明智地使用網絡：「提高防護」

保障在線安全的簡單步驟

網絡詐騙非新鮮事；每天，黑客和其他網絡犯罪分子都在網上尋找最易於侵入的目標。你是否認為你不值得成為網絡掠奪者的目標？再想清楚！

無論是你的身份、銀行帳戶資訊，或是你電子郵件中的內容，這些資訊都是有價值的，網絡犯罪份子將不擇手段地取得。他們指望你認為自己不是目標，是時候***提高防護***，並採取措施防止自己成為網絡犯罪的受害者。

讓我們從基礎的網絡衛生知識開始——簡單且常識性地在線保護自己。以下是你今天可以做的四件簡單事情，來確保自己的網絡安全：

- **於所有帳戶使用多於一項的身份驗證。**一個密碼不足以保證你在線的安全。通過加入第二層識別，例如確認短信、來自身份驗證應用程式的代碼、面部或指紋驗證或安全密鑰，你將向你的銀行、電子郵件提供商或正在登錄的任何其他網站，提供進入的額外安全層。多重身份驗證可以使被黑客入侵或資訊被盜的可能性降低 99%！
- **更新軟件。**黑客會嘗試利用軟件的缺陷和漏洞。更新所有設備，如手機、平板電腦和筆記本電腦上的系統軟件，確保定期檢查所有設備上的應用程式更新——尤其是網絡瀏覽器。只須打開所有設備、應用程式和操作系統的自動更新，便可以輕鬆處理。
- **點擊前請三思。**超過 90%的成功網絡攻擊始於你點擊網絡釣魚電子郵件中不熟悉的鏈接。網絡釣魚計劃是指鏈接或網頁看起來正規，但這是一種旨在讓你洩露密碼、信用卡號或其他敏感資訊的騙術。此外，網絡釣魚電子郵件可能會試圖讓你運行毒害軟件，也稱為惡意軟件。若是不認識的鏈接，請相信直覺，並在點擊前三思。
- **使用加強密碼。**加強密碼應該是八個或更多字符，使用字母、數字和特殊字符的組合。避免在不同帳戶上使用相同的密碼。理想情況下，個人還應使用密碼管理器來生成和存儲獨特密碼。

世界變得越來越數字化，相互聯繫越來越緊密，我們都有責任盡力保護我們所依賴的電腦網絡。成為網絡安全的擁護者，並與你的朋友、家人和鄰居分享這些提示。

欲了解更多資訊，請訪問 CISA 的提高防護網頁 (CISA's Shields Up webpage)。