STUDENT WORKBOOK · 學員手冊

學員手冊

Student Workbook

初中 IT 保安培訓工作坊 · Junior High Cyber Security Workshop · 3 hours

學員資料 · Student Info

姓名 / Name _____

日期 / Date _____

學校 / School _____

班別 / Class _____

目錄 · Contents

CHAPTER 01

互聯網點運作

How the internet works

重點筆記 · Key notes

1 IP 位址
IP address

每部上網機都有一個 IP, 類似屋企地址。
IPv4 例 :192.168.1.42
IPv6 例 :2404:6800:4003::1
Every device has an IP, like a postal address.

2 DNS
Domain Name System

互聯網「電話簿」, 將域名 google.com 轉做 IP 142.250.71.46 。
如 DNS 被改 , 打正確網址都會去到假網站。
Internet phonebook. If DNS is tampered, the right URL leads to a fake site.

3 數據包 Packet
Network packet

網絡傳輸基本單位 , 內含 :
[來源 IP] + [目標 IP] + [Port] + [Payload]
Basic transmission unit: src+dst IP, port, payload.

4 HTTP vs HTTPS
Encryption

HTTP = 明信片 (任人睇)
HTTPS = 入信封 (加密), 要見 🔒鎖頭
HTTP = postcard; HTTPS = sealed envelope. Look for the 🔒.

CHAPTER 01

互聯網點運作

How the internet works

動手練習 · Exercises

Q1

填空 :DNS 將 _____ 轉做 _____。

Q2

邊個比較安全 :HTTP / HTTPS? 為何？

Q3

寫低你最常去 3 個網站 , 睇有冇 🔒 鎖頭 :1) ____ 2) ____ 3) ____

CHAPTER 02

攻擊面

Attack surface — where you get hit

重點筆記 · Key notes

1 公共 Wi-Fi
Public Wi-Fi
開放（有密碼）Wi-Fi 任何人都可以連，駭客可開「Evil Twin」假熱點，你流量會經佢部機。

2 USB Drop
USB drop attack
駭客故意跌 USB 喺地下，等好奇心嘅人插入電腦 → 即時執行惡意程式。

3 舊路由器
Outdated router
幾年冇更新 firmware 有已知漏洞，可被遠端入侵改 DNS。

4 Shoulder surfing
Shoulder surfing
出面望到你個 mon = 影低你打密碼。咖啡店揀位面壁。

5 Quishing
QR phishing
駭客貼假 QR 蓋過真嘅，掃完去釣魚網站。

CHAPTER 02

攻擊面

Attack surface — where you get hit

動手練習 · Exercises

Q1

檢視你屋企部路由器有冇 update 過？上次幾時？

Q2

列出你今日見過嘅 QR Code (至少 3 個), 思考有冇可能係假嘅。

CHAPTER 03

釣魚實戰演練

Phishing live-fire

重點筆記 · Key notes

1 三招睇穿釣魚

3 spotting tricks

1) 睇 URL — 拼錯字母、奇怪域名
2) 睇寄件者 — 真域名 vs lookalike
3) 睇語氣 — 急、驚、貪 = 紅旗

Check URL, sender domain, tone (urgent/scary/greedy).

2 Lookalike 域名

Lookalike domains

m1crosoft.com (1=i)
netfllix.com (兩個 l)
faceb00k.com (0=o)

Watch for 0/o, 1/l/i, extra letters, doubled letters.

3 情緒勒索

Emotional scam

「個仔 ! 阿媽 phone 壞咗 , 急借錢」— 永遠打電話確認。

"Mom's phone broke, urgent loan" — always call to verify.

CHAPTER 03

釣魚實戰演練

Phishing live-fire

動手練習 · Exercises

Q1

收到「Netflix 24 小時內 update 信用卡」電郵 , 你會做咩 3 件事 ?

Q2

練習 : 寫一封自己嘅釣魚電郵範本 (練習用 , 絕不可寄出 !), 然後同同學交換找 red flag 。

CHAPTER 04

密碼破解 + 中間人攻擊

Cracking & MITM

重點筆記 · Key notes

1 字典攻擊
Dictionary

駭客先試 1000 萬條常用密碼。如果你個密碼喺入面 → 秒破。

Top 10M passwords tried first. If yours is in it → instant crack.

2 暴力破解
Brute force

8 位純小寫 : 數小時破。
8 位混合大小寫 + 數字 + 符號 : 幾年。

8 lower: hours. 8 mixed: years.

3 MITM 中間人
Man-in-the-Middle

駭客喺你同伺服器中間 relay 所有流量。
HTTP: 可竊聽 / 竄改
HTTPS: 加密 = 只見亂碼

Attacker relays all traffic. HTTP readable, HTTPS encrypted.

CHAPTER 04

密碼破解 + 中間人攻擊

Cracking & MITM

動手練習 · Exercises

Q1

邊個密碼最強？ A) P@ssw0rd! B) MyDog2009 C) tiger-violet-rocket-pizza D) qwerty123

Q2

估吓你目前最弱嘅密碼幾耐會被破 ?(回家上 Junior Cyber Security Workshop 網試吓)

CHAPTER 05

強密碼 + 雙重驗證

Strong passwords & 2FA

重點筆記 · Key notes

1 四詞密碼法
Four-word passphrase

4 個隨機英文字 + 「-」連住 , 如 :
tiger-violet-rocket-pizza
易記、難破。
Four random words joined by "-". Memorable + crack-resistant.

2 Password Manager
Password Manager

Bitwarden / 1Password / iCloud Keychain — 每個網站一個獨立密碼。
Unique password per site, auto-filled.

3 2FA 雙重驗證
2FA

即使駭客知密碼 , 冇你部手機都登入唔到。
Authenticator App (TOTP) 比 SMS 安全。
Even if password leaks, attacker can't log in. App TOTP > SMS.

4 Have I Been Pwned
HIBP

上 haveibeenpwned.com 睇自己 email 有冇被洩露 , 有就即刻改密碼。
Check if your email leaked; rotate passwords now.

CHAPTER 05

強密碼 + 雙重驗證

Strong passwords & 2FA

動手練習 · Exercises

Q1

設計一個你自己嘅 4 詞密碼 (只寫提示 , 唔好寫真嘢 !): 提示 :_____

Q2

回家行動清單 :☐ Email 開 2FA ☐ IG/Discord 開 2FA ☐ 安裝 Password Manager ☐ 查 HIBP

CHAPTER 06

真實工具實驗室

Real-tools lab

重點筆記 · Key notes

1 Wireshark

Packet analyzer

免費封包分析器。睇到網絡上每個包嘅 src/dst/proto 。
HTTP 可直接讀 ;HTTPS 加密只見亂碼。

Free packet analyzer. HTTP readable; HTTPS encrypted.

2 Fing

Network scanner

手機 App, 掃描你屋企網絡有咩裝置 , 發現陌生機就要警覺。

Mobile app — scans home network. Unknown device = warning.

3 Wi-Fi 掃描

Wi-Fi scan

睇 SSID + 加密類型 :Open 最危險 ,WEP 已破解 ,WPA2/WPA3 較安全。

Open dangerous, WEP broken, WPA2/3 safer.

4 ★ 守則 Code

Ethics

只可以喺自己嘅裝置或者明確得到允許嘅網絡用呢啲工具 , 否則違法 !

Only use on your own devices or networks with permission!

CHAPTER 06

真實工具實驗室

Real-tools lab

動手練習 · Exercises

Q1

回家用 Fing 掃自己屋企 Wi-Fi, 列出所有連線裝置（至少 5 件）。

Q2

檢視你最近連過嘅 3 個 Wi-Fi: 邊個係 Open 嘅？有冇即時改用流動數據？

Appendix A

名詞表 · Glossary

IP	Internet Protocol address — 裝置嘅網絡地址
DNS	Domain Name System — 域名轉 IP
HTTPS	HTTP Secure — 加密版 HTTP
TLS / SSL	加密通訊協定 (HTTPS 底層)
MITM	Man-in-the-Middle — 中間人攻擊
Phishing	釣魚 — 用假訊息呃資料
2FA / MFA	雙重 / 多重驗證
TOTP	Time-based OTP — Authenticator 6 位碼
Brute force	暴力破解 — 逐個試
Dictionary	字典攻擊 — 試常用密碼清單
Evil Twin	邪雙 — 駭客扮一樣 SSID 嘅假 Wi-Fi
Honeypot	蜜罐 — 故意露破綻引人連入
Sniffer	封包嗅探器 — Wireshark 之類
SSID	Wi-Fi 網絡名
Firmware	硬體入面嘅內建軟體

Appendix B

學員守則 · Student Code

- ✓ **我所學嘅一切，只會用嚟保護人，唔會用嚟傷害人。**

  I will use everything I learn only to protect, not to harm.

- ✓ **我唔會喺冇明確允許嘅情況下，測試或攻擊任何其他人嘅裝置 / 網站 / 帳户。**

  I will not test or attack anyone else's device/site/account without permission.

- ✓ **如果發現朋友 / 家人受網絡攻擊，我會幫佢報警或者搵大人協助。**

  If someone I know is attacked, I will help them get adult support.

- ✓ **真正嘅 IT 保安員，係互聯網嘅守護者。**

  A real IT defender is a guardian of the internet.

簽名 / Signature: _____ 日期 / Date: _____