2021年網路安全宣導月:
儘到您的責任。#BeCyberSmart

旅行期間的網路安全

在我們時時刻刻都連接的世界中，網路安全不能僅限於在家裏或辦公室。當您旅行時 — 無論是在國內還是國際旅行 — 實行安全的線上行為並採取積極措施來保護網際網路啟用的設備總是很重要的。我們旅行的次數越多，遭受網路攻擊的風險就越高。#BeCyberSmart 並使用這些提示在旅途中充滿信心地連接。

簡單提示

在您走之前

- **如果您連接它，就保護它。**無論是您的電腦、智慧型手機、遊戲設備還是其他網路設備，抵禦病毒和惡意軟體的最佳方法是更新到最新的安全軟體、網路瀏覽器和操作系統。如果您可以的話，請登記接受自動更新，並使用防毒軟體來保護您的設備。請參閱 釣魚郵件提示表以瞭解更多資訊。
- **備份您的資料。**將您的聯繫人、財務數據、照片、視訊和其他行動設備數據備份到另一台設備或雲端服務，以防您的設備受到損害，您必須將其重新設置為出廠時的設置。
- **只與您信任的人聯繫。**儘管某些社交網路可能看起來比較安全，因爲通過它們分享的個人資訊有限，但請與您認識和信任的人保持聯繫。
- **保持最新的版本。**將您的軟體更新到可用的最新版本。通過打開自動更新來維護您的安全設置以確保您的資訊安全，這樣您就不必考慮它並將安全軟體設置為執行定期掃描。
- **雙重登入保護。**啟用多重身份驗證 (MFA) 以確保只有您可以使用您的帳戶。將其用於電子信件、銀行業務、社交媒體和任何其他需要登入的服務。如果 MFA 是一個選項，請使用可信賴的行動設備來啟用它，例如您的智慧型手機、身份驗證器應用程式或安全令牌 - 一個小的可以掛在鑰匙圈上的實體設備。請參閱 多重身份驗證 (MFA) 操作指南 以瞭解更多資訊。

在您的旅途期間

- **停止自動連接**某些設備會自動地搜索並連接到可用的無線網路或藍牙設備。這種即時的連接為網路犯罪分子遠程使用您的設備打開了大門。關掉這些功能，以便您主動選擇何時連接到安全的網路。

- **連接時要保持保護。**在您連接到任何公共無線熱點－例如在機場、旅館或咖啡廳－之前，請務必與適當的工作人員確認網路名稱和準確的登入程序，以確保該網路為合法的。如果您確實使用不安全的公共接入點，請避免需要密碼或信用卡的敏感活動（例如銀行業務），以保持良好的互聯網衛生習慣。您的個人熱點通常比免費的無線傳輸系統（ Wi-Fi） 更安全。當網上購物或辦理銀行業務時，僅使用以“https://”開頭的網站。
- **儘力與陌生人相處。**網路犯罪分子使用網路釣魚策略，希望騙到他們的受害者。如果您不確定電子信件的發件人 － 即使細節看起來準確 － 或者電子信件看起來很像“釣魚”的樣子，請不要回覆，也不要點擊該電子信件中的任何連結或附件。如果得以使用的話，請使用“垃圾”或“攔阻”的選項以不再接收來自特定發件人的消息。請參閱 釣魚郵件提示表以瞭解更多資訊。
- **絕對不要點擊並告知。**限制您在社交媒體上發布的消息——從個人的地址到您喜歡去喝咖啡的地方。許多人沒有意識到，這些看似隨機的細節都是犯罪分子需要知道的，以便在網上和現實世界中盯上您、您的親人和您的實體財物。將社會安全號碼、帳號和密碼以及有關您自己的特定資訊，例如您的全名、地址、生日，甚至假期計劃保持私密。關掉允許任何人在任何給定的時間查看您的位置 － 和您不在的位置 － 的定位服務。請參閱 社交媒體網路安全提示表以瞭解更多資訊。
- **保護您的行動設備。**為了防止盜竊和未經授權的使用或丟失敏感的資訊，切勿將您的設備（包括任何 USB 或外部存儲設備）放在無人看管的公共場所。在計程車、機場、飛機和旅館房間內，請妥善保管您的設備。

聯繫CISA的網路安全宣導月團隊

感謝您對網路安全宣導月的持續支持與承諾，同時幫助所有美國人保持在線安全和可靠。請發電子信件給我們的團隊到 CyberAwareness@cisa.dhs.gov 或造訪 www.cisa.gov/cybersecurity-awareness-month 或 staysafeonline.org/cybersecurity-awareness-month/ 以瞭解更多。