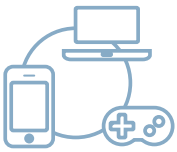
做好應對
網路攻擊準備

網路攻擊可能導致金錢損失、個人信息被盜以及您的聲譽和安全受損。

FEMA

FEMA P-2258/2018 年 6 月

網絡攻擊為惡意嘗試，以訪問或破壞計算機系統。



可使用電腦、手機、遊戲系統等設備

可包括欺詐或身份盜用

可阻止您的訪問或刪除您的個人文檔和圖片

可能針對兒童

可能導致商業服務、交通和電力方面的問題

保護自己免受網路攻擊

保持軟體和作業系統為最新狀態。

使用加密（安全）的網際網路通信。

使用強密碼和雙因素身份驗證（兩種方法驗證）。

創建備份檔。

注意可疑活動。如有疑問，請勿點擊。請勿提供個人資訊。

保護您的家庭 Wi-Fi 網路。

當網路攻擊來襲
如何保持安全

現在做好預防

及時更新您的防病毒軟體。

使用 具有 12 個字元或更長的強密碼。使用大寫和小寫字母、數字和特殊字元。每月更改密碼。使用密碼管理器。

使用更強的身份驗證, 例如只有 **您會知道的個人身份識別號碼 (PIN) 或密碼。**考慮使用可接收代碼或使用 **生物特徵掃描** 的單獨設備（例如指紋掃描儀）。

注意以下可疑活動: 要求您立即執行某些操作、提供給你聽起來好得難以置信的東西，或需要您的私人資訊。**點擊前, 請三思。**

定期檢查您的帳戶對帳單和信用報告。

使用安全的網際網路通訊。如果您將訪問或提供任何個人資訊，請使用帶有「HTTPS」的網址。請勿訪問證書無效的網址。使用創建 安全連接的虛擬專用網路（VPN）。

使用防病毒解決方案、惡意軟體和防火牆來攔截威脅。

定期備份文檔, 存於加密文件或加密文件存儲設備中。

限制您在線上共享的私人資訊。更改隱私設置，請勿使用定位功能。

通過定期更改網路管理和 Wi-Fi 密碼來保護您的家庭網路。配置路由器時，選擇 Wi-Fi 保護訪問 2 (WPA2) 高級加密標準 (AES) 設置，此爲最強的加密選項。

期間限制損害

限制損害。查看是否有不明原因收費、您信用報告上的奇怪帳戶、您信用卡意外被拒、帖子非您發的卻出現在您的社交網路上，以及您沒發電郵別人卻收到。

立即更改您所有線上帳戶的密碼。

掃描並清理您的裝置。

考慮關閉裝置。將其交給專業人士進行掃描和修復。

通知工作單位、學校或其他系統擁有者。信息技術 (IT) 部門可能需要警示其他人並升級系統.

與銀行、信用卡公司和其他金融帳戶聯繫。您可能需要暫停受到攻擊的帳戶。關閉任何未經授權的信貸或收費賬戶。報告有人可能盜用您的身份。

進行上報事後

如果您認為有人非法使用您的社會安全號碼，請向 **監察長室 (OIG)** 提交報告。**OIG 審查浪費、欺詐和濫用案件。**欲提交報告，請造訪 www.idtheft.gov。

您也可以撥打社會保障局熱線 1-800-269-0271。如需額外資源和更多資訊，請造訪 http://oig.ssa.gov/report。

通過 www.IC3.gov 向 FBI 網際網路犯罪投訴中心 (IC3) 提出投訴。投訴將予以審查，並提交至適當的機構。

請經 www.stopthinkconnect.org 來**瞭解技巧、工具等。**

FEMA

FEMA P-2258

主動掌控您的安全

请前往 **Ready.gov/cybersecurity。**請下載 **FEMA 應用程式**以獲取有關做好防**網路攻擊**準備的更多資訊。