網絡安全
學與教資源

數碼資產與相關風險管理

教育局 與 香港警務處

二零二三年十月

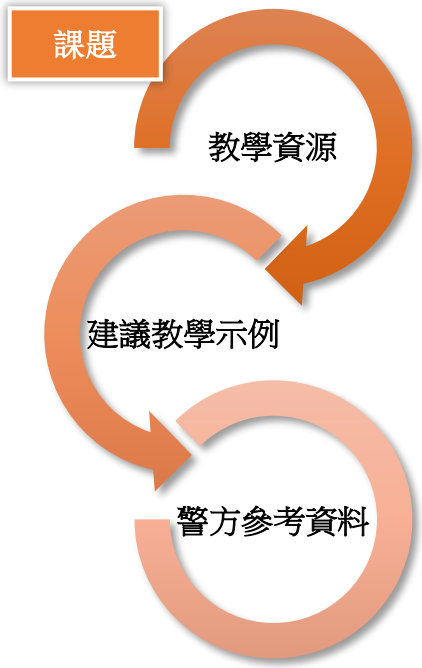
資源使用方法

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目標

（二） 建議教學模式：為學校提供可參考的教學模式，學校亦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



- 提供與課題相關的資料網頁及影片連結，教師可通過相關網頁獲取更多資訊

- 提供與課題相關的建議教學示例，教師可參考相關點子，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

- 提供載列於警方「守網者」網頁與課題相關的參考資料，讓教師能了解課題

（四） 參考資料：為學校提供更多的網上參考資源

學習對象： 中學適用

學習目標： 學生完成學習單元後，能夠：

1. 認識數碼資產及其應用
2. 評估數碼資產的安全風險及其所帶來的挑戰
3. 了解培養資訊素養能力的重要性
4. 了解遵守網絡法規的重要性及明白法律對網上活動的保護程度和風險。
5. 培育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. 讓學生認識數碼資產及其應用
2. 讓學生評估數碼資產應用帶來的安全風險、挑戰及相關罪案資訊
3. 教導學生如何保護數碼資產及自我保護

(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，並讓學生想想日常生活中有否遇到相似的情況，思考及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，學會自學及自我保護。

2. 善用課時：

教師可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，了解學生對相關課題的掌握。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（海報／漫畫／填色）、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，以及學會保護自己。

4. 善用學時：

學校可安排於早會／週會、班主任或德育及公民課、聯課活動和校園電視台等課堂以外的時間，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自我保護。

(三) 教學資料：

1. 數碼資產與相關風險

1.1. 電子貨幣及流動支付

1.1.1. 教學資源

1. 守網者 – 電子貨幣及流動支付〔相關內容詳列於第 1.1.3 節〕
   https://cyberdefender.hk/mobile–payment/
2. 教育局 – 初中科技教育學習領域課程資源《金錢的性質》
   https://www.edb.gov.hk/attachment/tc/curriculum-development/kla/technology-edu/resources/business-edu/E4-4_Nature_of_Money-Chi.pdf
3. 政府資訊科技總監辦公室 – 網絡安全資訊站：安全使用流動支付服務
   https://www.cybersecurity.hk/tc/learning-epayment.php
4. 投委會 – 虛擬資產
   https://www.ifec.org.hk/web/tc/financial-products/fintech/ico-bitcoin/index.page
5. 投委會 – 手機取代現金
   https://www.ifec.org.hk/web/tc/financial-products/fintech/mobile-phones-replace-cash.page
6. 香港金融管理局 – 電子錢包和預付卡
   https://www.hkma.gov.hk/chi/smart-consumers/e-wallets-and-prepaid-cards/
7. 香港金融管理局 – 電子支付和轉帳
   https://www.hkma.gov.hk/chi/smart-consumers/e-payment-and-transfer/
8. 香港金融管理局 – 轉數快
   https://www.hkma.gov.hk/chi/smart-consumers/faster-payment-system/
9. 香港金融管理局 – 儲值支付工具的監管制度
   https://www.hkma.gov.hk/chi/key-functions/international-financial-centre/stored-value-facilities-and-retail-payment-systems/regulatory-regime-for-stored-value-facilities/
10. 香港金融管理局 – 公眾教育短片〔影片〕
    https://www.hkma.gov.hk/chi/smart-consumers/public-education-videos/

1.1.2. 教學示例

通過多元化的學習活動（如：閱讀資料、小組分享、課外活動／比賽等）於課堂內外，讓學生認識各種電子貨幣及流動支付方式，並了解相關法例及監管，藉此提高學生對相關陷阱的危機意識，加強他們的自我保護能力。

示例一（專題報告／分組匯報）：

目的：讓學生認識「電子貨幣」、「流動支付」、「虛擬貨幣」以及「虛擬資產」等概念，並了解當中存在的風險，提高學生對相關陷阱的危機意識，加強他們的自我保護能力。

模式：學生通過資料搜集、分析及歸納，分組完成專題報告及匯報成果，並由學生及教師分享組別提問及回饋。

思考問題：

(i) 讓學生認識電子貨幣及流動支付的概念及種類〔參考教學資源第 1, 3, 5-10 項〕
- 甚麼是電子貨幣及流動支付？（學生可以通過預先搜集相關資料作預先了解）
- 試列舉兩個例子及分別簡述電子貨幣及流動支付在日常生活的應用。
- 在使用時是否存在安全風險？為甚麼？
- 如何安全使用電子貨幣及流動支付？

(ii) 讓學生認識「虛擬貨幣」〔參考教學資源第 4 項〕
- 甚麼是「虛擬貨幣」？
- 試列舉兩個例子及分別簡述「虛擬貨幣」在日常生活的應用。
- 在使用時是否存在安全風險？為甚麼？

(iii) 讓學生認識「虛擬資產」〔參考教學資源第 4 項〕
- 甚麼是「虛擬資產」？
- 試列舉兩個例子及分別簡述其在日常生活的應用。
- 應如何保護「虛擬資產」？

(iv) 延伸問題，讓學生想想：
- 現時，電子貨幣及流動支付能否取代現金交易？為甚麼？
- 在使用電子貨幣及流動支付時是否存在安全風險？為甚麼？
- 可以如何避免墮入相關陷阱？
- 如果受騙，應如何處理及持守甚麼態度？

<u>示例二（教案與練習）：</u>

目的：讓學生認識甚麼是金錢及認識不同形式的貨幣。

模式：教師參考《金錢的性質》課程資源，並按學生學習需要調整教案及課後練習。

思考問題：

(i) 讓學生認識金錢是甚麼？〔參考教學資源第 2 項〕
- 金錢有甚麼作用？為何需要金錢？
- 日常生活中，貨幣有哪些形式？有哪些使用的例子？
- 在使用時是否存在安全風險？為甚麼？
- 如何安全使用各種形式的貨幣作交易支付呢？

(ii) 延伸問題，讓學生想想：
- 是否需要存在不同類型的貨幣？為甚麼？
- 如何避免受騙？如果受騙，應如何處理及持守甚麼態度？

<u>示例三（課外活動）：</u>

目的：讓學生認識金錢、實體與虛擬貨幣等概念，提醒學生如何安全使用不同形式貨幣，了解當中風險，思考如何避免受騙，以及如果受騙，應如何處理及持守甚麼態度。

模式：學生設計海報／漫畫，選出較好的學生作品於校內展示，更可作為教材。

建議主題：

(i) 介紹不同形式的貨幣及其重要性，如何安全使用不同形式的貨幣，以免受騙

(ii) 如何提升持份者對不同形式貨幣／虛擬資產的認識，並了解當中風險

(iii) 如何面對風險，作出合適的選擇？應如何處理及持守甚麼態度

1.1.3. 由警方提供的參考資料〔相關內容節錄自「守網者」網頁〕

電子貨幣及流動支付

隨著流動科技及雲端運算技術廣泛應用，以及金融科技發展迅速，各式電子支付及流動支付日漸普及。大眾除了可以透過網上銀行進行各種的交易外，亦可透過電子錢包付款及收款，此外，部分的商店亦會使用虛擬點數作為付款及收款的方式。

坊間流行的不同術語，例如「電子貨幣」、「數碼貨幣」、「虛擬貨幣」、「加密貨幣」、「虛擬資產」等，究竟他們之間有甚麼分別呢？

(A) 「電子貨幣」VS「數碼貨幣」

各國對「電子貨幣」、「數碼貨幣」、「虛擬貨幣」、「加密貨幣」等並無統一定義。一般而言，「電子貨幣」和「數碼貨幣」兩者互相通用，指以數碼記賬的方式代替使用現金交易的貨幣系統。透過數碼貨幣支付，消費者無須攜帶大量現金，商戶同時無須人手點算現金，有助提高交易的效率和安全。

儲值支付工具（如八達通）和信用卡可分類為「電子貨幣」。由於它們都以數碼方式記賬，並以法定貨幣結算的交易系統，一般會歸類為「電子支付方式」。至於在智能裝置上使用的 Apple Pay 和 Google Pay 是將實體信用卡代幣化（Tokenised） 的流動支付方法。

(B) 「數碼貨幣」VS「虛擬貨幣」VS「虛擬資產」

電子貨幣主要劃分為以下兩類，即

(i) 有實體貨幣或機構支持；或

(ii) 沒有實體貨幣或機構支持。

有實體貨幣或發行機構支持和管理，而又可於不同平台廣泛使用的電子貨幣系統，例如：數字人民幣（又稱 DCEP 或 E–CNY）。

沒有實體貨幣或機構支持的電子貨幣，一般會歸類為「虛擬貨幣」。由於「虛擬貨幣」不具備貨幣特性，因此香港金融管理局界定它為「虛擬資產」。虛擬資產雖然沒有實體，但它在特定社群裡仍可用作購買商品和服務。

虛擬資產可分為：

(i) 是否有發行機構中央管理；和
(ii) 能否兌換成法定貨幣。

有發行機構管理的虛擬資產，例如：iTunes 禮品卡、Google Play 禮品卡、支援不同遊戲發行商的遊戲點數卡等，它們能在指定平台使用，而這些「點數卡」一般分類為「電子代幣」。

沒有單一發行機構管理的虛擬資產，例如：比特幣（Bitcoin）、以太幣（Ethereum）和泰達幣（Tether）等虛擬資產，是使用去中心化方式發行。這些虛擬資產能在跨平台使用，坊間也有機構把它們兌換成現金。

(C) 儲值支付工具

根據 2016 年生效的《支付系統及儲值支付工具條例》，儲值支付工具須受金融管理局的的發牌制度規管。截至 2022 年 2 月，本港共有 15 個儲值支付工具持牌人。儲值支付工具包括八達通、AlipayHK、PayMe、PayPal Hong Kong、Tap & Go、TNG、WeChat Pay HK 等都受條例規管，以保障消費者的權益。

現時，未有實名登記的儲值支付工具戶口的儲值上限為港幣 3,000 元，以降低戶口用作洗黑錢活動的風險。[1]

(D) 快速支付系統

快速支付系統，又稱「轉數快」，是 2018 年金融管理局推出的支付金融基建，由香港銀行同業結算有限公司負責運作。轉數快能二十四小時為消費者及商戶提供安全、有效率以及快捷的零售支付服務，以港元及人民幣進行交易，手續費全免。截至 2022 年 2 月，共有超過 200 間銀行及種儲值支付工具營運商等參與。轉數快用戶能進行跨平台、跨銀行的實時轉帳。

網上銀行或快速支付系統用戶在其中一個戶口登記使用轉數快後，有關登記的手機號碼及電郵地址便會綁定在該戶口。如需進行轉帳，只需輸入收款電話號碼、電郵地址、或掃描特定二維碼即可。

[1] 立法會九題：儲值支付工具儲值額的限制（2022）。
https://www.info.gov.hk/gia/general/202206/08/P2022060800241.htm

1.2. 加密貨幣

1.2.1. 教學資源

1. 守網者 – 加密貨幣〔相關內容詳列於第 1.2.3 節〕
   https://cyberdefender.hk/cryptocurrency/
2. 立法會四題：推動虛擬資產市場發展 （2022 年 11 月 30 日）
   https://www.info.gov.hk/gia/general/202211/30/P2022113000371.htm
3. 財經事務及庫務局 – 《有關香港虛擬資產發展的政策宣言》（2022）
   https://gia.info.gov.hk/general/202210/31/P2022103000455_404825_1_1667173459238.pdf
4. 投委會 – 「投資奇異博士 Dr Ben」短片系列：比特幣〔影片〕
   https://www.ifec.org.hk/web/tc/other-resources/multimedia/video/dr-ben-the-doctor-of-investments.page?videoKey=bitcoin
5. 投委會 – 虛擬資產
   https://www.ifec.org.hk/web/tc/financial-products/fintech/ico-bitcoin/index.page
6. 投委會 – 虛擬資產的監管與保障
   https://www.ifec.org.hk/web/tc/blog/2022/11/regulation-and-protection-of-virtual-assets.page
7. 投委會 – 了解虛擬資產的風險
   https://www.ifec.org.hk/web/tc/financial-products/fintech/ico-bitcoin/virtual-asset-risks.page
8. 投委會 – 基本概念：比特幣／「加密貨幣」
   https://www.ifec.org.hk/web/tc/financial-products/fintech/ico-bitcoin/basic-concept-bitcoin.page
9. 投委會 – 了解風險：比特幣／「加密貨幣」
   https://www.ifec.org.hk/web/tc/financial-products/fintech/ico-bitcoin/risks-bitcoin.page
10. 投委會 – ICO、比特幣及其他「加密貨幣」
    https://www.ifec.org.hk/web/tc/financial-products/fintech/ico-bitcoin/ico-bitcoin-cryptocurrencies.page
11. 投委會 – 比特幣：不可不知的 5 個要點
    https://www.ifec.org.hk/web/tc/financial-products/fintech/ico-bitcoin/five-things-about-bitcoin.page
12. 投委會 – 加密貨幣 識得至好投資
    https://www.ifec.org.hk/web/tc/blog/2021/09/dont-get-swept-up-by-the-investment-hype.page
13. 投委會 – 提防加密貨幣騙案
    https://www.ifec.org.hk/web/tc/blog/2021/09/beware-of-cryptocurrency-scams.page
14. 投委會 – 在數碼世代保管個人財產
    https://www.ifec.org.hk/web/tc/blog/2023/06/managing-finances-in-a-digital-era.page
15. 香港金融管理局 –《虛擬資產與貨幣》2018
    https://www.hkma.gov.hk/chi/news–and–media/insight/2018/09/20180921/

1.2.2. 教學示例

讓學生認識各種虛擬資產及加密貨幣，並了解相關的網絡技術，提高學生對網絡安全的關注，以及相關陷阱的危機意識。

示例一（跨科協作）：

目的：通過不同科目的協作，以多角度方式，讓學生了解貨幣與資訊科技的關係、加密貨幣的技術、由資訊科技發展至加密貨幣的出現等議題。

模式：商業科目與電腦科目合作，以專題研習方式，讓學生閱讀新聞、政府文件及官方資料，並分組搜集、分析及歸納資料，再於課堂討論及匯報，同學互相提問及教師回饋。

思考問題：

(i) 商業科目：讓學生認識虛擬資產及加密貨幣的概念及種類〔參考教學資源第 1-15 項〕
- 甚麼是「虛擬資產」？日常生活中，是否常見？有何應用？
- 甚麼是「加密貨幣」？日常生活中，是否常見？有何應用？
- 使用加密貨幣是否安全？為甚麼？

(ii) 電腦科目：讓學生認識加密貨幣應用技術和資訊科技的關係〔參考教學資源第 1, 5,8 項〕
- 加密貨幣的買賣、存款及交易應用了哪些技術？
- 這些技術有甚麼優點和缺點？
- 這些技術是否提升了加密貨幣的安全？為什麼？

(iii) 延伸問題，讓學生想想：
- 如現存一筆投資金額，你會否選擇購買加密貨幣嗎？為甚麼？
- 騙徒會如何騙取他人的虛擬資產？如何避免？
- 如果受騙，應如何處理及持守甚麼態度？

示例二（觀看影片）：

目的：通過觀看相關影片，加深學生對加密貨幣的認識，提高他們注意貨幣的多樣性，以及他們對加密貨幣及虛擬資產風險的認識，避免他們受騙。

模式：學生觀看影片（「投資奇異博士 Dr Ben」短片系列：比特幣），提問學生對加密貨幣的認識，並讓學生反思日常生活中只應用加密貨幣的可行性?。〔參考教學資源第 4 項〕

思考問題：

(i) 影片中受訪者對加密貨幣都有不同的見解，那你認為應如何選擇？

(ii) 應否繼續購買加密貨幣？為甚麼？

(iii) 延伸問題，讓學生想想：
- 如現存一筆投資金額，你會否選擇購買加密貨幣嗎？為甚麼？
- 騙徒會如何騙取他人的虛擬資產？可以如何避免？
- 如果受騙，應如何處理及持守甚麼態度？

1.2.3. 由警方提供的參考資料〔相關內容節錄自「守網者」網頁〕

1. 甚麼是加密貨幣?

由於加密貨幣不備貨幣特性，因此香港政府把它界定為「加密資產」或「虛擬資產」

於 2008 年，一位自稱中本聰（Satoshi Nakamoto）的人士在網絡上發表了一篇論文介紹一個點對點電子貨幣系統—比特幣（Bitcoin），並以區塊鏈（Blockchain）作為記帳。整套比特幣系統於 2009 年開始運作，成為世上第一種去中心化（decentralization）的加密資產，整套系統均毋須經過任何銀行或中介便能操作。

2010 年 5 月，一位美國人花了 10,000 個比特幣購買了兩個薄餅，成為實體世界第一項以比特幣進行的交易。

隨著比特幣的成功，其他加密資產陸續出現。至今全球有超過 17,000 種加密資產在網絡上活躍流通，以比特幣（Bitcoin）、以太幣（Ether）、泰達幣（Tether）（又稱 USDT）等最為活躍。

2. 為甚麼叫「加密」資產?

加密資產是一種虛擬資產。它需依附在一個加密資產地址，並不能以實體方式存在。電視上或網絡上看到的實體比特幣，只是構想出來的圖像。

加密資產是利用密碼學原理，由自願連接加密資產網絡的電腦共同運算，確保交易完整性及控制交易。加密資產一般透過區塊鏈技術，以建立去中心化及分散式的公開帳目（open ledger）記錄交易，令加密資產能在網絡上流通。加密資產的交易紀錄是公開透明的，任何人都可以查看區塊鏈記載的交易紀錄（如透過 blockchain.com 網站）。

3. 虛擬資產的基本元素：

(i) 區塊鏈

由區塊（block）串連成區塊鏈。以比特幣為例，每個區塊的容量大約是 1MB。系統每隔約十分鐘便把這段時間的交易記錄製作成區塊，附加在原有區塊鏈的末端。區塊鏈能記載所有交易記錄的公開帳目，而帳目資料包括：（i）付款人加密資產地址、（ii）收款人加密資產地址、（iii）交易日期和時間、（iv）交易金額及（v）交易序號。資料一經寫入區塊鏈便不能修改或刪除。帳目並無記錄包括能辨別用戶身份的資料，如 IP 地址、付款人或收款人姓名等，因此交易的隱密性甚高。

(ii) 加密貨幣地址

它像銀行帳戶號碼或郵寄地址，是公開顯示予任何人用作收款。該地址是按特定數學公式隨機產生的加密公鑰 （public key）。每一個加密鑰組合包含一條公鑰和一條私鑰 （private key），各自由數字和英文字母組合而成。加密鑰組合可在不同公開來源取得 （如 http://walletgenerator.net）。

(iii) 私鑰

它像郵箱鑰匙，它的持有人可謂擁有儲存在相關地址的加密資產。私鑰持有人能將有關加密資產轉至另一地址。每個地址只有一條對應的私鑰。由於私鑰組合數目繁多，即使以超級電腦的運算能力，要破解地址的私鑰可能需要花上數百年。惟一旦遺失了私鑰，便不能取回相關地址的虛擬資產。如把私鑰告訴他人，他人便可盜取你的虛擬資產。

(iv) 錢包

它像鑰匙包。一個錢包能存放多個虛擬資產地址及私鑰。錢包能以軟件或硬件形式存在，一般以密碼保護。軟件錢包通常包含軟件用作傳送加密資產。持有人能將有關虛擬資產轉至另一地址。每個地址只有一條對應的私鑰。由於私鑰組合數目繁多，即使以超級電腦的運算能力，要破解地址的私鑰也可能需花上數百年。

4. 甚麼是「挖礦」？

以比特幣為例，自願連接比特幣網絡的電腦（又稱「節點」或「礦工」）共同記錄一式一樣的區塊鏈並共同核實帳目。在參與核實交易記錄的過程中，最快解決加密學難題的節點會得到加密資產作獎勵，這個過程稱為「挖礦」（mining）。該獎勵包括由系統新產生的加密資產和有關交易支付的交易費。

為了防止過度挖礦，系統限制了產生比特幣的上限定為 2,100 萬枚。系統並有減半基制，即每隔約四年，系統獎勵礦工的比特幣數量便會減少 50%。換句話說，比特幣可能會在 2140 年掘完。當所有比特幣被掘完後，礦工們只能靠收取交易費作為獎勵。

5. 如何買賣虛擬資產

網上有不同平台買賣虛擬資產。在香港有以下三大途徑購買虛擬資產：

(i) 虛擬資產櫃員機

虛擬資產買家只需在該櫃員機以按鍵或掃描二維碼方式輸入虛擬資產地址，並將現鈔放入櫃員機，相應的虛擬資產便會即時儲存至該地址，毋須登記。要以賣家身份將虛擬資產轉成現金，用家只需輸入私鑰和出售金額，相關幣值的現鈔便會彈出，虛擬資產亦隨即被轉帳至櫃員機所屬公司的地址。

(ii) 虛擬資產交易所平台

在香港的交易所平台開設帳戶一般需要身份證明文件、住址證明、銀行戶口等資料。註冊用戶需要登入交易所平台方可買賣虛擬貨幣。在香港的交易所平台開設帳戶一般需要身份證明文件、住址證明、銀行戶口等資料。註冊用戶需要登入交易所平台方可買賣虛擬資產。

(iii) 場外交易平台

指虛擬資產交易所或櫃員機以外的平台或渠道。場外交易平台包括用戶對用戶（C2C）的平台，如拍賣網站或討論區。虛擬資產的售價、付款及送貨方式由買賣雙方自訂。

6. 虛擬資產相關罪行

(i) 以虛擬資產收取犯罪得益

由於虛擬資產交易雙方的個人資料或 IP 地址均不會記錄在區塊鏈內，因此它具有極高的匿名性。不少罪犯在進行勒索、敲詐、援交騙案、網上情緣騙案等過程中，以收取虛擬資產取代金錢以隱藏身份並進行清洗黑錢活動。

(ii) 以虛擬資產作為藉口行騙

例子有網上購物騙案罪犯訛稱出售虛擬資產或挖礦機，或投資騙案罪犯以虛構虛擬資產投資計劃作餌誘。

(iii) 不當使用電腦／入侵電腦以挖礦

不法分子入侵電腦系統盜取加密資產，或注入惡意程式碼利用他人電腦進行挖礦。

7. 投資虛擬資產的風險

(i) 不受法例監管

現時，虛擬資產在香港及很多國家都不是法定貨幣，投資虛擬資產亦不受當地金融機構監管。消費者或投資者在香港及海外進行虛擬資產交易，難免缺乏保障。

(ii) 沒有內在價值

虛擬資產一般沒有實質基礎，因此其格價波幅十分巨大。同時，生產虛擬資產的成本極低（近乎零成本！），網上也有不少教材教授如何在十分鐘內產生新代幣。過往幾年曾經出現過「首次代幣發行」（ICO）熱潮，即發起人以發行虛擬資產方式為投資項進行眾籌，投資者會因為憧憬投資收益會反映在代幣格價上因而買入代幣。此類投資估值透明度低，對投資者亦沒有法定保障，因此風險極高。

(iii) 容易墮入投資陷阱

坊間有騙徒以出售「雲端挖礦機」或投資虛擬資產名義等行騙，誘騙對虛擬資產認識不深的投資者投入巨額資金或將虛擬資產轉入騙徒帳戶後，平台便會停止運作或顯示投資失利或回報極低，投資者亦未能取回本金。

1.3. 非同質化代幣 （Non-fungible token (NFT)）

1.3.1. 教學資源

1. 守網者 – 非同質化代幣 （NFT）〔相關內容詳列於第 1.3.3 節〕
   https://cyberdefender.hk/non–fungible–token/
2. 投委會 – 一圖了解 NFT
   https://www.ifec.org.hk/web/tc/financial-products/fintech/ico-bitcoin/NFT-at-a-glance.page
3. 投委會 – NFT 與藝術品投資
   https://www.ifec.org.hk/web/tc/blog/2022/11/investing-in-nfts-and-art.page
4. 投委會 – NFT 是數碼熱潮，還是真實資產?
   https://www.ifec.org.hk/web/tc/blog/2021/05/non-fungible-token.page
5. 立法會十題：數碼資產交易 (2022 年 2 月 16 日)
   https://www.info.gov.hk/gia/general/202202/16/P2022021600157.htm
6. 財經事務及庫務局 – 有關香港虛擬資產發展的政策宣言 (2022 年 10 月 31 日)
   https://gia.info.gov.hk/general/202210/31/P2022103000455_404825_1_1667173459238.pdf
7. 司長隨筆 – 穩慎推進虛擬資產業在港發展 (2022 年 11 月 3 日)
   https://www.fso.gov.hk/chi/blog/blog20221113.htm
8. 香港電腦保安事故協調中心 – NFT 熱潮下，如何保護自己的 NFT 資產
   https://www.hkcert.org/tc/blog/nft-boom-how-to-protect-your-nft-assets

1.3.2. 教學示例

讓學生認識 NFT 的原理、製作及相關知識，了解 NFT 的應用及價值，提高學生對市場上買賣 NFT 及虛擬貨幣等虛擬資產存在風險的危機意識，以保護自己避免誤墮相關產品騙案陷阱。

示例一（跨科協作）：

目的：各科協作讓學生認識 NFT 的原理、製作及相關知識，了解 NFT 的應用及價值，例如：視藝科教授學生 NFT 圖像設計技巧；商業科目可以介紹 NFT 的商業應用和價值；電腦科可以介紹 NFT 相關技術及網絡安全相關議題，藉此加強學生對 NFT 及虛擬貨幣等虛擬資產的認識及提高學生對其風險的危機意識。

模式：商業科目、電腦科目與視覺藝術科目跨科協作，並舉辦校本 NFT 圖像設計、製作及營銷比賽。學校更可以邀請外間機構講解 NFT 的應用、技術及安全性等。

思考問題：

(i) 視覺藝術科目：學生認識 NFT 圖像設計技巧〔參考教學資源第 1-3 項〕

- NFT 是甚麼類型的檔案？（數碼圖像、影音、及短片等等）
- NFT 圖像設計與一般電腦圖像設計有何不同？
- 欣賞和比較不同的 NFT 圖像，並了解其設計要點。
- 如何設計合適的 NFT 圖像？學生設計 NFT 圖像。

(ii) 商業科目：學生認識 NFT 的商業應用和價值〔參考教學資源第 1-7 項〕
- 甚麼是「虛擬資產」？
- 甚麼是「非同質化代幣」（NFT）？其發展如何？
- 現金貨幣、電子貨幣與虛擬資產有甚麼關係？有何分別？
- NFT 在商業上有甚麼應用例子？
- 投資 NFT 類產品有風險嗎？為甚麼？
- 如何避免墮入投資陷阱？

(iii) 電腦科目：學生了解 NFT 技術及相關數據和網絡安全風險〔參考教學資源第 1,2,7,8 項〕
- NFT 應用了哪些技術？（例如：元宇宙 (Metaverse)、區塊鏈(Blockchain)）
- 這些技術可以應用到哪些領域？
- 如何保護個人資料私隱及 NFT 資產？
- 進行 NFT 交易會否帶來數據和網絡安全風險？

示例二（新聞研讀）：

目的：學生通過閱讀有關 NFT 的最新發展資訊及相關政府政策，以了解虛擬資產在香港的發展情況、相關的投資及網絡安全風險。

模式：於課堂以外課時，例如：閱讀課、網上預習、班主任課，讓學生閱讀相關資料，並回答問題及反思。亦可請學生在週會分享。

思考問題：〔參考教學資源第 1,2,5-8 項〕

(i) 甚麼是 NFT？
(ii) 現時政府對虛擬資產業務的發展有何政策？
(iii) 你對虛擬資產在香港的發展有何想法？為甚麼？
(iv) 延伸問題，讓學生想想：
- 如現存一筆投資金額，你會購買 NFT 嗎？為甚麼？
- 騙徒如何騙取他人的 NFT？如何避免？
- 如果受騙，應如何處理及持守甚麼態度？

1.3.3. 由警方提供的參考資料〔相關內容節錄自「守網者」網頁〕

1. 甚麼是非同質化代幣 （NFT）?

NFT 是新興另類虛擬資產投資，常見的 NFT 包括數碼圖像、影音、及短片等等，並透過加密形式放到區塊鏈。該 NFT 私密鑰匙的擁有人會視為該作品的真正擁有人。

2. NFT 與比特幣、以泰幣、泰達幣等有共通點嗎?

NFT 的概念跟這些代幣差不多。以比特幣為例，當比特幣存放在特定地址，該地址私密鑰匙的擁有人可視作擁有加密資產，NFT 的概念只不過將比特幣換成一件數碼藝術品而已，而且同樣存放在加密資產錢包或平台內。跟傳統貨品買賣不同，而買賣一件 NFT 基本上是以虛擬資產（如以泰幣）支付。

3. 與 NFT 有關的風險

最常見是釣魚詐騙，騙徒假冒 NFT 錢包平台發放短訊或電郵，誘騙進入假網站並輸入錢包恢復短語（recovery phrase）[2]，或透過假網站彈出虛假交易信息，要求用戶連接錢包並確認交易。用戶一旦簽署確認交易，錢包內的 NFT 便會被轉走。另一情況是用戶手機或電腦遭木馬程式等入侵，黑客進入錢包並將資產轉走。

其次，投資者和收藏者也要留意盜版和侵權 NFT 藝術品的風險。由於數碼圖像、影音藝術品等易於複製，侵權者也易於把實體藝術品未經授權製作成 NFT 藝術品出售圖利。因此，投資者或收藏者可能購入盜版或侵權藝術品而不自知。

再者，不法分子可能會對 NFT 藝術品進行「洗售」（wash trading，又稱「假售回購」），即在短時間內進行多次往返買賣，以抬高 NFT 藝術品價格。「洗售」是古老的證券市場操縱方式，在香港證券屬於違法行為，但操縱 NFT 藝術品和虛擬商資產價格則不受規管。因此，投資者應充分了解所有風險。

4. 有關損失 NFT 的案件

警方於 2022 年 1 月接獲一宗有關盜竊 NFT 的報案，一名女子稱儲存在虛擬資產平台的 16 件 NFT 畫作被出售，並將出售所得的以泰幣轉走，損失港幣近 87 多萬。警方提醒市民，黑客會透過釣魚攻擊及其他網絡安全漏洞，盜取虛擬資產平台帳戶資料，在登入後把 NFT 藝術品圖像及其他虛擬資產轉走，因此市民要留意有關資訊安全風險。

1.4. 數碼港元

1.4.1. 教學資源

1. 守網者 – 數碼港元〔相關內容詳列於第 1.4.3 節〕 https://cyberdefender.hk/e–hkd/
2. 香港金融管理局 – 香港貨幣 https://www.hkma.gov.hk/chi/key-functions/money/hong-kong-currency/
3. 香港金融管理局 – 新聞稿：金管局公布「金融科技 2025」策略（2021 年 06 月 08 日） https://www.hkma.gov.hk/chi/news-and-media/press-releases/2021/06/20210608-4/%20
4. 香港金融管理局 – 《從政策及設計角度看「數碼港元」》（2022 年 04 月 27 日） https://www.hkma.gov.hk/media/chi/doc/key–functions/financial–infrastructure/e–HKD_A_Policy_and_Design_Perspective.pdf

[2] **恢復短語** (Recovery Phrase **或「助記詞」**) **是首次設置加密資**產錢包 (**如** MetaMask) **時**，**系統自動**產生的多組詞語。技術上，它是錢包私鑰 (private key) **的一種表現方式**，**方便用**戶記錄和記憶。用戶一旦忘記錢包登入密碼，也可用它作「後備密碼」復原帳戶。取自：https://cyberdefender.hk/recovery_phrase/ 。

5. 香港金融管理局 –「數碼港元」的四條必答題（2022 年 04 月 27 日）
https://www.hkma.gov.hk/chi/news-and-media/insight/2022/04/20220427/
6. 「數碼港元」先導計劃啟動（2023 年 05 月 18 日）
https://www.hkma.gov.hk/chi/news-and-media/press-releases/2023/05/20230518-4/

1.4.2. 教學示例及學生課堂反思

讓學生認識「數碼港元」的原理及應用，以及了解數碼貨幣與電子支付的關係，思考推行數碼貨幣與電子支付的挑戰與機遇。

示例一（資料搜集）：

目的：學生通過閱讀及搜集相關資料，了解「數碼港元」的推行與應用，及香港如何推動數碼貨幣與電子支付的應用。

模式：學生進行預習，閱讀及搜集相關資料後，於課堂與同學討論及分享。

思考問題：〔參考教學資源第 1,2,5 項〕

(i) 甚麼是「數碼港元」（e-HKD）？
(ii) 零售央行數碼貨幣（Central Bank Digital Currency，CBDC）與現有電子支付方式有何分別？
(iii) 香港推行「數碼港元」會面對甚麼挑戰與機遇？

示例二（資料研讀）：

目的：學生通過閱讀相關資料，了解香港的貨幣政策、貨幣體制及認識「數碼港元」，思考「數碼港元」與現時香港的貨幣的關係，以及當中的挑戰與機遇。

模式：於課堂以外時間，例如：閱讀課、網上預習、班主任課，讓學生閱讀相關政策文件和資料，並於課堂與同學討論及分享。此外，亦可請學生在週會分享。

思考問題：〔參考教學資源第 1,3,4-6 項〕

(i) 香港的貨幣政策目標及貨幣體制是甚麼？
(ii) 甚麼是「數碼港元」（e-HKD）？
(iii) 以現時香港的貨幣政策，推行「數碼港元」會帶來甚麼挑戰與機遇？

1.4.3. 由警方提供的參考資料〔相關內容節錄自「守網者」網頁〕

1. 甚麼是數碼港元？

構思中的數碼港元是全新的電子形式央行貨幣，由香港政府按聯繫匯率制度發行，價值會跟紙幣及硬幣對等。發行數碼港元對香港的主要潛在效益包括：

(A) 部署應對新型貨幣帶來的挑戰

近年，虛擬資產迅速冒起，有私人機構發行名為「穩定幣」的記帳單位，試圖透過與其他資產掛鈎（例如把每單位「穩定幣」以$1 美元作擔保）以減低價格波幅。然而，有關發行機構並不受監管，它們存在信用、流動性及業務操作等風險，缺乏用戶保障。近期最著名的例子，就是名列全球首五大的「穩定幣」TerraUSD（UST）和其關聯代幣 LUNA 崩盤，令投資者在幾天內損失近$400 億美元。由政府發行的數碼港元由於不存在信用風險，並有由外匯基金持有的美元資產支持，確保本港金融穩健。

(B) 推動數碼經濟的創新及滿足未來支付的需要

金管局會探索運用新科技，例如分布式分類帳技術（例如區塊鏈）、代幣化以及支援編程功能。編程功能實現智慧合約（smart contract） ，促進自動化付款。例如在購買旅遊保險時，旅客可在航班延誤時自動獲發賠償金。

(C) 提升支付系統的穩健程度及效率

縱使本地電子支付系統（如信用卡、轉數快、儲值支付工具）已非常穩健及高效，推出「數碼港元」能為消費者提供多一個支付選項。

2. 發行數碼港元有甚麼的潛在挑戰？

金管局預視推出數碼港元可能帶來以下潛在風險：

(A) 銀行被「去中介化」

近年，虛擬資產迅速冒起，有私人機構發行名為「穩定幣」的記帳單位，試圖透過與其他資產掛鈎（例如把每單位「穩定幣」以$1 美元作擔保）以減低價格波幅。然而，有關發行機構並不受監管，它們存在信用、流動性及業務操作等風險，缺乏用戶保障。近期最著名的例子，就是名列全球首五大的「穩定幣」TerraUSD（UST）和其關聯代幣 LUNA 崩盤，令投資者在幾天內損失近$400 億美元。由政府發行的數碼港元由於不存在信用風險，並有由外匯基金持有的美元資產支持，確保本港金融穩健。

(B) 銀行面臨較高的擠提風險

在發生金融危機，公眾為尋求安全資產，可能會把銀行存款轉換為數碼港元。雖然在只有實物現金存在時，銀行也面對相似的擠提風險，但由於數碼港元將會更容易和更快被取得，因此可能加劇有關風險。同樣，上述情況發生的情況可謂微乎其微。

(C) 網絡安全及軟件漏洞

由於數碼港元系統牽涉大量資金，網絡攻擊者可能會用不同方法入侵銀行系統、假冒金融機構提供惡意的電子錢包應用程式等。假如數碼港元支援智能合約，便會有可能出現編碼風險和外部數據來源風險（例如攻擊者偽造航班延誤訊息令智能合約錯誤執行）。

金管局就數碼港元在發行機制、與大額支付系統兼容性、私隱及數據保障、貨幣發行的法律考慮、打擊犯罪活動的法律考慮等方面仍在進行研究，期望數碼港元能為香港的金融科技發展，帶來新機遇。

2. 個人投資與風險

2.1. 個人投資風險

2.1.1. 教學資源

1. 教育局 – 商業科目 學與教資源 https://www.edb.gov.hk/tc/curriculum–development/kla/technology–edu/resources/business–edu/resources.html
2. 教育局 – 初中理財教育學與教資源 (2020) https://www.edb.gov.hk/tc/curriculum-development/kla/pshe/references-and-resources/cross-curricular-resources/financial-education.html
3. 教育局 – 「三分鐘概念」動畫視像片段系列：「個人資源管理：理財篇」（動畫及工作紙）https://www.edb.gov.hk/tc/curriculum-development/kla/pshe/references-and-resources/life-and-society/3-min-concept.html
4. 投委會 – 後生仔開始投資前，必須做好的 3 件事 https://www.ifec.org.hk/web/tc/blog/2023/06/before-start-investing.page
5. 投委會 – 在數碼世代保管個人財產 https://www.ifec.org.hk/web/tc/blog/2023/06/managing-finances-in-a-digital-era.page
6. 投委會 – 春季大掃除：4 招整理個人財務 https://www.ifec.org.hk/web/tc/blog/2023/03/4-ways-to-tidy-up-finances.page
7. 投委會 – 做好預算 https://www.ifec.org.hk/web/tc/retirement/features/retirement-money-management/making-a-sound-budget.page
8. 投委會 – 風險，是要分散的 https://www.ifec.org.hk/web/tc/blog/2019/11/risk-diversification.page
9. 投委會 – 優點與風險 https://www.ifec.org.hk/web/tc/investment/investment-products/leveraged-and-inverse-products/benefits-risk.page
10. 投委會 – 風險 https://www.ifec.org.hk/web/tc/investment/investment-products/stock/ipo-investing/risks.page
11. 投委會 – 《虛擬資產》小心無牌及海外交易平台的風險 https://www.ifec.org.hk/web/tc/financial-products/fintech/ico-bitcoin/unlicensed-and-overseas-platforms.page

2.1.2. 教學示例及學生課堂反思

讓學生學習個人理財策略及資產管理，並提升他們對管理個人財務的重要性及投資風險的意識，保護自己以免誤墮投資陷阱。

示例一（課堂講解與程式應用）：

目的：讓學生認識理財的重要性，並學習使用不同的理財應用程式或工具，學習管理個人日常收入與支出，以及理財應有的態度，好好管理個人財務。

模式：教師於課堂可通過講解，以及學生透過閱讀相關資料以獲取相關知識，明白不同的理財應用程式和工具，可應用於日常理財中。

思考問題：〔參考教學資源第 1-3, 6, 7 項〕

(i) 了解學生有否為個人的收入與支出作記錄？如有，請學生分享。
(ii) 讓學生想想自己最近一個月的收入及支出情況，並將其分類。
(iii) 學生分享如何分類及其原因，並指出哪些類別的支出最多。
(iv) 學生想想如何為自己一年的收入及支出作預算。

示例二（分組討論及匯報）：

目的：加強學生對個人投資及其風險的認識，並提升投資風險的意識。

模式：學生通過分組討論及小組匯報，分享他們對個人理財的心得及投資的想法。

思考問題：〔參考教學資源第 4, 5, 8-11 項〕

(i) 如何管理個人財務？
(ii) 「投資」是甚麼？如何運作？有甚麼風險？
(iii) 如何避免墮入投資陷阱？
(iv) 如果投資失敗／墮入投資陷阱，應如何處理及持守甚麼態度？

示例三（全校參與活動）：

目的：讓學生認識理財和投資，培養他們正確的態度，並了解潛在的風險和陷阱，以免受騙。

模式：學校為每級學生設定不同的主題（如：個人理財、投資資訊及風險等），於課堂內外，通過教師講解，以及學生分享，讓學生認識個人理財及投資風險概念。學校可以舉辦校內活動／比賽，由學生設計理財和投資相關的吉祥物，並可以把吉祥物製成文具或學校宣傳品，分發給學校的訪客，以作公眾教育。學校亦可以讓學生創作四格漫畫、海報設計、班級壁報等，將學生作品於學校展示，以讓更多學生認識相關概念。

2.2. 網上投資騙案

2.2.1. 教學資源

1. 守網者 – 網上投資騙案〔相關內容詳列於第 2.2.3 節〕
   https://cyberdefender.hk/investment_fraud/
2. 守網者 – 投資騙案 老是常出現〔影片〕 https://youtu.be/C3BJyzgmOlA
3. 守網者 – 《全城守網》特輯六・網上投資騙案〔影片〕 https://youtu.be/JGQxLMmarqw

4. 反詐騙協調中心 – 投資騙案.瘋投偽機〔影片〕 https://youtu.be/44llWVUYeuk
5. 反詐騙協調中心 – 假投資 app 輸身家〔影片〕 https://youtu.be/1WBH0dTUfZ8
6. 教育局 – 商業科目 學與教資源 https://www.edb.gov.hk/tc/curriculum–development/kla/technology–edu/resources/business–edu/resources.html
7. 教育局 – 初中理財教育學與教資源 (2020) https://www.edb.gov.hk/tc/curriculum-development/kla/pshe/references-and-resources/cross-curricular-resources/financial-education.html
8. 香港警務處及香港電台 – 防騙攻略：網上投資騙案 – 利用假投資應用程式 〔影片〕 https://www.youtube.com/watch?v=I9D_G_igFjw
9. 投委會 – 五招防金融騙局 https://www.ifec.org.hk/web/tc/moneyessentials/scams/5–tips–avoid–financial–fraud.page
10. 投委會 – 網上詐騙 https://www.ifec.org.hk/web/tc/moneyessentials/scams/scam-websites.page
11. 香港金融管理局 – 小心騙徒! https://www.hkma.gov.hk/chi/smart-consumers/beware-of-fraudsters
12. 投委會 – 電子「股壇達人」 https://www.ifec.org.hk/web/tc/other-resources/programmes/digital-stock-trading-guru.page

2.2.2. 教學示例及學生課堂反思

讓學生認識理財及投資的知識，了解審慎理財的重要性，以及投資存在的風險，保護自己避免誤墮投資騙案及陷阱。

示例一（觀看影片）：

目的：讓學生學習投資的知識，了解不同網上投資騙案的手法，提高他們防範意識，保護自己避免誤墮投資陷阱。

模式：學生觀看影片，並思考當中的問題（例如：正確的態度；如何防範及避免受騙；如何應對）。

思考問題：〔參考教學資源第 2-6, 8 項〕

(i) 讓學生反思，影片中的主角為何會墮入投資陷阱？
(ii) 如果你是影片中的主角，你會如何選擇？為甚麼？
(iii) 讓學生思考，如何保護自己避免誤墮投資陷阱？
(iv) 如果受騙，應如何處理及持守甚麼態度？

示例二（分組討論）：

目的：讓學生認識理財及投資，並了解審慎理財的重要性及投資的風險。

模式：讓學生搜集和閱讀相關資料，於課堂分組討論。

思考問題：〔參考教學資源第 6,7, 9-11 項〕

(i) 甚麼是財富管理？應如何管理自己的財富？
(ii) 甚麼是投資？市面上有哪些流通的投資工具？
(iii) 投資會有甚麼潛在風險？投資者應持甚麼投資態度？

示例三（桌上／網上遊戲或比賽）：

目的：加強學生的財務管理的知識，並了解具備正確投資態度的重要性。

模式：學生通過參與理財或模擬投資桌上／網上遊戲或比賽，體驗理財及投資的操作。

思考問題：〔參考教學資源第 12 項〕

(i) 甚麼是股票？如何進行交易？當中有甚麼需要注意？
(ii) 市面上很多不同類型的股票交易平台及流動應用程式，應如何選擇？當中有甚麼潛在風險？
(iii) 投資者應持甚麼投資態度？
(iv) 如何保護自己避免誤墮投資陷阱？
(v) 如果受騙，應如何處理及持守甚麼態度？

2.2.3. 由警方提供的參考資料〔相關內容節錄自「守網者」網頁〕

1. 甚麼是網上投資騙案?

騙徒在網上社交平台、討論區貼文或在即時通訊軟件發放訊息，以低風險、高回報作招徠，吸引素未謀面的網民參與投資。然而，這些投資大多是不存在或充滿陷阱。有騙徒會偽造獲利的交易記錄，誘使受害人投放更多資金後，便會失去聯絡。

(A) 網上尋找獵物

漁翁撒網地識新朋友，經常上載「生活照」炫富，提高可信性

(B) 假扮投資顧問或基金經理

訛稱有豐富投資虛擬資產、貴金屬或外匯的經驗

(C) 唱高散貨

推介受害人購買「仙股」。實際上騙徒早在低位大量入貨，當受害人買入股票被推股價，騙徒隨即沽貨離場

(D) 虛假投資應用程式

誘使受害人安裝虛假投資應用程式，當中顯示虛假交易和回報

(E) 套現時被要求繳交手續費 / 出現系統故障

受害人如欲套現，騙徒會以須繳交高昂手續費，或聲稱系統故障拖延付款

(F) 建立曖昧關係 （又稱「殺豬盤」）

與受害人建立曖昧或網戀關係，以獲取受害人信任，繼而誘騙投資

2. 有哪些防騙建議？

(A) 學生不應參與網上投資或金錢上的交易活動，並應該明白金錢的概念及養成正確使用金錢的價值觀和態度

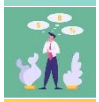
(B) 提防網上認識的「高富帥」或「白富美」推介投資項目。如有懷疑，可利用搜尋器搜尋對方社交帳戶的照片、查看對方帳戶的朋友圈是否有異常或要求與對方視像通話

(C) 不要隨便簽署任何投資授權書

(D) 騙徒以本小利大來誘騙投資，提防回報高得不切實際的投資計劃

(E) 切勿下載不明來歷的應用程式

(F) 切勿輕信在社交平台上發放的「內幕消息」



(G) 切勿將本金轉帳至個人名義的戶口。如透過加密貨幣轉帳更應審慎

(H) 在投資虛擬資產前，應充分了解相關產品特性和資訊安全風險

(I) 如有懷疑，可在「防騙視伏器」輸入電話號碼、社交媒體帳號等評估風險，或致電 18222 查詢

(J) 如懷疑不慎受騙，應立即向家長、監護人或教師尋求協助

2.3. 信用卡盜用

2.3.1. 教學資源

1. 守網者 – 信用卡盜用〔相關內容詳列於第 2.3.3 節〕 https://cyberdefender.hk/creditcard_misuse/
2. 守網者 – 《全城守網》特輯十・信用卡盜用〔影片〕 https://youtu.be/f1JjXXOpQfo
3. 教育局 – 商業科目 學與教資源 https://www.edb.gov.hk/tc/curriculum–development/kla/technology–edu/resources/business–edu/resources.html

4. 教育局 – 初中理財教育學與教資源 (2020) -- 信用卡與借貸 https://www.edb.gov.hk/tc/curriculum-development/kla/pshe/references-and-resources/cross-curricular-resources/financial-education.html
5. 立法會十六題：信用卡被盜用作網上購物 https://www.info.gov.hk/gia/general/202212/07/P2022120600336.htm
6. 香港金融管理局 – 信用卡 https://www.hkma.gov.hk/chi/smart-consumers/credit-cards/
7. 香港金融管理局 – 公眾教育短片〔影片〕 https://www.hkma.gov.hk/chi/smart-consumers/public-education-videos/

2.3.2. 教學示例及學生課堂反思

學生通過認識信用卡的運作原理及使用，比較實體信用卡與電子信用卡支付工具的優點和缺點，了解使用信用卡的潛在風險，提高使用信用卡時的防範意識，保護自己以免誤墮陷阱。

示例一（觀看影片）：

目的：讓學生認識信用卡的運作原理及使用，比較實體信用卡與電子信用卡支付工具的優點和缺點，了解信用卡與借貸的異同，以及使用信用卡的潛在風險，藉以提高防範意識。

模式：讓學生觀看影片，並思考當中的問題（例如：正確的態度；有何風險；如何防範等）。

思考問題：〔參考教學資源第 2, 7 項〕

(i) 信用卡的運作原理是怎樣的？試舉出使用信用卡的兩個例子。
(ii) 實體與電子信用卡有何不同？
(iii) 使用信用卡有何風險？應如何防範？
(iv) 如果信用卡被盜用，應如何處理及持守甚麼態度？

示例二（教案及分組討論）：

目的：教導學生正確的理財及商業知識，讓他們了解消費的需要，認識不同財務產品的特徵（例如：信用卡及其運作原理）。

模式：學生於網上搜集資料及閱讀，配合教師課堂講解，再讓學生作小組討論及分享。

思考問題：〔參考教學資源第 1, 3-6 項〕

(i) 通過題為「精明消費」及「金錢的性質」教材，學生了解金錢的性質及不同財務產品的特徵（例如：信用卡及其運作原理）。
(ii) 透過題為「當自己的財務策劃師」及「運用個人財務預算展示消費模式」教材，讓學生學習計劃理財方案及運用金錢應有的態度。

示例三（全校參與活動）：

目的：讓學生了解信用卡的應用和運作，以及當中的潛在風險，提高學生的防騙意識。

模式：學校透過舉辦以「信用卡支付陷阱」為主題的校內影片製作比賽，或由校園電視台製作影片，影片可於早會、周會及／或校園電視台播放。

2.3.3. 由警方提供的參考資料〔相關內容節錄自「守網者」網頁〕

1. 甚麼是信用卡盜用?

使用信用卡進行網上交易十分普遍，交易過程亦十分方便。可是，當信用卡資料包括卡號碼、到期日及保安碼，一旦落入騙徒手上，資料便可能被盜用，因而蒙受損失。那麼，信用卡資料會怎樣被盜取？以下會介紹一下信用卡資料失竊途徑：

(A) 信用卡遺失或被盜：
騙徒可直接使用你遺失或被盜的信用卡進行消費，直至信用額用盡為止

(B) 實體商戶盜用卡資料：
在實體商戶使用信用卡結帳時，立心不良的店員可能會複製信用卡資料以作轉售或其他非法用途

(C) 釣魚攻擊：
騙徒／黑客設置虛假網站，並發放釣魚電郵或 SMS 短訊，以不同藉口，例如戶口更新、或被凍結等，誘使用戶輸入信用卡資料

(D) 零售系統（POS）終端機被入侵：
零售系統伺服器如受到 POS 惡意程式感染，連接伺服器的電腦便會被黑客控制並盜取信用卡資料

(E) 非法盜取個人資料以申請信用卡
騙徒假冒卡主向銀行報失信用卡，其後從卡主信箱偷取銀行補發的新信用卡。騙徒或會利用非法盜取個人資料向銀行提供偽造住址證明，以便新卡寄到騙徒指定信箱

2. 應如何安全使用信用卡？

學生應在家長或監護人陪同下使用信用卡。

收到新卡時，應盡快更改預設帳戶名稱及密碼

應在可靠及商譽良好的網店購物

只在有 https 加密保護的網站進行網上付款

切勿以公共電腦登入網上銀行或輸入信用卡資料

小心保管信用卡資料，切勿輕易向任何人披露自己的卡資料

提防釣魚網站或電郵，不要隨意點擊電郵內含的超連結或附件

如懷疑不慎受騙，應立即向家長、監護人或教師尋求協助

3. 數碼資產相關科技及網絡安全風險

3.1. 元宇宙

3.1.1. 教學資源

1. 守網者 – 元宇宙〔相關內容詳列於第 3.1.3 節〕
   https://cyberdefender.hk/metaverse/
2. 立法會十題：促進元宇宙在香港的發展 （2022 年 6 月 1 日）
   https://www.info.gov.hk/gia/general/202206/01/P2022060100182.htm
3. 立法會十七題：元宇宙的發展 （2022 年 11 月 30 日）
   https://www.info.gov.hk/gia/general/202211/30/P2022113000264.htm
4. 香港貿易發展局 – 提升網絡保安 邁向元宇宙時代（2022 年 04 月 13 日）
   https://research.hktdc.com/tc/article/MTAyOTM4MzA1MQ
5. 香港貿易發展局 – 探索元宇宙：超越 NFT 風潮（2022 年 05 月 04 日）
   https://research.hktdc.com/tc/article/MTA0ODE0MjE4MQ
6. 港貿易發展局 – 探索元宇宙：創建數碼資產（2022 年 11 月 09 日）
   https://research.hktdc.com/tc/article/MTIxMTQ4MzMyOA
7. 香港電台 –《鏈上元宇宙》#19 Metaverse 元宇宙是甚麼？
   https://www.rthk.hk/radio/radio2/programme/blockchain_and_web3/episode/875814
8. 香港教育城 Go eLearing - 學與教博覽 2022 – 元宇宙的教育迷思：如何為學生設計一個有效和安全的元宇宙學習空間？
   https://www.hkedcity.net/goelearning/resource/63ad1bfd0da87e21621bfd4c

3.1.2. 教學示例及學生課堂反思

各科目通過學生親身體驗、教師講解或學生自行搜尋資料（如：收聽錄音節目），讓學生認識甚麼是元宇宙，與其相關的應用和技術。同時，培養學生溝通能力、自信和責任感，成為合乎道德的網絡公民。

示例一：

目的：讓學生認識元宇宙的發展、其相關的應用和技術。

模式：透過學生親身體驗、閱讀相關資料或收聽錄音節目。

思考問題：〔參考教學資源第 1-7 項〕

(i) 甚麼是元宇宙？
(ii) 元宇宙與日常生活有甚麼關係？
(iii) 虛擬世界與現實世界有甚麼不同？
(iv) 你認為現實世界的規則和法例是否適用於虛擬世界？為甚麼？
(v) 你認為香港應否發展元宇宙？為甚麼？

示例二（與外間機構協作）：

目的：透過認識及體驗元宇宙世界，讓學生了解元宇宙應用的技術及潛在風險，以進一步加強他們對網絡安全的意識。

模式：學校可與專上院校、專業機構及／或社區組織等合作，為學生提供不同的校內外的學習計劃。

3.1.3. 由警方提供的參考資料〔相關內容節錄自「守網者」網頁〕

1. 甚麼是元宇宙？

元宇宙概念源自美國小說家尼爾・史蒂芬森（Neal Stephenson）於 1992 年出版的科幻小說《潰雪》（Snow Crash），當中描述的「Metaverse」是一個虛擬世界讓人們化身為各種網路分身進行互動。「Meta」解作「超越」；「Verse」則為宇宙，組合成「元宇宙」。

2. 如何進入元宇宙？

只需透過 VR 眼鏡、手機或電子遊戲進入虛擬環境裏，人們便可使用虛擬身份進行各種日常活動，如玩遊戲、看電影、交朋友等，甚至可以成為現實世界的延伸，在元宇宙建設虛擬社群、與同事進行會議及各類商業活動，令現實世界和虛擬世界融合。

3. 元宇宙依賴哪些技術？

透過沉浸式體驗，如虛擬實境（Virtual Reality）、擴增實境（Augmented Reality）、混合實境（Mixed Reality）及其他穿戴裝置，讓用家親歷其境在元宇宙進行互動。舉個例子，身穿體感背心的遊戲玩家會在被拳頭擊中時會產生痛感。

5G 通訊技術的低延遲特性令人與人之間，或人與機器之間的互動延遲時間減至幾毫秒，接近實時互動。

虛擬資產、非同質化代幣（NFT）和用戶在元宇宙的行踪都是使用區塊鏈技術令每一個「存在」和每一項交易成為獨一無二，而且不可被篡改。

任何能連接至網絡的裝置形成物聯網 (Internet of Things, IoT)，是指該些裝置在現實世界中收集數據（如天氣、人流、溫度等）並回傳至虛擬世界的技術，為元宇宙與現實世界更緊密連接。

人工智慧（AI）會發展出更像真的虛擬角色，將來有可能會到元宇宙看虛擬醫生、見到虛擬警員在虛擬街道巡邏。

4. 元宇宙存有風險嗎？

所有網上世界的風險也會延伸至元宇宙。在沒有法律監管下，欺詐、盜用身份、個人私隱外洩、假資訊、加密勒索等網絡安全隱患統統有機會在元宇宙發生。此外，近期有元宇宙虛擬地皮被炒至逾六千美元一塊。若平台突然關閉或出現網絡事故，相關資產便可能變成零價值。由於現時本地法例並沒有規管有關虛擬資產投資活動，如投資者蒙受損失，要追討賠償將十分困難。

3.2. 釣魚攻擊

3.2.1. 教學資源

1. 守網者 – 釣魚攻擊〔相關內容詳列於第 3.2.3 節〕 https://cyberdefender.hk/phishing_attack/
2. 守網者 – 全城守網：釣魚攻擊〔影片〕 https://youtu.be/09hDi1ZclRM
3. 守網者 – 同你擊破釣魚攻擊〔影片〕 https://youtu.be/tP0mr1mcSKs
4. 反詐騙協調中心 – 假投資 app 輸身家〔影片〕 https://youtu.be/1WBH0dTUfZ8
5. 反詐騙協調中心 – 唔準諗，即刻答〔影片〕 https://youtu.be/1XPVRSWZqHk
6. 政府資訊科技總監辦公室 – 網絡安全資訊站：提防仿冒詐騙攻擊〔自學課程〕 https://www.cybersecurity.hk/tc/learning-scam.php
7. 香港金融管理局 – 小心騙徒！ https://www.hkma.gov.hk/chi/smart-consumers/beware-of-fraudsters/#fraudulent-bank-websites-phishing-emails-and-similar-scams
8. 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
9. 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〔影片〕 https://youtu.be/aWk7LPO5zs4?feature=shared

3.2.2. 教學示例及學生課堂反思

通過教師課堂講解、學生搜集資料及觀看影片，讓學生認識「釣魚攻擊」的類型、特徵、影響，以及了解應對「釣魚攻擊」的方案，並提高學生對「釣魚攻擊」的防騙意識，避免他們誤墮騙局。

示例一（電腦課堂）：

目的：讓學生認識「釣魚攻擊」的原理、類型、特徵、影響，以及應對「釣魚攻擊」的方案，並提高學生對「釣魚攻擊」的防騙意識，避免他們誤墮騙局。

模式：電腦科教師可於網絡安全課題講解「釣魚攻擊」，以及讓學生分組討論和分享。

思考問題：〔參考教學資源第 1, 6-8 項〕

(i) 甚麼是「釣魚攻擊」？其原理是甚麼？

(ii) 「釣魚攻擊」有甚麼類型及特徵？
(iii) 如何防範「釣魚攻擊」？
(iv) 如誤中「釣魚攻擊」，應如何處理及持守甚麼態度？

示例二（觀看影片）：
目的：讓學生明白「釣魚攻擊」與日常生活息息相關，並了解「釣魚攻擊」的運作及提高防騙意識，避免誤墮騙局。

模式：觀看影片，與同學分享影片中提及的情況和問題，並提出解決方案。

思考問題：〔參考教學資源第 1, 2-5, 9 項〕
(i) 日常生活中會否遇到「釣魚攻擊」？試舉出兩個例子。
(ii) 如何防範「釣魚攻擊」？
(iii) 如誤中「釣魚攻擊」，應如何處理及持守甚麼態度？

示例三（全校活動）：
目的：讓學生認識「釣魚攻擊」的原理，並提高學生的防騙意識，避免他們誤墮騙局。

模式：學校通過舉辦「釣魚攻擊」為主題的吉祥物創作及海報設計比賽，並把學生得獎作品製成不同的學校宣傳物品、屏幕保護圖等，讓更多人注意「釣魚攻擊」。

3.2.3. 由警方提供的參考資料〔相關內容節錄自「守網者」網頁〕

1. 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。

取得收訊人的信用卡資料後，騙徒會在網上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。

2. 有甚麼常見的攻擊方式？

「網絡釣魚」當中，黑客以**假冒金融機構**和**郵遞服務**佔大多數。

(A) 假冒金融機構 / 電子支付平台

(i) 黑客假冒金融機構，例如銀行發出的釣魚短訊，聲稱戶口有異常或有轉帳指示，要求用戶立即處理或確認。誘騙用戶進入假網站並提供手機號碼和一次性密碼，然後用另一手機騎劫帳戶並將錢轉走。由於騙徒隱藏發訊人的電話號碼，並假冒銀行暱稱，手機系統會把同一暱稱發出短訊視為同一人發出，令真假短訊放在一起，令人難以分辨。

(ii) 也有黑客從不同渠道（如系統漏洞、暗網等）取得市民個人資料，假扮銀行職員來電，聲稱要求用戶提供「交易密碼」及以手機接收「一次性密碼」以更新支付平台帳戶，否則會凍結其戶口。由於騙徒能準確地講出市民的個人資料，因而容易取得市民信任。取得上述資料後，騙徒隨即騎劫戶口並將錢轉走。

(B) 假冒郵遞服務／公營機構

(i) 「由於欠缺資料，包裹未能付運」、「未能順利付款，已暫停有關服務，請更新付款方式」、「Your package with track number xxxx still waiting your instruction（你的包裹編號 XXX 仍等待指示）」，都是假冒郵遞服務或電力公司、煤氣公司、港鐵等公營機構釣魚訊息的開場白，誘騙用戶打開連結進入假網站。由於釣魚網站的介面設計幾可亂真，而且使用了迫切的字眼如「暫停服務」、「會被退件」等，令收件人在情急之下提供個人或信用卡資料。

3. 如何辨識釣魚攻擊？

(A) 假電郵

注意寄件者的電郵標題，檢查電郵地址的域名（domain）是否與官方域名有出入或有異樣

標題包含「帳號即將關閉」等字眼，利用收件者擔憂的心理以減低其警覺性

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

(B) 假網站

網站的域名與官方網站的域名極為相似（如數字「1」取代字母「l」）

網站或會有部分連結失效

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

4. 應如何防範釣魚攻擊呢？

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

如有懷疑，應向家長、監護人或教師請教或尋求協助。

如懷疑受騙，應保存相關電郵或訊息，並儘快報警

3.3. 盜用身份

3.3.1. 教學資源

1. 守網者 – 盜用身份〔相關內容詳列於第 3.3.3 節〕
   https://cyberdefender.hk/theft_of_identity/
2. 反詐騙協調中心 – 防騙宣傳短片：偽冒會員獎勵計劃〔影片〕https://youtu.be/WMj3FVczty0
3. 反詐騙協調中心 – 防騙宣傳短片：優惠禮品騙局〔影片〕https://youtu.be/x20u5Ltlr3U
4. 政府資訊科技總監辦公室 – 網絡安全資訊站：身份盜竊
   https://www.cybersecurity.hk/tc/learning-identity-theft.php

3.3.2. 教學示例及學生課堂反思

通過教師課堂講解、學生資料搜集及觀看影片，讓學生認識身份如何被盜用、有何影響，以及防範措施和應對方案，明白這是與他們日常生活息息相關，並提高學生對保護個人資料的意識，避免被人盜用身份。

示例一（觀看影片）：

目的：讓學生認識個人資料如何被盜用、有何影響，以及防範措施和應對方案，並提高對保護個人資料的意識，避免被人盜用身份。

模式：觀看影片，課堂分組討論並分享影片中提及的情況和問題，並想想防範方案。

思考問題：〔參考教學資源第 2, 3 項〕

(i) 騙徒一般會以怎樣的手法騙取他人的個人資料？
(ii) 當個人資料被盜用後，會產生甚麼後果呢？
(iii) 如何防範個人資料被盜用？
(iv) 如發現個人資料被盜用，應如何處理及持守甚麼態度？

示例二（全校活動）：

目的：讓學生認識「洩露個人資料」的風險及如何「保護個人資料」，明白這些都是與日常生活息息相關，並提高學生的防騙意識，避免他們被人盜用身份。

模式：學校通過舉辦「保護個人資料」為主題的校內問答比賽，每級分別有不同主題（包括：甚麼是「個人資料」、如何保護「個人資料」、正確的態度）

3.3.3. 由警方提供的參考資料〔相關內容節錄自「守網者」網頁〕

1. 甚麼是盜用身份？

不法分子在互聯網盜取他人資料，例如姓名、地址、出生日期、身份證號碼、電郵地址、電話號碼、銀行資料、信用卡資料及個人相片等，從而冒充當事人進行欺詐等不法行為。

2. 身份如何被盜用？

不法分子可透過盜取身份的方法，例如：釣魚電郵、偽冒網站或偽冒 Wi–Fi 熱點等方式。

3. 應如何防範身份被盜用呢？

- 提防釣魚網站或偽冒電郵
- 在社交帳戶採用合適的私隱及安全設定
- 不應隨便在網上披露個人資料或相片
- 將網上帳戶設置高強度的密碼或啓用多重驗證
- 妥善保管及加密儲存含有個人資料的裝置
- 棄置電子裝置或儲存有個人資料的媒體前，須妥善刪除資料（如進行低階格式化）
- 如有懷疑，應向家長、監護人或教師請教或尋求協助

- 如涉及個人資料，可向個人資料私隱專員公署作出投訴
- 若身份被盜用，應報警求助並與有關機構聯絡

(四) 參考資料：

1. 守網者 – 網絡罪案
   https://cyberdefender.hk/cybercrime/?playlist=15cabd5&video=531c9cd
2. 反詐騙協調中心
   https://www.adcc.gov.hk/zh-hk/home.html
3. 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
4. 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
5. 教育局 – 「聰明 e 主人」電子學習資源套
   https://www.hkedcity.net/teencampus/zh–hant/resource/5b28a46b32c8bf8d553c9869
6. 教育局 – 理財教育學與教資源
   https://www.edb.gov.hk/tc/curriculum–development/kla/pshe/reference–and–resources/financial_education.html
7. 教育局 – 初中理財教育學與教資源 （2020）
   https://www.edb.gov.hk/tc/curriculum–development/kla/pshe/references–and–resources/cross–curricular–resources/financial–education.html
8. 教育局 – 公民、經濟與社會（中一至中三）支援教材：單元 1.3：理財教育
   https://www.edb.gov.hk/attachment/tc/curriculum–development/kla/pshe/references–and–resources/ces/support_materials_S1/CES%20M1.3_Managing%20Finance%20and%20Sensible%20Consumption%20（Chi）_20230208.pdf
9. 教育局 – 商業科目 – 學與教資源
   https://www.edb.gov.hk/tc/curriculum-development/kla/technology-edu/resources/business-edu/resources.html
10. 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
11. 香港警務處及香港電台 – 防騙攻略
    https://www.rthk.hk/tv/dtt31/programme/antideceptionprog
12. 投委會 – 網上詐騙
    https://www.ifec.org.hk/web/tc/moneyessentials/scams/scam–websites.page
13. 香港電台 – 堅哥防騙攻略
    https://www.rthk.hk/tv/dtt31/programme/kingor_antideception
14. 香港電台 – 電台直播《鏈上元宇宙》
    https://www.rthk.hk/radio/radio2/programme/blockchain_and_web3
15. 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