對網路要變得聰明起來

#CyberMonth

2021年網路安全宣導月

什麼是網路安全宣導月？

網路安全宣導月提高對我們整個國家網路安全重要性的認識。

網路安全 “那又怎樣?”

您知道嗎？

防病毒軟體可用於行動設備，這是駭客和其他不良行為者的一個簡單、常見的目標。

網路安全常識

- 在線安全與在實體世界中的安全沒有太大的區別！
- 保持冷靜並相信您的直覺！

一般常用術語

- 不良行為者
- 駭客
- 網路攻擊

儘到您的責任。
#BeCyberSmart。

網路安全從您開始，
並且是每一個人的責任。

目前估計有
52億網際網路的用戶或
佔世界人口的 **63%**。

網路犯罪

那是什麼？

網路犯罪是指通過電子手段實施的任何犯罪。

這可能包括...

- 盜竊
- 詐騙
- 有時甚至謀殺

例子

- 身份盜竊
- 兒童性虐待材料
- 金融盜竊
- 侵犯知識產權
- 惡意軟體
- 惡意的社交工程

您爲何應該關心？

- 犯罪無論是線下還是線上都是一種危險！
- 網路自衛基本知識可以讓您和您的數據不會落入不良行為者的手中。

惡意軟體

那是什麼？

任何軟體其目的為：

- 損害
- 不能使用
- 或者讓他人未經授權使用您的電腦或其他網際網路連接的設備

您爲何應該關心？

- 大多數網路犯罪始於某種惡意軟體。如果惡意軟體進入您的電腦或設備，您、您的家人和您的個人資料幾乎一定會處於危險之中。

例子

- 勒索軟體
- 廣告軟體
- 殭屍網路
- 駭客程式
- 間諜軟體
- 病毒
- 電腦蠕蟲

勒索軟體

那是什麼？

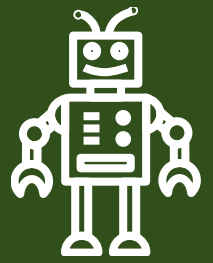
惡意軟體的設計在使受害者在支付贖金之前無法使用數據或硬體。

例子

- 密碼鎖
- Winlock
- 密碼牆
- Reveton
- 壞兔子
- 孤島危機
- 想要哭

您爲何應該關心？

- 通常作為惡意電子信件的連結下載
- 使得金融穩定和聲譽受損
- 即使您付款，也不能保證您會取回您的數據
- 通常用作其他惡意活動的誘餌



機器人程式

那是什麼？

機器人程式是一種用於在網際網路上自動執行任務的程式。

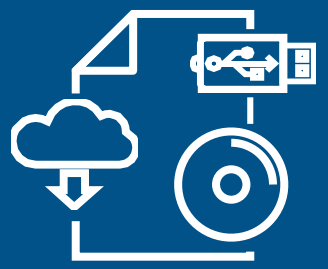
您爲何應該關心？

惡意的機器人程式可以：

- 收集密碼
- 記錄擊鍵
- 獲取財務資料
- 劫持社交媒體帳戶
- 使用您的電子信件發送垃圾信件
- 打開受感染設備的後門

您知道嗎？

並非所有的機器人程式都是壞的。當您使用搜索引擎時，這些結果是在機器人程式“爬行”在網際網路和索引內容的幫助下而實現的。Siri 和 Alexa 等聊天機器人程式是另一種常見的“好”機器人程式。



實體網路攻擊

那是什麼？

實體網路攻擊使用硬體、外部存儲設備或其他實體攻擊媒介來感染、破壞或以其他方式危害數位系統。這可能包括...

- USB 存儲設備
- CD / DVD
- 物聯網 (IoT)

您爲何應該關心？

- 易於忽略
- 難以識別和偵測
- 極難去除
- 可以做任何事情，從安裝勒索軟體到發送或修改資訊系統的副本，再到拆除網路

您知道嗎？

從電動滑板車到筆記本電腦再到貨船，任何連接到網際網路的東西都可能受到攻擊。

社交工程

那是什麼？

- 網路犯罪分子可以利用您，通過使用常見的資訊來自...
- 社交媒體平台
- 位置分享
- 面對面的對話

您爲何應該關心？

- 您的隱私不僅僅是一種奢侈品 – 它還是一種安全措施
- 攻擊可以在幾乎沒有程式設計知識或能力的情況下成功進行
- 科技的安全措施只能保護您這麼多 – 您才是您的最佳防禦

例子

- 網路釣魚
- 假託
- 誘餌
- 交換條件
- 尾隨
- 內應作案
- 拍打

網路釣魚

那是什麼？

來自看似可信賴或信譽良好的來源的虛假消息，目的在說服您...

- 揭示訊息
- 允許未經授權使用一個系統
- 點擊一個連結
- 承諾一筆財務交易

例子

- 電子信箱
- 發簡訊
- 打電話
- 社交媒體訊息和帖子
- 可疑的超連結

您爲何應該關心？

- 極爲常見
- 可能會有嚴重的後果
- 魔鬼就在細節

這封電子信件會騙到您嗎？

新消息

來自 Legitimate-Looking-Source@notquiteyourworkemail.com

主題 緊急 IT 更新：軟體漏洞

軟體更新

湯姆（Tom）下午好，

“知名軟體”中發現了一個全漏洞，攻擊者可以利用該漏洞在您不知的情況下從您的電腦錄製通話和視訊。請在當天結束前安裝受攻擊的更新，否則您的工作站將被上鎖。

我們還為所有員工創建了應用程式，以阻止們受到此安全漏洞的影響。**點擊** 此處 以執行該應用程式。

www.fakewebsite.com/gotcha.exe
點擊或輕按以跟隨連結。

真摯地，

博斯曼（BossMann）

您公司的 IT 部門

回覆

拍打

那是什麼？

一場以位置分享為中心的攻擊，其中不良行為者打電話給警察，聲稱受害者犯了罪...

- 炸彈威脅
- 武裝入侵者
- 暴力事件

您爲何應該關心？

- 生理上和直接後果
- 有時只是為了惡作劇
- 可能會導致逮捕和重傷
- 僅與可信賴的人分享您的位置，並僅在您安全回家後分享度假照片，從而降低風險

例子

您的位置作為元數據嵌入到您用手機拍攝的每張照片中。當您不使用位置服務時，請將其關閉，以使不良行為者更難查看此資訊。

其他攻擊途徑

那是什麼？

- 萬物聯網
- 任何連接到您網路的設備
- 資料收集
- 遠程使用
- 藍牙
- 開放端口

您爲何應該關心？

- 您的網路可能被利用去攻擊他人
- 任何存儲資料或連接到網際網路的設備都可能是一個安全漏洞
- 假設您有漏洞，同時採取措施以瞭解並降低風險
- 不要成為“唾手可得的果實”

例子

- 智慧型設備
- 行動電話
- 調溫器
- 車輛
- 遊戲機
- 印列機
- 醫用器材
- 工業系統

如何在網上更好地保護您自己？

保護您的網路。

無線路由器是網路犯罪分子使用線上設備的一種方式。

保持最新的版本。

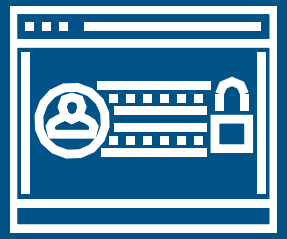
將軟體更新到最新版本，並將安全軟體設置為執行定期掃描。

如果您連接它，就保護它。

一種行之有效的入侵防禦措施是更新到最新的病毒防護軟體。

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。



密碼提示

您知道嗎？

密碼或憑證填充是一種網路攻擊，它嘗試將已經包含用戶名和密碼的“填充”從一個網站“填充”到另一個網站，希望用戶跨平台使用相同的登入資訊。

- ****** 在不同的系統和帳戶上使用不同的密碼
- ****** 使用允許的最長密碼
- ****** 混合使用大小寫字母、數字和符號
- ****** 每隔幾個月重新設置一次密碼
- ****** 使用密碼管理程式

網路安全宣導月主題

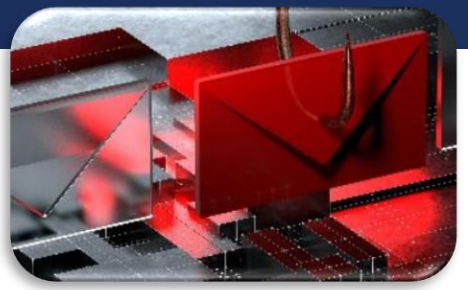
主題：

- 儘到您的責任。**#BeCyberSmart**。

2021年網路安全宣導月時間安排

10 月 1 日：
正式開始

第 1 週：
10 月 4 日週
對網路要變得聰明起來。

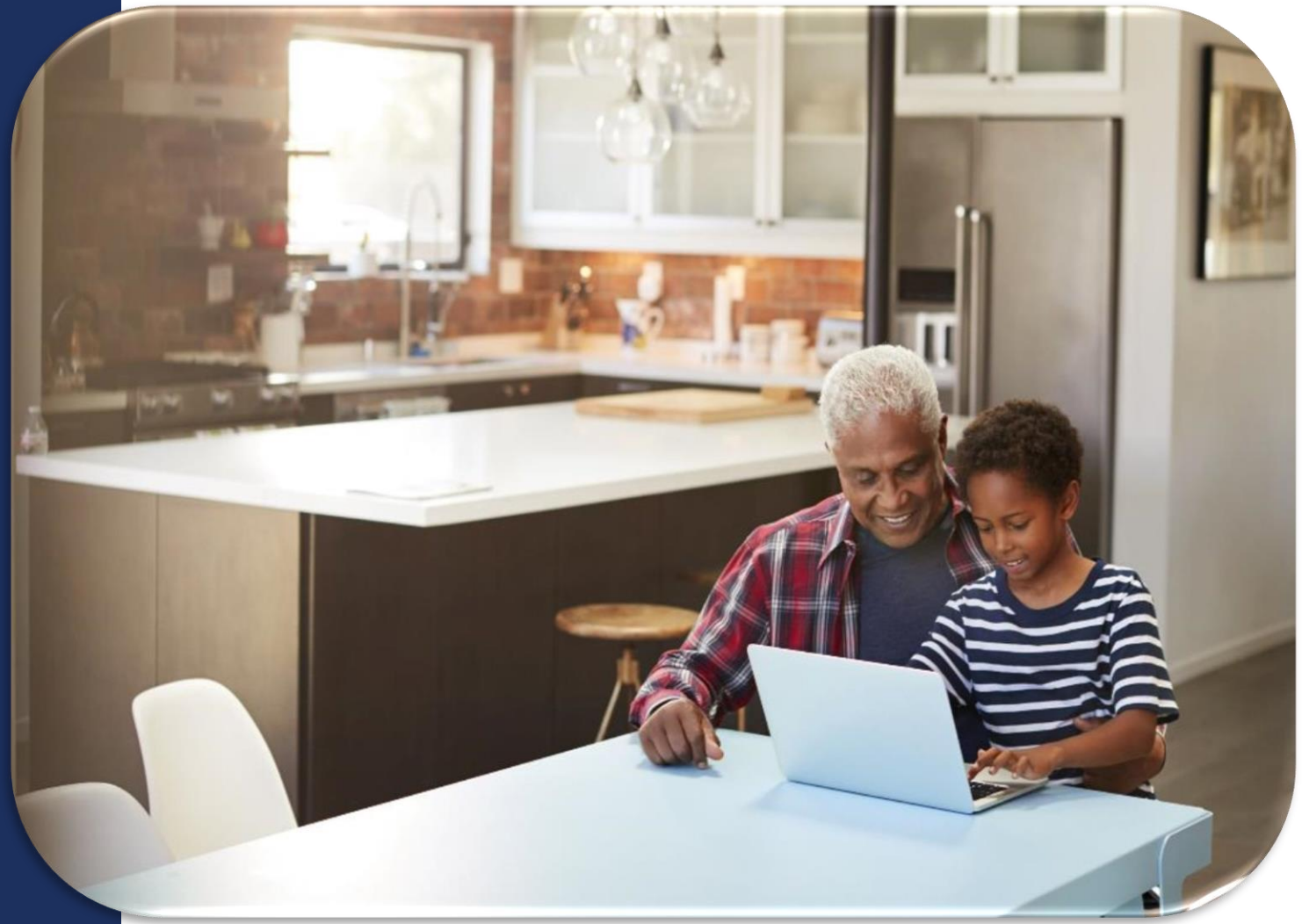


第2週：
10 月 11 日週
打擊網路釣魚！

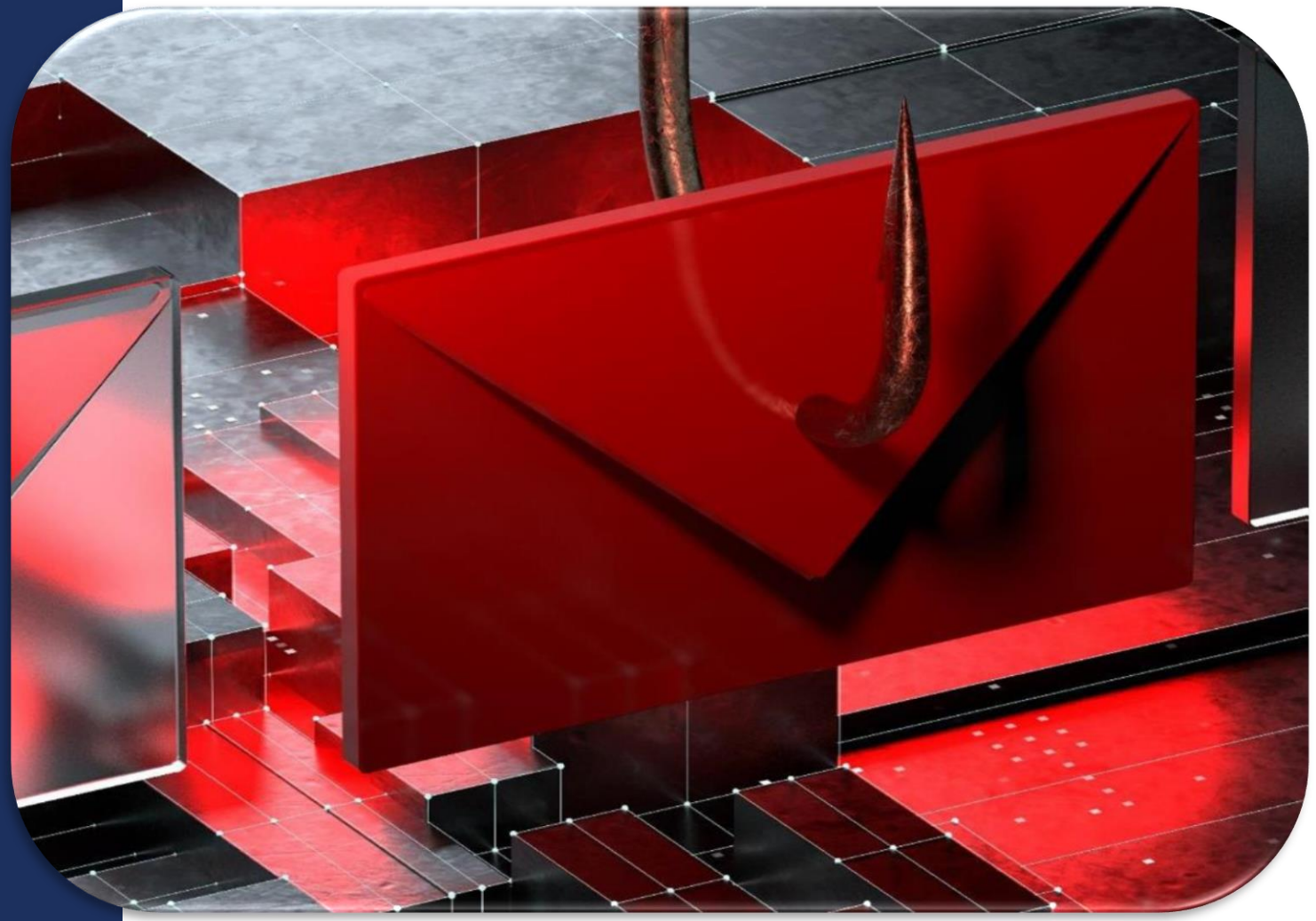
第3週：
10 月 18 日週
探索。體驗。分享。(網路安全事業宣導週)

第4週：
10 月 25 日週
網路安全第一

第1週：
對網路要變得聰明起來。



第2週：
打擊網路釣魚！



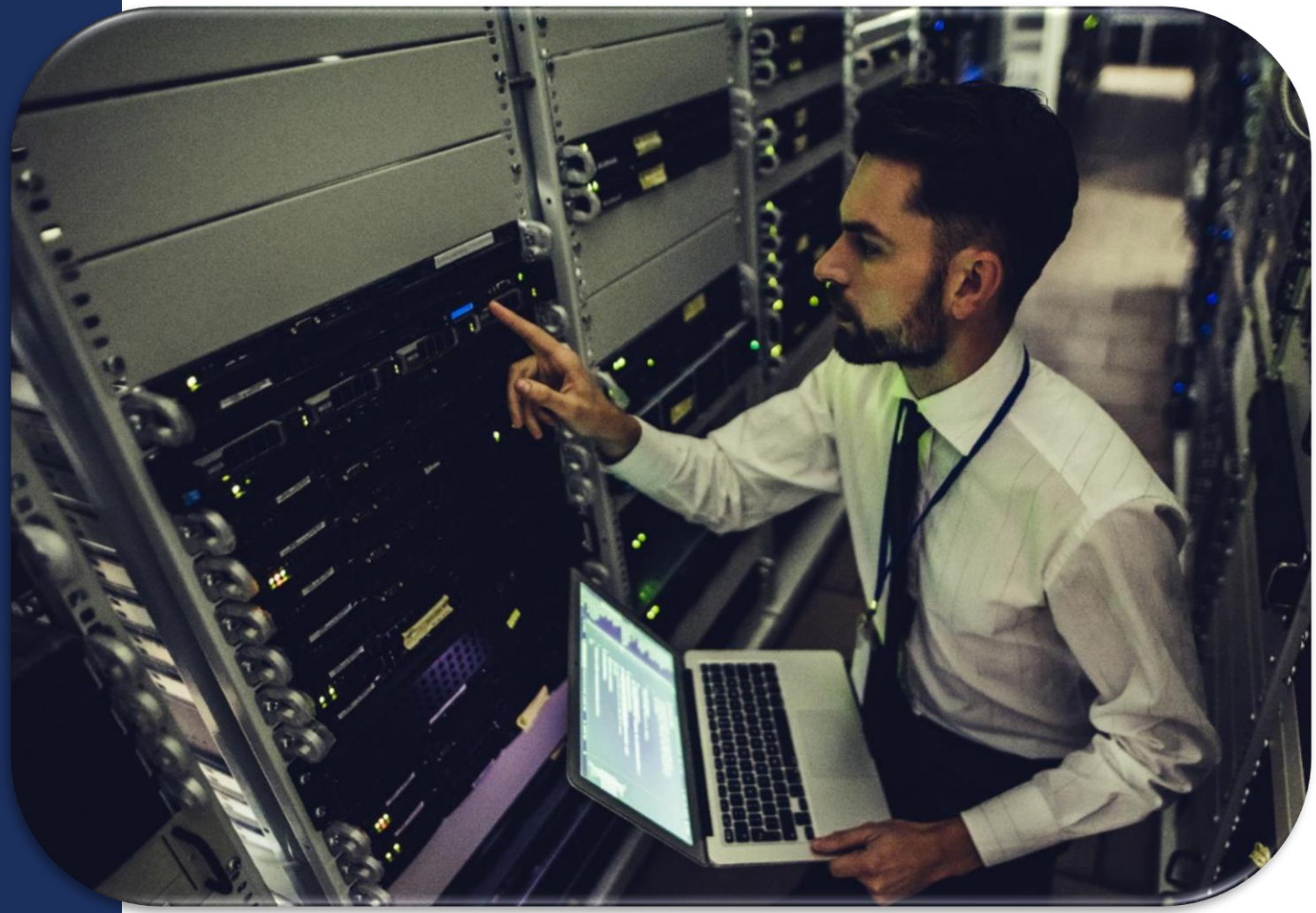
第3週：

探索。

體驗。

分享。

網路安全事業宣導週



第4週：
網路安全第一。

提高認識並參與進來

- 成為一名網路安全月的優勝者
- 在社交媒體上推廣網路安全宣導月； 使用 #BeCyberSmart 的主題標籤
- 志願在網路安全宣導月活動中發言
- 將網路安全提示傳遞給您的朋友、家人和同事

有關更多資訊，請聯繫 CyberAwareness@cisa.dhs.gov

請造訪 cisa.gov/cybersecurity-awareness-month 或 staysafeonline.org/cybersecurity-awareness-month/ 以查找更多的資源。