Cybersecurity: Dos and Don’ts
網路安全知多少

We live in the world where more and more devices are connected to the Internet. Greater connectivity brings convenience and opportunities but also comes with higher security risks. Governments, businesses, and individuals are increasingly exposed to various kinds of cybersecurity threats. This August, chipmaker giant TSMC (Taiwan Semiconductor Manufacturing Company Limited) was forced to shut down several factories for three days after their computer systems were infected by a variant of the notorious ransomware WannaCry. This incident costs a roughly 2 percent loss in their third-quarter revenue. According to the public statement made by TSMC, the virus outbreak was not a result of cyber attacks launched by hackers but the consequence of an operational error. It is quite surprising that a big industry player like TSMC was vulnerable to security flaws.

現今，連網裝置的數量愈來愈多。高度的連結性帶給我們各種便利與商機，卻也提升了安全風險。政府、企業與個人都面臨愈來愈多的網路安全威脅。今年八月，半導體龍頭台積電的電腦系統受到名為「想哭」的勒索病毒變種感染，導致部分廠區生產停擺三天，使得第三季營收損失約 2%。據台積電聲明，此次病毒感染事件並非駭客攻擊，而是操作不當導致。連台積電這樣的科技大廠也出現資安漏洞，實在令人訝異。

Word Bank (字彙表)

1. cybersecurity (n.) 網路安全
2. infect (v.) 感染
3. variant (n.) 變體、變種
4. notorious (adj.) 惡名昭彰的
5. ransomware (n.) 勒索軟體
6. incident (n.) 事件
7. flaw (n.) 缺點、瑕疵
8. install (v.) 安裝
9. sophisticated (adj.) 複雜的
10. awareness (n.) 意識

When it comes to cybersecurity, many of us may think that as long as there is anti-virus software installed on our devices, we have nothing to worry about. However, as cyber threats and attacks become more sophisticated, anti-virus software is no longer enough. The incident at TSMC shows that human error is a big security problem. Cybersecurity starts with every individual. We as users of the Internet should have proper security awareness and practice good habits.

提到網路安全，很多人可能認為只要裝上防毒軟體就好了。然而，如今網路威脅與攻擊愈來愈複雜，防毒軟體已經不足以提供完整的防護。台積電的事件顯示，人為錯誤是資安的一大隱憂。網路安全要從每個人做起。身為使用者的我們，必須有正確的資安意識與良好的使用習慣。

Here is a list of dos and don’ts that can help you examine your cybersecurity habits.

Dos

1.Update your software and OS regularly.

Set up automatic updates for your software and OS so that whenever security patches are released, you can install them immediately.

2.Use complicated passwords.

Your password should be a combination of numbers, uppercase, and lowercase letters. Cybersecurity specialist Bruce Schneier proposes that a simple way to create a secure password is by using an English sentence and taking out the letters or words. For example, you can turn the following sentence “This little piggy went to market” into a strong password “tlpWENT2m.”

以下的網路安全守則，可以幫助你檢視自己是否具有良好的安全防護習慣。

應該做的事

1. 定期更新軟體與作業系統

設定好軟體與作業系統的自動更新，以即時安裝更新，修補安全漏洞。

2. 採用複雜的密碼

密碼最好是由數字、大寫字母與小寫字母組成。資安專家布魯斯・施奈爾指出，設定密碼的一個好方法，就是從一句英文句中擷取字母或字。例如，以下這句英文「This little piggy went to market」（這隻小豬到市場去）就可以轉成 tlpWENT2m 的高強度密碼。

3.Back up regularly.

Back up your data by using an external hard drive or a cloud storage service. Save more than one copy.

4.Use two-factor authentication.

Passwords are easy to guess and are sometimes too weak. Use two-factor authentication whenever possible to enhance the defense.

3. 定期備份資料

你可以利用外接硬碟或雲端儲存服務來備份資料，而且最好備份不只一份。

4. 使用雙重身份驗證

密碼很容易猜測，有時防護力也太弱。能使用雙重驗證的時候就使用，才能提升安全性。

Don’ts

1.Do not click on suspicious links or open unknown attachments.

Think twice before you click on any link in an email or in a social networking app. You might fall victim to a phishing scam. Also, never open untrusted attachments as they may contain malware.

2.Do not use the same password for different accounts.

Even if you have a strong password, it is unwise to use the same one across your accounts. Once your password is leaked, hackers can get access to all your account information.

3.Do not trust free stuff on the Internet.

Avoid downloading software or videos from unknown websites. They may contain spyware or malware that could compromise your computer.

4.Do not leave your computer unattended in a public place.

It is better not to leave your computer in a public place like a coffee shop or a restaurant. If you have to do so, remember to lock your screen so that no one can access your data without a password. You might also need a physical lock to chain your laptop to a table to protect it from being stolen.

不應該做的事

1. 不要點選可疑的連結或打開未知的附加檔案

   點選電子郵件或社交 app 上的連結前，務必三思。這些連結可能是網路釣魚詐騙的陷阱。不明的附加檔案也不要任意開啟，因為裡面可能含有惡意軟體。

2. 不要多個帳號共用密碼。

   即便你設定了強度夠強的密碼，多個帳號共用一個密碼也是不明智的作法。一旦你的密碼外洩，駭客就有機會獲取這些帳號的資料。

3. 不要相信網路上的免費好康

   避免從不明網站上下載免費影片或程式，裡面可能含有間諜軟體或惡意軟體，會導致你的電腦受感染。

4. 不要在公共場所離開自己的電腦

   在咖啡店或餐廳等公共場所使用電腦時，最好電腦不離身。如果要離開，記得鎖定螢幕，讓其他人無法登入來取得資料。必要時，請使用電腦鎖，避免電腦被偷。

Word Bank (字彙表)

1. patch (n.) 補丁、修補程式
2. release (v.) 發佈
3. authentication (n.) 認證
4. suspicious (adj.) 可疑的
5. phishing (n.) 網路釣魚
6. scam (n.) 詐騙
7. malware (n.) 惡意軟體
8. spyware (n.) 間諜軟體
9. compromise (v.) 危害
10. unattended (adj.) 無人看管的

◎資料來源

(1)https://www.secplicity.org/2018/01/26/top-security-habits-everyone-building-breaking-year/
(2)https://security.berkeley.edu/resources/best-practices-how-to-articles/top-10-secure-computing-tips
(3)https://www.schneier.com/blog/archives/2014/03/choosing_secure_1.html

◎圖片來源

(1)https://blog.trendmicro.com.tw/?p=50013
(2)http://www.sohu.com/a/165387504_99895981
(3)https://ppt.cc/fpIPtx
(4)https://ppt.cc/fVCrPx

◎應用外語系 丘羽先老師 編譯