SANS SECURITY AWARENESS

安全意識部署指引–
如何家中安全工作

執行摘要

由於冠狀病毒關係，許多機構將工作場所從公司改為家中。這可能會帶來挑戰，因為許多機構缺乏保障遙距工作員工的安全政策、技術和培訓。甚至眾多員工可能不明白或不熟機在家工作要注意的安全要點。本指引的目的是讓你能夠快速訓練員工，讓大家盡可能安全工作。如果你對本指引有任何疑問，請透過support@sans.org與我們聯絡。

由於你的員工很可能正經歷龐大的壓力和變化，再加上你的機構很可能受到時間和資源的限制，因此本指引的重點是讓訓練盡可能簡單。我們建議你著重在會帶來重大影響的事物，以及最重大的風險，這些內容將在下方進一步介紹。請將這些視為起點。如果你要加入其他風險或主題，請務必這樣做。你要理解如果要求員工完成的行為、流程或技術越多，則員工會確切實踐所有指示的可能性就越低。

如何使用本指引

我們建議你首先閱讀本指引中的教材，並瀏覽指引內所提供的不同教材連結，以便你對可用的教材有所了解。你會注意到我們對於每種風險，提供各種不同的教材，你可以使用這些教材來管理和訓練你的組織。這使你能夠選擇最合適自己需求和文化的方式。在閱讀完本文件後，請閱讀此套裝附件的「宣導範例」和「概況介紹」，以更加了解你要實踐的目標。閱讀完文件後，你需要與兩個核心團隊溝通。

1. **資訊安全團隊**：與你的資訊安全團隊溝通，這樣可以更加了解你要管理的主要風險。我們在本指引中，列出了在家中工作的員工將會面臨到的常見風險，但你遇到的風險可能會有所不同。提醒一下，資訊安全團隊常犯的一個錯誤，便是試圖控制所有風險，並以諸多的政策和要求，讓大家眼花瞭亂。嘗試將要解決的風險降到最低。一旦了解並確定了這些風險的優先順序，請確認管理這些風險的行為。如前面所提，如你的機構沒有足夠的時間或資源，請利用我們下面提供的文件。

2. **宣導**：一旦確定了最高級別的人為風險和風險管理的核心行為，便可與你的宣導團隊合作，並採用這些行為與員工互動。最有效的安全意識課程，便是要與他們的宣導團隊有著牢固的伙伴關係。如果可行，請看一下你是否可以將某人從宣導單位中併入到你的資訊安全團隊中。向員工宣導時，你可以說明這種訓練不單是可以確保他們在工作中的安全，還可以幫他們建立安全的家庭網路，更能夠保護自己和家人，這是非常有效的誘因。

最後，透過與這兩個團隊合作，可以讓員工的資訊安全性變得更容易實踐，更能激發員工主動積極配合，而有兩個核心元素是行為和改變。我們建議你建立一個由重要人員組成的顧問委員會，你需要他們的回饋和建議，才可順利推行訓練。除了你的安全和宣導團隊外，你可能希望與其他部門合作，包括人力資源和法律部門。

MGT433數碼下載包

SANS Institute提供為期兩天的培訓課程MGT433：如何建立、維護和評估高影響力的安全意識課程。這個速成班提供所有理論、技能、框架和資源，以建立高影響力的意識課程，使你能夠有效管理和衡量人為風險。作為本指引中的一部分，我們免費提供課程的數碼下載包的範例和計畫資源。即便這些教材很有可能超出了這個計劃的需求，但對於較大的機構或更複雜的部門而言，這些教材可能有用。

回應員工的問題

除了與你的員工進行宣導和訓練外，我們強烈建議你使用技術討論區或論壇，以便可以即時回答大家的問題。這些討論可以在像是專用的電郵別名、Skype或Slack聊天媒體，或是如Yammer的網上論壇等進行。另一個想法是每週舉行數次安全性網路直播，以便大家可以選擇最合適的時間參加活動，甚至可以提出問題。目的是要將安全意識盡可能地宣導給大家知道，並幫助他們解決問題。這是一個非常好的機會，可以鼓勵你的員工，並讓安全議題變得容易親近，請試著利用直播帶來的優勢。請記住，為了有效做到這一點，我們建議你使用這些資源來審核這些管道和回應問題。

風險與培訓教材

我們已明白應該要為遙距工作的員工定下三個核心風險管理措施。這是只是起始步驟，但很可能會為你帶來龐大的價值。以下每個風險管理措施都有多個相關資源的連結，以協助宣導和培訓。我們提供多種宣導教材，因此你可以選擇你合適的教材。此外，幾乎所有教材都提供多種語言版本。如果這些內容還是太多，而你的時間也非常有限，那麼我們建議你簡單使用並部署下面列出的兩種教材。

1. 在家安全工作指引(此指引附在你的部署套件)。
2. 建立安全的家庭網路影片(英文)可選擇其他語言。

社交工程

社交工程攻擊是遙距工作員工所面臨的最大風險之一，尤其是在這瞬息萬變的形勢和緊迫的環境。社交工程是一種心理攻擊，攻擊者誘導或欺騙他們犯錯，這在緊張和混亂時會更容易發生。關鍵是要讓大家了解什麼是社交工程，如何發現最常見的社交工程攻擊跡象，以及發現社交工程攻擊時該怎麼應對。確保你不僅是專注在電子郵件網路釣魚攻擊，還關注其他途徑，如電話、短訊、社交媒體或假新聞。你可以在我們的社交工程支援教材資料夾中，找到你可用來進行培訓和教學的教材。另外，這是你可以連結的兩部SANS安全意識影片，再次提醒你，影片有多種語言可選擇。

- 社交工程(英文)可選擇其他語言
- 網路釣魚(英文)可選擇其他語言

高強度密碼

正如一年一度由Verizon DBIR發表的資料洩露調查報告中所指出，弱強度密碼仍然是全球破壞力最高的問題之一。下面列出了四種有助於管理此風險的關鍵行動。你可以在我們的密碼資料夾中，找到可用來進行培訓和教學的素材。

- 密碼短語(注意，密碼複雜度和密碼期限已無效)。
- 每個帳號皆設定獨一無二密碼。
- 密碼管理員
- MFA(多重驗證)。通常稱為兩步驗證或雙重驗證

更新系統

第三個風險是確保你的員工所使用的任何科技產品都是執行最新版本的操作系統、應用程式和行動應用程式。如果使用個人裝置，則可能需要開啟自動更新。你可以在我們的惡意軟件或者建立家庭網路安全資料夾中，找到你可用來進行培訓和教學的素材。

思考其他議題

- **Wi-Fi**：保護你的Wi-Fi存取點這包括在建立家庭網路安全教材中，此外，你也可以在建立家庭網路安全影片(英文)選擇其他語言。
- **VPN**：什麼是VPN，為什麼你需要使用的原因。我們建議瀏覽OUCH電子報關於VPN的說明。
- **遙距工作**：這適用於不是在家中工作的遙距工作，例如咖啡店、機場客運大樓或酒店。參考我們的遙距工作培訓影片(英文) 可選擇其他語言。
- **孩童或客人**：為了強化家庭或客人不應使用與工作相關的設備的想法，參考我們的遙距工作培訓影片(英文)可選擇其他語言。
- **發現或回應**：你是否會想讓大家回報，他們在家中工作時發生了事情？如果是，你希望他們在什麼時間回報？這在我們的侵入攻擊教材**時有提到。**

OUCH電子報

此外，考慮使用公開且實用的OUCH電子報來協助你的培訓，每份電子報都會翻譯成20多種語言。以下列出的是OUCH電子報，這些電子報是我們認為可以很有效協助你在家中安全地工作的要點。你可以在網上找到所有的電子報OUCH安全意識電子報檔案。

總覽

Four Steps to Staying Secure (確保安全的四大步驟)
https://www.sans.org/security-awareness-training/resources/four-simple-steps-staying-secure

Creating a Cybersecure Home (建立一個網路安全的家園)
https://www.sans.org/security-awareness-training/ouch-newsletter/2018/creating-cybersecure-home

社交工程

Social Engineering (社交工程)
https://www.sans.org/security-awareness-training/ouch-newsletter/2017/social-engineering

Messaging / Smishing (訊息釣魚攻擊/簡訊釣魚攻擊)
https://www.sans.org/security-awareness-training/resources/messaging-smishing-attacks

Personalized Scams (量身打造的詐騙)
https://www.sans.org/security-awareness-training/resources/personalized-scams

CEO Fraud (CEO詐騙)
https://www.sans.org/security-awareness-training/resources/ceo-fraudbec

Phone Call Attacks / Scams (電話攻擊或詐騙)
https://www.sans.org/security-awareness-training/resources/phone-call-attacks-scams

Stop That Phish (預防網路釣魚)

https://www.sans.org/security-awareness-training/resources/stop-phish

Scamming You Through Social Media (社交媒體詐騙)
https://www.sans.org/security-awareness-training/resources/scamming-you-through-social-media

密碼

Making Passwords Simple (讓管理密碼更簡單)
https://www.sans.org/security-awareness-training/resources/making-passwords-simple

Lock Down Your Login (2FA) (把關登入大門，採用雙重驗證)
https://www.sans.org/security-awareness-training/ouch-newsletter/2017/lock-down-your-login

補充資料

Yes, You Are a Target (沒錯，你就是目標)
https://www.sans.org/security-awareness-training/resources/yes-you-are-target

Smart Home Devices (智能家居裝置)
https://www.sans.org/security-awareness-training/resources/smart-home-devices

快速提示

你可以輕鬆分享提示和技巧。

- 要在家中保護無線網路，最有效的步驟就是更改預設的管理員密碼，開啟WPA2加密並為無線路使用高強度密碼。
- 隨時注意連接到家庭網路的所有裝置，包括嬰兒閉路電視、遊戲機、電視、家庭電器甚至汽車。確保這些裝置都受到高強度的密碼保護和/或正在執行最新版本的操作系統。

- 在家中保護電腦的最有效的方法之一，就是確保操作系統和應用程式都進行了軟件更新和修正。另外，請盡可能開啟自動更新功能。
- 到頭來，常識才是你的最佳保護。如果電子郵件、電話或網上訊息看起來很奇怪、可疑或太過美好，則可能是攻擊。
- 確保每個帳號都有一個獨一無二的密碼。無法記住所有密碼/密碼短語嗎？不妨使用密碼管理員來幫你安全管理所有密碼。
- 兩步驗證是確保任何帳號安全的最佳方法之一。兩步驗證即是需要密碼和提供傳送至流動裝置或由流動裝置產生的驗證碼。支援兩步驗證的服務例子，包括Gmail、Dropbox和Twitter。
- 網路釣魚是指攻擊者試圖欺騙你點擊惡意連結或開啟電子郵件中的附件。對任何產生緊張感、拼寫錯誤、稱呼你為「尊敬的客戶」的電郵或網上訊息要時刻保持懷疑。

度量

在這種情況下，行為度量非常困難，因為要衡量大家在家中的行為更加困難。此外，其中某些行為並非特定於工作上(例如保護他們的Wi-Fi裝置)。但是，你可以測量參與度。我們發現像這樣的個人或創新主題可能非常吸引人，比起其他主題引起了更大的興趣。因此，類似的度量可能很有用。

- **互動**：大家經常在你負責的平台或論壇上提問、發表想法或尋求幫助嗎？
- **模擬**：進行某種社交工程的模擬，例如網路釣魚、發短訊或電話攻擊。

要獲取更完整的度量列表，請從MGT433數碼下載包中下載互動式安全意識度量矩陣。

授權

部署套件作者

Lance Spitzner在研究網路威脅、安全性架構以及意識和培訓方面擁有20多年的資訊安全經驗。他透過創辦Honeynet和成立Honeynet計畫，幫助開拓了網路詐欺和網路情報的領域。作為SANS的講師，他撰寫了MGT433：安全意識以及MGT521：安全文化的課程。此外，Lance還出版了三本資訊安全的書籍，並在25個國家提供諮詢，並幫助了350多個組織建立了安全意識和文化計劃以管理人為風險。Lance經常演講、在推特發布推文(@lspitzner)，以及在眾多團體安全項目中工作。在從事資訊安全範疇前，Spitzner先生曾在陸軍快速部署部隊擔任裝甲官，並在伊利諾大學取得了工商管理碩士學位。

關於SANS Institute (系統與網路安全協會)

SANS Institute (系統與網路安全協會)成立於1989年，是一個共同研究和教育的組織。SANS現為最大網路安全培訓和認證的供應商，派出專業人員提供課程給全球政府和商業機構。著名的SANS講師已教授了高達200多場的網路安全培訓活動，以及在網上教授60多種不同的課程。GIAC是SANS Institute的認證機構，透過測試超過35個項目來驗證從業者是否具有網路安全技術認證的資格。SANS Technology Institute是一家獲得地區認可的獨立子公司，提供網路安全碩士學位。SANS為InfoSec社區提供了許多免費資源，包括共識計畫、研究報告和新聞通訊；它還執行著網路預警系統—互聯網風暴中心。SANS的組成核心是安全從業人員，他們代表公司到大學等各種全球組織，共同為打造資訊安全的社會提供協助。(https://www.sans.org)