DELL Technologies

網路安全速查表

在這個日漸虛擬的世界中，網路犯罪的成長速度充滿隱憂，卻也不令人意外。事實上，**網路犯罪在 2021 年產值約 6 兆美元**，躍升為繼美國和中國之後的第三大經濟體！*攻擊者越來越聰明，手法也越趨縝密，但只要注意最新威脅趨勢並設置好防護措施，保持線上安全並非難事。**試舉一些 Dell 網路安全專家致力防堵的威脅，並與您分享保護工作場所與住家安全的小祕訣。**

路過式入侵

小祕訣：
將瀏覽器和附掛程式保持在最新版本

惡意人士會在您誤入不安全或遭入侵網站時取得您系統的存取權限。

如何發現此情況：

您的系統出現新的檔案或網路連線，但不是您加入的來路不明的要求索取設定資訊

您的連線並不安全。

不安全的硬體

小祕訣：
向授權的銷售商購買產品

您知道印表機也會遭駭客攻擊嗎？

威脅發動者會將漏洞直接嵌入硬體和配件之中。

如何發現此情況：

過度誘人的好處

社交工程

小祕訣：
政府機關 (IRS 等) 會先透過 USPS 聯繫您

詐騙人士會假冒公司行號或其他權威機構操縱人們，藉此竊取他們的**個人或財務資訊** (即「網路釣魚」)。惡意程式碼則會透過連結或電子郵件附件、私訊及簡訊傳送。

如何發現此情況：

來路不明的電子郵件或簡訊要求索取個人資訊，並指示開啟連結和附件

奇怪的寄件者電子郵件地址、措辭、拼字

其中事有蹊蹺嗎？

USB 惡意軟體攻擊

小祕訣：
對未知的 USB 隨身碟保持警戒，就算是朋友的也不能掉以輕心

嗯...
插上這個
USB 隨身碟
安全嗎？

犯罪人士會使用卸除式儲存裝置，例如 USB 隨身碟、可攜式硬碟、智慧型手機、音樂播放器、SD 卡及光學媒體 (CD、DVD、藍光) 來感染電腦或網路。

如何發現此情況：

裝置上原有或新建檔案意外的存取權

受信任的關係

小祕訣：
使用不重複的高強度密碼

駭客會入侵受信任的第三方 (例如醫師辦公室)，並藉由醫師的聲望惡意利用病患。

如何發現此情況：

不尋常的登入行為

你是誰？

如何保持網路安全：

請務必

對所有帳戶使用多因素驗證和不重複的高強度密碼。

任何連線至網際網路的裝置都可能成為攻擊目標。請將軟體保持在最新版本。

保持警覺並處處提防。學習辨別詐騙伎倆。

積極知會相關人士。向 IT 團隊通報攻擊事件，並通知同事、家人和朋友。

應避免

切勿懈怠。請持之以恆地遵守所有資安規定。

切勿點按來路不明電子郵件或私訊內嵌的任何連結。

切勿忽略瀏覽器警告，例如：「您的連線不安全」或「您的連線並非私人連線」。

小祕訣：
如需詳細資訊，請前往：
Dell.com/Endpoint-Security

DELL Technologies

---

*Cybersecurity Ventures: 2022 Cybersecurity Almanac: 100 Facts, Figures, Predictions and Statistics (2022 年網路安全年鑑：百大事實、數據、預測及統計資料)