對網路要變得聰明起來
#CyberMonth

2021年網路安全宣導月:
儘到您的責任。#BECYBERSMART

保護您的數位住家

我們更多的家用設備—包括恆溫器、門鎖、咖啡機和煙霧報警器—現在都連接到了網際網路。這使我們能夠在智慧型手機上的控制設備，從而節省了我們的時間和金錢，同時還提供了便利甚至安全。這些科技進步具有創新性和吸引力，但是它們也帶來了一系列新的安全風險。#BeCyberSmart 充滿信心地連接並保護您的數位住家。

簡單提示

- **保護您的無線傳輸系統（Wi-Fi）網路。**您家中的無線路由器是網路犯罪分子使用您所有連接設備的主要入口。通過更改默認密碼和用戶名來保護 Wi-Fi 和數位設備。有關保護您家裏網路的更多資訊，請查看 CISA 的保護無線網路的網頁。
- **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。
- **如果您連接，您必須保護。**無論是您的電腦、智慧型手機、遊戲設備還是其他網路設備，最佳的防禦措施是更新到最新的安全軟體、網路瀏覽器和操作系統。如果您可以選擇啟用自動更新以防禦最新的風險，請將其打開。還有，如果您將某些東西放入設備中，例如用於外部硬碟的 USB，請確保您設備上的安全軟體對病毒和惡意軟體進行掃描。最後，使用防病毒軟體來保護您的設備，並確保定期備份任何無法重新創建的數據，例如照片或個人文件。
- **密切注意您的應用程式。**大多數聯網電器、玩具和設備都由一個行動應用程式來支持。您的行動設備可能充滿了在後台運行的可疑應用程式，或者使用您從未意識到自己已批准的默認權限——在您不知情的情況下收集您的個人資料，同時還將您的身份和隱私置於危險之中。檢查您的應用程式的權限並使用“最小權限規則”刪除您不需要或不再使用的功能。要學會對沒有意義的特權請求說“不”。僅從可信賴的供應商和來源下載應用程式。

- **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。
- **使用檔案分享時要小心。**不需要時應禁用設備之間的檔案分享。您應該始終選擇只允許通過在家裏或工作的網路來分享檔案，而不要在公共網路上分享。您可能需要考慮為檔案分享創建一個專用的目錄並限制對所有其他目錄的使用。此外，您應該用密碼保護您分享的任何內容。
- **檢查您的網際網路提供商或路由器製造商的無線安全選項。**您的網際網路服務提供商和路由器製造商可能會提供資料或資源來幫助保護您的無線網路。查看其網站的客戶支持區域以獲取具體的建議或說明。
- **使用虛擬專用網路 (VPN) 進行連接。**許多公司和組織都有 VPN。VPN 允許員工在離開辦公室時安全地連接到他們的網路。VPN 在發送端和接收端對連接進行加密，並將未正確加密的流量拒之在外。如果您可以使用 VPN，請確保在需要使用公共無線接入點時隨時登入。
- **限制使用。**只允許授權的用戶使用您的網路。連接到網路的每個硬件都有一個媒體使用控制 (MAC) 地址。您可以通過過濾這些 MAC 地址來限制對網路的使用。有關啟用這些功能的具體資訊，請查閱您的用戶文件。您還可以使用“訪客”帳戶，這是許多無線路由器上廣泛使用的功能。此功能允許您使用單獨的密碼在單獨的無線信道上授予訪客無線使用的權限，同時保護您的主要憑據的隱私。

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。