親愛的家長：

給家長的信

網上帳戶騎劫案件近日在本地迅速蔓延。今年八月至九月，本港共錄得1,366宗相關案件，涉及損失金額達$2,820萬，當中絕大部分涉及WhatsApp平台。今期我們將探討有關犯案手法及防罪建議。

就WhatsApp帳戶騎劫案件，騙徒會大量發放SMS短訊，訛稱市民的WhatsApp帳戶異常，誘使受害人點擊假WhatsApp網站連結，其後要求受害人輸入電話號碼及轉移代碼，騙徒隨即使用另一裝置登入受害人的WhatsApp帳戶並向其親友借貸以騙取金錢。另外，騙徒也會把虛假的WhatsApp登入網站在搜尋器以「WhatsApp」作關鍵字投放廣告，當市民搜尋「WhatsApp」字串時，假網站便會以置頂廣告形式出現。如果市民進入假網站並掃描二維碼，騙徒便可通過網上版WhatsApp登入市民帳戶並向其親友騙財。日前，一名女子收到其十七歲女兒的WhatsApp帳戶發出的訊息，要求她繳付$14,000元補習費。女子不虞有詐，轉賬後始發現女兒帳戶較早前被入侵。

為防範你及子女因帳戶被騎劫，我們有以下建議：

- 啟用帳戶的雙重認證功能。
- 定期檢視帳戶是否有連結不明來歷的裝置。如有的話，應馬上登出。
- 切勿隨便向他人透露密碼、驗證碼或掃描不明的二維碼。
- 收到任何短訊時，留意短訊內容和連結是否有異樣，例如錯字、繁簡字夾雜等，以識別及避免登入假網站。
- 如親友透過訊息要求轉賬或匯款，應直接致電對方確認。

網絡騙案手法層出不窮，為免不法之徒有機可乘，提升自己及子女的數碼素養極為重要。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

Dear parents,

Letter to Parents

Recently, online account hijacking cases have been spreading rapidly in Hong Kong. In August and September this year, there were 1,366 reported cases involving $28.2 million loss, mainly involving the WhatsApp platform. In this issue, we will explore the methods used by WhatsApp hijackers and provide relevant crime prevention advice.

Regarding WhatsApp account hijacking, scammers send out numerous SMS messages purporting abnormality in WhatsApp accounts, enticing victims to click on links that lead to bogus websites requesting input of mobile numbers and transfer codes. The scammers will then use another device to log into victims' WhatsApp accounts and deceive their acquaintance by soliciting loans. Other than that, some scammers advertise bogus websites resembling WhatsApp log-in page by adopting the keyword "WhatsApp" on search engines. When the public searches for "WhatsApp", bogus websites are shown as top advertisements. If someone scans the QR codes on bogus websites, scammers could infiltrate the account via web WhatsApp and carry out scams.

Recently, a woman received a message from the WhatsApp account of her 17-year-old daughter requesting $14,000 tuition fee. Without second thought, transfer was made and scam was unveiled upon discovering daughter's account was hijacked.

To prevent you and your children from account hijacking, here are some tips for you:

- Enable the two-factor authentication feature of your accounts.
- Review if your account is linked to any unfamiliar device regularly. If any, log out immediately.
- Avoid disclosing passwords and verification codes to others casually or scanning unusual QR codes.
- If received any message, pay attention to unusual contents in text messages or URLs, e.g. misspellings, mix of traditional and simplified Chinese characters, etc. to identify and avoid access to bogus websites.
- If anyone requests for money transfers through messages, call directly to confirm.

Online scammers evolve quickly. It is crucial to enhance the digital literacy of your own and your children to prevent adversaries from taking advantages. For more information on online 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