網路安全

組員：劉才裔、蘇振豪、王柏鈞、蕭顗謙

指導老師:張彥森老師

一、學習動機：

隨著科技快速發展，生活中出現許多便利的**應用程式**與**工具**，但同時也增加了遭受**駭客攻擊**與**病毒**入侵的風險。有鑑於此，本人曾**親身經歷**中毒事件，深刻體會**資安的重要性**，因此希望透過本研究深入了解**網路安全**的威脅與**病毒的運作**方式，進而尋找有效的預防措施，提升自我及他人對資安的**防護能力**，避免個人資料或財產遭受損失，強化日常生活中的**安全意識**與**防護行為**。

二、預期目標

本計畫旨在**提升**台灣民眾對**網路安全**的**認知**與**實務能力**，內容涵蓋網路安全等級說明、常見病毒防範技巧及個人資料保護方法，透過介紹**五大資安等級**，並針對日常生活中常見的資安威脅與病毒，協助民眾在日常生活中建立正確的**資安觀念**與**應對能力**。

三、歷程與成果

網路安全等級 (WPA)

WPA 是無線網路（Wi-Fi）加密的標準：**WPA**、**WPA2**、**WPA3**

現在夠用的是哪一個？

目前 **WPA2** 仍是主流，**建議升級到 WPA3**，因為：

- **WPA3 防破解能力更強**
- 公共 **Wi-Fi 安全性更高**（防**中間人攻擊**）
- 使用「**前向保密**」（Forward Secrecy）**技術**

網路安全等級 (WPA)

1. 現在主流用是**WPA2**， 但我之前做了一些實驗其實不夠。
2. 跟大陸人買了個**網路阻斷器**， 可切斷掉周邊的**WIFI**連接，及發送一堆無用WIFI 以下是實際操作影片

   https://youtu.be/sdDy6bY3U0M?si=vcEXytZgfug9Cstn

- 只能攻擊**WPA3**以下。

WIFI攻擊

WIFI攻擊有分為三種

1. 使用密碼辭典破解WIFI連接的密碼(類似於暴力破解)
2. 入侵後台管理頁面，可能性較低，除非後台登入密碼沒改。
3. 改路由器設定 (例如：重新導向你所有網頁到釣魚網站)
   (1) 種**後門程式** (**修改韌體**可以藏**後門**)
   (2) 開啟**DNS Spoofing**、**MITM** (**中間人攻擊**)
   (3) **攔截**或**記錄**你家所有裝置的**上網**內容

WIFI 釣魚

虛假網路網站：

是讓你連上後會跳個**登入頁面**，

可能是 GOOGLE 或**各大網站**之類的，藉由這種假頁面去騙你的**密碼**。

其他在網路上可見病毒

常見的病毒：**特洛伊木馬病毒** (木馬)

這種病毒常夾雜在你網路上**下載的東西**，比如說上來路不明的**網站遊戲**，它的功用就是**竊取電腦資訊**，類似被**開戶**，你所有資訊都會被**窺視**及被**竊取**。

中了木馬病毒對方會得到什麼?

右邊這張圖是我之前中了木馬(對方提供)

由圖可得知**IP**、**國籍**、**電話**、**COOKIES**、**儲存帳密**。

(可以直接透過**COOKIES**登入**你的帳號**)

CStealer (Telegram Version)
[redacted]

Team Name: Default
Worker ID: 0001

Name: yinin516
Phone: +88696[redacted]
E-Mail[redacted]6@gmail.com
IP: [redacted] (Taiwan 🇹🇼)
OS: Windows 10 (10.0.22621)

Messengers: 1
└ Discord

Files: 24
└ exception_hierar[...].txt
└ exception_hierar[...].txt
└ ...

Passwords: 98
└ Google Chrome (Profile 1): 49
└ Microsoft Edge (Default): 49

Cookies: 1215
└ Google Chrome (Profile 1): 1140
└ Microsoft Edge (Default): 75

Size: 4.1 MB
Password: u([redacted]
Link: [redacted] 11:59

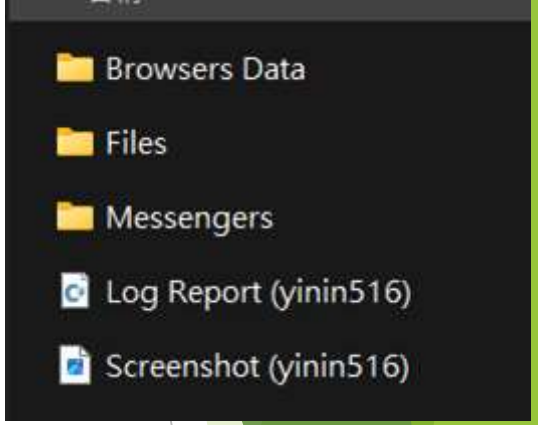
Log (yinin516).zip
4 MB

CStealer (Log Backup)

Team Name: Default
Worker ID: 0001

Victim: [redacted]
OS: Windows 10 (10.0.22621)

Password: [redacted]
Link: [redacted] 12:00



此頁是先前買來研究時給自己種的，開出來幾乎**個人資料**一目了然。

怎麼預防

1. 購買好一點的**路由器**(**WPA3**)。
2. 在外**不亂連接網路**。
3. 不亂下載**來路不明的資料**。
4. **密碼**設難一點(比如：**ds5kh2ujfk@#*&特殊符號、英數夾雜**)
5. 使用**多重驗證**，雖然麻煩但安全。
6. 使用**VPN**跟**防毒軟體**，但治標不治本，改變個人**使用習慣**。

四. 學習反思

- 在學習過程中遇到什麼**困難**?你是如何**面對及克服**的呢?你是如何**面對並克服**這項挑戰的呢？
- 在學習過程中有什麼地方是值得再**努力或改進**的呢?為什麼?
- 在課堂結束後是否有興趣再進一步做學習的**延伸及探究**呢?為什麼?
- 是否能將學習到的東西**應用在生活**中呢?

四. 學習反思

- 主動向指導老師請教，並善用各類線上**學習資源**進行**補強**。
- 透過**網路安全等級**（如 **WPA**）與 **VPN** 等技術工具，有效聚焦學習重點，提升理解效率與學習成效。
- 延伸至網路安全的多元面向，更與**全球資訊化目標**及**永續發展策略**緊密相連。
- 轉化為**實質行動**，發揮深遠而積極的社會影響力。

資料來源

📡【WPA 安全等級與現況】

Wi-Fi Alliance – WPA3 Overview

🔗 https://www.wi-fi.org/discover-wi-fi/security

國家資通安全研究院（NICS） – 無線網路安全白皮書

🔗 https://www.nics.nat.gov.tw/

▫ WPA2 路由器被入侵的可能性

- Kaspersky – Can Routers Be Hacked?
  ☞https://www.kaspersky.com/resource-center/threats/can-routers-be-hacked
- CISA – Home Router Security Tips
  ☞ https://www.cisa.gov/news-events/news/securing-home-routers

🔓 常見 Wi-Fi 攻擊方式

- Perimeter81 – Wi-Fi Security Risks
  ☞ https://www.perimeter81.com/blog/zero-trust/wifi-security-risks
- Haptic Networks – 8 Wi-Fi Security Threats
  ☞ https://www.haptic-networks.com/wifi/8-wifi-security-threats
- CISA（美國資安局）– 無線網路安全建議
  ☞https://www.cisa.gov/news-events/news/securing-wireless-networks
- Portnox – Wireless Network Security Risks
  ☞https://www.portnox.com/cybersecurity-101/wireless-network-security-risks
- Cisco – What is Wi-Fi Security?
  ☞https://www.cisco.com/c/en/us/products/wireless/what-is-wi-fi-security.html
- ArXiv.org – Wi-Fi Security Vulnerabilities
  ☞ https://arxiv.org/abs/2412.15381

🍪 Cookies 是什麼？是否能被利用登入？

- Cloudflare – What Are Cookies?
  ☞https://www.cloudflare.com/learning/privacy/what-are-cookies/
  Mozilla MDN – HTTP Cookies Explained
  ☞https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
- OWASP – Session Hijacking via Cookies
  ☞https://owasp.org/www-community/attacks/Session_hijacking_attack

謝謝大家