DELL Technologies

您是否比網路攻擊者聰明？

開始測驗

第 1 題 (共 14 題)

網路釣魚

您收到「Windows Defender 訂單」的電子郵件，其發票內容為官方格式，顯示您以 399.99 美元訂購 Microsoft Defender 帳戶的一年訂用方案。發票內容清楚說明：「請勿回覆此電子郵件」，但提供「說明與連絡」按鈕與電話號碼。您不記得曾訂購過任何此類服務。

您會如何處理？

#1

選取下方最適當的答案

A 立即按下「說明與連絡」按鈕，因為您非常不希望這筆費用掛在信用卡帳上！

B 使用網頁瀏覽器無痕視窗開啟該封電子郵件，然後按下「說明與連絡」按鈕。

C 查看線上信用卡帳單，確認該筆費用是否已經掛帳，然後使用該電話號碼嘗試探索其他資訊。

D 檢查電子郵件地址，發現其看似網路釣魚，因此您透過電子郵件程式按下「通報網路釣魚」，並且/或者轉寄至 IT 部門進行調查，而您當然不會開啟該電子郵件！

E 刪除該封電子郵件，不要開啟。

DELL Technologies

回答

網路釣魚

#1

非常好！

通報網路釣魚！

當您收到可疑的電子郵件，因任何原因要求您按下連結時，最佳行動方案為刪除該封電子郵件不要開啟，或按下 Outlook 功能表列中的「通報網路釣魚」，將該電子郵件通報給 IT 部門進行調查。**如果內容看似網路釣魚，可能就是網路釣魚郵件。**

下一題

DELL Technologies

回答

網路釣魚

#1

非常好，
但是...

通報網路釣魚！

您可能會使自己處於風險之中，因為您撥打的號碼可能會是假的電話號碼。此清單中的另一個選項會是更好的解決方案。**如果內容看似網路釣魚，可能就是網路釣魚郵件。**

下一題

DELL Technologies

回答

網路釣魚

#1

已遭駭客入侵！

通報網路釣魚！

請記得，當您收到可疑的電子郵件，因任何原因要求您按下連結時，最佳行動方案為刪除該封電子郵件不要開啟，或按下 Outlook 功能表列中的「通報網路釣魚」，將該電子郵件通報給 IT 部門進行調查。**如果內容看似網路釣魚，可能就是網路釣魚郵件。**

下一題

DELL Technologies

第 2 題 (共 14 題)

社群媒體網路釣魚

您正在查看 Instagram 帳戶，Lyle Lovett 直接在其貼文上回應您的留言。他邀請您透過私訊連絡，並傳送一則連結給您，只要按下即可存取極為珍貴的限定版內容。

您：

#2

選取下方最適當的答案

A 不敢相信自己如此幸運，立即按下該連結。

B 複製該連結，然後在無痕視窗中開啟。

C 將連結分享給社群媒體上的朋友。

D 將滑鼠移至連結上方，懷疑該連結可能會是網路釣魚，因此您刪除該訊息並封鎖該傳送者。

E 封鎖該傳送者並通報，而且沒有按下任何連結。

DELL Technologies

回答

社群媒體網路釣魚

#2

非常好！

通報網路釣魚！

當您收到可疑的電子郵件，因任何原因要求您按下連結時，最佳行動方案為刪除該封電子郵件不要開啟，或按下 Outlook 功能表列中的「通報網路釣魚」，將該電子郵件通報給 IT 部門進行調查。**如果內容看似網路釣魚，可能就是網路釣魚郵件。**

下一題

DELL Technologies

回答

社群媒體網路釣魚

#2

已遭駭客入侵！

通報網路釣魚！

請記得，當您收到可疑的電子郵件，因任何原因要求您按下連結時，最佳行動方案為刪除該封電子郵件不要開啟，或按下 Outlook 功能表列中的「通報網路釣魚」，將該電子郵件通報給 IT 部門進行調查。**如果內容看似網路釣魚，可能就是網路釣魚郵件。**

下一題

DELL Technologies

第 3 題 (共 14 題)

密碼安全性

IT 部門要求您設定強式密碼，因為此類「認證」為攻擊者尋找的最高價值目標。所以...

如何使您的密碼變得更加安全？

#3

選取下方最適當的答案

A 設定長度為 8 個字元的密碼，建議長度可加長。

B 使用字母、數字及字元組合。

C 避免在其他帳戶或網站中重複使用任何密碼 (使每個密碼都是唯一的密碼)。

D 以上皆是。

E 以上皆非。

DELL Technologies

回答

密碼安全性

#3

非常好！

使用強式密碼！

安全密碼必須是不重複的密碼，且結合至少 8 個字母、數字及字元，或甚至使用您記得的不重複的複雜密碼。請勿使用寵物狗的名稱！此外，請務必使用雙因素驗證，此方式結合強式密碼將可發揮最佳的保護效果。

下一題

DELL Technologies

回答

密碼安全性

#3

非常好，
但是...

使用強式密碼！

安全密碼係結合下列所有安全性措施：必須是不重複的密碼，並包含至少 8 個字母、數字及字元。請勿使用寵物狗的名稱！若要加強安全性，請使用雙因素驗證與數字和字元組合的複雜密碼，而非一般密碼。

下一題

DELL Technologies

回答

密碼安全性

#3

已遭駭客入侵！

使用強式密碼！

安全密碼必須為不重複的密碼，並結合至少8 個字母、數字及字元。若要加強安全性，請使用雙因素驗證與數字和字元組合的複雜密碼，而非一般密碼。

下一題

DELL Technologies

社交工程

您在手機上接到某人來電，聲稱自己是 IT 部門人員，通知您密碼已過期，必須設定新的密碼。該電話號碼看似相當安全。該人員要求您提供員工編號、社會安全號碼及出生日期進行驗證。

您會如何處理？

#4

選取下方最適當的答案

A 將資訊提供給該人員，因為您希望重設密碼，並返回工作。

B 要求該人員提供連絡人電子郵件和電話號碼以驗證其身分，然後提供其所要求的資訊。

C 立即掛斷電話，然後將此事件通報給 IT 部門。

D 將員工號碼和出生日期提供給該人員，但不提供社會安全號碼。

E 以上皆非。

DELL Technologies

回答

社交工程

#4

非常好！

掛斷電話並連絡 IT 部門！

部分攻擊者會利用社交工程的伎倆，透過電話操控您交出敏感資訊。即使您可確認該人員為體系內的員工，仍無法保證您確實是與其本人通話。**您應隨時自發地進行密碼重設。**

下一題

DELL Technologies

回答

社交工程

#4

已遭駭客入侵！

掛斷電話並連絡 IT 部門！

部分攻擊者會利用社交工程的伎倆，透過電話操控您交出敏感資訊。即使您可確認該人員為體系內的員工，仍無法保證您確實是與其本人通話。**您應隨時自發地進行密碼重設。**

下一題

DELL Technologies

第 5 題 (共 14 題)

電腦入侵

當您接聽通話時，發現畫面上出現詭異行為，例如滑鼠自行移動、文字視窗或主控台視窗開啟又關閉，或功能表突然顯示又消失，

所以：

#5

選取下方最適當的答案

A 您認為這是無害的電腦問題，並繼續工作。

B 您與 IT 部門確認該問題，但仍繼續工作。

C 您立即停止使用並關閉電腦，然後使用其他裝置連絡 IT 部門通報該問題。

DELL Technologies

回答

電腦入侵

#5

非常好！

立即連絡 IT 部門！

如果您的滑鼠會在畫面上「自行」移動，可能表示發生嚴重攻擊，其中可能涉及資料外洩和鍵盤側錄。您的 IT 部門必須儘早瞭解此問題，才可有效進行後續處理。

下一題

DELL Technologies

回答

電腦入侵

#5

已遭駭客入侵！

立即連絡 IT 部門！

異常行為可能表示攻擊者正在監控您的電腦，且可能同時在外洩資料和擷取按鍵輸入 (包括密碼和其他重要資訊)。您的最佳選擇就是立即關閉電腦，然後將該問題通報 IT 部門。

下一題

DELL Technologies

第 6 題 (共 14 題)

USB 啟動的惡意軟體攻擊

當您走在公司的停車場時，看見有個購物袋放在兩台車之間。您發現袋子內有五個 USB 隨身碟仍套著原始包裝未拆封，每個隨身碟容量為 500 GB！

您會如何處理？

#6

選取下方最適當的答案

A 拆開其中一個隨身碟包裝，然後將隨身碟插入電腦的 USB 插槽，並將其餘四個分送給同事。

B 將隨身碟全部帶回家，然後在個人電腦上使用這些 USB 隨身碟。

C 將發現隨身碟的事件通知大樓保全和 IT 部門，並將 USB 隨身碟交給他們。

D 在節日時，將 USB 隨身碟當作禮物轉送給孩子。

E 以上皆非。

DELL Technologies

回答

USB 啟動的惡意軟體攻擊

#6

非常好！

通知保全和 IT 部門！

此類型的攻擊可讓攻擊者透過員工將惡意軟體植入組織作為「騾子」，將惡意負載插入網路。切勿將來路不明的 USB 隨身碟或其他配件插入您擁有的任何裝置。這些隨身碟將會是糟糕的禮物！

下一題

DELL Technologies

回答

USB 啟動的惡意軟體攻擊

#6

已遭駭客入侵！

通知保全和 IT 部門！

此類型的攻擊可讓攻擊者透過員工將惡意軟體植入組織作為「騾子」，將惡意負載插入網路。切勿將來路不明的 USB 隨身碟或其他配件插入您擁有的任何裝置。這些隨身碟將會是糟糕的禮物！

下一題

DELL Technologies

第 7 題 (共 14 題)

勒索軟體

某個銷售人員來到您的辦公室，向您介紹公司可能會有興趣購買的新技術。該人員將簡報存放在 USB 隨身碟中，然後請您將隨身碟插入電腦，以便其說明時播放投影。

您會如何處理？

#7

選取下方最適當的答案

A 按照指示進行，將 USB 隨身碟插入電腦。

B 詢問是否可另外下載簡報，因為公司政策禁止使用外部 USB 隨身碟，惟該人員無法下載時，再按照其要求將 USB 隨身碟插入電腦。

C 請該人員在不播放投影的情況下進行簡報，並且不要插入 USB 隨身碟。

D 確保該人員的 USB 隨身碟不是在停車場中找到後，再插入電腦。

E 額外複製 USB 隨身碟內容，然後交給您的經理。

DELL Technologies

回答

勒索軟體

#7

非常好！

不要播放投影或插入 USB 隨身碟。

您不知道的是，該銷售人員曾收受攻擊者的大筆賄賂，且該 USB 隨身碟中包含勒索軟體負載，可能會鎖定您的系統；但是，只要不插入 USB 隨身碟，並且不要下載任何其他檔案，即可防止攻擊者取得存取權。好險！

下一題

DELL Technologies

回答

勒索軟體

#7

已遭駭客入侵！

不要投影或插入 USB 隨身碟。

您不知道的是，該銷售人員曾收受攻擊者的大筆賄賂，且該 USB 隨身碟和下載的檔案皆包含勒索軟體負載，將會鎖定您的系統。避免接受路不明的外部 USB 隨身碟，以及將檔案下載至個人或公司電腦。

下一題

DELL Technologies

第 8 題 (共 14 題)

雙因素驗證

您的銀行建議您在登入其網站時使用雙因素驗證。其他網站亦會使用此程序來確保使用者安全。

下列何者為雙因素驗證的範例？

#8

選取下方最適當的答案

A 當您輸入使用者名稱和密碼後，系統要求您輸入 PIN 碼才可存取網站。

B 您要輸入使用者名稱和密碼，以及透過選擇包含路標的方塊通過 CAPCHA 驗證。

C 當您輸入使用者名稱和密碼後，該網站會傳送包含單次代碼的簡訊至您的手機，您必須將該代碼輸入網站所提供的方塊。

D 當您輸入使用者名稱後，該網站會要求您輸入安全性權杖提供的代碼 (每分鐘變更一次，且會安裝至您的手機)。

E 僅 A 和 C。

F 僅 C 和 D。

G 以上皆非。

DELL Technologies

回答

雙因素驗證

#8

非常好！

兩者皆需要！

雙因素驗證需要密碼和第二個不同的識別碼 (例如透過簡訊傳送的代碼，或由應用程式產生的號碼)，才可識別和驗證使用者。此層安全防護會讓攻擊者更難以存取您的資訊。

下一題

DELL Technologies

回答

雙因素驗證

#8

非常好，
但是...

兩者皆需要！

您幾乎快答對了！ 本題的雙因素驗證有兩個範例，
請重試一次，看是否可找出另一個範例。

下一題

DELL Technologies

回答

雙因素驗證

#8

已遭駭客入侵！

抱歉！兩者皆需要！

雙因素驗證需要密碼和第二個不同的識別碼 (例如透過簡訊傳送的代碼，或由應用程式產生的號碼)，才可識別和驗證使用者。此層安全防護會讓攻擊者更難以存取您的資訊。如未使用雙因素驗證，可能會使您遭受攻擊者入侵。

下一題

DELL Technologies

第 9 題 (共 14 題)

藍牙竊賊

當您開車到步道入口，開始美好的午後健行活動後，發現筆記型電腦仍放在後背包裡，而且手機也沒有訊號。您需要將電腦和手機放在車內，但希望確保兩者安全。

您會如何處理？

#9

選取下方最適當的答案

A 關閉所有 Wi-Fi。

B 將筆記型電腦設定為睡眠模式。

C 將筆記型電腦和手機鎖在後車箱。

D 使用後毛毯將筆記型電腦和手機包起來。

E 完全關閉筆記型電腦和手機，如此即可關閉藍牙。

DELL Technologies

回答

藍牙竊賊

#9

非常好！

關閉筆記型電腦和手機！

當您無法看顧裝置時，雖然將其藏匿起來會是最佳方法，但竊賊會使用藍牙掃描器找出上鎖車輛內的裝置，而且並非所有裝置都會在處於「睡眠」模式時關閉藍牙。竊盜事件通常發生在步道入口，以及擁有者會長時間不在的地點，而竊賊經常虎視眈眈！因此，健行前必須謹慎小心！

下一題

DELL Technologies

回答

藍牙竊賊

#9

已遭駭客入侵！

關閉筆記型電腦和手機！

當您無法看顧裝置時，雖然將其藏匿起來會是最佳方法，但竊賊會使用藍牙掃描器找出上鎖車輛內的裝置，而且並非所有裝置都會在處於「睡眠」模式時關閉藍牙。竊盜事件通常發生在步道入口，此處是擁有者會長時間不在的地點。因此，健行前必須謹慎小心！

下一題

DELL Technologies

USB 攻擊第 2 部分

佳節氣氛濃厚，您帶來使用 USB 供電的迷你聖誕樹裝飾辦公室。

您會如何為聖誕樹供電？

#10

選取下方最適當的答案

A 將 USB 插頭插入電腦。

B 將 USB 插頭插入連接電腦的 USB 延長線。

C 使用專用的 USB 充電器，將裝置插入一般電源插座。

D 沒有方法可以供電，聖誕節慶祝取消。

E 以上皆非。

DELL Technologies

回答

USB 攻擊第 2 部分

#10

非常好！

使用專用的 USB 充電器！

此種 USB 型攻擊會將惡意軟體放入許多裝置 (甚至是小型的聖誕樹！)，以期最後能侵入珍貴的企業網路。切勿將不明的 USB 裝置插入電腦，即使只是用來供電。

下一題

DELL Technologies

回答

USB 攻擊第 2 部分

#10

已遭駭客入侵！

使用專用的 USB 充電器！

此種 USB 型攻擊會將惡意軟體放入許多裝置 (甚至是小型的聖誕樹！)，以期最後能侵入珍貴的企業網路。切勿將不明的 USB 裝置插入電腦，即使只是用來供電。

下一題

DELL Technologies

邪惡女傭

您將出席中國上海的網路安全會議，入住 5 星級的飯店。您在外出吃晚餐前，將電腦鎖在房內的保險櫃裡。

您的電腦是否能免於攻擊和竊盜？

#11

選取下方最適當的答案

A 否，因為任何未受看顧的裝置皆可能會遭到入侵。

B 是，因為您安全地將裝置鎖在保險櫃裡。

C 是，因為您亦將衣物吊掛於衣櫃內來遮蔽保險櫃。

D 是，因為這是一間非常優質的飯店。

E 是，因為這不是一台非常優質的電腦。

DELL Technologies

回答

邪惡女傭

#11

非常好！

否，任何裝置皆可能遭到入侵！

任何未受看顧的裝置皆可能透過一般稱為「邪惡女傭」攻擊的方式開啟與入侵，攻擊者可藉由此方式實際開啟電腦並插入惡意軟體，以取得存取權。如果您未實際將裝置隨身攜帶，即容易遭受攻擊。此外，切勿讓陌生人保管您的裝置，尤其如果他們是邪惡女傭。

下一題

DELL Technologies

回答

邪惡女傭

#11

已遭駭客入侵！

否，任何裝置皆可能遭到入侵！

任何未受看顧的裝置皆可能透過一般稱為「邪惡女傭」攻擊的方式開啟與入侵，攻擊者可藉由此方式實際開啟電腦並插入惡意軟體，以取得存取權。為確保安全，所有裝置皆必須隨身攜帶。切勿讓陌生人保管您的裝置，尤其如果他們是邪惡女傭。

下一題

DELL Technologies

第 12 題 (共 14 題)

間諜軟體

您收到不明電話號碼的簡訊，表示您的女兒發生意外，被送往醫院。該簡訊提供一則連結，讓您能夠立即聯絡。

您：

#12

選取下方最適當的答案

A 立即按下連結，因為您相當擔心您的女兒。

B 確實查詢號碼後，發現該號碼來自您女兒的所在區域，接著按下連結。

C 切勿按下連結，另向女兒傳送簡訊，確認她平安無恙。

D 以上皆非。

DELL Technologies

回答

間諜軟體

#12

非常好！

切勿按下連結！

此類攻擊會嘗試將間諜軟體植入您的手機，該間諜軟體會入侵您的手機，且可能散播至企業網路。您發現事情似乎「不對勁」，並使用其他方式確認女兒安全。做得好！

下一題

DELL Technologies

回答

間諜軟體

#12

已遭駭客入侵！

切勿按下連結！

此類攻擊會嘗試將間諜軟體植入您的手機，該間諜軟體會入侵您的手機，且可能散播至企業網路。按下連結會使間諜軟體負載傳遞至您的裝置。杜絕陌生的簡訊，無論內容有多麼緊迫。

下一題

DELL Technologies

端點安全

威脅執行者 (您可能甚至會稱呼其為心懷惡意的駭客) 會鎖定端點作為目標。

端點的定義為：

#13

選取下方最適當的答案

A 桌上型電腦。

B 桌上型電腦和筆記型電腦。

C 桌上型電腦、筆記型電腦及伺服器。

D 桌上型電腦、筆記型電腦、伺服器及雲端等。

E 桌上型電腦、筆記型電腦、伺服器、雲端及我在 GPS 上的最後目的地。

DELL Technologies

回答

端點安全

#13

非常好！

任何遠端連線裝置皆是！

端點為任何遠端連線至網路的任何裝置。端點安全性對於保護組織裝置與資料而言，至關緊要因此您的防範必須搶先攻擊者一步！

下一題

DELL Technologies

回答

端點安全

#13

非常好，
但是...

任何遠端連線裝置皆是！

端點為任何遠端連線至網路的裝置。端點安全性對於保護組織裝置與資料而言，至關緊要，因此您的防範必須搶先攻擊者一步！

下一題

DELL Technologies

回答

端點安全

#13

已遭駭客入侵！

任何遠端連線裝置皆是！

端點為任何遠端連線至網路的裝置。端點安全性對於保護組織裝置與資料而言，至關緊要，因此您的防範必須搶先攻擊者一步！

下一題

DELL Technologies

端點安全第 2 部分

心懷惡意的駭客會鎖定桌上型電腦、筆記型電腦、行動電話、無線印表機及伺服器 (任何連線至網路的裝置) 等端點作為目標。

您應該採取哪些步驟才能有助於防範攻擊？

#14

選取下方最適當的答案

A 當我未使用裝置時，要確實將其鎖上並鎖定。

B 定期更新和修補裝置。

C 落實良好的電子郵件使用習慣：通報可疑的電子郵件。

D 切勿將不明裝置插入端點。

E 以上皆是。

DELL Technologies

回答

端點安全第 2 部分

#14

非常好！

以上皆是！

您已了解如何維持網路安全，並已開始進行落實。端點安全性對於保護組織裝置與資料而言，至關緊要，因此您的防範必須搶先攻擊者一步！

下一題

DELL Technologies

回答

端點安全第 2 部分

#14

非常好，
但是...

您還必須進行更多的防範措施！

若要保護您的裝置，您不單只有一件事必須做到。端點安全性對於保護組織裝置與資料而言，至關緊要，因此您的防範必須搶先攻擊者一步！

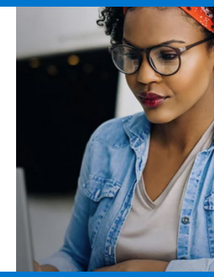
下一題

DELL Technologies

感謝您！

如需詳細資訊：

請造訪 **Dell.com/Endpoint-Security**



DELL Technologies