# 網絡安全
# 學與教資源

# 常見與網絡及
# 新興和先進資訊科技相關的
# 罪案資訊

教育局 與 香港警務處

二零二五年一月

## 資源使用方法

本學與教資源分為四部分，詳情如下：

（一） 建議教學內容：為學校提供整體教學內容。

（二） 建議教學模式：為學校提供可參考的教學模式，學校可因應校情自行調適。

（三） 教學資料：為學校提供不同課題的教學資源、建議教學示例及警方提供的參考內容，學校可因應校情自行調適。


- 提供載列於香港警務處「守網者」網頁及與課題相關的參考資料，讓教師能了解課題。

- 提供與課題相關的參考教學建議，教師可參考相關點子自行調適，並通過多元化的學習活動，善用學時，讓學生於課堂內外，學習相關的知識和技能，並培養學生正確的態度和價值觀。

- 提供與課題相關的網頁及影片連結，教師可藉此獲取更多資訊。

（四） 參考資料：為學校提供全面的網上參考資源。

**學習對象：** 小四至小六（高小）及 中一至中六適用

**學習目標：** 學生完成學習單元後，能夠：

1. 認識網絡及新興和先進資訊科技相關的資訊
2. 辨別網絡資訊真偽，洞悉資訊中存在的欺詐及捏造成份
3. 了解培養資訊素養能力的重要性
4. 明白法律適用於現實和網上世界，了解遵守法規的重要性，以免誤墮網絡陷阱
5. 培養面對網絡騙局時應持守的態度，加強自我保護意識，提防受騙。

**建議時間：** 每節約 35 – 40 分鐘（教師可按需要選擇合適的教學內容及調整教節）

## (一) 建議教學內容：

1. 了解常見與網絡及新興和先進資訊科技的知識，包括：原理、相關罪案和陷阱、防範方式等
2. 提升學生於網絡活動時的自我保護意識
3. 認識現時香港於網絡安全推廣的各項支援和活動，例如：網絡安全攻防演練

## (二) 建議教學模式：（教師可按學校情況選擇合適的教學模式）

### 1. 自主學習：

教師通過課前預習及課後練習，為學生提供相關閱讀材料、影片、問題或模擬情境，以了解學生能掌握多少知識及他們處理問題的態度，並讓學生思考日常生活中有否遇到相似的情況，尋找問題解決方案及面對問題時正確的態度，再於課堂與同學討論，使學生多加留意身邊發生的事情，學會自學，並關注保護網上私隱及提高自我保護意識。

### 2. 善用課時：

教師因應學生能力及學習方式，於課堂以提問、投票決定、或角色扮演等多元模式，了解學生對課題的掌握。教師亦可通過課堂教授及設計相關討論題目，讓學生分組討論相關要點、問題、解決方案等，以演示檔、圖表等方式展示及作分組匯報。此外，教師更可讓學生通過實踐體驗，培養他們正確的價值觀和資訊素養，學會多角度思考，懂得慎思明辨。

### 3. 跨學科學習：

各學習領域科目教師通過共同整合課程及備課，規劃跨學科學習方案，讓各科配合學校課程整體發展，於現有學習框架內加入網絡及資訊安全和創新科技等相關元素。此外，亦可通過多元化的跨科活動，如：跨科專題探究、視藝創作（如：海報、漫畫、填色等）、角色扮演、話劇等，讓學生有系統地學習相關知識、技能及培養他們正確的價值觀和態度，並關注保護網上私隱及學會保護自己。

### 4. 善用學時：

學校可安排於課堂以外的時間（如：早會／週會、班主任或德育及公民課、聯課活動和校園電視台等），以不同的方式，如安排學生演講、專家講座、工作坊、參觀活動等，讓學生了解網絡及資訊安全的重要性，創新科技的發展與挑戰，以及進一步關注保護網上私隱及懂得自我保護。

## (三) 教學資料：

# 1. 常見與網絡及新興和先進資訊科技相關的罪案

## 常見與網絡及新興和先進資訊科技相關的罪案

[資料來源：守網者 – 網絡罪案 https://cyberdefender.hk/cybercrime/]

### 常見與網絡相關的科技罪案

勒索軟件

釣魚攻擊

分散式阻斷服務攻擊

### 常見與新興和先進資訊科技相關的罪案


物聯網攻擊

人工智能

深度偽造

# 2. 常見與網絡相關的科技罪案資訊

## 2.1. 勒索軟件

### 2.1.1. 參考資料（香港警務處提供）

[資料來源：守網者－勒索軟件 https://cyberdefender.hk/ransomware/]

### 甚麼是勒索軟件？

勒索軟件（Ransomware）是一種阻止或限制用戶使用電腦系統的惡意軟件。黑客會透過電郵、網站或惡意廣告等途徑感染並入侵用戶或目標的電腦系統，被植入軟勒索軟件的電腦或其網絡內其他裝置的特定檔案，如文件檔、試算表、數碼相片等，便會被加密，令用戶無法存取。受害人的電腦隨即出現訊息要求以比特幣等加密資產支付贖金以換取解密鑰。

一款名為 WannaCry 的勒索軟件於 2017 年在全球網絡世界散佈，受感染的電腦會彈出死亡紅色視窗通知受害者，並要求支付比特幣（Bitcoin）來解鎖。

### 勒索軟件的種類

**勒索軟件的種類演變繁多，黑客近年甚至利用雙重勒索、三重勒索甚至四重勒索等策略。**

- **雙重勒索：**黑客透過釣魚攻擊、系統漏洞等手法感染目標電腦系統，令電腦內的資料無法讀取之餘，更會竊取其敏感資料。拒絕繳付贖金的受害人除了可能無法解密受影響的文件外，被盜取的文件亦可能在網上公開。

- **三重勒索：**黑客先竊取目標公司的敏感資料，包括與客戶或生意伙伴往來的商業機密。除了威脅目標公司外，還會向其客戶或生意伙伴進行勒索，以獲取更多的贖金。

- **四重勒索：**不止於上述三重勒索，黑客會進一步要脅對目標公司發動分散式阻斷服務攻擊，透過制造大量網絡流量癱瘓目標公司的網絡，以迫使目標公司繳付贖金。

2021 年初，有一家境外電腦製造商被黑客利用三重勒索攻擊，勒索近四億港元贖金。黑客盜取該公司與合作夥伴的產品設計圖，並警告如非按時支付，贖金將翻倍。由於該公司拒絕就範，黑客陸續於網上公開設計圖，更直接勒索其合作夥伴。

## 保安貼士

| 必需要做 | 不可以做 |
| --- | --- |
| ✓ 定期備份資料和不要把備份資料連接電腦 | × 開啓可疑的電郵及短訊，或內含的附件/連結 |
| ✓ 為作業系統及軟件安裝最新的修補程式 | × 瀏覽可疑網站，或從該網站下載任何檔案 |
| ✓ 更新抗惡意程式碼軟件及識別碼至最新版本 | |
| ✓ 定期全面掃描電腦，以偵測及防預惡意攻擊 | |

## 電腦受到感染後應如何處理？

- ❖ 切斷受感染電腦的網絡連線，以免影響網絡磁碟機及其他電腦。
- ❖ 關上電腦的電源，防止勒索軟件把電腦內更多檔案加密。
- ❖ 記下感染前曾經執行過的程式和檔案、開啓過的電郵及瀏覽過的網站，並報警求助。
- ❖ 從備份復原數據至未受感染的電腦裝置。
- ❖ 切勿繳付贖金，此舉不能保證能夠取得解密鑰，亦會助長黑客的犯罪行為。
- ❖ 如懷疑不慎受騙，應立即向家長、監護人、教師或學校社工尋求協助。

### 2.1.2. 參考教學建議

通過多元化的學習活動，讓學生認識甚麼是勒索軟件及其影響，知道電腦受到感染時的應對方法，並讓學生懂得如何防範及明白日常網絡安全的重要性，並培養他們資訊素養能力。

## 中學

**目的：**讓學生認識甚麼是勒索軟件及其影響，知道電腦受到感染時的應對方法，並讓學生懂得如何防範及明白日常網絡安全的重要性，並培養他們資訊素養能力。

示例一：

**模式：**讓學生搜集網上相關的新聞資訊、閱讀相關資料〔參考資源第 1-8 項〕及觀看影片〔參考資源第 9 及 10 項〕，並於課堂與同學分享或作分組討論。讓他們認識甚麼是勒索軟件及其影響，知道電腦受到感染時的應對方法，並讓學生懂得如何防範及明白日常網絡安全的重要性，並培養他們資訊素養能力。

**思考問題：**

(i) 讓學生認識勒索軟件及影響

- 甚麼是勒索軟件？
- 電腦如何感染勒索軟件？有何徵兆？
- 當電腦設備感染勒索軟件會有何影響？

(ii) 讓學生明白網絡安全及培養資訊素養能力的重要性

- 你認為有那些網絡安全措施有助預防及應對電腦設備感染勒索軟件？
- 你認為電腦使用者應具備怎樣態度，以保護自己的電腦設備減少感染勒索軟件的風險？
- 如果電腦設備不幸感染勒索軟件，會如何處理及應持守怎樣的態度？

示例二：

**模式**：學校通過舉辦「預防勒索軟件」為主題的海報設計比賽，並把得獎學生作品製成不同的學校宣傳物品、屏幕保護圖等，提升學生關注「預防勒索軟件」。

## 小學

**目的**：讓學生關注日常網絡保安的重要，培養資訊素養能力。

示例一：

**模式**：教師於課堂向學生講解勒索軟件〔參考資源第 1 及 4 項〕，並教導學生正確使用電腦的方法和態度，培養學生資訊素養能力及正確價值觀和態度。

**思考問題：**

(i) 讓學生認識勒索軟件及影響

- 甚麼是勒索軟件？
- 當電腦設備感染勒索軟件會有何影響？

(ii) 讓學生學會正確使用電腦的方法和態度

- 當你收到不明來歷的電郵，你會開啟當中的附件或連結嗎？為甚麼？
- 當你收到不明來歷的 USB 外置儲存器，你會開啟嗎？為甚麼？
- 你會瀏覽不明網站嗎？為甚麼？
- 你會如何保護自己的電腦設備，減少電腦設備感染勒索軟件的風險？

示例二：

**模式**：學生通過專題研習，以小組方式化身成為校園小記者，設計簡單問卷，訪問家長、親友或同學，以搜集日常生活中各人如何正確使用互聯網，包括：網頁、網上電郵、即時通訊工具、社交媒體等，並在課堂進行匯報及報告，與同學分享或於學校展示。

### 2.1.3. 參考資源

(i) 網頁：

1. 守網者－勒索軟件
   https://cyberdefender.hk/ransomware/
2. 香港警務處－「拒絕勒索軟件」計劃
   https://www.police.gov.hk/ppp_tc/04_crime_matters/tcd/project_nmr.html
3. 網絡安全資訊站－預防勒索軟件
   https://www.cybersecurity.hk/tc/learning-ransomware.php

4. 資訊安全網：預防勒索軟件
   https://www.infosec.gov.hk/tc/knowledge-centre/ransomware
5. 香港電腦保安事故協調中心－齊抗勒索軟件
   https://www.hkcert.org/tc/publications/fight-ransomware
6. 香港電腦保安事故協調中心－勒索軟件的進化：雙重勒索和虛假解密工具
   https://www.hkcert.org/tc/blog/ransomware-evolved-double-extortion-and-fake-decryptor
7. 香港電腦保安事故協調中心－勒索軟件不斷進化：多重勒索
   https://www.hkcert.org/tc/blog/ransomware-keep-evolving-multiple-extortion
8. 香港電腦保安事故協調中心－勒索軟件的新陣線 揭露香港面臨的最新威脅
   https://www.hkcert.org/tc/blog/ransomware-s-new-front-uncovering-the-latest-threats-facing-hong-kong

**(ii)** 影片：

9. 醫健通－防禦勒索軟件入侵
   https://www.youtube.com/watch?v=MAcOjJ-e6Ow
10. 個人資料私隱公署－「防範網絡攻擊 提升數據安全」講座
    https://www.youtube.com/watch?v=3xk5sYnZHcc

## 2.2. 釣魚攻擊

### 2.2.1. 參考資料（香港警務處提供）

[資料來源：守網者－釣魚攻擊 https://cyberdefender.hk/phishing_attack/]

### 甚麼是釣魚攻擊？

釣魚攻擊（Phishing Attack），又稱「網絡釣魚」，泛指不法份子透過發放短訊、電郵、語音、二維碼等作餌，誘騙受害人上當。

近期騙徒常以釣魚手法進行詐騙（即釣魚詐騙），以漁翁撒網方式發放偽裝由快遞公司、電訊商、連鎖零售商店的會員獎賞計劃、網上付款服務商、政府部門等機構的電郵或短訊，聲稱收訊人的帳戶有異常、積分到期需換領禮品、需要核實帳戶等，要求收訊人點擊內含的連結進入假網站，留下帳戶登入憑證、信用卡資料、個人資料等。

### 釣魚電郵及短訊

取得收訊人的信用卡資料後，騙徒會在網上購刷卡消費或在實體商店購買商品並銷贓圖利；如取得獎賞計劃平台的帳戶登入憑證，騙徒也會登入帳戶並轉移積分或換取禮品。

不法分子亦可能會在訊息或電郵內嵌惡意連結或檔案附件。如收件者不慎點擊連結或開啟附件，其裝置便可能受惡意軟件感染。

除了騙取敏感資料，騙徒亦會透過釣魚短訊接觸收訊人，從而進行不同類型詐騙，如援交騙案、求職騙案、網戀投資騙案、網購騙案以及盜取虛擬資產等。

## 釣魚訊息／網站特徵

- ❖ 短訊或電郵內容前後矛盾、文法不通或拼字錯誤。
- ❖ 電郵內有可疑連結、二維碼或附件。
- ❖ 電郵地址和網址的域名（domain）與官方域名有出入。
- ❖ 網址用上 .cc / .top / .vip /.today /.club 等較冷門的延伸。
- ❖ 網站未能轉換語言、部分按鈕或連結失效。
- ❖ 在網站輸入不正確的帳戶或信用卡資料也能順利去到下一版面。

## 保安貼士

- ❖ 不要開啟來歷不明的郵件或訊息。
- ❖ 查看清楚寄件者的資料。
- ❖ 切勿點擊可疑電郵或訊息內的超連結。
- ❖ 切勿登入未經查證的網站。
- ❖ 如網站要求提供個人或信用卡資料，應加倍小心。
- ❖ 如懷疑受騙，應保存相關電郵或訊息，並儘快報警。
- ❖ 如懷疑不慎受騙，應立即向家長、監護人、教師或學校社工尋求協助。

### 2.2.2. 參考教學建議

通過多元化的學習活動，讓學生認識甚麼是釣魚攻擊及其影響。同時，讓學生明白日常網絡安全及保護個人資料私隱的重要性，並培養他們資訊素養能力。

## 中學

**目的：**讓學生認識甚麼是釣魚攻擊及其影響。同時，讓學生明白日常網絡安全及保護個人資料私隱的重要性，並培養他們資訊素養能力。

示例一：

**模式：**讓學生搜集網上相關的新聞資訊、閱讀相關資料〔參考資源第 1-5 項〕及觀看影片〔參考資源第 6-10 項〕，於課堂與同學分享或作分組討論，讓他們認識甚麼是釣魚攻擊，明白網絡安全及保護個人資料私隱的重要性，並培養他們資訊素養能力。

**思考問題：**

(i) 讓學生認識釣魚攻擊及影響

- 甚麼是釣魚攻擊？
- 日常生活中你有遇過嗎？試舉一例子說明。
- 釣魚網站或短訊有何特徵？你會如何辨別真偽網站或短訊？
- 為何受害者會誤墮釣魚攻擊？釣魚攻擊會對受害者產生甚麼影響？

(ii) 讓學生明白網絡安全及保護個人資料私隱的重要性

- 你認為有那些網絡安全措施有助預防及應對釣魚攻擊？
- 你認為自己應具備怎樣態度，以保護自己誤墮釣魚攻擊的風險？

示例二：

**模式**：學校通過舉辦「預防釣魚攻擊」為主題的活動，包括舉辦講座、早會或週會分享、影片拍攝比賽等，讓更多學生關注「預防釣魚攻擊」。

## 小學

**目的**：讓學生關注日常網絡保安及保護個人資料私隱的重要性，並培養學生資訊素養能力。

示例一：

**模式**：教師於課堂向學生講解釣魚攻擊〔參考資源第 1-5 項〕，並讓學生觀看影片〔參考資源第 7, 10 及 11 項〕，並教導學生正確使用電腦的方法和態度，培養學生資訊素養能力及正確價值觀和態度。

**思考問題：**

(i) 讓學生認識釣魚攻擊及影響

- 甚麼是釣魚攻擊？
- 你會如何分辨網頁或短訊的真偽？
- 釣魚攻擊對個人有何影響？
- [影片 7] 如果你是影片中的主角，你會如何？
- [影片 10] 影片中的主角為何會收到不明來歷的電郵？

(ii) 讓學生學會正確使用電腦的方法和態度

- 你會把個人資料完整填寫至遊戲網站以換取小禮品嗎？為甚麼？
- 當你收到不明來歷的電郵，你會開啟當中的連結嗎？為甚麼？
- 你認為自己應具備怎樣態度，以保護自己誤墮釣魚攻擊的風險？

### 2.2.3. 參考資源

**(i) 網頁：**

1. 守網者 – 釣魚攻擊
   https://cyberdefender.hk/phishing_attack/
2. 守網者 – 如何保護你的私隱
   https://cyberdefender.hk/protect_privacy/
3. 網絡安全資訊站 – 提防仿冒詐騙攻擊
   https://www.cybersecurity.hk/tc/learning-scam.php
4. 香港電腦保安事故協調中心 – 網絡釣魚 全城防禦
   https://www.hkcert.org/tc/publications/all-out-anti-phishing

5. 香港電腦保安事故協調中心 – 新一代釣魚攻擊：不斷進化的網絡威脅
   https://www.hkcert.org/tc/blog/next-level-phishing-the-evolving-threat-landscape

**(ii)** 影片：

6. 守網者 – 全城守網：釣魚攻擊
   https://youtu.be/09hDi1ZclRM
7. 守網者 – 提防釣魚攻擊 有 Link 唔好亂 click！
   https://www.youtube.com/watch?v=tP0mr1mcSKs
8. 反詐騙協調中心 – 唔準諗，即刻答
   https://youtu.be/1XPVRSWZqHk
9. 網絡安全資訊站 – 什麼是仿冒詐騙？
   https://www.youtube.com/watch?v=NbS2Y3ZFG2E
10. 香港電腦保安事故協調中心 – 釣魚攻擊要小心 不明電郵咪亂開
    https://www.youtube.com/watch?v=aWk7LPO5zs4
11. 教育局 –「聰明 e 主人」電子學習資源套 – 故事二「上網謹記保私隱」
    https://student.edcity.hk/sec/zh-hant/guidance/1488/

## 2.3. 分散式阻斷服務攻擊

### 2.3.1. 參考資料（香港警務處提供）

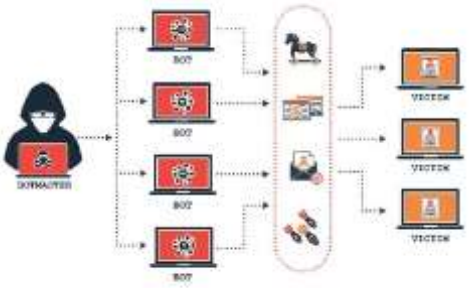
[資料來源：守網者 – 分散式阻斷服務攻擊 https://cyberdefender.hk/ddos/]

### 甚麼是分散式阻斷服務攻擊？

分散式阻斷服務攻擊是演變自傳統的阻斷服務攻擊。黑客利用網絡上多個被感染的電腦系統（即「殭屍網絡」），制造大量網絡流量使目標伺服器的網絡過度繁忙或系統資源嚴重消耗，導致其網絡癱瘓，無法提供正常服務。情況就像是高速公路上出現交通堵塞，阻斷了交通工具正常到達目的地。

### 甚麼是殭屍網絡？

電腦裝置受惡意程式感染並遭到控制，便會成為「殭屍網絡」一部分。「殭屍網絡」可能由成千上萬部裝置形成。這些被操控的裝置結合起來，能發動強大破壞力及精密的攻擊，例如發送以億計的垃圾電郵、巨大頻寬的分散式阻斷服務攻擊(DDoS)及針對性的財務詐騙。受感染的物聯網裝置（如網絡鏡頭、路由器、智能電視）也可能成為殭屍網絡的一部分。



### 2.3.2. 參考教學建議

通過多元化的學習活動，讓學生認識分散式阻斷服務攻擊及殭屍網絡的原理和影響，亦讓學生明白日常網絡設計及保安的重要性。

## 中學

**目的：**讓學生認識分散式阻斷服務攻擊及殭屍網絡的原理和影響，亦讓學生明白日常網絡設計及保安的重要性。

示例一：

**模式：**讓學生搜集網上相關的新聞資訊、閱讀相關資料〔參考資源第 1-6 項〕，於課堂與同學分享或作分組討論，讓他們認識分散式阻斷服務攻擊及殭屍網絡的原理和影響，亦讓學生明白日常網絡設計及保安的重要性。

**思考問題：**

(i) 讓學生認識分散式阻斷服務攻擊及殭屍網絡及影響

- 甚麼是分散式阻斷服務攻擊
- 甚麼是殭屍網絡？
- 如何偵測網絡受到分散式阻斷服務攻擊？
- 分散式阻斷服務攻擊對機構網絡會造成怎樣的影響？

(ii) 讓學生明白網絡設計及網絡保安的重要性

- 如何設計網絡能減少分散式阻斷服務攻擊的風險？
- 有那些家居設備較容易成為殭屍網絡的其中一種裝置？試舉一個例子說明。
- 你認為有那些網絡安全措施有助預防及應對分散式阻斷服務攻擊？

示例二：

**模式：**學校通過舉辦「殭屍網絡」攻擊為主題的短片或動畫創作比賽，以加深學生「殭屍網絡」的認識，並反思網絡保安的重要性。

### 2.3.3. 參考資源

**(i) 網頁：**

1. 守網者 – 分散式阻斷服務攻擊
   https://cyberdefender.hk/ddos/
2. 資訊安全網 – 拒絕服務/分布式拒絕服務攻擊
   https://www.infosec.gov.hk/tc/knowledge-centre/ddos
3. 資訊安全網 – 防禦分布式拒絕服務（DDoS）攻擊
   https://www.infosec.gov.hk/tc/best-practices/business/defending-against-ddos-attack
4. 資訊安全網 – 殭屍網絡
   https://www.infosec.gov.hk/tc/knowledge-centre/ctbotnet
5. 香港網絡安全事故協調中心 – 提防 DDoS 勒索攻擊
   https://www.hkcert.org/tc/blog/beware-of-latest-ddos-extortion-attacks
6. 香港網絡安全事故協調中心 – 殭屍網絡偵測及清理
   https://www.hkcert.org/tc/publications/botnet-detection-and-cleanup

# 3. 常見與新興和先進資訊科技相關的科技罪案資訊

## 3.1. 物聯網攻擊

### 3.1.1. 參考資料（香港警務處提供）

[資料來源：守網者 – 物聯網攻擊 https://cyberdefender.hk/iot_attack]

### 甚麼是物聯網？

利用互聯網將手提裝置或家居設備串連一起，並於互聯網互相交換及處理數據和資料，對指定裝置或設備作出指令及控制。例如大家普遍使用的智能手機和平板電腦，甚至是汽車、燈泡和雪櫃，只要配備互聯網功能的， 都是物聯網。

### 使用物聯網的風險

隨着現今科技進步，物聯網發展迅速，海量的物聯網裝置推陳出新，當中大量的用戶資料及龐大的雲端數據庫，自然成為黑客偷取或攻擊的對象。及形形色色的物聯網裝置不斷推出，既不像一般電腦有熟知的操作系統及結構，亦沒有已成熟且針對所有物聯網裝置的保安軟件或保安裝置。很多物聯網裝置於出廠時並沒有提供任何保安措施或保護建議，但於網絡上已開啟一些不必要的服務功能(如:檔案傳輸協定及遠端桌面協定等)。

另外用戶對使用物聯網裝置的保安意識不足，往往為求方便使用而忽略更改高強度密碼的重要性，甚至使用預設密碼令黑客有機可乘。當黑客掌握你物聯網裝置上的用戶名稱及密碼，而你的裝置亦與你其他裝置（如: 路由器、個人電腦、手提電話，甚至數碼門鎖）連繫着，加上已開啟高風險的網絡功能，令黑客除了入侵及接管了你的物聯網裝置外，進而可入侵你其他裝置及奪取權限。然後黑客會於設備安裝惡意程式， 除了你自己會因此而喪失私隱甚至金錢外，你的設備更有機會成為「殭屍網絡」其中一員，成為攻擊其他電腦的幫兇。

### 物聯網保安

- ❖ 很多物聯網裝置均設有預設密碼，使用前必須更改預設密碼，使用複雜組合的密碼更好。若裝置設有雙重認證、電子證書或生物特徵認證，亦應考慮使用。
- ❖ 若裝置上開啟了一些預設服務，例如 FTP、TELNET 等，如沒有必要使用，請關閉這些服務。
- ❖ 如裝置設有活動記錄功能，建議開啟，並不時翻看記錄以偵測可疑的活動。
- ❖ 必須安裝防毒軟件或網絡保安軟件，並定期更新軟件和病毒定義。另外，若能安裝防火牆或系統與網絡監察軟件或硬件裝置更佳。
- ❖ 大部份物聯網裝置採用手機應用程式作為遙控介面，當需要遙距使用時，應為物聯網設置加密傳輸。

### 3.1.2. 參考教學建議

通過多元化的學習活動，讓學生認識物聯網的原理，及明白日常物聯網設備保安的重要性。

## 中學

目的：讓學生認識物聯網的原理，及明白日常物聯網設備保安的重要性。

示例一：

**模式：**學生通過搜集網上相關的新聞資訊、閱讀相關資料〔參考資源第 1-5 項〕，及觀看影片〔參考資源第 6-9 項〕，並於課堂與同學分享或作分組討論，讓他們認識物聯網的原理及物聯網設備保安的重要性。

**思考問題：**

(i) 讓學生認識物聯網的原理及相關設備

- 甚麼是物聯網？
- 物聯網與智慧城市的關係？
- 物聯網如何有助智慧城市的發展？
- 如物聯網受到攻擊會造成怎樣的影響？

(ii) 讓學生明白物聯網設備保安的重要性

- 有那些物聯網設備較容易成為攻擊的其中一種裝置？試舉一個例子說明。
- 如何減少物聯網設備受攻擊的風險？
- 你認為有那些網絡安全措施有助預防及應對物聯網攻擊？

示例二：

**模式：**學生通過編寫程式控制物聯網裝置及感應器，讓他們了解物聯網的用途，以及在編程時要注意的保安事項。

**思考問題：**

(i) 讓學生認識物聯裝置及感應器

- 你認識那些物聯網裝置？
- 你知道物聯網裝置的有那些感應器嗎？試舉一個例子說明。
- 你知道物聯網裝置的感應器是如何收集資訊的？

(ii) 讓學生明白物聯網裝置保安的重要性

- 物聯網及相關裝置有甚麼潛在風險？
- 如何保障物聯網裝置能數據安全及個人私隱？
- 如何減低物聯網受到網絡攻擊？
- 編程時要有那些要注意的物聯網保安需要？

## 小學

**目的：**讓學生認識物聯網，及關注日常物聯網設備保安的重要性。

示例一：

**模式：**讓學生觀看影片〔參考資源第 6-8 項〕，讓學生認識物聯網，及關注日常物聯網設備保安的重要性。

**思考問題：**

(i) 讓學生認識物聯網及相關設備

- 甚麼是物聯網？
- 日常生活會如何應用物聯網？試舉一個例子說明。
- 日常生活會中有那些是物聯網的設備？試舉一個例子說明。

(ii) 讓學生明白物聯網設備保安的重要性

- 有那些家居設備較容易成為攻擊的其中一種裝置？試舉一個例子說明。
- 如何減少物聯網設備受攻擊的風險？

示例二：

**模式：**學校通過舉辦「物聯網設備保安」為主題的海報設計比賽，讓更多學生注意物聯網設備保安的重要性。

### 3.1.3. 參考資源

**(i) 網頁：**

1. 守網者 – 物聯網攻擊
   https://cyberdefender.hk/iot_attack
2. 網絡安全資訊站 – 切勿輕視物聯網的安全
   https://www.cybersecurity.hk/tc/expert-2018-11-30-iot.php
3. 網絡安全資訊站 – 家居網絡安全有辦法
   https://www.cybersecurity.hk/images/resources/infographic_home_network_tc.pdf
4. 香港網絡安全事故協調中心 – 數碼時代 IoT 安全：保護你的物聯網世界
   https://www.hkcert.org/tc/blog/iot-security-in-the-digital-age-protecting-your-connected-world
5. 香港網絡安全事故協調中心 – 物聯網設備（網絡攝影機）保安研究
   https://www.hkcert.org/tc/security-guideline/iot-device-webcam-security-study

**(ii) 影片：**

6. 守網者 – 《全城守網》特輯八・物聯網攻擊
   https://www.youtube.com/watch?v=aF2UrYxuxNQ
7. 守網者 – 物聯網安全・不容小覷
   https://www.youtube.com/watch?v=B2xBMGZ1GPo
8. 香港網絡安全事故協調中心 – 注意物聯網保安 享受智慧生活
   https://www.youtube.com/watch?v=JStt5R7GKkk
9. 數字政策辦公室 – 樂齡 IT 易學站 – 第一堂：認識物聯網（教學短片）
   https://www.it2.gov.hk/tc/onlinecourse/video.php?chapter_id=226

## 3.2. 人工智能

### 3.2.1. 參考資料（香港警務處提供）

[資料來源：守網者 – 人工智能 https://cyberdefender.hk/artificial-intelligence/]

## 甚麼是人工智能？

人工智能（Artificial Intelligence，簡稱 AI）是一種讓機器模擬人類智慧的技術。早在上世紀五十年代，已有科學家提出製造能夠模仿人類學習、決策和解決問題的機器。經過數十年發展，不同 AI 技術已經逐漸成熟，包括：

- **機器學習（Machine learning）**：如語音辨識、自動駕駛
- **自然語言處理（Natural language processing）**：如翻譯、產生和分析文字
- **電腦視覺（Computer vision）**：能夠理解圖像的內容，辨識物件
- **專家系統（Expert system）**：針對高度專業知識的領域，發展系統解決問題，如分析疾病

時至今日，AI 在不同領域已經被廣泛應用。以下是我們日常生活所見的例子：

- **電子商貿**：商店按照你的瀏覽喜好推薦你可能喜歡的產品
- **智能助理**：只說一句「Hey Siri」、「Hey Google」、「小愛小愛」等便可使用手機的智能助理
- **自動導航**：幾乎是能踏足的地方，地圖應用程式都會建議最短的行程路線
- **防盜系統**：鏡頭一旦偵測到有人闖入指定地帶，便會自動發出警報

## 甚麼是「生成式人工智能」（Generative AI）？

生成式 AI 技術能夠產生文字、圖像、聲音、視頻等，當中 ChatGPT 最廣為人知。GPT 的全寫是 Generative Pre-trained Transformer，它是一個基於大型的語言模型訓練而成的聊天機械人。坊間估計，最新的 GPT 4.0 版本收集了超過 10,000 億項參數。除了由 OpenAI 研發的 GPT，坊間還有 Google 的 BERT 和 Meta 的 LLaMA 模型等，各有不同的特點。

## AI 的發展帶來甚麼隱患？

AI 近年急速發展，逐漸融入我們生活的各個領域，為生活帶來便利，而 ChatGPT 的流行更令全球掀起熱烈討論。當 AI 開始取代人類的工作，不法分子同時亦利用 AI 進行犯罪活動。AI 的發展為人類帶來甚麼隱患？

**法律責任：**AI 協助使用者分析問題、提供決策建議和執行指令。假如過程中出現偏差而導致錯誤或損害，責任應由誰負責？例如，無人駕駛汽車發生交通意外導致傷亡或財產損失，責任應由人工智能系統供應商、汽車生產商、駕駛者、道路設計者或其他道路使用者承擔？

**侵犯個人私穩：**AI 系統在進行分類、提出建議等任務時或需要收集和處理大量用戶信息，如用戶出行習慣、身體狀況、通訊內容、瀏覽喜好等，或會對用戶的安全帶來隱憂，例如不法分子可以追踪用戶行蹤、惡意結識用戶進行詐騙等。然而，現時《個人資料（私隱）條例》並沒有覆蓋個人資料以外的個人私隱資訊，市民的私隱應如何被保障？

**資料來源公平性：**AI 系統資料庫的來源取決於開發商的資源和商業考慮，例如某個自然語言處理模型以訓練英語場景為主，資料庫可能偏向取材自英語為母語地區的內容，而訓練人員也可能是來自英語為母語的地區，這或會導致 AI 回應問題時產生對種族、宗教或性別的歧視或偏差。

**道德和倫理：**AI 正面臨倫理、道德和被不法分子不恰當使用的隱患。不法分子可利用 AI 系統降低犯罪成本，如撰寫假新聞影響選舉公平性、深度偽造語音和圖像進行詐騙、撰寫惡意程式進行網絡攻擊等。

**侵犯知識產權：**AI 依賴海量資料進行學習，絕大部分均來自網上免費或付費資訊、電子圖書雜誌等。 知識產權持有人的權益應如何受保障，如何確保版權持有人對資料擁有控制權？

人工智能是人類科技進程中重要的一環，同時也是一張兩面刃。要建立本港在 AI 科研的能力以及推動普及應用 AI，關鍵在於訂立監管框架，令 AI 得以道德和規劃地發展和使用。提升市民利用 AI 技術的素養和人材培訓同樣不可或缺。以上種種都是政府和社會各界急需共同積極協作的一個議題。

### 3.2.2. 參考教學建議

通過多元化的學習活動，讓學生認識人工智能的原理、應用、發展、對人類的影響及產生的問題，亦明白資訊素養、數據安全、人工智能安全的重要性，並以符合道德及守法的態度應用人工智能。

#### 中學

目的：讓學生認識人工智能的原理、應用、發展、對人類的影響，以及會產生的問題，亦明白資訊素養、數據安全、人工智能安全的重要性，以及應用時應有的態度。

示例一：

**模式：**讓學生閱讀相關資料〔參考資源第 1, 3, 4, 9 及 10 項〕，並通過教師教授參考資源〔參考資源第 2 項〕，讓學生學習人工智能理論，並通過實踐機械學習和編程，了解人工智能在視覺、聽覺及語音和語言上的應用，同時，亦讓學生認識人工智能倫理和對社會的影響。

**思考問題：**

(i) 讓學生認識人工智能的理論

- 甚麼是人工智能？在日常生活中有何應用？試舉一個例子。
- 人工智能是如何訓練出來的？
- 人工智能能如何應用在視覺、聽覺及語音和語言上？
- 人工智能的發展對世界有何影響？

(ii) 讓學生學習人工智能的應用

- 你知道甚麼是「提示工程」（Prompt Engineering）嗎？有何應用？試舉一個例子。
- 你知道甚麼是「生成式人工智能」（Generative AI）嗎？有何應用？試舉一個例子。
- 你會如何應用人工智能輔助你的工作？試舉一個例子。
- 你認為人工智能可以取代人類的工作嗎？為甚麼？

(iii) 讓學生認定人工智能倫理

- 你認為人工智能可以辨別是非嗎？為甚麼？
- 你認為人工智能會如何面對兩難局面？
- 人工智能會產生甚麼問題？
- 你會如何安全及符合道德地使用人工智能？

示例二：

**模式：**讓學生閱讀相關資料〔參考資源第 4-8 及 11 項〕，及觀看影片〔參考資源第 12 項〕，並於課堂討論或作小組匯報，讓學生了解人工智能對社會的影響及規管。

**思考問題：**

(i) 讓學生認識人工智能

- 甚麼是人工智能？
- 人工智能如何影響人類的日常生活？
- 人工智能在日常生活中有何應用？試舉一個例子。
- 應用人工智能有何優點和缺點？

(ii) 讓學生了解人工智能的影響

- 你會如何應用人工智能輔助學習？
- 不當使用人工智能會產生甚麼影響？
- 人會用人工智能會犯罪嗎？為甚麼？試舉一個例子。
- 應用人工智能會如何導致數據、私隱、知識產權，以及網絡威脅嗎？

(iii) 讓學生了解人工智能的規管及態度

- 如何保障應用人工智能應用時的數據、私隱、知識產權，以及網絡安全？
- 香港有何法例保障應用人工智能安全？
- 應怎樣以符合道德及守法的態度使用人工智能？

示例三：

**模式**：學校通過舉辦辯論比賽，以「人工智能」為題（例如：道德相關議題、人工智能發展限制等），讓學生了解並反思人工智能對社會的影響及限制。

## 小學

**目的**：讓學生認識人工智能，及關注人工智能裝置安全和應用時應有的態度。

示例一：

**模式**：教師通過教導學生人工智能知識〔參考資源第 1, 3 及 10 項〕，及讓學生觀看影片〔參考資源第 12 項〕，讓學生認識認識人工智能，及關注人工智能安全和應用時應有的態度。

**思考問題：**

(i) 讓學生認識人工智能

- 甚麼是人工智能？
- 日常生活會如何應用人工智能？試舉一個例子說明。

(ii) 讓學生明白智能裝置保安的重要性

- [影片 11] 影片中的機械人為何失靈？
- [影片 11] 如果你是影片中機械人的主人，你會如何避免機械人被黑客入侵？
- 應怎樣以符合道德及守法的態度使用人工智能？

示例二：

**模式**：學校於課後通過安排多元化的與人工智能相關活動（例如：午間遊戲、問答比賽等），讓學生了解認識人工智能的日常應用，並讓學生思考人工智能為他們的日常帶來的方便及對他們的影響。

### 3.2.3. 參考資源

**(i) 網頁：**

1. 守網者 – 人工智能
   https://cyberdefender.hk/artificial-intelligence/
2. 教育局 – 初中人工智能課程單元
   - 初中人工智能課程單元 (第一冊)
     https://www.edb.gov.hk/attachment/tc/curriculum-development/kla/technology-edu/resources/InnovationAndTechnologyEducation/Booklet1_CHI.zip
   - 初中人工智能課程單元 (第二冊)
     https://www.edb.gov.hk/attachment/tc/curriculum-development/kla/technology-edu/resources/InnovationAndTechnologyEducation/Booklet2_CHI.zip
   - 初中人工智能課程單元 (第三冊)
     https://www.edb.gov.hk/attachment/tc/curriculum-development/kla/technology-edu/resources/InnovationAndTechnologyEducation/Booklet3_CHI.zip

3. 全民國家安全教育日 – 人工智能安全
https://www.nsed.gov.hk/national_security/index.php?a=national_security_main_focus&d=ai_security
4. 香港網絡安全事故協調中心 – 人工智能與網絡保安
https://www.hkcert.org/tc/blog/adopt-good-cyber-security-practices-to-make-ai-your-friends-not-foes
5. 香港網絡安全事故協調中心 – 人工智能武器化：網絡安全新領域
https://www.hkcert.org/tc/blog/weaponisation-of-ai-the-new-frontier-in-cybersecurity
6. 數字政策辦公室 – 人工智能道德框架
https://www.digitalpolicy.gov.hk/tc/our_work/data_governance/policies_standards/ethical_ai_framework/
7. 私隱專員公署 – 發布《人工智能 (AI)：個人資料保障模範框架》
https://www.pcpd.org.hk/tc_chi/news_events/media_statements/press_20240611.html
8. 新聞公報 – 立法會十八題：人工智能的發展和應用（2024 年 1 月 24 日）
https://www.info.gov.hk/gia/general/202401/24/P2024012400319.htm
9. 新聞公報 – 立法會五題：發展人工智能（2024 年 1 月 31 日）
https://www.info.gov.hk/gia/general/202401/31/P2024013100367.htm
10. 中西區民政事務處 – 智樂通培訓課程：人工智能簡介小冊子
https://www.had.gov.hk/file_manager/docs/my18_olympism/CW_Guide_Book_AI.pdf
11. 知識產權署 – 版權與人工智能的公眾諮詢 (2024 年)
https://www.ipd.gov.hk/tc/copyright/current-topics/public-consultation-on-copyright-and-artificial/index.html

**(ii)** 影片：

12. 守網者 – 故事繪本「AI 機械人大對決」
https://www.youtube.com/watch?v=eTzRjbGXSaA
13. 私隱專員公署記者會 (11-06-2024) – 《人工智能 (AI)：個人資料保障模範框架》
https://www.youtube.com/watch?v=Z280whvzubE

## 3.3. 深度偽造

### 3.3.1. 參考資料（香港警務處提供）

[資料來源：守網者 – 深度偽造 https://cyberdefender.hk/deep-fake/]

### 甚麼是深度偽造？

深度學習 (Deep learning) 和偽造 (fake) 組成的混合詞，指利深度學習（人工智能的一種技術）進行影像合成以偽造影像。隨著深度偽造的技術愈趨成熟，只要一部智能手機和一個 app 已經可輕易將某人甚至動物的臉移花接木至現有的影片上，甚至改變口形，效果幾可亂真。

這個用 Avatarify 手機 app 製作的「螞蟻呀嘿」短片（原曲為羅馬尼亞組合 O-Zone 2003 年的作品《Dragostea Din Tei》）在內地風靡一時。(圖片來源：互聯網)

深度偽造技術亦擴展至語音層面。現時的人工智能技術只需擷取你五秒鐘的對話，足可以模擬你的聲音創造不同對話。有了影像和聲音的深度偽造技術，便可以虛構出一條從來不存在的影片。

## 深度偽造帶來的風險

著深度偽造技術普及，眼見未必為真，有圖有片亦不一定有真相。根據英國倫敦大學學院於 2008 年發表的一份研究指出，深度偽造被評級為最具威脅的人工智能犯罪隱患。以下是其中一些深度偽造可能會被濫用的情景：

- **身分盜用：**曾有騙徒偽造一家能源公司首席執行官（CEO）的聲線，指示下屬將金錢轉帳至第三方銀行戶口而導致超過 200 萬港元損失。
- **勒索：**不法分子偽造影片，藉威脅公開發布片段損害名聲以向受害人勒索金錢。
- **發佈色情物品：**一般來說，深度偽造的色情物品會把色情片主角的頭像轉換成女藝人的頭像。另外，也有部分屬於「報復式色情」，即未經當事人同意下把該人的頭像轉成情色片主角以損害其名聲。
- **侵害知識產權和個人私隱：**雖然香港法例並沒有訂定肖像權，但未經版權擁有人同意竄改影像片段可以會干犯《版權條例》，而採集載有他人影像相片的目的是辯識個人身分，該收集和使用他人的個人資料也會受《私隱條例》規管。
- **虛假新聞：**政客的頭像經常成為網民「惡搞」的對像，但一般讀者未必有能力分辨真偽。因此，政客利用深度偽造去製造假資訊和輿論的威力往往會很大。

由於應用深度偽造的門檻不斷降低，而「製成品」的像真度也愈來愈高，有科技企業已開始研究自動辨識深度偽造的方法，以人工智能對抗人工智能；而多國正研究從立法及業界規管等不同方向，應對深度偽造帶來的道德和法律問題。

## 防範深度偽造騙案的方法

- 要求對方在鏡頭前做指定動作。
- 作出提問測試對方身份真偽。
- 切勿輕易提供人臉、指紋等生物辨識資料。
- 提防親友及公司職員在視頻或錄音中提出的匯款要求。
- 避免接聽陌生視像通話來電。
- 如對網上資訊、社交專頁或平台真偽有懷疑，可以使用「守網者」網站（https://cyberdefender.hk）的「防騙視伏器」或「防騙視伏 App」手機應用程式，查核可疑電話號碼、網址或收款帳號；或致電「防騙易 18222」熱線查詢。
- 如懷疑不慎受騙，應立即向家長、監護人、教師或學校社工尋求協助。

### 3.3.2. 參考教學建議

通過多元化的學習活動，讓學生認識深度偽造的原理，並具備資訊素養的能力，懂得辨別資訊的真偽、保障知識產權和個人私隱，及以符合道德及守法的態度應用科技。

## 中學

目的：讓學生認識深度偽造的原理，並具備資訊素養的能力，懂得辨別資訊的真偽、保障知識產權和個人私隱，及以符合道德及守法的態度應用科技。

示例一：

**模式：**通過學生搜集網上相關的新聞資訊、閱讀相關資料〔參考資源第 1-10 項〕，及觀看影片〔參考資源第 11 及 12 項〕，並於課堂與同學分享或作分組討論或分組匯報，讓他們認識深度偽造的原理，懂得辨別資訊的真偽，保障知識產權和個人私隱，以符合道德及守法的態度應用科技。

**思考問題：**

(i) 讓學生認識深度偽造技術的原理和影響

- 甚麼是深度偽造？
- 深度偽造技術可以生成甚麼類型的資訊？試舉一個例子說明。
- 如深度偽造技術被濫用會造成怎樣的影響？

(ii) 讓學生明白資訊素養的重要性

- 如何辨別資訊（如：文字、圖像、語音、視訊等）的真偽？
- 如何保障知識產權和個人私隱？
- 如何免避誤墮深度偽造技術生成的陷阱？

示例二：

**模式：**通過校內舉辦短片拍攝比賽，講解資訊真偽（包括視訊、語音、文字），並將學生作品於校園電視播放，讓學生關注要對資訊作事實查核（Fact-check）及辨別資訊的真偽的重要性。

**思考問題：**

(i) 讓學生關注要對資訊作事實查核

- 你認為有圖、有片、有文字是否就是真？
- 你認為何謂真？何謂假？
- 你知道甚麼是深度偽造？甚麼是內容農場嗎？

(ii) 讓學生明白資訊素養的重要性

- 如何辨別資訊（如：文字、圖像、語音、視訊等）的真偽？
- 如何保障知識產權和個人私隱？
- 如何免避誤墮深度偽造技術生成的陷阱？

## 小學

**目的：**讓學生意識深度偽造技術的影響，並培養他們資訊素養的能力，學習辨別資訊的真偽、保障知識產權和個人私隱，及以符合道德及守法的態度應用科技。

示例一：

**模式：**通過教師講解深度偽造技術〔參考資源第 1-10 項〕及讓學生觀看影片〔參考資源第 11-13 項〕，讓學生意識深度偽造技術會產生的問題，並培養他們資訊素養的能力，學習辨別資訊的真偽、保障知識產權和個人私隱，及以符合道德及守法的態度應用科技。

**思考問題：**

(i) 讓學生認識深度偽造技術

- 甚麼是深度偽造？
- 日常生活會如何應用深度偽造技術？
- 如深度偽造技術被濫用會造成怎樣的影響？

(ii) 讓學生資訊素養的重要性

- 如何辨別資訊（如：文字、圖像、語音、視訊等）的真偽？
- 如何保障知識產權和個人私隱？
- 如何免避誤墮深度偽造技術生成的陷阱？

示例二：

**模式：**學校通過舉辦漫畫創作比賽，以辨別資訊真偽（包括視訊、語音、文字）為題材，作品於學校活動或壁報展示，以提高學生辨別資訊真偽及保護個人資料私穩的意識及其重要性。

**思考問題：**

(iii) 讓學生提高學生對資訊真偽的懷疑

- 你認為有圖、有片、有文字是否就是真？為甚麼？
  - 如果你於網上看到一段由某知名人士介紹一種食了會變聰明的食物影片，你會信嗎？
  - 如果有一個陌生來電告知你家人在醫院要求幫忙付醫療費用，你會如何是好？
  - 如果有陌生來電要求以視像通話，你會接聽嗎？
  - 如果有陌生人要求幫你影相放到社交媒體作宣傳用，你會應允嗎？
- 你知道甚麼是深度偽造嗎？

(iv) 讓學生明白資訊素養的重要性

- 如何辨別資訊（如：文字、圖像、語音、視訊等）的真偽？
- 如何保障知識產權和個人私隱？
- 如何免避誤墮深度偽造技術生成的陷阱？

### 3.3.3. 參考資源

**(i) 網頁：**

1. 守網者－深度偽造
   https://cyberdefender.hk/deep-fake/
2. 守網者－分辨虛假資訊
   https://cyberdefender.hk/fakenews/

3. 全民國家安全教育日 – 人工智能安全
   https://www.nsed.gov.hk/national_security/index.php?a=national_security_main_focus&d=ai_security
4. 資訊安全網 – 深度偽造
   https://www.infosec.gov.hk/tc/knowledge-centre/deepfake
5. 香港網絡安全事故協調中心 – 人工智能與網絡保安
   https://www.hkcert.org/tc/blog/adopt-good-cyber-security-practices-to-make-ai-your-friends-not-foes
6. 香港網絡安全事故協調中心 – 人工智能武器化：網絡安全新領域
   https://www.hkcert.org/tc/blog/weaponisation-of-ai-the-new-frontier-in-cybersecurity
7. 香港網絡安全事故協調中心 – 釣魚警報 – 公眾應對利用 AI Deepfake 技術的偽造視像會議詐騙提高警惕
   https://www.hkcert.org/tc/security-bulletin/phishing-alert-phishing-campaigns-targeting-instagram-backup-codes-to-bypass-2fa-on-the-rise_20240207
8. 香港網絡安全事故協調中心 – 深度偽造：有圖未必有真相
   https://www.hkcert.org/tc/blog/deepfake-where-images-don-t-always-speak-truth
9. 私隱專員公署推防騙六招 – 私隱專員示範深度偽造實時換臉
   https://www.pcpd.org.hk/tc_chi/news_events/media_statements/press_20240801.html
10. 新聞公報 – 立法會九題：打擊涉及深度偽造的詐騙罪案
    https://www.info.gov.hk/gia/general/202406/26/P2024062600193.htm

**(ii)** 影片：

11. 私隱專員公署 – 生成式人工智能「深度偽造」（Deepfake）模擬影片
    https://www.youtube.com/watch?v=76x0aOzLHVo
12. 香港網絡安全事故協調中心 – 深度偽造: AI 換臉示範
    https://www.youtube.com/watch?v=MEPzI-bnhTQ
13. 香港警務處 – 愚人節 x 明福俠
    https://www.youtube.com/watch?v=9dvwhhZzebg

## (四) 參考資料：

1. 守網者－網絡罪案
   https://cyberdefender.hk/cybercrime/
2. 守網者－網絡安全事件簿–故事繪本
   https://cyberdefender.hk/story/
3. 教育局網絡安全教師參考資源
   https://www.edb.gov.hk/cybersecurity
4. 教育局－媒體和資訊素養－學與教資源
   https://www.edb.gov.hk/tc/curriculum–development/kla/technology–edu/resources/mil/resources.html
5. 教育局－資訊素養及電子安全相關支援－香港學生資訊素養
   https://www.edb.gov.hk/il/chi
6. 教育局－「共建更好的網絡世界」電子學習資源套
   https://www.hkedcity.net/parent/learning/ict/page_58fd847d316e83c22a000000
7. 教育局－「聰明 e 主人」電子學習資源套
   https://www.hkedcity.net/teencampus/zh–hant/resource/5b28a46b32c8bf8d553c9869
8. 教育局－價值觀教育漫畫資源「未來」教你應做的十件事–單元八謹慎上網
   漫畫：https://www.edb.gov.hk/attachment/tc/curriculum–development/4–key–tasks/moral–civic/Comic/8_Comic.pdf
   教師錦囊：https://www.edb.gov.hk/attachment/tc/curriculum–development/4–key–tasks/moral–civic/Comic/8_TeachingNote.pdf
9. 教育局－公民、經濟與社會（中一至中三）學與教資源
   中一：https://www.edb.gov.hk/tc/curriculum-development/kla/pshe/references-and-resources/ces/support_materials_S1.html
   中二：https://www.edb.gov.hk/tc/curriculum-development/kla/pshe/references-and-resources/ces/support_materials_S2.html
   中三：https://www.edb.gov.hk/tc/curriculum-development/kla/pshe/references-and-resources/ces/support_materials_S3.html
10. 教育局－價值觀教育－性教育的相關「生活事件」教案
    https://www.edb.gov.hk/tc/curriculum-development/4-key-tasks/moral-civic/L_and_T/Sex_Education/SexEd_LEA.html
11. 教育局－理財教育動畫系列
    https://www.edb.gov.hk/tc/curriculum-development/kla/pshe/references-and-resources/cross-curricular-resources/financial_education_animation_series.html
12. 香港警務處公共關係部–《青少年罪行誌・師長攻略》
    https://www.police.gov.hk/ppp_tc/03_police_message/ycpb.html
13. 投委會–網上詐騙
    https://www.ifec.org.hk/web/tc/moneyessentials/scams/scam–websites.page
14. 網絡安全資訊站
    https://www.cybersecurity.hk/tc/index.php

教育局
Education Bureau
課程支援分部 科技教育組

香港警務處
HONG KONG POLICE FORCE
網絡安全及科技罪案調查科

https://www.edb.gov.hk/cybersecurity