全球與冠狀病毒有關的網絡釣魚電子郵件攻擊上升了600%以上

釣魚攻擊行之有效，持續發酵是因為網絡犯罪分子針對人們對疫情的已知、未知、恐懼、壓力，好奇心和迫切感下，利用疫苗相關的資訊進行電郵詐騙，令受害人在判斷電郵的真實性前已作出錯誤的反應。

著名安全專家Bruce Schneier曾指出:

人性弱點是網絡安全鏈中最大的漏洞

網絡釣魚(Phishing)是一種網絡詐騙。黑客藉由發出大量的惡意郵件作攻擊，誘使收件人打開郵件內的附件或連結。郵件一般會訛稱由信譽良好的商戶或機構發出，目的是降低受害的戒心，將其導向虛假的網站以達到竊取用戶數據、帳戶密碼和信用卡資料等詳細信息。

有針對性的攻擊稱為「魚叉式網絡釣魚 (Spear Phishing)」，是近年最為著名的企業網絡攻擊之一。黑客會先從社交媒體鎖定受害人並進行前期研究，從而製作出具說服力的郵件內容，使騙局看起來更真實。釣魚郵件往往帶有惡意程式，程式通過內嵌連結、二維碼(QR Code)或檔案散播。一旦錯誤點擊，惡意軟件即會自動下載並植入到受害人的裝置內，使黑客可隨時發起攻擊，進行駭客活動。

魚叉式網絡釣魚成功率達到70%

超過90%的電郵騙局都是通過網絡釣魚進行的。網絡釣魚還被用作間諜的工具，超過78%的國家級別的網絡間諜事件都使用網絡釣魚。既然網絡釣魚如此盛行，我們可以如何避免呢？

注意！網絡釣魚郵件具有以下的特徵:

1 極端的壓迫感
郵件一般帶有威嚇字句，例如有可疑的帳戶活動，須要緊急處理，使收件人沒有時間去思考。黑客亦可能會要求接收者繞過標準程序或政策來達致特定目的。

2 要求敏感信息
要求收件人提供敏感信息，例如社交媒體帳號、密碼等資料來出售或作其他惡意用途。

3 通用的問候語或語言
由於釣魚郵件可能針對大量受害者，所以郵件內很少會提及收件人的名字，而且大多帶有通用的問候語或語言，如「您好」，「尊敬的客戶」等。

4 來源不可靠
郵件可能來自不可靠的來源，切勿被寄件者名稱蒙蔽。「寄件者」欄位可隨意更改，黑客可盜用官方機構的名義來發送釣魚郵件。在確認可疑郵件之前可先留意「寄件人」或「回覆」電子郵件的地址是否與該公司之名稱存在差異或使用個人的郵件帳戶。如仍對真偽存有疑問，可以致電該公司或同事進行驗證和確認。

5 破綻百出
郵件可能包含拼寫錯誤的單詞或不正確的文法。大多數大型信譽良好的公司在發送之前都會仔細編輯其信息。

6 中獎/折扣優惠
以中獎為題的電子郵件，利用人性的貪婪，貪小便宜的心態來進行詐騙勒索。

7 可疑的網站連結
許多網絡釣魚電子郵件都包含指向假網站的連結，誘使收件人點擊連結並在偽冒網站上提供個人資料及信息。如對連結有任何懷疑，點擊前可先將鼠標懸浮在連結上(切勿點擊超連結)，系統會彈出提示框顯示完整的超連結地址。如懷疑自己誤進仿冒的網站，在輸入個人資料之前，可先查看網站有否獲得數碼證書簽發，網址會以https開頭。

8 附件檔案
仿冒的電子郵件可能包含惡意附件，但Windows檔案總管預設了隱藏所有檔案的副檔名，所以附件為.exe、.com、.jar、.bat、.cpl、.scr、.js、.pif、.exe的執行檔、Office巨集檔或檔名為.jpg的檔案都可能隱藏了黑客攻擊。如錯誤點擊附件，當中的惡意軟件可能會感染電腦。

反制訣竅

亡羊補牢不如預先防禦，我們應時刻對可疑的電郵保持警惕，先冷靜判斷寄件者及外部連結網域資料，避免直接點擊附件和連結，並使用防毒軟件來過濾及隔離垃圾郵件。

遭到網上誘騙攻擊，可以執行以下操作:

A 更改任何受釣魚攻擊影響的網站帳戶資料及密碼

B 在電腦上執行病毒掃描，檢查是否感染了惡意軟件

C 如信用卡信息不幸洩露，請立即致電信用卡公司通報

如果您懷疑在工作期間收到網絡釣魚郵件，請向IT支援同事尋求幫助。另可參閱eGarden內的電子郵件政策(Email Policy)

切記：知識是我們打擊網絡犯罪分子的最大武器

「防騙易18222」反詐騙諮詢熱線