青少年理財教育

提防網絡安全隱患

滙豐 HSBC
滙見新可能
Opening up a world of opportunity

目錄

點擊可瀏覽各個章節

提防騙子，由你開始

我哋好多時都認為詐騙只會發生喺其他人身上，直到我哋自己都受騙。

識穿詐騙就好似破解魔術一樣，如果你唔知道當中嘅竅門，佢就會令你感到好困惑。不過當你知道佢係點樣運作嘅時候，你就好易睇穿佢。如果我哋可以搞清楚咗呢啲伎倆，就唔會咁容易「中伏」。

詐騙嘅種類

電郵詐騙「網絡釣魚」

「網絡釣魚」係騙徒嘗試透過電子郵件得到用戶名稱同密碼等等敏感資料嘅一種方法。呢啲電郵睇落去好似來自你信任嘅人，例如銀行。

需要注意嘅係：

呢啲電郵會要求你提供個人資料，或者直接帶你去一個同真實網站極度相似嘅假網站嗰度，要求你分享資料。電郵嘅開頭可能只係用一個普通嘅稱謂（一般都唔會用你個名），電郵內容亦可能出現串字同語法問題。

點樣防騙：

每次都要檢查寄件者嘅電郵地址。唔好輕易撳入任何連結，或打開任何附件。千祈唔好透露你嘅敏感資料。如果你係滙豐客戶，你可以將電郵轉寄去 phishing@hsbc.com，我哋會跟進調查。

小測驗：如何識別「網絡釣魚」

短訊詐騙「短訊釣魚」

騙徒可能向你發出詐騙短訊，假扮成你信任嘅人，例如銀行或者電話服務供應商。

需要注意嘅係：

佢哋會嘗試令你撳入連結或者呃你回覆你嘅個人或銀行資料俾佢哋。

點樣防騙：

如果你唔確定佢係咪詐騙短訊，就千祈唔好撳入任何連結，亦唔好回覆。先查清楚平時由嗰間機構發出嘅短訊係點樣。

電話詐騙「電話釣魚」

騙徒可能會打電話俾你，仲聲稱自己係銀行或者警察等等你通常會信任嘅身分，但其實佢哋係想呃你錢，或者攞到你嘅資料後，再用嚟呃你。

需要注意嘅係：

佢哋會嘗試說服你將錢存入一個 「安全嘅地方」。佢哋仲會要求你提供個人資料，例如你嘅戶口密碼、個人身分識別碼或者安全鑰匙密碼。

點樣防騙：

正常咁收線，然後等15秒，直至電話完全斷線。然後，等多15秒先好再用電話，打去騙徒聲稱嘅公司熱線核實。如果係你間銀行，咁就打去銀行卡背面嘅電話號碼。

盜用身份

騙徒可能會嘗試攞到你重要嘅個人資料，然後用你嘅名義開新戶口或者接管你嘅戶口。

需要注意嘅係：

一啲網上嘅心理或性格測驗網站睇落好似冇問題，但係佢哋可能會洩露你嘅個人資料俾盜用身份嘅賊人。通常，接受呢啲測驗嘅條款同細則代表你允許佢哋將你輸入咗嘅資料出售俾其他人。

點樣防騙：

唔好撳入任何出現喺社交媒體上睇落去好似好有趣嘅簡單測驗，同將你嘅個人版面設定為私人狀態。仲有，你要將睇完嘅銀行月結單同其他有個人資料嘅文件小心銷毀。

購物詐騙

喺社交媒體上面搵二手嘢或者優惠係一個買平嘢嘅好方法。但要小心有好多假戶口同騙子都等緊你上當。

需要注意嘅係：

注意唔好幫襯嗰啲最近先開，但又好似賣緊好多嘢，或者用啲好大路嘅產品相嘅帳戶。

點樣防騙：

小心嗰啲要求訂金或者要你轉賬到一個好似冇關係嘅戶口或公司嘅賣家。

學識點樣避免呢種類型嘅騙局係好重要嘅，因為如果你不幸成為受害者，通常你所損失嘅金錢都無辦法獲得賠償。

防騙：保護自己

詐騙或者騙局係指罪犯為咗錢而呃你。

詐騙可能喺你完全唔知情底下發生，而騙局則係有人慫恿你代表佢地完成某件事情。

我哋成日以為詐騙同騙局只會發生喺其他人身上，但其實所有人都同樣有機會「中伏」。
騙徒非常熟悉點樣向我哋施壓，令我哋跌入陷阱。

當你覺得唔對路，可以問自己以下問題：

- 佢係催緊我緊急作出行動，定係威脅緊我，如果我唔快啲行動就會凍結我個戶口？
- 佢係咪話我知我嘅銀行戶口喺我唔知情底下有一筆錢存咗入嚟？
- 佢係咪想我攞入去嗰啲不明來歷嘅訊息或者電郵裏面嘅連結？
- 佢係咪要我提供個人資料?
- 佢係咪要我回覆或者驗證我嘅戶口？
- 佢發出嚟嘅訊息係咪有串字、格式或者語法問題？
- 佢係咪要我驗證新嘅收款人、交易或者電子設備？
- 佢係咪睇落去好似係真嘅，但當我仔細研究嘅時候，竟然發現有啲地方「伏伏地」?
- 佢係咪要我將錢轉入「安全戶口」或者攞現金，然後交俾「警方」進行調查？
- 佢係咪俾咗一個好到難以置信嘅優惠我？
- 佢有冇用唔同嘅理由，要求我更改付款資料？

保護你嘅財產

恭喜你終於儲到第一筆錢！而家你需要學點樣確保你嘅財產安全。

你可以透過一啲日常小習慣去確保財產安全，例如經常檢查銀行月結單睇吓有冇唔正常嘅交易。你亦可以採取進一步嘅行動，例如喺俾錢嘅時候檢查收款人或者公司係咪真實存在。

你可以用以下嘅情境，測試一下你識別詐騙嘅能力。

情景	答案
1 你其中一位朋友喺社交媒體上發訊息俾你，話佢有**急事**，急需一筆現金。 **你會點做，同點解呢？** 	唔好轉錢俾佢。打電話俾你嘅朋友，確定佢係咪真係需要借錢。唔好喺社交媒體上聯絡佢。如果你朋友嘅戶口被黑客入侵或者有人冒充佢嘅社交媒體帳戶，你就可能會成為下一個受害者。
2  你出街買嘢嘅時候，將手機連接到商場嘅公共無線網絡。然後，你睇到一對好鍾意嘅鞋，但係要**睇吓戶口嘅結餘**先知係咪買得起。 **你會點做，同點解呢？**	連線到公共無線網絡嘅時候，千祈唔好用手機檢查銀行結餘。公共無線網絡並唔安全，騙徒可能利用佢攞到你嘅銀行資料。最好用正常嘅流動數據上網，或者去自動櫃員機查結餘。
3 你同朋友出街食飯。你喺去廁所嘅時候將自己張卡交俾佢哋「埋單」，但係佢哋驚個感應式支付用唔到，所以問你攞個**卡密碼**。 **你會點做，同點解呢？** 	即使係你最好嘅朋友，都千祈唔好將自己嘅卡交俾其他人保管。亦唔好將密碼話俾任何人知，尤其係喺可能會俾人偷聽到嘅公共場所。你係唯一知道密碼同可以用呢張卡嘅人。

點樣安全地喺網上理財同付款

喺網站或者流動應用程式買嘢同理財又快又方便。

但係都要小心保護自己，就好似用任何其他方式買嘢或者理財一樣。以下有啲貼士可確保你嘅安全：

確保你電子設備嘅安全性

經常更新你手機、平板電腦或者電腦嘅作業系統到最新版本，去確保安全。

只要喺手提電腦同桌上電腦設定咗軟件自動更新功能，佢會當每逢有軟件更新就自動下載同安裝；喺你電子設備上嘅其他應用程式都係一樣。你可以選擇喺電子設備連接咗無線網絡或者喺夜晚叉電嘅時候，先至自動安裝最新版本。咁樣你嘅電子設備就會有為防止黑客入侵而設嘅最新安全功能。

仲有，你應該安裝信譽良好同值得信賴嘅防毒軟件，去保護電子設備免受任何惡意攻擊。想知更多就要去我哋嘅網絡安全及防詐騙資訊中心喇。

定一啲唔易破解嘅密碼

複雜嘅網上密碼可能感覺好麻煩，但佢哋確實可以保護你嘅個人資料。

當講到密碼，梗係越長就越安全啦。可以用大階同細階字母、數字加符號嘅組合令密碼更加難破解。另一種增強密碼安全嘅方法就係將唔相關嘅詞語串連起嚟。

如果你用緊銀行嘅網上或流動理財服務，你可以設定一啲其他嘅安全措施。例如，你可以加返指紋或人臉識別等生物認證功能，令流動理財服務更加安全；呢啲就係雙重認證。當你喺網上付款嘅時候，滙豐仲會用埋行為生物認證技術，去驗證你嘅身份添。

安全連結

要檢查你連結嘅網站係咪安全，就要睇吓網址列上面係咪有一個掛鎖咁樣嘅圖示。不過記住，有掛鎖圖示並唔保證網站係真嘅。

例如，如果你喺度睇緊 hsbc.com.hk，同見到綠色嘅掛鎖圖示，咁代表你喺安全嘅情況下同緊滙豐互動。但如果你去嘅係 hs8c.com.hk，你仍然可以見到綠色掛鎖，雖然咁代表你嘅連線安全，但係你就唔係同緊滙豐互動喇。你可能喺一個假網站度，令你以為自己睇緊嘅係滙豐網站。

所以，你要再三確定網站嘅真實性，檢查網址係咪有啲字串錯、多咗啲字或符號，又或者其他唔正常嘅地方。守網者等網站可以幫你搵出網站係咪真係正當。

網上購物同銀行轉賬

買嘢嘅時候，喺輸入你嘅個人資料或者付款資料之前，要再次檢查網址列上面嘅掛鎖圖示，而且唔好提供交易需要以外更多嘅資料。例如，淨係填寫必填欄位。

通常你唔需要建立帳戶就可以買嘢—所以如果冇咩必要，就唔好建立帳戶。如果喺可以嘅情況下，唔好俾賣家儲存你嘅付款資料。

如果你唔識個賣家，千祈唔好用銀行轉賬方式俾錢。最好用信用卡、扣賬卡、PayPal 或者有提供防騙保護嘅其他付款方式。

如果你發現戶口有任何可疑情況，就馬上打電話去 +852 2233 3000 聯絡我哋。

防範騙局

即使你已用晒以上嘅安全措施，你仍要注意一啲常見嘅騙局。以下係兩個值得注意嘅警號。

要求你轉移資金：真正嘅銀行係唔會要求你將錢轉去另一個戶口嘅，亦唔會冇啦啦要求你提供個人識別碼、密碼或者其他個人資料。

不明寄件者：千祈唔好攞啲來歷不明嘅連結或者附件。

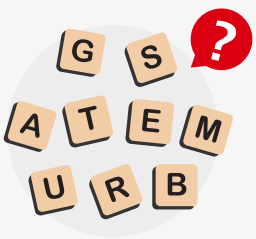
如何識別「網絡釣魚」

認清虛假郵件和網站

騙徒會試圖設下陷阱獲取你的密碼和銀行資料，這種騙局俗稱「網絡釣魚」。他們會設置看起來很真實的電子郵件和網站。但你其實可以從細節上分辨真假：

偽裝或修改過的連結

仔細檢查連結處顯示的網址，例如：你是否進入「H5BC.com」網站

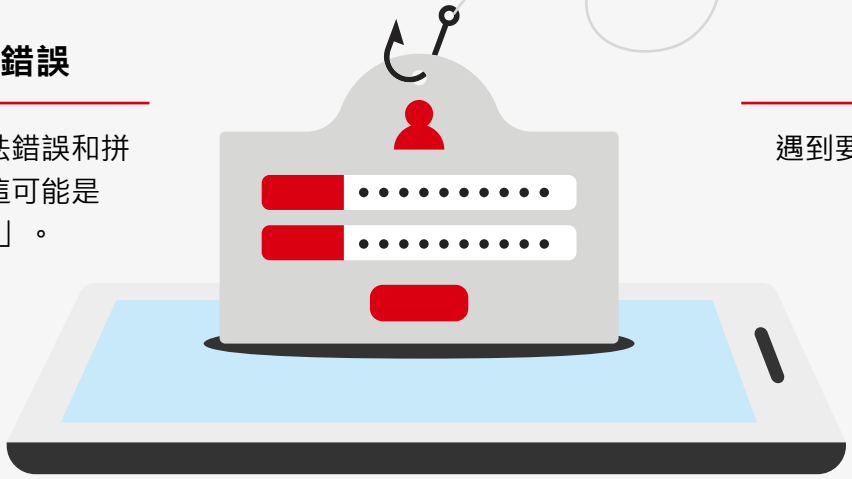


語法和拼寫錯誤

句子不流暢、語法錯誤和拼寫錯誤都表示這可能是「網絡釣魚」。

個人資料

遇到要求提供個人資料的訊息要小心



緊急情況和戶口威脅

警告你的戶口有緊急變更，需要立即進行驗證。

公司標誌或署名

不要因為電郵裡有看起來像官方的標誌或署名，就認為這是真的官方郵件。

電郵挑戰 1：
發現騙局中的蛛絲馬跡

在一些騙局裡，騙徒會嘗試透過電郵盜取受害人的銀行戶口或金錢。雖然有時要分辨電郵真偽並不容易，但你仍然可透過一些蛛絲馬跡識別偽冒電郵。你能從以下示例中找出端倪嗎？

在這裏輸入...

答案：

提示 1：「親愛的客戶」：你的銀行知道你的姓名，並會在電郵內附上你的姓名。

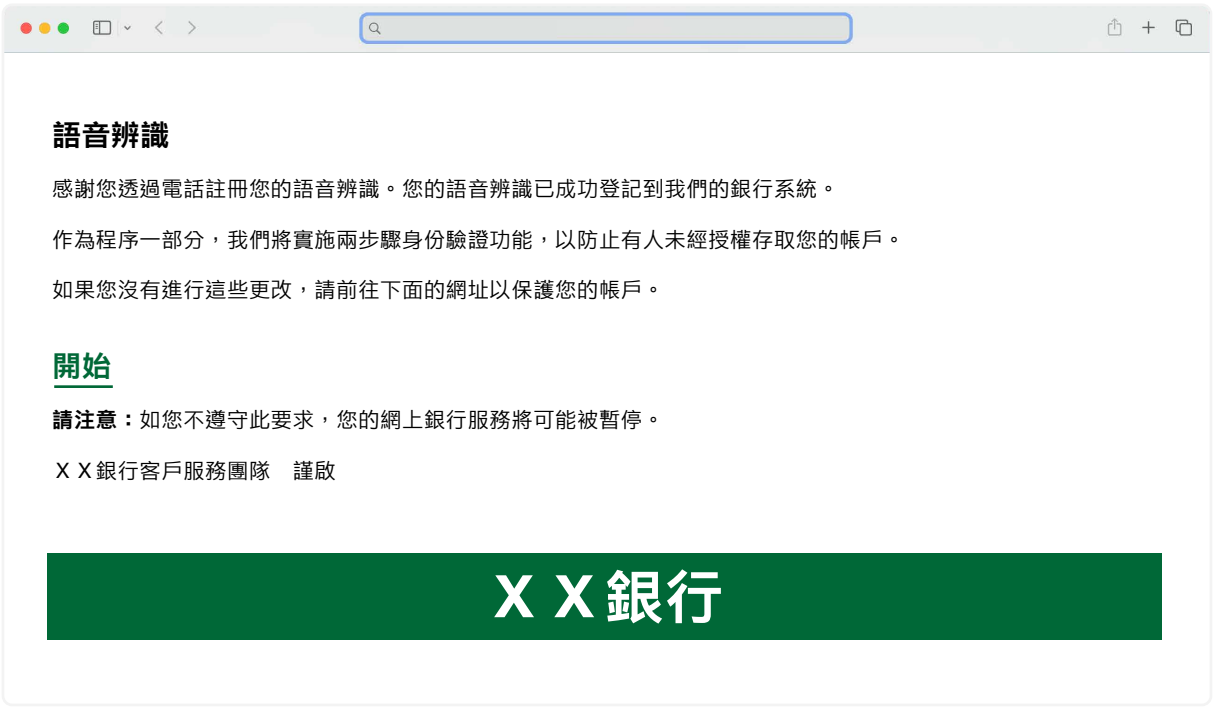
提示 2：檢查寄件人的電郵地址 - 此處通常會顯示寄件人的真正電郵地址，有可能是一個看起來很可疑的電郵地址。

提示 3：檢查語法錯誤和錯別字。你的銀行不會說你的資料「有輕微錯誤」- 如有問題，銀行會直接要求你經安全途徑更新資料。

提示 4：你認識這個網站連結嗎？不要點擊任何你不認識的網站連結。

電郵挑戰 2:
察覺騙局中的蛛絲馬跡

有些電郵看起來非常專業，讓你以為他們是真實的。但仍然有些端倪 - 你能發現它們嗎？



語音辨識

感謝您透過電話註冊您的語音辨識。您的語音辨識已成功登記到我們的銀行系統。

作為程序一部分，我們將實施兩步驟身份驗證功能，以防止有人未經授權存取您的帳戶。

如果您沒有進行這些更改，請前往下面的網址以保護您的帳戶。

開始

請注意：如您不遵守此要求，您的網上銀行服務將可能被暫停。

ＸＸ銀行客戶服務團隊　謹啟

ＸＸ銀行

答案：

提示 1：點擊連結可能帶來風險 - 例如，它可能會將你引導至詐騙網站，或讓騙徒竊取你電腦中的資訊。在點擊之前，將滑鼠移至連結上方，查看連結的去向。

提示 2：訊息寫得太差，使用不同的字體大小和顏色，並威脅你立刻行動，讓人生疑。

提示 3：沒有寫客戶姓名。

提示 4：你註冊語音認證了嗎？如果收到這封郵件的人沒有註冊，收到訊息時記得想一想此訊息是否符合你的真實情況。

短訊挑戰 1：識別偽造訊息

收到短訊時，你能看出詐騙短訊的端倪嗎？

答案：

要分辨短訊內容是真的還是詐騙就更難了。

停下來思考幾分鐘。

你有沒有買過短訊提及過的東西？不要撥打短訊中的號碼。這類詐騙現在很常見。請打給銀行的電話號碼（例如你銀行卡背面的號碼），而不是打給短訊中的號碼。

短訊挑戰2:
識別偽造訊息

1

☐ 官方短訊 ☐ 詐騙短訊

2

☐ 官方短訊 ☐ 詐騙短訊

答案

1. 詐騙短訊　2. 詐騙短訊

短訊挑戰3:
識別偽造訊息

3

☐ 官方短訊 ☐ 詐騙短訊

4

☐ 官方短訊 ☐ 詐騙短訊

答案

3. 詐騙短訊　4. 詐騙短訊

快問快答：
最後考考你

1 **學校裡的朋友要你告訴他們你的密碼。**
你會告訴他們嗎？
A. 會 / B. 不會

2 **你在社交媒體上看到一則訊息，請你將他的錢保管在你的戶口，然後付給你報酬。**
你會接受嗎？
A. 會 / B. 不會

3 **你在社交媒體上收到陌生人的好友請求。**
你會接受嗎？
A. 會 / B. 不會

4 **你的朋友在社交媒體 (WhatsApp、Facebook、Instagram、Snapchat)上向你借錢。**
你會答應嗎？
A. 會 / B. 不會

5 **當你使用自動櫃員機時，有人試圖分散你的注意力。**
你會轉身回應嗎？
A. 會 / B. 不會

6 **你遺失了銀行卡。**
接下來你會怎麼做？
A. 什麼都不做 / B. 盡快向銀行報失

答案：

1.B - 永遠不要告訴任何人你的密碼。

2.B - 這叫「錢騾」，在香港是非法的。

3.B - 如果接受，騙徒可能會獲取你的個人資料。

4.B - 可能不是你的朋友提出請求 - 先與他們當面確認。

5.B - 請確保遮蓋你的 PIN 碼。如果你覺得不安全，直接取走你的卡，並離開自動櫃員機。銀行分行內部的自動櫃員機可能是更好的選擇。

6.B - 確保你將遺失或被盜卡背面的號碼記錄在手機內。