Subject line：網絡安全提示，幫助您保持網絡安全

致 NYCHA 居民:

現正值開展網絡安全宣傳月，我們想向您介紹一些有助於您在家和工作中使用網絡時保持網絡安全的信息。感謝您幫助我們的世界保持網絡安全。

做好本份。#BeCyberSmart.

保障網絡安全是每個人應盡的責任。您可盡自己的努力，報告任何可疑現象，採取更強的安全措施，並幫助提高警惕。

如何明智使用网络

去年，針對美國企業的網絡攻擊導致的破壞情況上昇了百分之 17。 全國共有 1,474 起系統被成功入侵的案例。網絡罪犯不僅僅是使用技術偷竊資料 -他們還利用人類的錯誤和我們分享日常生活信息的漏洞。

保持警惕：只因一個錯誤。 數據泄露很少是由於犯罪分子通過機構的基礎設施進行黑客攻擊的結果。通常，他們利用一個簡單的弱點開始。用戶只要被誘騙泄露了其密碼和其它信息，那麼所有關於這個用戶所使用的信息和數據將會被暴露。時刻保持警惕，防止網絡釣魚和社會工程的攻擊。時刻謹慎處理不尋常的信息來源，不要點擊陌生的鏈接，並立刻通過發送電郵 (郵址：phish@nycha.nyc.gov) 舉報與 NYCHA 相關的可疑信息或郵件。

保持網絡安全的簡單技巧

1. **如果您看到什麼，就說出來**

   如果您發現 NYCHA 的網頁或 NYCHA 的應用程序有任何異常，請致電 NYCHA 客戶服務中心 (CCC)舉報，電話：718-707-7771。

2. **商業信息就是個人信息** 很多人在工作中處理敏感的資料或數據。這些資料不一定是信用卡或社會安全號碼 -可以是任何職員或客戶的資料，特別是任何屬於某個特定用戶的資料。不要向機構以外的任何人泄露公司數據。

3. **保持密碼智能和安全** 用戶所設置的密碼應該是容易記住但難以被猜測的。您可使用一個詞組或一系列單詞，但記得包括足夠多的隨機元素讓人無法猜測您的密碼。謹記，尤其是當您在家辦公，保持所使用的路由器，網絡，和所連接設備的正確備置。

4. **隨時更新** 確保您的軟件定期使用最新的版本更新。 確保您用於辦公的電腦都安裝了病毒/惡意軟件保護程序，並定期進行病毒掃描。

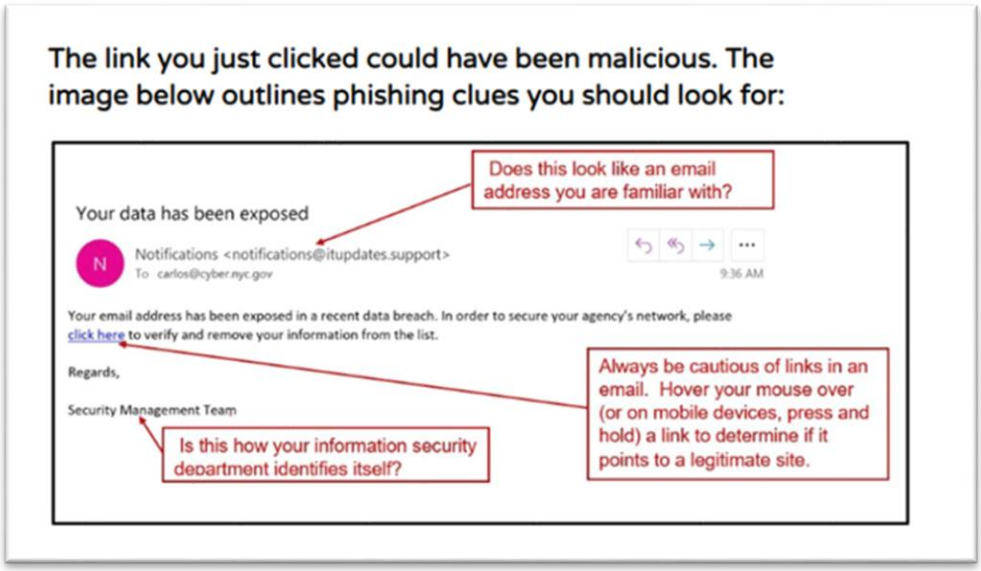
5. **工作結束後，仍要明智使用网络** 社交媒體也屬於詐騙工具的一部份。 網絡攻擊者可以通過谷歌 (Google), 臉書 (Facebook) 或任何網站查找有關您的信息。 避免在社交媒體或任何網絡分享潛在的敏感信息，切勿使用社交平台進行與工作相關的業務或交換敏感信息。

了解更多

點擊 觀看這些互動視頻了解更多如何 #BeCyberSmart 明智使用網絡的詳情

什麼是網絡釣魚 (Phishing)？

您在郵件，社交媒體帖子，短信和網上廣告中所看到的鏈接通常都是網絡罪犯試圖竊取您的個人資料的手段。 即使您知道其來源，如果這些鏈接可疑，請刪除。不要點擊陌生人發送的鏈接。 下圖是辨別企圖網絡釣魚的方法：



什麼是勒索軟件 (Ransomware)？

勒索軟件是一種流氓軟件，或惡意軟件，阻止您進入您的電腦文件，連接系統或網絡並要求您支付贖金才能再次進入或連接。 您可通過打開郵件的附件，點擊廣告，關注鏈接，或瀏覽惡意軟件關聯的網站，在不知不覺中將勒索軟件下載至您的電腦上。一旦下載了勒索軟件，它將鎖定您電腦或所存儲的資料和文件。當您發現您無法再打開您的資料或文件或看到電腦顯示的受到攻擊並要求您支付贖金的提示信息時，您才會發現您的電腦已受到病毒感染。

避免下載勒索軟件-或任何類型的惡意軟件的最好方法是做一個謹慎和盡責的電腦用戶。 惡意軟件的經銷商越來越精明，您需要格外謹慎您所下載和點擊的鏈接或程序。

謝謝合作！

格雷戈里· 羅斯 (Greg Russ)
主席兼行政總監