■ 資料來源：資訊安全網

資訊安全：防範「仿冒詐騙」

2017年，香港曾發生數十宗有關欺詐銀行網站、偽冒電郵及類似的詐騙事件，今期《香港印刷》將分享仿冒詐騙電郵和網站的特徵，以及其攻擊的常用技倆，大家應時刻防範，免招損失。

何謂仿冒詐騙？

「仿冒詐騙攻擊」採用的手法涉及大量散播附有回郵地址、連結和品牌標記的「偽冒」郵件，令郵件看似來自銀行、保險代理、零售商或信用卡公司。這類欺詐電郵旨在誘騙收件人披露帳戶名稱及密碼、信用卡號碼、身份證號碼等個人認證資料。

近期仿冒詐騙攻擊

根據香港金融管理局的網頁，2017年香港曾有42宗關於欺詐銀行網站、偽冒電郵及類似的詐騙事件，而今年年初亦接二連三發生不同類型的詐騙事件，詳情可瀏覽< www.hkma.gov.hk/chi/ >。為免誤墮陷阱，收件人應了解有關仿冒詐騙攻擊概念及技倆，小心防範。

仿冒詐騙攻擊概念及技倆

有報告指出，仿冒詐騙者可能使用受騙者的個人資料，開啟假冒的帳戶及損害受騙者的信譽。由於這些郵件幾可亂真，因此有些收件人會作出回應，結果導致財務損失、身份盜用和其他欺詐行為等。

仿冒詐騙電郵的特徵

仿冒詐騙電郵通常具備下列特徵：

- 這類郵件一般以重要告示、緊急更新通告或警報的形式示人，其虛假的標題旨在令收件人相信發件的來源可靠，從而打開電郵。郵件的標題可能包含數字或其他字母，以逃避受濫發電郵過濾軟件過濾。
- 郵件的內文有時並無威嚇性，反而含有令人欣喜的信息，例如告知收件人中獎。

- 郵件通常使用假冒的發件人地址或偽冒的機構名稱，令郵件看似確是發自其偽冒的機構。
- 郵件通常會複製合法網站的網頁內容，包括文字、公司標記、圖像及樣式等。為求以假亂真，甚至連合法網頁的用字或語調仍會照樣抄襲。有些虛假郵件甚至設有連接真網站的超連結，以騙取收件人的信任。
- 這類郵件所設的超連結，通常會誘導收件人連接到一個欺詐網站，而非連結表上面所顯示的合法網站。
- 這類郵件通常設有表格，讓收件人填上個人／財務資料後發送出去。過程通常涉及執行小程式，把資料轉送至數據庫或臨時儲存區，供騙徒事後提取。

仿冒詐騙網站的特徵

仿冒詐騙網站通常具備下列特徵：

- 這類網站使用外表真確的內容，例如圖像、文字或公司標記，甚至會複製合法網站，以誘騙訪客輸入帳戶或財務資料。
- 這類網站設有真正連結，連接合法網站中的「聯絡我們」或「私隱及免責聲明」等網頁內容，藉以蒙騙訪客。
- 這類網站可能使用與合法網站相似的域名或子域名。
- 這類網站可能使用與合法網站相似的表格來收集訪客的資料。
- 這類網站可能以真正網頁為背景，而本身則採用彈出的視窗形式，藉以誤導和混淆訪客，令他們以為自己身處在合法網站中。
- 這類網站假設訪客未必會察覺，可能會在訪客的地址欄上展示互聯網規約地址或假地址。有些騙徒則可能透過小程式或超文本標示語言指令，使用網址偽冒手法建立假地址欄，以代替原來的地址。

仿冒詐騙攻擊的常用方法

騙徒誘使收件人相信郵件是來自合法機構後，通常會使用以下方法進行攻擊：

1. 在收件人的電腦中，安裝暗藏於電郵附件的特洛伊程式或蠕蟲，以尋找保安弱點及漏洞或拍下系統「快照」，藉以取得收件人的個人資料。
2. 使用鍵盤側錄程式之類的間諜軟件，擷取收件人的電腦資料，然後發送給騙徒。
3. 使詐博取收件人的信任，誘使收件人瀏覽看似合法網站的欺詐網站，並在站內的表格輸入個人資料。

仿冒詐騙攻擊的常用技倆

使用「仿真」網址

仿冒詐騙電郵經常使用社交工程學的手段，即是在信息中模仿合法機構的語調，並盜用其商標或稱號，以誘騙收件人至虛假網站輸入個人資料。這類虛假網站的網址在外表上通常與原來網站的網址非常相似。

以下列出多個香港銀行虛假網站所用的「仿真」網址：

香港銀行名稱	真實網站網址	「仿真」網站網址
中國銀行（香港）有限公司 Bank of China (Hong Kong) Limited (BOCHK)	www.bochk.com	www.bochkvip.com www.bchk.cn
東亞銀行 Bank of East Asia, Limited (BEA)	www.hkbea.com	www.onlinebea.com www.boeasiauk.com www.boeauk.com www.ebeauk.com
大新銀行 Dah Sing Bank Limited (DSB)	www.dahsing.com	www.daxinte.com www.dlfh.com www.dasxin.com
星展銀行（香港）有限公司 DBS (Bank) Hong Kong Limited	www.dbs.com	www.dbshk.net www.dbsbankhk.com
富邦銀行 Fubon Bank	www.fubonbank.com.hk	www.fubonhk.com
匯豐銀行 The Hongkong and Shanghai Banking Corporation Limited	www.hsbc.com	www.hkhsbc.com www.hkebc.com www.hsbccom.hk
港基國際銀行有限公司 International Bank of Asia Limited (IBA)	www.iba.com.hk	www.hkiba.com www.ibabankhk.com
中國工商銀行（亞洲） Industrial and Commercial Bank of China (Asia) Limited	www.icbcasia.com	www.icbc-online.com www.icbcasiachina.com www.icbcasiachina.cn
渣打銀行（香港）有限公司 Standard Chartered Bank (Hong Kong) Limited	www.standardchartered.com.hk	www.stbhk.com
永隆銀行有限公司 Wing Lung Bank Limited	www.winglungbank.com.hk	www.winglungonline.net

使用虛假網址（Bogus URL）和利用瀏覽器的弱點

有些不法分子會利用統一資源識別符號（URI）的語法編寫假網址，以隱藏其地址。URI 語法容許在格式上使用「@」、「%」編碼及「統一碼」編碼。

過去，微軟曾指出 IE 瀏覽器在處理網址方面有保安漏洞。有惡意的用者可以利用此弱點建立超連結，令連結通往假網站而非其假冒的合法網站。這手法同時可防止假網址在瀏覽器的地址欄及狀態欄上被顯示出來。

其他慣用技倆

- 使用合法網站的外觀，但實際上把訪客連接到虛假網站或彈出的視窗，藉以混淆訪客。
- 使用跨網址程式編程（Cross-site scripting）技術，在合法網站安裝有惡意程式碼或小程式。這些含惡性的程式會隨著合法網站的內容，傳送至訪客的瀏覽器，然後自動執行，以盜取電腦內的個人保密資料、尋找瀏覽器的漏洞或轉接瀏覽器至其他欺詐網站。
- 視覺仿冒：開啟一個彈出的瀏覽器，不顯示原來的網址、選單及狀態欄，而顯示仿冒者重建並帶虛假資料的網址、選單及狀態欄。

在左下角的狀態欄顯示一個「 鎖形 」的圖標，以混淆訪客，使他們覺得保密插口層（SSL）已被下載及啟動，以隱藏在背後的 Meta 標籤把真正的網頁轉向欺詐的網頁。

防範仿冒詐騙攻擊

對一般用戶的建議

防範措施

1. 不要連接濫發電郵等不可信來源或電郵所載的 URL 連結，以免被看似合法的惡意連結轉往惡意網站。
2. 不要登入可疑網站，或連接這類網站提供的連結。
3. 不要從搜尋器的結果連接到銀行或其他金融機構的網址。
4. 開啟電郵附件時要提高警覺，常常檢查附件的伸展部分，不要打開伸展部分是“pif”、“exe”、“bat”、“vbs”的附件。
5. 以人手打入 URL 位址或進入之前已加入書籤的連結。
6. 避免在設於咖啡室或圖書館等場所的公用終端機或不穩妥終端機，進行網上銀行或財務查詢／交易。這些公用終端機可能裝有入侵工具或特洛伊程式。
7. 在進行網上銀行或財務查詢／交易時，不要使用瀏覽器從事其他網上活動或連接其他網址。在完成交易後，切記要打印或備存交易記錄或確認通知，以供日後查核。
8. 提供敏感的個人或帳戶資料時，應時刻保持警惕。銀行及金融機構很少會以電郵的方式要求客戶提供個人或帳戶資料。如有疑問，應向相關機構查詢。
9. 確保電腦採用最新的保安修補程式和病毒識別碼，以減低欺詐電郵或網站利用軟件漏洞的機會。此舉亦有助保護電腦免受其他保安或電腦病毒攻擊。
10. 宜考慮安裝桌面濫發電郵過濾產品，以偵察和阻截欺詐電郵。不過，同時應避免杯弓蛇影。最好是學習一些基本技術常識，以充分發揮這些工具的效用。

偵察措施

1. 收到信用卡或銀行月結單後應立即細察，以確定是否有未經授權的交易或繳費。
2. 定期登入網上戶口，檢查帳戶狀況及上次登入日期，以確定是否有任何可疑活動。
3. 以書面或電話方式與銀行等機構聯絡，以核實其機構網站的合法性。

回應措施

1. 如果懷疑已被詐騙（例如你已對仿冒詐騙電郵作出回應，或向欺詐網站提供個人／財務資料），應立即更換密碼。經查核帳戶狀況後，立即聯絡有關機構及／或向警方報案。
2. 把仿冒詐騙電郵傳送給有關機構及／或警方，以便進行調查。

對公司／機構的建議

防範措施

1. 直接通知用戶（例如透過月結單、小冊子、刊物或網站內容等媒介）機構已採取的防範措施。例如說明其公司／機構：
   - 不會向用戶發出載有連接網站連結的電郵；以及
   - 不會要求用戶透過電郵披露個人身份或密碼等個人資料或帳戶資料。
2. 經常更新網站證書，向用戶就網站的合法性作出保證。
3. 向網站的用戶提供聯絡電話號碼，以供用戶就聲稱由機構發出並要求用戶提供資料的可疑郵件，向機構查證及舉報。
4. 考慮註冊與機構現行使用域名相近的新域名。例如，若果原來的域名是“www.abcbank.com.hk”，機構可另行註冊“www.abcbank.com”、“www.abc.com”或“www.abcbank.hk”等域名。
5. 為機構的域名設計一個商標，並將其註冊，以減少被誤用或抄襲的風險。
6. 加強機構在網站、應用系統及電郵系統各方面的保安管制，例如使用保密插口層、雙因子認證技術、數碼證書、防火牆和防電腦病毒方案，以改善對詐騙的監察及報告機制等技術方案。

7. 加強運作管制，例如調低每日交易或撥款的最高款額，或規定須先行註冊，才會獲授權透過互聯網進行某類網上交易。
8. 向用戶灌輸有關優良作業模式的知識，讓他們使用網上服務時有規可循。

偵察措施

1. 監察互聯網，留意其機構名稱、公司商標、標誌或網址有否被仿冒。
2. 監察互聯網，留意涉及其機構的仿冒詐騙電郵。
3. 監察公司網站，留意可有任何可疑活動。
4. 一確認有關網站可疑活動或仿冒詐騙電郵的任何報告，需要立即通知管理人員。

回應措施

1. 即時透過新聞公布、網站內容及電子郵件，向用戶、有關方面以至市民發出有關欺詐網站警報，提醒各方不要對可疑或仿冒詐騙郵件作出回應。
2. 若發現可疑網站，可向警方及有關機構（例如香港金融管理局）舉報。
3. 勸喻懷疑受騙的用戶立即更換密碼，並從速聯絡有關機構或向警方報案。
4. 向員工管理人員、或機構網站的服務供應商發出警報，著令加強保安措施，以及提防任何可疑活動。
5. 若發現密碼遺失、被盜取或保密失效，應立即停止使用該密碼及有關裝置。

常見問題

如果我已經向騙徒披露個人財務資料，應該怎辦？

請保持冷靜，先把可疑的電郵或通信記錄妥為保存。如果你已經披露如網上銀行帳戶名稱和密碼等個人財務資料，應立刻更換帳戶密碼、查看帳戶的狀況，並聯絡銀行或其他有關機構以作核證。若有需要的話，應立即向警方報案。

通常騙徒會如何使用騙取得來的個人資料？

騙徒通常會以下列方法使用騙取得來的資料：

- 在互聯網上的黑市市場出售
  騙徒會透過互聯網的聊天室或網站把偷來的個人或財務資料，賣給網上黑市市場的犯罪集團。這些歹徒會把買來的資料開設新的銀行或信用卡戶口，然後透支提款或購買物品，再轉售套現。
- 操控網上購物戶口
  騙徒取得網上購物者的帳戶及個人資料後，可以更改帳戶的登入密碼，實行把戶口接管和參與網上拍賣。帳戶的原來持有人對拍賣的電郵確認通知及有關資料將一無所知，直至收到銀行的帳單才會驚覺受騙。

如果想了解更多有關資訊保安管理的內容，請聯絡香港特區政府資訊科技總監辦公室製作和管理的「資訊安全網」：

資訊安全網

網址：www.infosec.gov.hk
電郵：webmaster@infosec.gov.hk
傳真：+852 2989-6073
地址：香港數碼港道一百號數碼港一座六樓