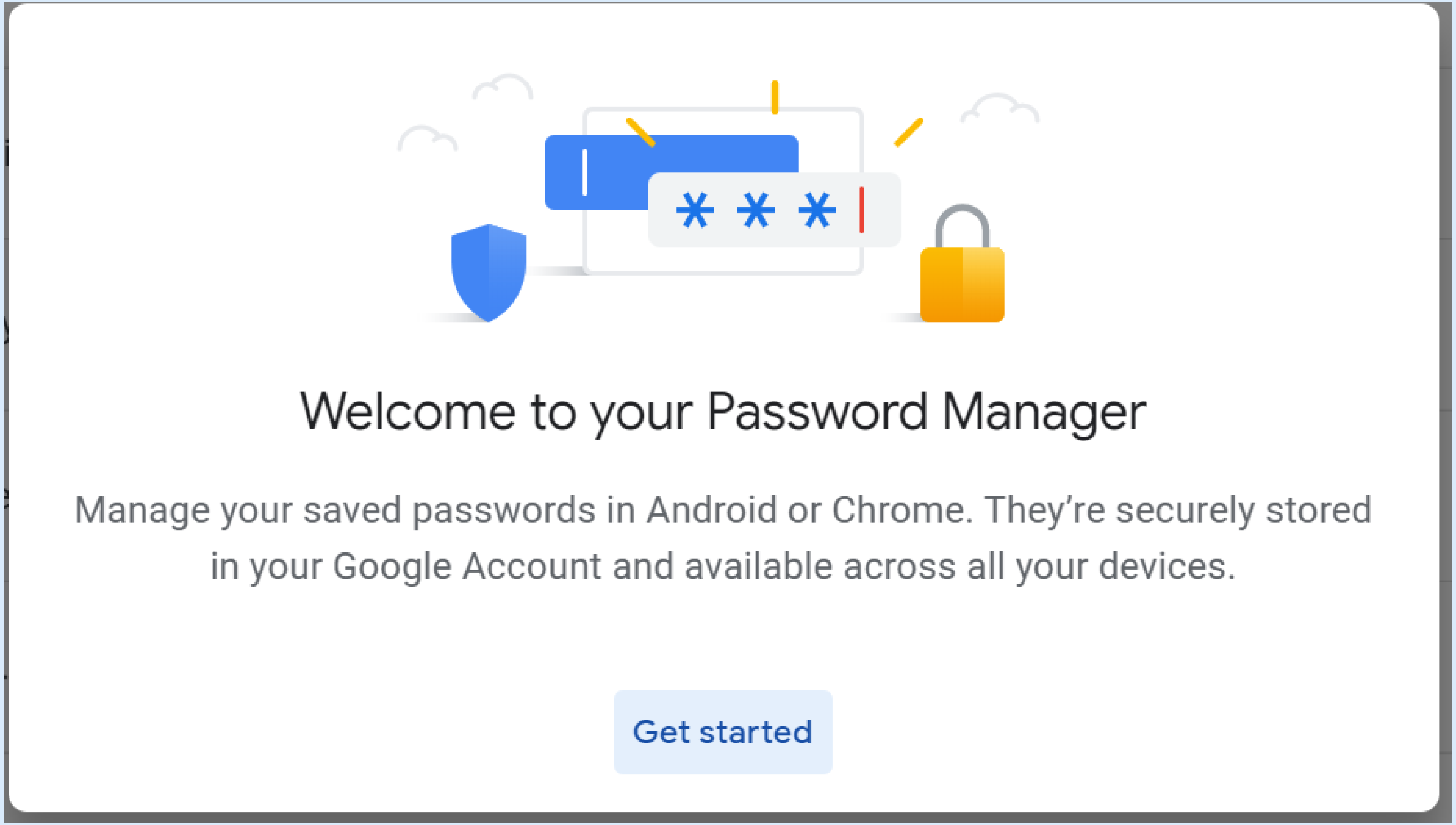
這個帳戶有安全風險

http://10.130.100.140
aple

有 27 個重複使用的密碼
設定專屬密碼

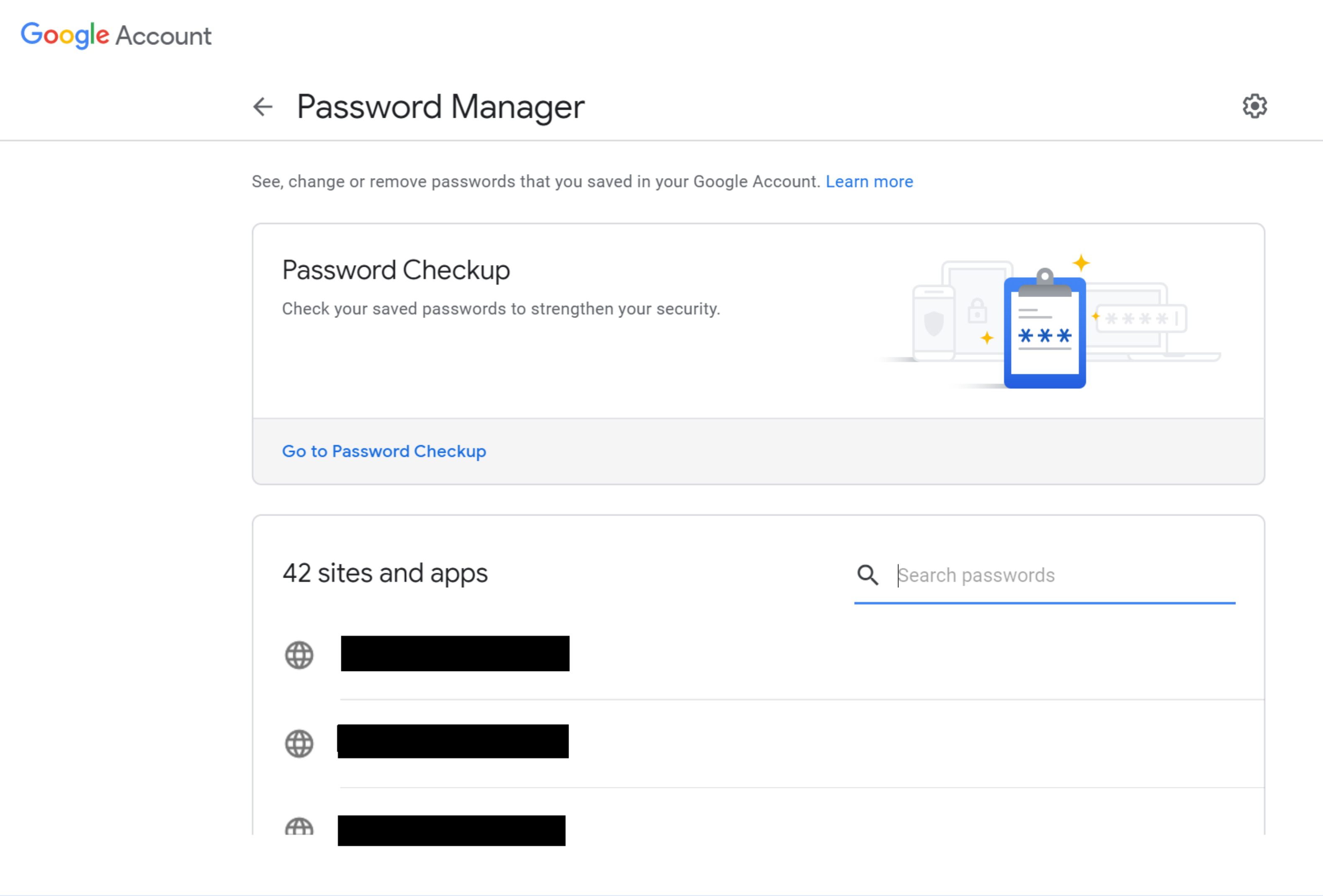
目前有 37 個帳戶使用低強度密碼
設定高強度密碼

# https://passwords.google.com/



Welcome to your Password Manager

Manage your saved passwords in Android or Chrome. They’re securely stored in your Google Account and available across all your devices.



Google Account

## Password Manager

See, change or remove passwords that you saved in your Google Account. Learn more

### Password Checkup

Check your saved passwords to strengthen your security.

Go to Password Checkup

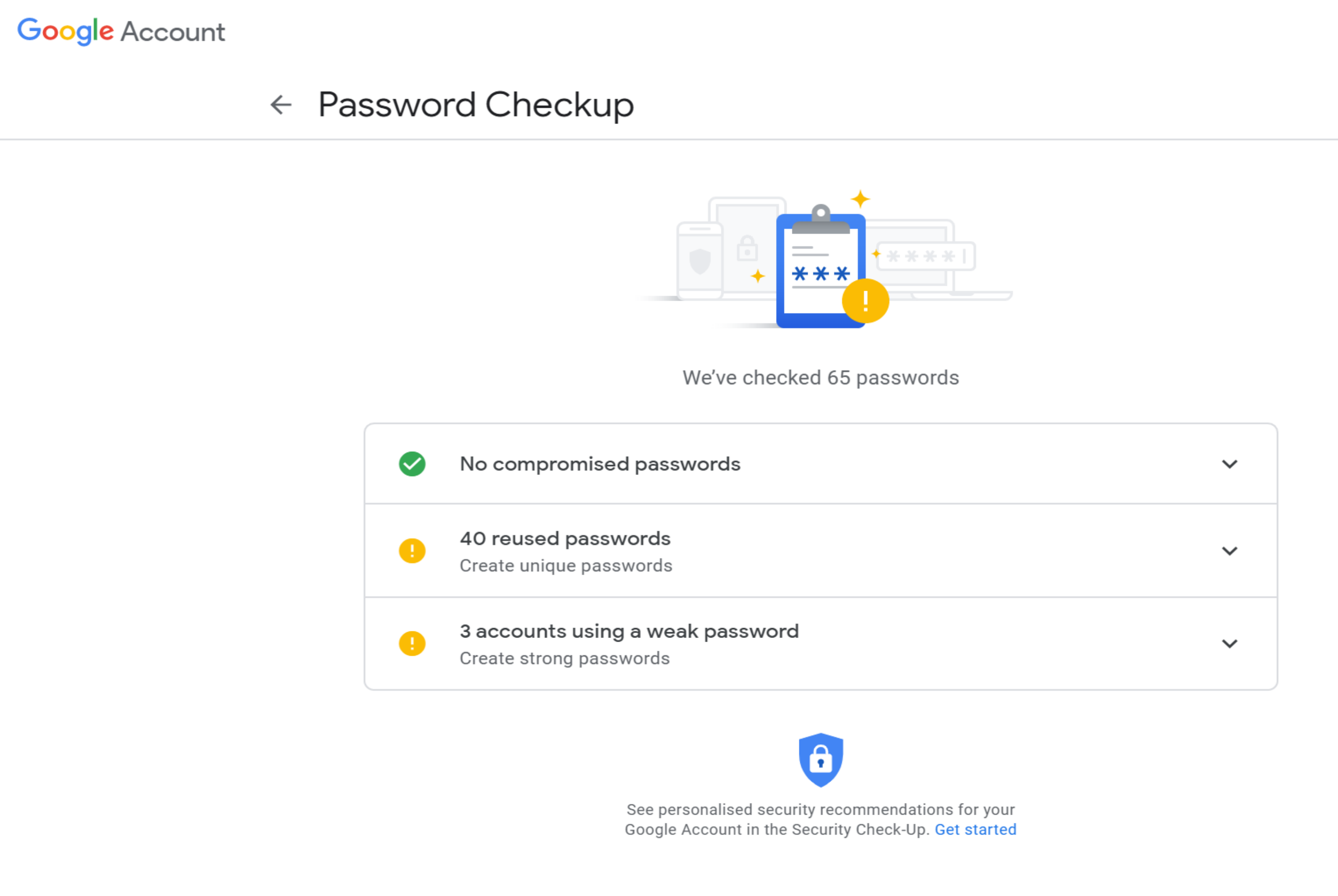
### 42 sites and apps

Search passwords

[redacted]

[redacted]

[redacted]



Google Account

Password Checkup

We've checked 65 passwords

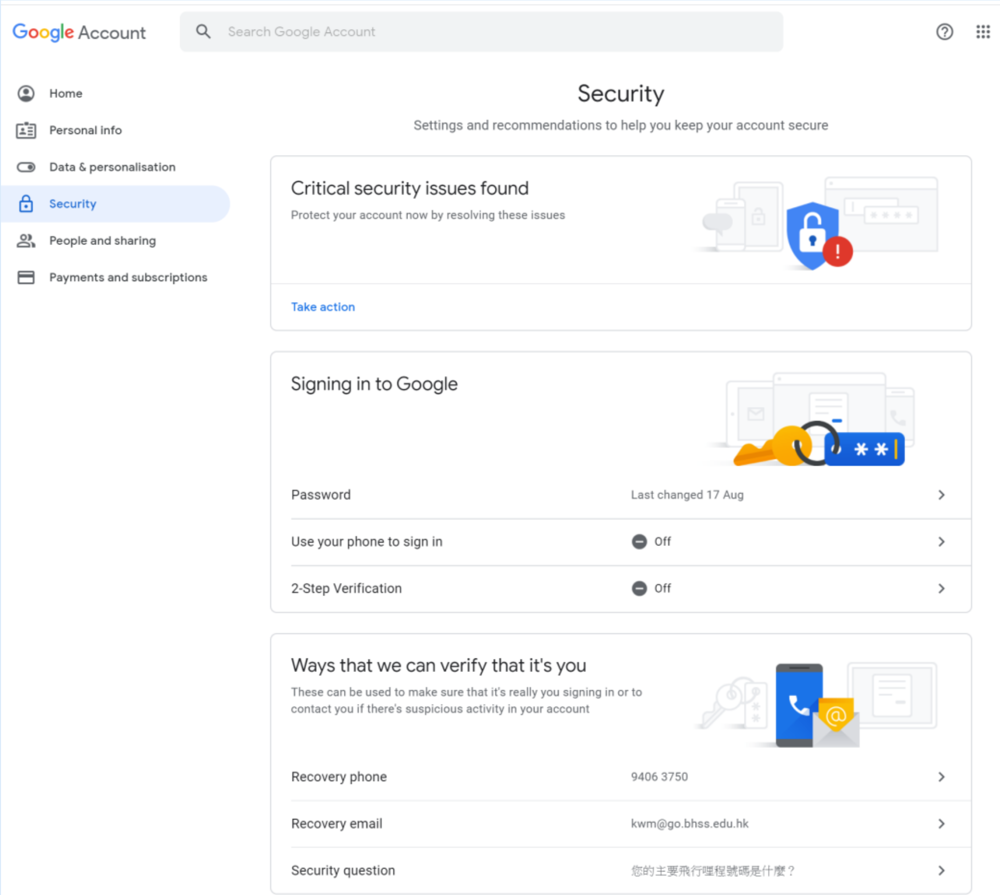
✓ No compromised passwords

! 40 reused passwords
Create unique passwords

! 3 accounts using a weak password
Create strong passwords

See personalised security recommendations for your Google Account in the Security Check-Up. Get started

# Two Steps Authentication



## Security

Settings and recommendations to help you keep your account secure

### Critical security issues found

Protect your account now by resolving these issues

Take action

### Signing in to Google

| | |
|---|---|
| Password | Last changed 17 Aug |
| Use your phone to sign in | Off |
| 2-Step Verification | Off |

### Ways that we can verify that it's you

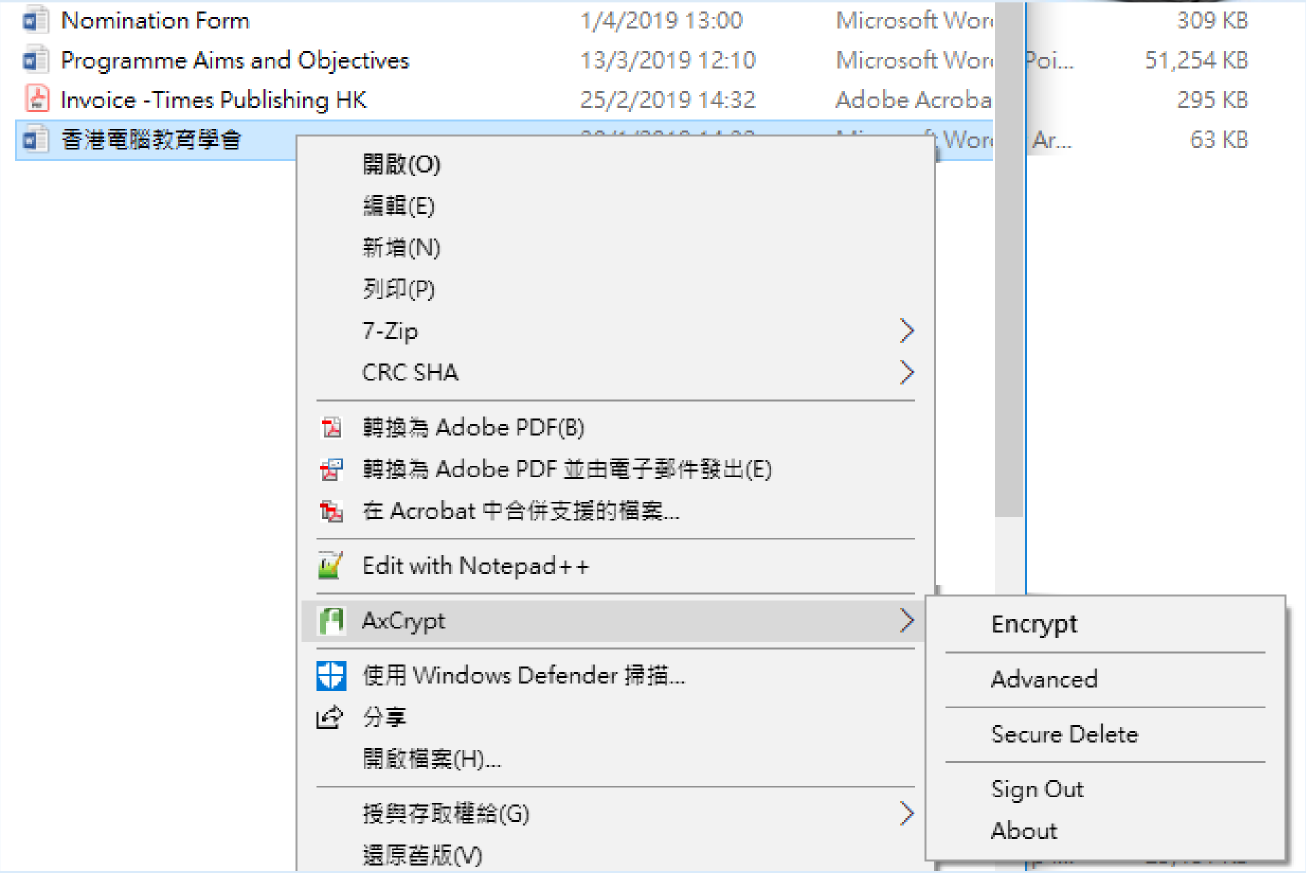
These can be used to make sure that it's really you signing in or to contact you if there's suspicious activity in your account

| | |
|---|---|
| Recovery phone | 9406 3750 |
| Recovery email | kwm@go.bhss.edu.hk |
| Security question | 您的主要飛行哩程號碼是什麼？ |

# Tools for Encryption

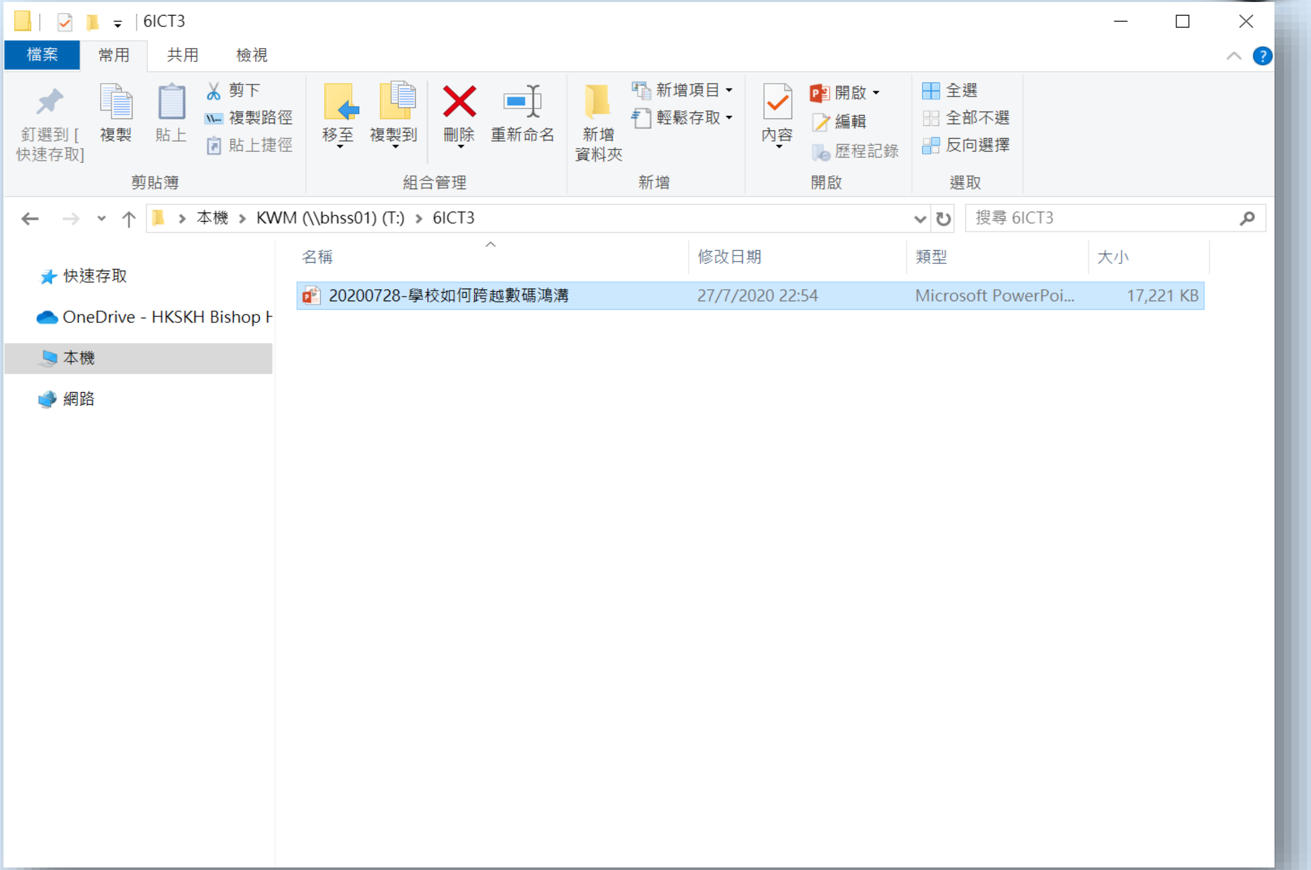
AxCrypt

File security for you and your team



| | | | | |
|---|---|---|---|---|
| Nomination Form | 1/4/2019 13:00 | Microsoft Wor | | 309 KB |
| Programme Aims and Objectives | 13/3/2019 12:10 | Microsoft Wor | Poi... | 51,254 KB |
| Invoice -Times Publishing HK | 25/2/2019 14:32 | Adobe Acroba | | 295 KB |
| 香港電腦教育學會 | | Word | Ar... | 63 KB |

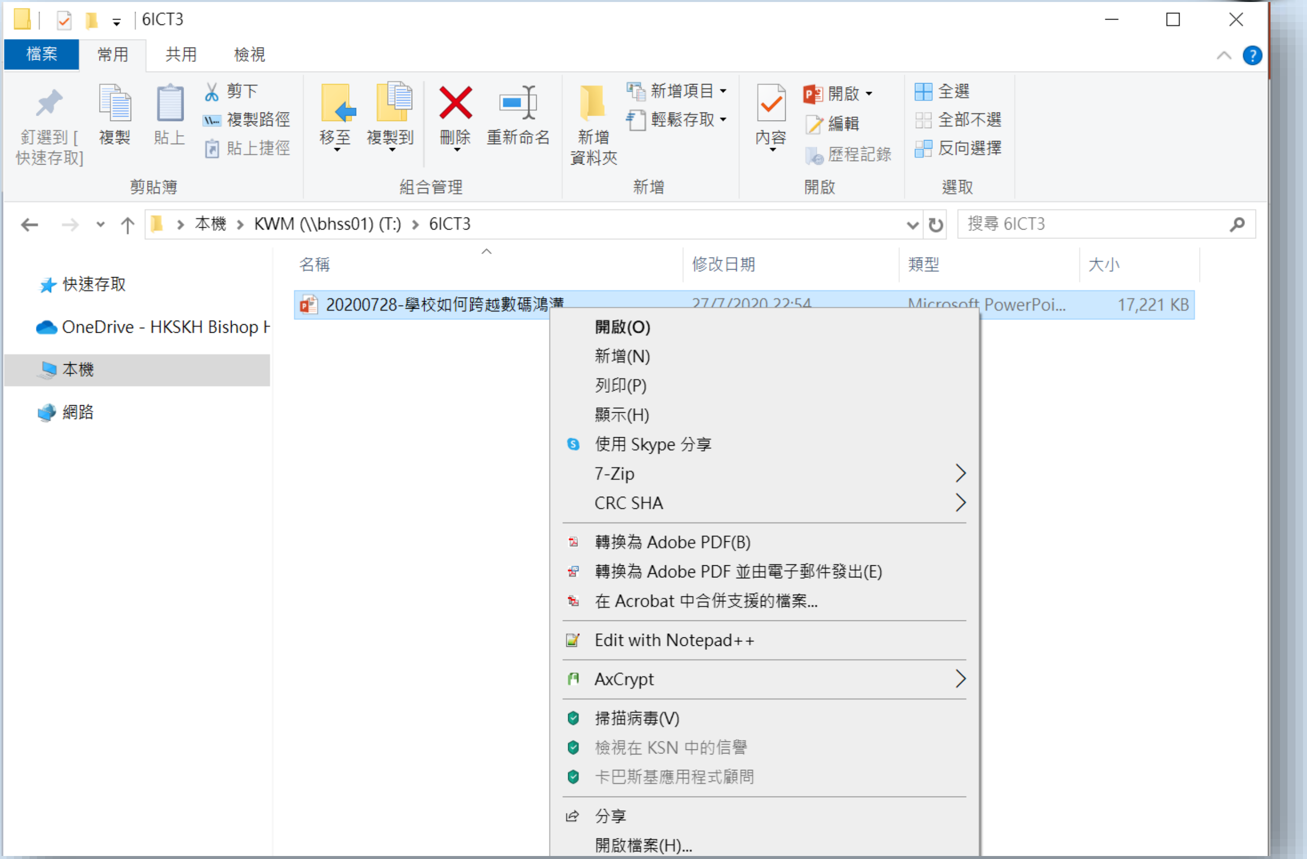
# Tools for Encryption



本機 > KWM (\\bhss01) (T:) > 6ICT3

| 名稱 | 修改日期 | 類型 | 大小 |
|---|---|---|---|
| 20200728-學校如何跨越數碼鴻溝 | 27/7/2020 22:54 | Microsoft PowerPoi... | 17,221 KB |

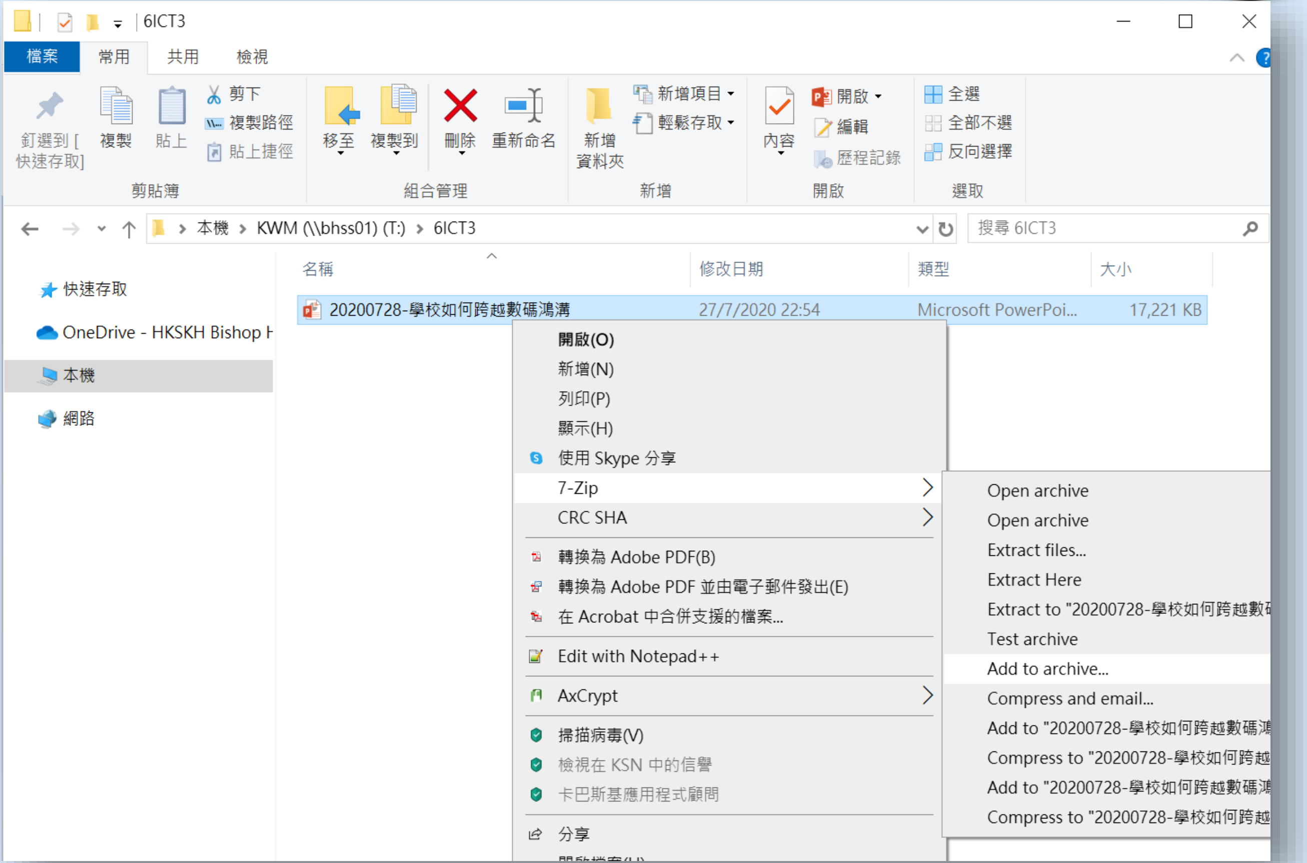
# Tools for Encryption



| 名稱 | 修改日期 | 類型 | 大小 |
|---|---|---|---|
| 20200728-學校如何跨越數碼鴻溝 | 27/7/2020 22:54 | Microsoft PowerPoi... | 17,221 KB |

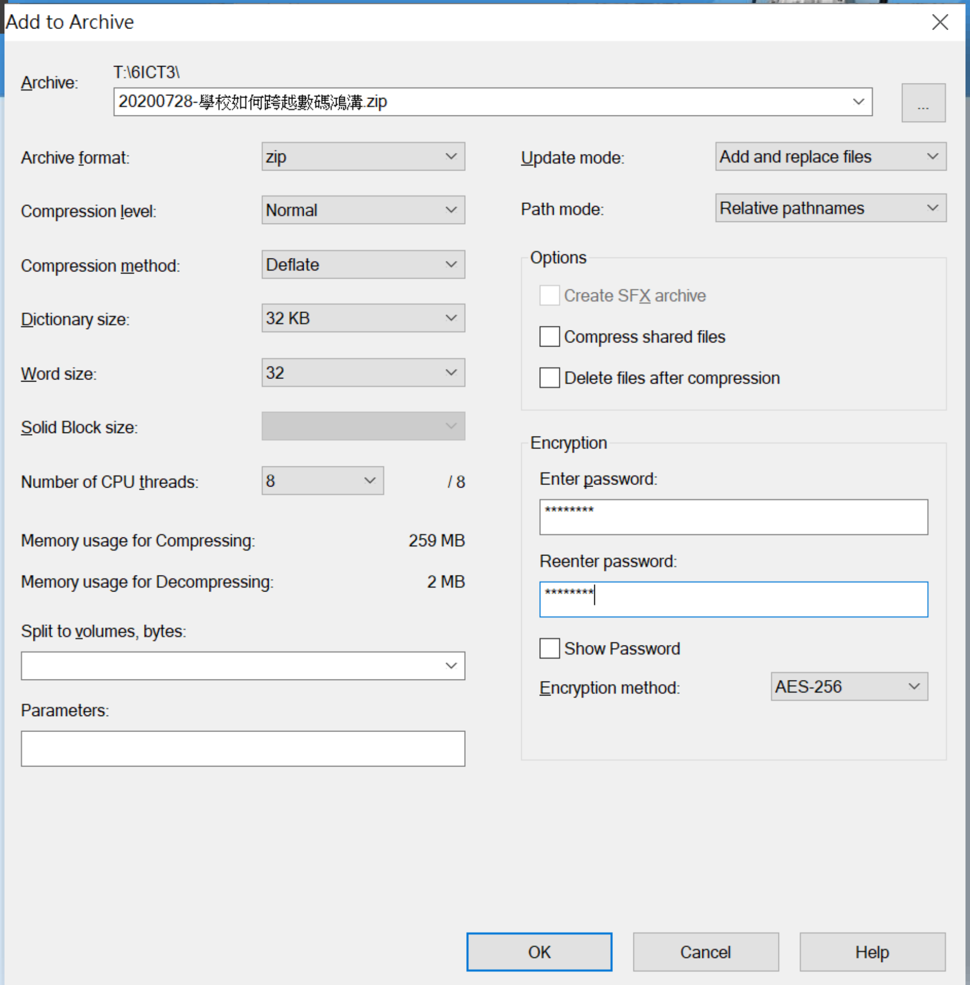
# Tools for Encryption

7 ZIP



# Tools for Encryption

7 ZIP



Add to Archive

Archive: T:\6ICT3\

20200728-學校如何跨越數碼鴻溝.zip

Archive format: zip

Compression level: Normal

Compression method: Deflate

Dictionary size: 32 KB

Word size: 32

Solid Block size:

Number of CPU threads: 8 / 8

Memory usage for Compressing: 259 MB

Memory usage for Decompressing: 2 MB

Split to volumes, bytes:

Parameters:

Update mode: Add and replace files

Path mode: Relative pathnames

Options

- □ Create SFX archive
- □ Compress shared files
- □ Delete files after compression

Encryption

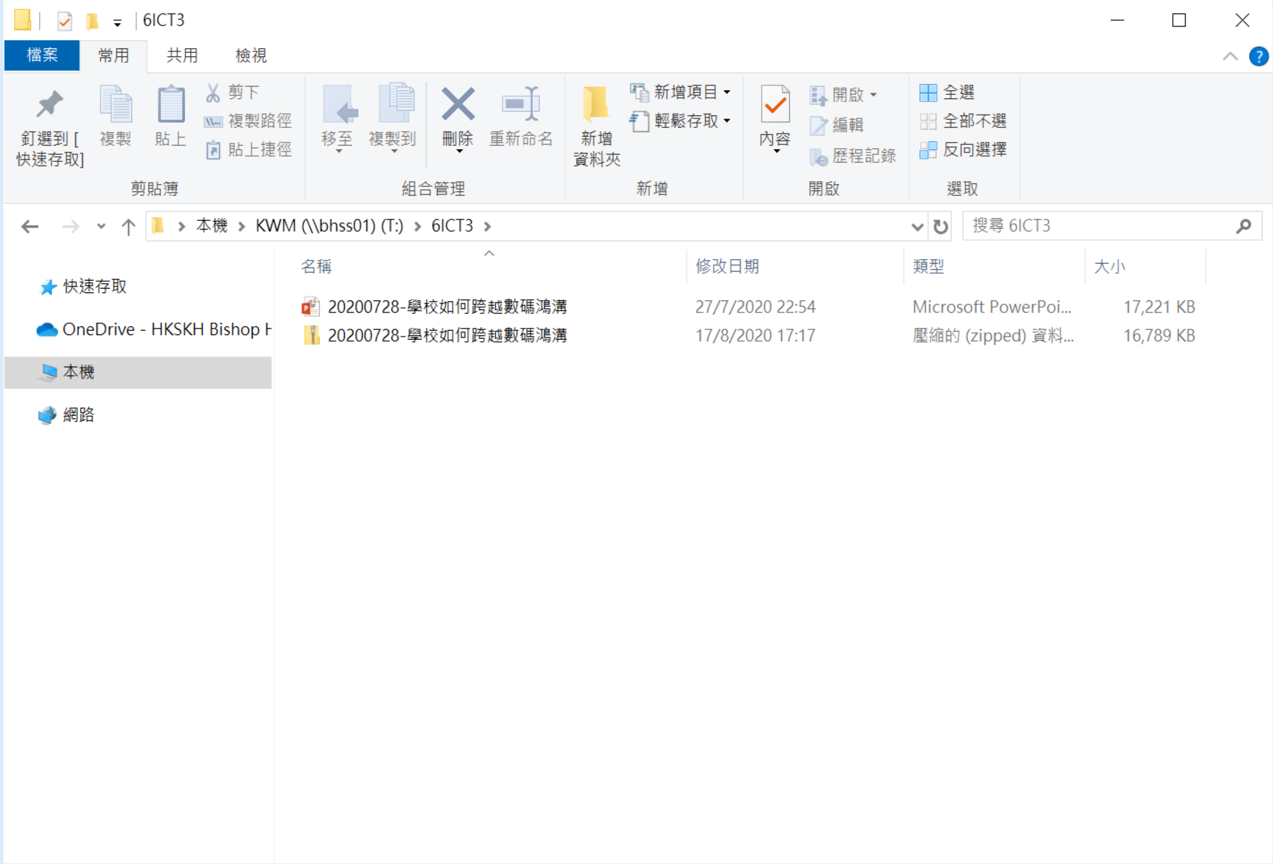
Enter password: ********

Reenter password: ********

□ Show Password

Encryption method: AES-256

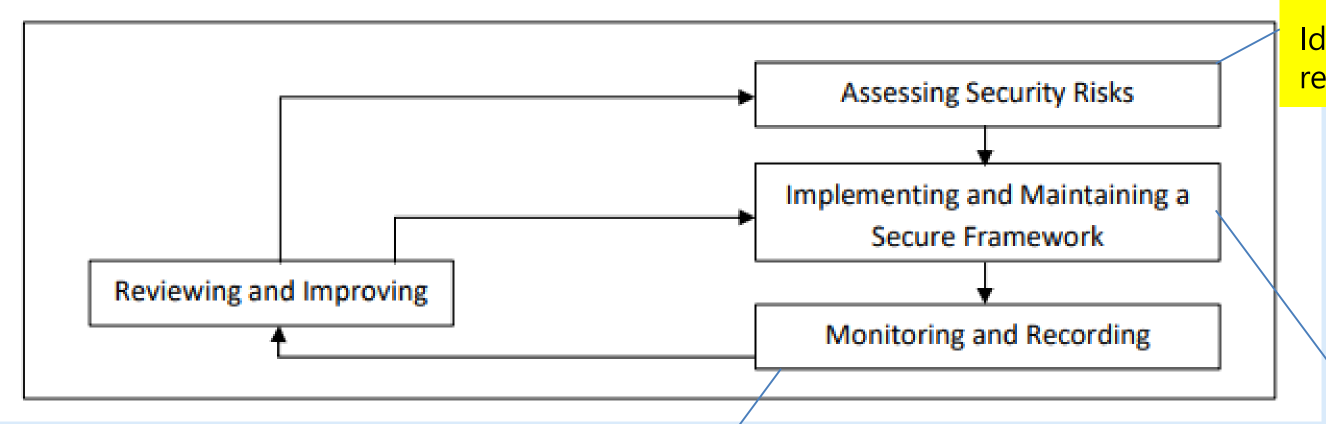
# Tools for Encryption



| 名稱 | 修改日期 | 類型 | 大小 |
|---|---|---|---|
| 20200728-學校如何跨越數碼鴻溝 | 27/7/2020 22:54 | Microsoft PowerPoi... | 17,221 KB |
| 20200728-學校如何跨越數碼鴻溝 | 17/8/2020 17:17 | 壓縮的 (zipped) 資料... | 16,789 KB |

# The Role of School Management

## Security Management Cycle

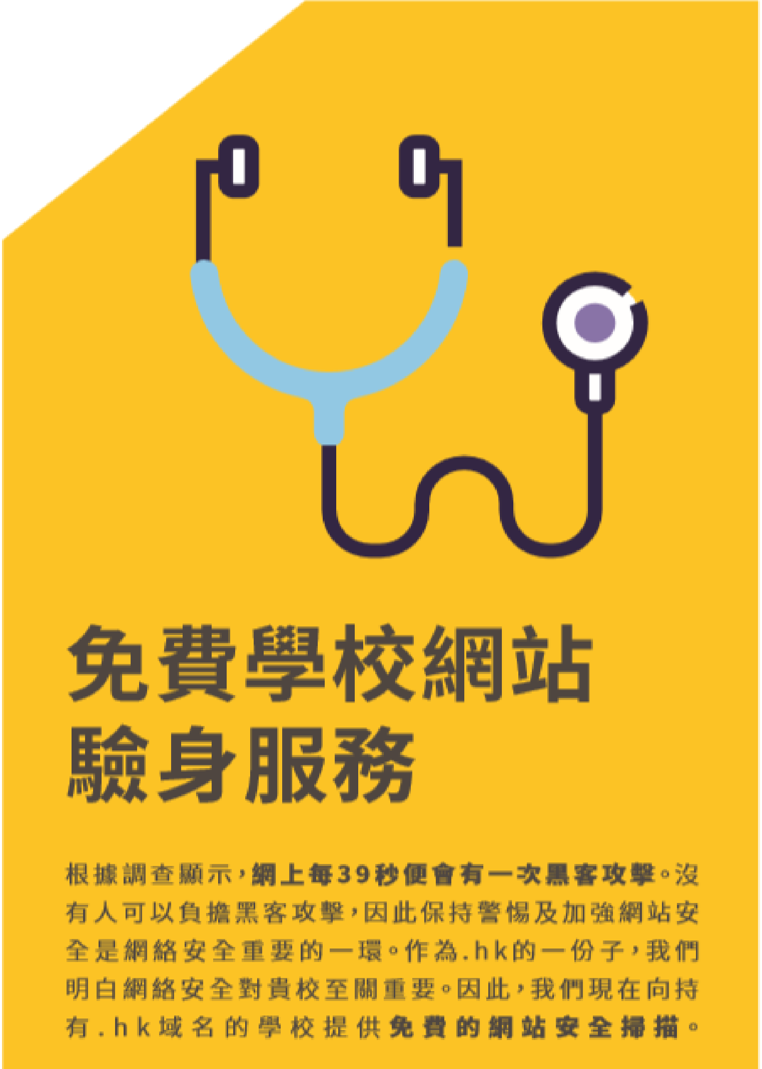


Identifying the risks and consequences associated with vulnerabilities.

Identify what assets to protect, their relative importance.

Developing security policies and guidelines, assigning security responsibilities and implementing technical and administrative security measures.

Constant monitoring and recording so that proper arrangements can be made when tackling a security incident.



# 免費學校網站驗身服務

根據調查顯示，**網上每39秒便會有一次黑客攻擊**。沒有人可以負擔黑客攻擊，因此保持警惕及加強網站安全是網絡安全重要的一環。作為.hk的一份子，我們明白網絡安全對貴校至關重要。因此，我們現在向持有.hk域名的學校提供**免費的網站安全掃描**。

https://www.hkirc.hk/zh-hant/community_programme/sme/

# 資訊科技保安風險評估 - 學校篇

自第四個資訊科技教育策略推出至今，學校的無線網絡基建已基本完成，以自攜裝置（BYOD）進行電子學習的學校亦逐漸增加。在推行電子學習的同時亦要提高學校對保護學校、學生和家長的資料及資訊科技資產的警覺。根據教育局的《學校資訊保安建議措施》所述，學校有責任採取適當的資訊科技保安措施，以保護學校的資訊科技系統和數據。

資訊科技保安風險評估跟體檢大致相同，藉著定期檢查希望能夠發現一些隱藏的病毒或潛在的風險。透過重複評估與使用資訊科技相關之保安風險的程序，過程中把收集到的數據進行評估和分析，呈報已發現的保安漏洞，並作出評估及提出相關安全性的建議。

## 資訊科技保安風險評估

在眾多的資訊科技系統中，學校最多使用而又連接到互聯網的便是學校的網站。要使有關網站的數位服務系統和應用系統的安全，良好的設計和開發過程是必須重視的。有見及此，我們顆拍了專業網絡安全管理專家 **UDomain** 為學校進行保安風險評估，以網站弱點性測試及滲透測試*為學校網站分析和測試數位服務的安全性。這樣的安全測試工作，應當作是學校專案中要持續進行的活動，不應當作是最後或有需要時才執行的一項檢查。

### 網站弱點測試 (Vulnerability Test) –

- **找出網站漏洞**
- **進行系統掃瞄**
- **有助系統達致符合保安及審查的標準**

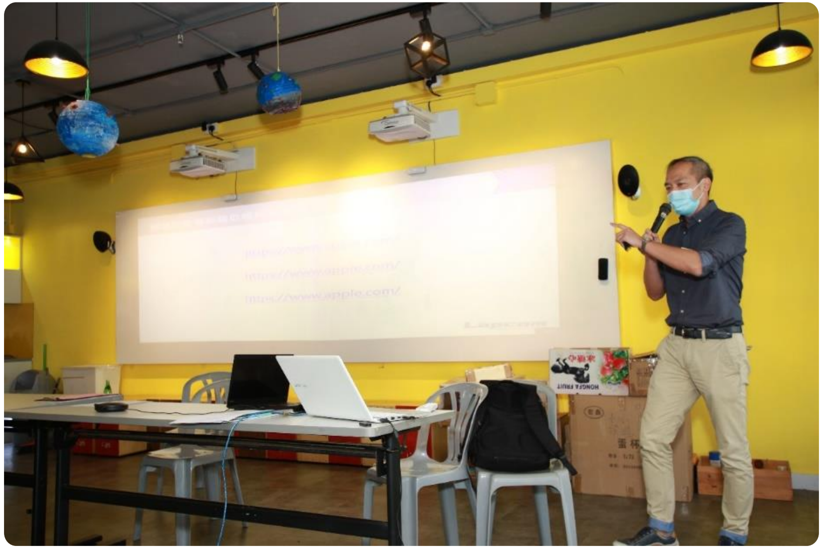
**免費評估 名額 10 個**
**(由專業網絡安全管理專家 UDomain 提供)**

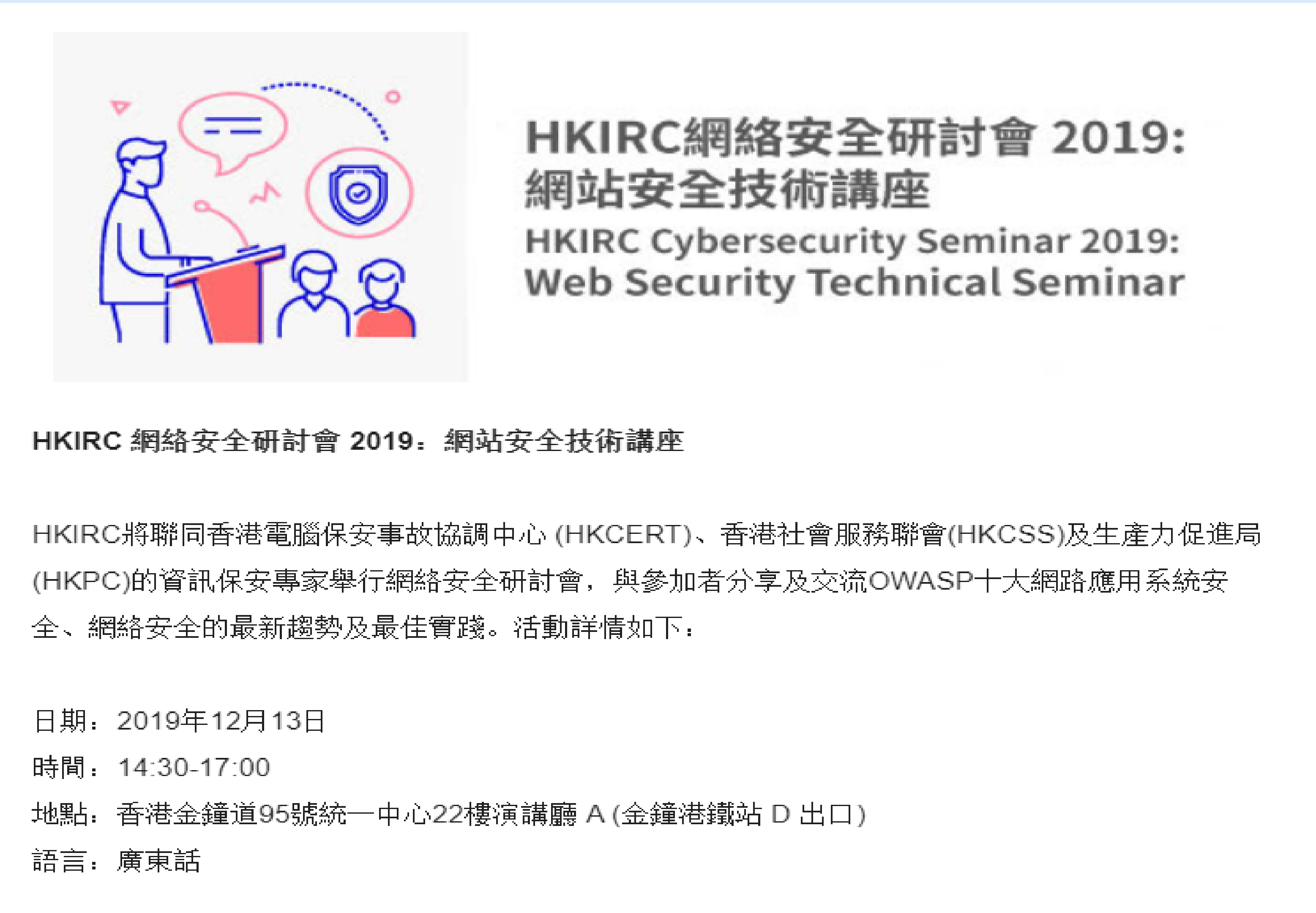
# Cyber Security in a Connected World Seminar

27 June, 2020

香港電腦教育學會

The Hong Kong Association for Computer Education



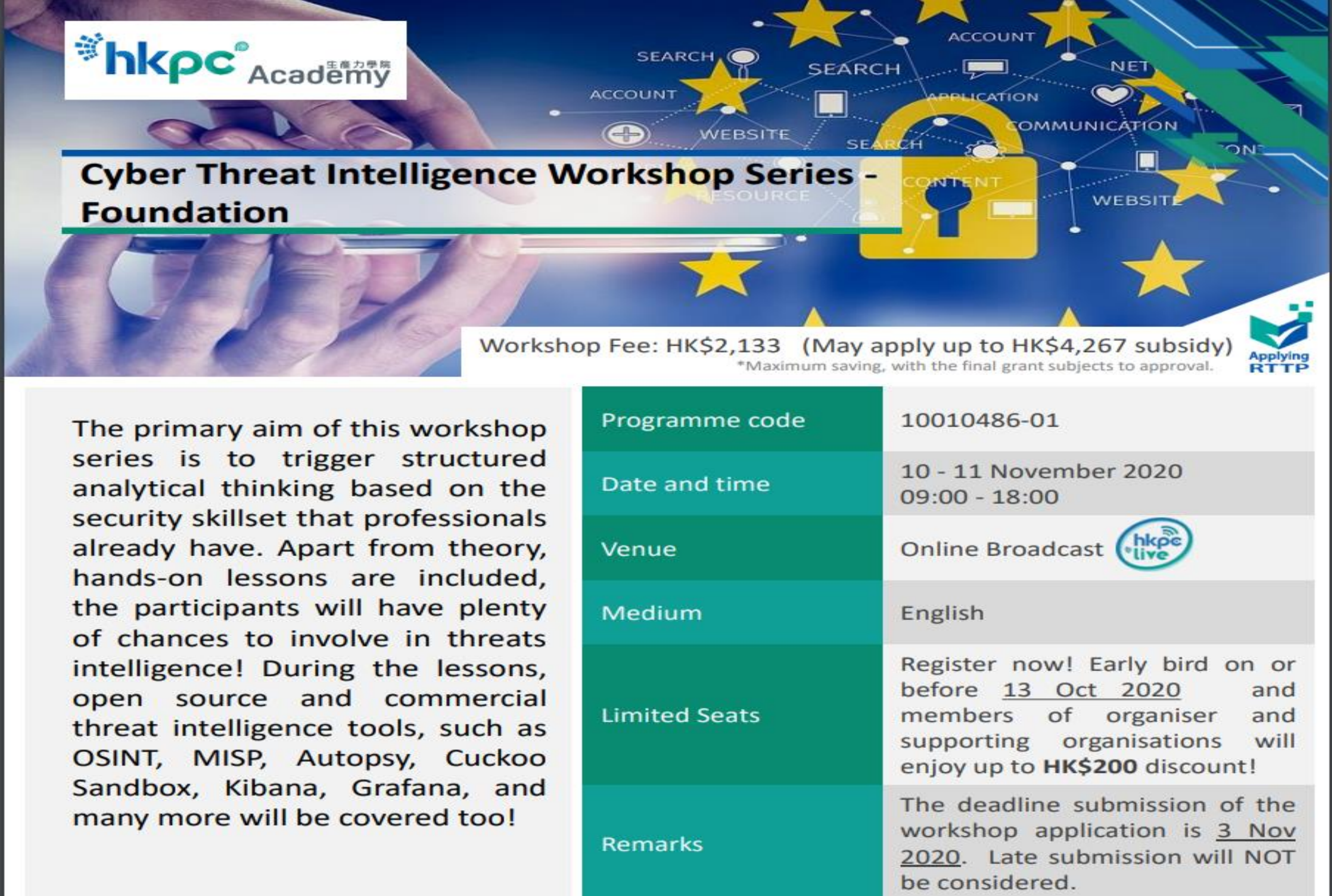


HKIRC網絡安全研討會 2019:
網站安全技術講座
HKIRC Cybersecurity Seminar 2019:
Web Security Technical Seminar

**HKIRC 網絡安全研討會 2019：網站安全技術講座**

HKIRC將聯同香港電腦保安事故協調中心 (HKCERT)、香港社會服務聯會(HKCSS)及生產力促進局(HKPC)的資訊保安專家舉行網絡安全研討會，與參加者分享及交流OWASP十大網路應用系統安全、網絡安全的最新趨勢及最佳實踐。活動詳情如下：

日期：2019年12月13日
時間：14:30-17:00
地點：香港金鐘道95號統一中心22樓演講廳 A (金鐘港鐵站 D 出口)
語言：廣東話


hkpc Academy 生產力學院
SEARCH
ACCOUNT
WEBSITE
SEARCH
APPLICATION
ACCOUNT
NET
COMMUNICATION
SEARCH
CONTENT
RESOURCE
WEBSITE
Applying RTTP
hkpc live

# Cyber Threat Intelligence Workshop Series - Foundation

Workshop Fee: HK$2,133 (May apply up to HK$4,267 subsidy)

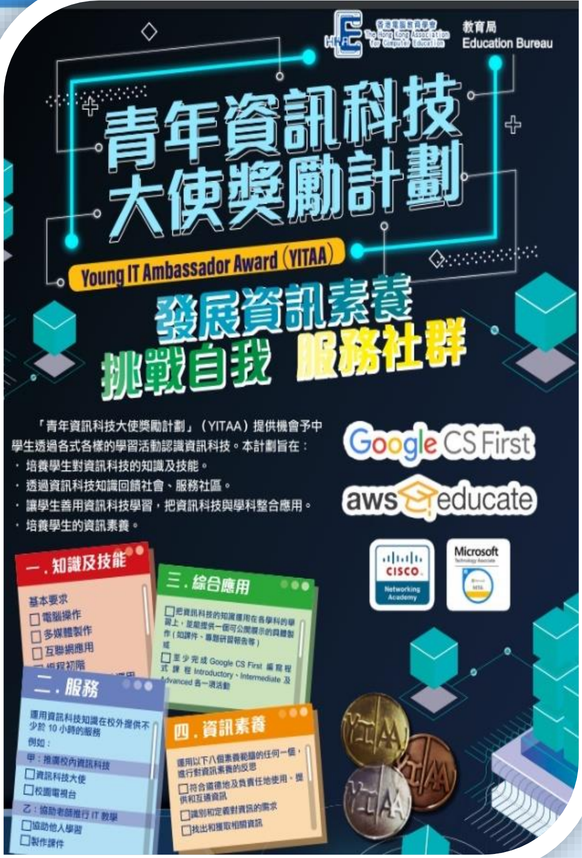
*Maximum saving, with the final grant subjects to approval.

The primary aim of this workshop series is to trigger structured analytical thinking based on the security skillset that professionals already have. Apart from theory, hands-on lessons are included, the participants will have plenty of chances to involve in threats intelligence! During the lessons, open source and commercial threat intelligence tools, such as OSINT, MISP, Autopsy, Cuckoo Sandbox, Kibana, Grafana, and many more will be covered too!

| | |
|---|---|
| Programme code | 10010486-01 |
| Date and time | 10 - 11 November 2020<br>09:00 - 18:00 |
| Venue | Online Broadcast |
| Medium | English |
| Limited Seats | Register now! Early bird on or before 13 Oct 2020 and members of organiser and supporting organisations will enjoy up to **HK$200** discount! |
| Remarks | The deadline submission of the workshop application is 3 Nov 2020. Late submission will NOT be considered. |

# HKACE 學生獎勵計劃

資訊科技挑戰獎勵計劃
IT Challenge Award
挑戰自我
主動學習
服務
*金章級
*銀章級
*銅章級
*證書級
技能
專題研
主辦
協辦
HKACE
香港電腦教育學會
教育局
Education Bureau
香港教育城
HKedCity


香港電腦教育學會
The Hong Kong Association for Computer Education
教育局
Education Bureau
青年資訊科技
大使獎勵計劃
Young IT Ambassador Award (YITAA)
發展資訊素養
挑戰自我 服務社群
Google CS First
aws educate
CISCO Networking Academy
Microsoft Technology Associate
YITAA

「青年資訊科技大使獎勵計劃」（YITAA）提供機會予中學生透過各式各樣的學習活動認識資訊科技。本計劃旨在：

- 培養學生對資訊科技的知識及技能。
- 透過資訊科技知識回饋社會、服務社區。
- 讓學生善用資訊科技學習，把資訊科技與學科整合應用。
- 培養學生的資訊素養。

一．知識及技能

基本要求
□ 電腦操作
□ 多媒體製作
□ 互聯網應用
□ 編程初階

二．服務

運用資訊科技知識在校外提供不少於 10 小時的服務
例如：
甲：推廣校內資訊科技
□ 資訊科技大使
□ 校園電視台
乙：協助老師推行 IT 教學
□ 協助他人學習
□ 製作課件

三．綜合應用

□ 把資訊科技的知識應用在各學科的學習上，並能提供一個可公開展示的具體製作（如課件、專題研習報告等）
□ 至少完成 Google CS First 編程程式課程 Introductory、Intermediate 及 Advanced 各一項活動

四．資訊素養

運用以下八個素養範疇的任何一個，進行對資訊素養的反思
□ 符合道德地及負責任地使用、提供和互通資訊
□ 識別和定義對資訊的需求
□ 找出和獲取相關資訊

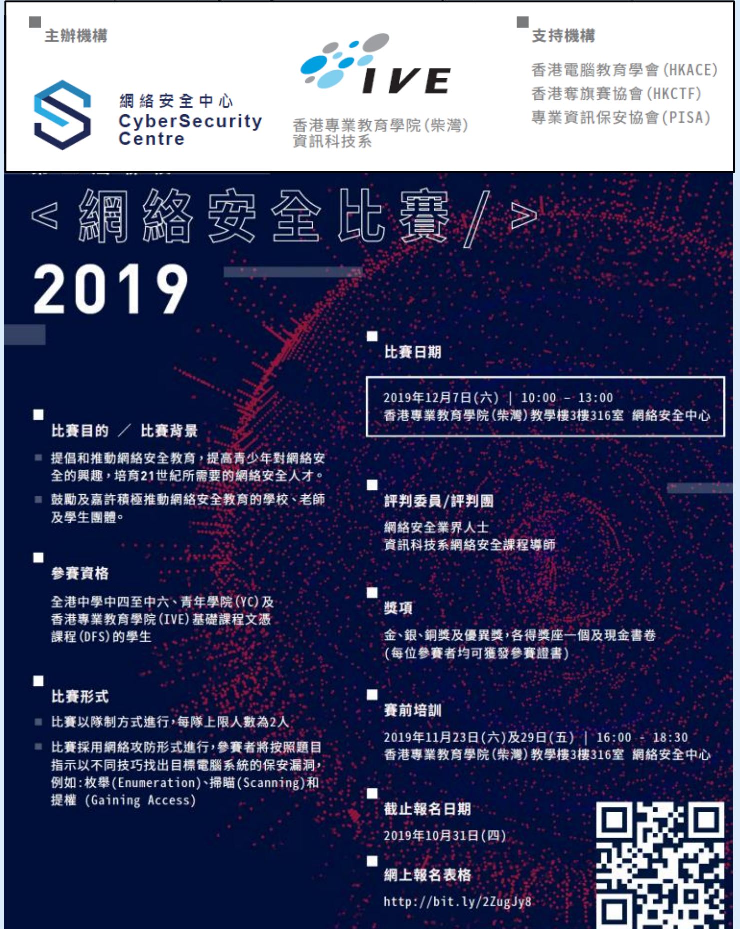
# HKACE 支持活動：新媒體素養

htt

PROJECT NET
新媒體素養提升計劃
香港青年協會媒體輔導中心
新媒體素養
教案比賽
查詢及報名
2788 3433
medialiteracy.hk
主辦機構
香港青年協會
the hongkong federation of youth groups
贊助
優質教育基金
Quality Education Fund
支持機構
教育局
香港浸會大學傳理學院新聞系
香港翻轉教學協會
The Hong Kong Association for Computer Education
媒體伙伴
明報
香港教育城
HKedCity

PROJECT NET
新媒體素養
提升計劃
Your Turn
http://medialiteracy.hk
REC
新媒體素養
短片拍攝
比賽
VIDEO
主辦機構
香港青年協會
the hongkong federation of youth groups
贊助
優質教育基金
Quality Education Fund
支持機構
香港浸會大學傳理學院
The Hong Kong Association for Computer Education
媒體伙伴
明報
香港教育城
HKedCity

# HKACE 支持活動：網絡安全比賽



主辦機構

網絡安全中心
CyberSecurity Centre

香港專業教育學院(柴灣)
資訊科技系

支持機構

香港電腦教育學會(HKACE)
香港奪旗賽協會(HKCTF)
專業資訊保安協會(PISA)

## < 網絡安全比賽 / >
## 2019

**比賽目的 ／ 比賽背景**

- 提倡和推動網絡安全教育，提高青少年對網絡安全的興趣，培育21世紀所需要的網絡安全人才。
- 鼓勵及嘉許積極推動網絡安全教育的學校、老師及學生團體。

**參賽資格**

全港中學中四至中六、青年學院(YC)及
香港專業教育學院(IVE)基礎課程文憑
課程(DFS)的學生

**比賽形式**

- 比賽以隊制方式進行，每隊上限人數為2人
- 比賽採用網絡攻防形式進行，參賽者將按照題目指示以不同技巧找出目標電腦系統的保安漏洞，例如：枚舉(Enumeration)、掃瞄(Scanning)和提權 (Gaining Access)

**比賽日期**

2019年12月7日(六) | 10:00 - 13:00
香港專業教育學院(柴灣)教學樓3樓316室 網絡安全中心

**評判委員/評判團**

網絡安全業界人士
資訊科技系網絡安全課程導師

**獎項**

金、銀、銅獎及優異獎，各得獎座一個及現金書卷
(每位參賽者均可獲發參賽證書)

**賽前培訓**

2019年11月23日(六)及29日(五) | 16:00 - 18:30
香港專業教育學院(柴灣)教學樓3樓316室 網絡安全中心

**截止報名日期**

2019年10月31日(四)

**網上報名表格**

http://bit.ly/2ZugJy8

香港電腦教育學會

The Hong Kong Association for Computer Education

| | | |
|---|---|---|
| Website | : | https://www.hkace.org.hk |
| Facebook | : | https://www.facebook.com/hkace.org/ |
| Tel | : | 2406 6683 |
| Fax | : | 8200 1738 |
| Email | : | ask@hkace.org.hk |
| Whatsapp | : | https://cutt.ly/TtJBrt9 |