CyberDefender.hk

數碼素養系列

2023 年 12 月

親愛的家長：

給家長的信

惡意手機App (下稱「毒App」) 近期在本地迅速蔓延。今年九月至今，本港已錄得24宗相關案件，涉及損失金額達$1,100萬，當中全部與網上購物有關，任何年齡和背景的人士均可能成為受害人。今期我們將探討相關犯案手法及防罪建議。

上述手法均針對Android手機系統，騙徒會先建立社交專頁出售商品或服務，之後透過WhatsApp與市民聯絡，期間發送檔案或連結要求市民下載手機App以進行訂購。市民不虞有詐下載了毒App並透過毒App付款時，毒App會出現假頁面要求輸入銀行用戶名稱、密碼和保安編碼。

上述毒App不斷偽裝成購物或影視串流等平台，而且極具侵入性。它會要求用戶給予完全控制權，以取得用戶手機的敏感資料，並登入用戶的銀行帳戶轉移資金。就今年最大損失的一宗案件，一名男子因為誤裝毒App購買食品，被騙徒登入其網上銀行帳戶並轉走$600萬元。騙徒也能透過毒App取得用戶的相片、電話簿、電郵及通訊記錄，並用作其他不法用途。

為防範你及子女的電子裝置受到惡意軟件入侵，我們有以下建議：

- 只從官方渠道下載應用程式，避免點擊任何不明來歷的連結。
- 切勿允許應用程式存取不合理的權限。
- 如懷疑安裝了手機 App，應把手機還原至出廠設定。
- 不要輕易透露個人或敏感資料。
- 安裝抗惡意軟件工具及經常保持更新。

儲存了大量數碼資產和敏感資料的手機往往會成為不法之徒的目標，因此提升我們的數碼安全意識極為重要。想知更多網絡安全資訊及提升子女辨識網絡陷阱的能力，請瀏覽「守網者」網頁 (https://CyberDefender.hk) 或下載「防騙視伏 APP」手機應用程式。

香港警務處

網絡安全及科技罪案調查科

CyberDefender.hk

Digital Literacy Series
December 2023

Dear Parents,

Letter to Parents

Malicious apps have been spreading rapidly in Hong Kong recently. Since September this year, there have been 24 reported cases involving $11 million of loss, among which most of the cases were related to online shopping, thus citizens from all walks of life are at risk. In this issue, we will study how malicious app works and provide relevant crime prevention advice.

Malicious apps target Android operating system. Scammers would first set up pages on social media platforms to sell services or products, then contact citizens via WhatsApp. Scammers would then send citizens a file or link, requesting them to install and place an order through the app. Citizens would then unknowingly download a malicious app. Upon payment, the malicious app will display a fake page asking the citizen to input their online banking username, password and PIN.

These malicious apps masquerade as online shopping or entertainment platforms and are highly intrusive. The apps require users to give full permission, thus enabling scammers to obtain sensitive information from their mobile phones and log into their bank accounts to transfer fund. For the case with the biggest loss this year, a man was conned to install a malicious app for ordering food. His bank account was hacked by scammers who then stole HK$6 million therefrom. Scammers could also access to users' photo albums, phone books, emails and messages through malicious apps for other nefarious purposes.

To prevent malware from compromising the mobile devices of you and your children, we have some tips for you:

- Download apps only through official channels, and avoid clicking links of unknown origin.
- Do not grant apps with excessive permissions.
- If you suspect that a malicious app is installed, reset your mobile to factory settings.
- Do not disclose personal or sensitive information easily.
- Install anti-malware tools and keep them updated frequently.

As mobile phones that store voluminous digital assets and sensitive data are often targeted by criminals, raising our awareness of digital security is of utmost importance. For more information on cyber safety and enhancing your children's ability to differentiate cyber traps, please visit CyberDefender website (https://CyberDefender.hk) or download the Scameter+ mobile app.

Cyber Security and Technology Crime Bureau
Hong Kong Police Force