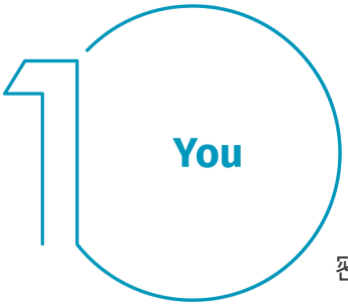
SANS SECURITY AWARENESS

在家中安全工作的五大步驟

我們明白你可能從未嘗試過在家工作，因此在適應新的情況時，可能感到不知所措。我們的目標之一，便是讓你能夠在家中盡可能地安全工作。以下有五個簡單的步驟可讓你安全工作。這些步驟不僅有效並可協助保護你的工作，而且如果你擁有網路安全的家園，能使你和你的家人更加安全。



你：首先，最需要了解的是，技術不能完全保護你，因為你才是最好的防禦。攻擊者明白要怎樣才能得到他們想要的東西，最簡單的方法是鎖定你，而不是你的電腦或者其他裝置。如果他們想要你的密碼、工作資料或者電腦控制權，他們會試圖製造迫切感來威脅你提供給他們。例如，他們可以打給你，自稱是微軟技術支援人員，告知你的電腦已被感染。又或者，他們可能發送電子郵件給你，警告你的包裹無法派送，從而欺騙你點擊惡意連結。社交工程攻擊最常見的跡象包括：

- 有些人會營造出極大的迫切感，經常是利用恐懼、恐嚇、危機或重要的最後期限。網路攻擊者擅長製作令人信任的訊息，這些訊息似乎來自受信任的機構，例如銀行，政府或國際組織。
- 利用急迫感要求繞過或忽視安全政策或步驟，或者報酬美好得不切實際(不要想了，你才沒有中獎！)
- 你收到來自朋友或同事發出的訊息，但訊息中的簽名、語氣或措辭聽起來並不像他們。

因此到頭來，抵禦這些攻擊的最佳方法就是你。

家庭網路：幾乎每個家庭網路都使用無線網路(通常稱為Wi-Fi)。這讓你所有裝置都能夠連接到網際網路。大部分家中的無線網路都經由路由器或單獨的專用無線存取點控制。兩者的運作方式相同：通過廣播無線訊號的方式，讓家中裝置能夠連接。這代表保護你的無線網路，就是保護你家中的重要部分。我們建議執行以下步驟來保護它：

- 更改你無線網路裝置的預設管理員密碼。管理員帳號讓你能夠設定無線網路的參數。
- 確保只有你信任的人才可連接到你的無線網絡。透過這一步能夠實施強大的安全性。若啟用此功能，其他人需要密碼才能連接到你的無線網路，而且一旦連接，他們的網上活動就會被加密。
- 務必確認用來連接到你的無線網路的密碼是使用高強度密碼，並且要與管理員密碼不同。請謹記，你只需為每個裝置輸入密碼一次，因為它們會儲存並記住密碼。

不確定要如何執行這些步驟嗎？諮詢你的網路服務供應商、查詢他們的網站、閱讀無線存取點所附的文件，或者瀏覽供應商的網站。

密碼：若網站要求你建立密碼，請建立一個高強度密碼，字元越多，密碼強度越高。使用密碼短語是確保你擁有高強度密碼的最簡單方法之一。密碼短語是由多個單詞組成的密碼，例如「*蜜蜂 蜜糖 波本酒。*」使用獨一無二的密碼短語，代表對每個裝置或網上帳號均使用不同的密碼。如此一來，即使有人知道其中一個密碼短語，也不會影響到其他帳號和裝置的安全。無法記住所有密碼短語嗎？

你可以使用密碼管理器，密碼管理器是一個密碼儲存專用程式，可以安全地以加密格式儲存所有密碼短語，並且還具有許多強大的功能！最後，請盡可能地使用兩步驗證(又稱為雙重驗證)。它使用了你的密碼，但還增加了第二個步驟，例如傳送驗證碼到智能手機，或為你產生驗證碼的應用程式。兩步驗證可能是保護網上帳號最重要的步驟，而且比你想像中容易得多。

更新：確保你每台電腦、流動裝置、程式和應用程式都是執行最新版本的軟件。網路攻擊者一直都在尋找你正在使用的裝置中所有軟件的新漏洞。當他們發現漏洞時，會使用特殊程式來利用它們，並入侵你正在使用的裝置。與此同時，為這些裝置開發軟件的公司，正在努力透過發布更新來修復它們。確保你經常為你的電腦和流動裝置安裝這些更新，這樣便可以使他人更難入侵。若要保持在最新狀態，盡可能開啟自動更新即可。此規則幾乎適用於可連接到網路的所有科技產品，不僅包括你工作上的裝置，還包括連接到網路的電視、嬰兒閉路電視、監控閉路電視、家用路由器、遊戲機，甚至你的汽車。

孩童或客人：在辦公室時你最不會擔心的是，正在使用你的工作上手提電腦或其他工作裝置的孩童，客人或其他家庭成員。確保家人和朋友明白不可使用你的工作裝置，因為他們可能會不小心誤刪或修改資料，或者更糟糕的是不小心感染裝置。