2021年網路安全宣導月:
儘到您的責任。#BECYBERSMART

身份盜竊和網際網路詐騙

今天的科技使我們能夠連接到世界各地，在線上進行銀行業務和購物，並通過我們的智慧型手機控制我們的電視、住家和汽車。這種額外的便利也增加了身份盜竊和網際網路詐騙的風險。#BeCyberSmart 在網際網路上 — 在家中、在學校、在工作中、在行動設備上以及在旅途中。

您知道嗎？

- 2020 年一家美國公司數據外泄的平均損失為 884 萬美元 [1]。這比 2019 年 864 萬美元的數字有所增加。
- 7-10% 的美國人口每年都成為身份欺詐的受害者，其中 21% 的人經歷過多次身份欺詐 [2]。
- 在2020 年, 47% 的美國居民曾經歷過身份盜竊[3]。

常見的網際網路詐騙

隨著科技的不斷發展，網路犯罪分子將使用更複雜的技術來利用系統、帳戶和設備來竊取您的身份、個人資訊和金錢。為了保護自己免受線上的威脅，您必須知道要可疑的跡象。一些最常見的網際網路詐騙包括：

- **2019年冠狀病毒疾病（COVID-19）詐騙**採用帶有惡意的附件或欺詐網站連結的電子信件的形式，誘使受害者透露敏感的資訊或向欺詐性慈善機構或慈善事業進行捐款。在處理任何帶有 COVID-19 相關的主題行、附件或超連結的電子信件時要謹慎小心，並警惕與 COVID-19 相關的社交媒體的請求、簡訊或電話。
- **冒名頂替的詐騙**就在您收到自稱是政府官員、家人或朋友要求提供個人或財務資訊的電子信件或電話時發生。例如，冒名頂替者可能會從社會安全局來聯繫您，通知您您的社會安全號碼 (SSN) 已被暫停，希望您能透露您的 SSN 或付費以重新使用它。
- **COVID-19 經濟補助金詐騙**針對美國人的刺激經濟補助金。CISA 敦促所有美國人注意與 COVID-19 經濟影響補助金相關的犯罪欺詐 - 特別是利用冠狀病毒為誘餌來竊取個人和財務資訊的欺詐行為，以及經濟影響補助金本身 - 以及試圖破壞補助金支付工作的敵對方。

簡單提示

- **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。
- **改變您的密碼協議。**根據美國國家標準與科技研究院 (NIST) 的指導方針，您應該考慮使用允許的最長密碼或密碼短語。發揮創意並為不同的網站定制標準密碼，這可以防止網路犯罪分子使用這些帳戶並在發生違規情況時保護您。使用密碼管理程式來為您的每個帳戶產生並記住不同的複雜密碼。請參閱 創建密碼提示表 以瞭解更多資訊。
- **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

保護您自己免受線上欺詐

連接時要保持保護: 最重要的是，只要您在線上，您就很容易受到攻擊。如果您的聯網的設備因任何原因遭到入侵，或者駭客突破了加密防火牆，則有人可能正在竊聽您 - 即便是在您自己家中使用加密的無線傳輸系統（Wi-Fi）。

- 通過檢查瀏覽器欄中的“綠色鎖”或掛鎖圖標，無論您身在何處，都可以實行安全的瀏覽網頁 - 這表示連接安全。
- 當您發現自己身處一望無際的“曠野 Wi-Fi 西部”時，請避免使用沒有加密的免費網際網路連接。
- 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綫傳輸系統（Wi-Fi） 更安全。
- 不要向未知的來源透露個人身份資訊，例如您的銀行帳號、SSN 或出生日期。
- 直接在地址欄中打入網站的 URL，而不是點擊連結或從電子信件中進行剪貼。

您可以使用的資源

如果您發現自己成為網路犯罪的受害者，請立即通知當局提出投訴。保留並記錄該事件及其可疑來源的所有證據。如果您是網路犯罪的受害者，以下的清單略述哪些政府組織您可以向其提出投訴。

- **FTC.gov**: 聯邦貿易委員會（FTC）的免費一站式資源, www.identitytheft.gov/可以幫助您舉報身份盜竊並進行恢復工作。向 FTC 舉報欺詐行為，可在 ftc.gov/OnGuardOnline 或 www.ftccomplaintassistant.gov/ 上進行。
- **US-CERT.gov**: 通過熱線向美國電腦應急準備小組（US-CERT）舉報電腦或網路安全漏洞：1-888-282-0870 或 us-cert.cisa.gov。通過 phishing-report@us-cert.gov 將網路釣魚電子信件或網站轉發給 US-CERT。
- **IC3.gov**: 如果您是線上犯罪的受害者，請在 www.ic3.gov/向網際網路犯罪投訴中心 (IC3) 提出投訴。
- **SSA.gov**: 如果您認為有人正在使用您的 SSN，請致電社會安全局的欺詐熱線 1-800-269-0271。

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 https://www.cisa.gov/cybersecurity-awareness-month 或 staysafeonline.org/cybersecurity-awareness-month/ 以瞭解更多。

資源

1. 布魯克，克里斯（Brook, Chris）。(2020年 8 月18日)。*2020 年數據外泄的損失是多少?* 數位衛士。 https://digitalguardian.com/blog/what-does-data-breach-cost-2020
2. 里克斯，A，歐文-埃里克森，Y（Ricks, A, Irvin-Erickson, Y），博士 (2021年)。*研究簡報：身份盜竊和欺詐。* 受害者研究中心。https://ncvc.dspacedirect.org/bitstream/item/1228/CVR Research Syntheses_Identity Theft and Fraud_Brief.pdf
3. GIACT。(2021)。*美國身份盜竊：*赤裸裸的現實。GIACT 系統有限責任公司。https://www.giact.com/aite-report-us-identity-theft-the-stark-reality/