親愛的家長：

給家長的信

近年來，科技犯罪和虛假資訊不斷演變，對社會造成了嚴重的威脅。為了應對這挑戰，警方深信培養學生的網絡安全意識和事實查證的習慣至關重要。大家亦深知，只有讓年輕一代具備這些技能，他們才能更有效地抵抗不斷增長的網絡威脅。

為了提供可靠的事實查證途徑，警方於 2022 年推出了一個名為「防騙視伏器」的一站式詐騙和網絡陷阱搜尋平台。這個平台為市民提供了查證信息的工具，讓他們能夠更有能力地識別詐騙及虛假資訊。警方於翌年 2 月推出了「防騙視伏 App」手機應用程式，今年 2 月更推出了升級版的「防騙視伏 App」，引入三項新功能及人工智能技術。

升級版「防騙視伏 App」引入兩項新功能：「可疑來電警示」和「可疑網站偵測」。這些功能讓市民能夠將接收到的電話和訪問的網站自動與警方維護的騙案資料庫進行比對。如果應用程式檢測到潛在的詐騙風險，將立即發出警示，避免用戶受騙。希望能做到「自動偵伏，舉報騙局」。

然而，打擊詐騙活動不僅需要警方和相關機構的努力，還需要市民的積極參與。為了鼓勵公眾參與，「防騙視伏 App」應用程式引入第三項新功能 – 「公眾舉報平台」。市民可以通過這個平台直接向警方提供可疑電話號碼或網站的信息。警方將對市民提交的舉報進行人工智能分析，並對舉報的電話號碼和網站進行風險評估。警方將進一步核實這些信息，以確保詐騙資料庫的準確性。

去年，一名受害人收到騙徒的「白撞」訊息，對方聲稱是投資專家並說服受害人投資虛擬貨幣。受害人有感興趣而被騙，於去年五月至今年二月期間，共轉賬一千八百萬元至九個本地銀行戶口。經警方調查後，發現九個由騙徒提供的轉帳戶口中，其中六個曾牽涉較早前的騙案，並已記錄在「防騙視伏器」的資料庫中。如受害人在過數前使用防騙視伏器核查，就有可能避免損失。

另一名受害人在網上看見一個盜圖偽冒本地股評人的廣告而被騙加入群組學習投資，隨後被騙下載一個手機應用程式及在程式上開設投資戶口。受害人不虞有詐一共注入五十萬元資金，但資金隨即被凍結。及後，受害人在「防騙視伏器」查看風險，發現受騙而報警求助。

為了保護您和您的孩子，我們強烈建議您下載並更新「防騙視伏 App」[1]應用程式，並開啟功能權限，以減少受騙的風險。如需更多關於網絡安全和提高孩子識別網絡陷阱能力的信息，請瀏覽「守網者」官方網站 (https://cyberdefender.hk)。

香港警務處
網絡安全及科技罪案調查科

[1] 市民可以從 Apple App Store，Google Play Store 及華為 AppGallery 免費下載升級版「防騙視伏 App」。

Dear Parents,

Letter to Parents

In recent years, technology crimes and misinformation have evolved, posing a serious threat to the community. Police strongly believe that cultivating cybersecurity awareness and fact-checking habits among students is of utmost importance to meet this challenge. As we all know, only by equipping the younger generation with these skills can they more effectively combat the ever-growing cyber threats.

To provide a reliable means of fact-checking, Police launched the one-stop scam and online pitfall search engine, the Scameter, in 2022. The platform provides the public with a tool to verify information, empowering them to better identify frauds and misinformation. In February 2023, Police launched the Scameter+ mobile application and further upgraded it in February this year, introducing three new features and artificial intelligence (AI) technology.

The upgraded Scameter+ introduces two new features: "Suspicious Call Alert" and "Suspicious Website Detection". These features allow automatic comparison of incoming calls and websites being visited with the fraud database maintained by Police. If the app detects a potential fraud risk, it will immediately issue an alert to prevent the user from being scammed, thus achieving protection to the user with automatic detection.

However, combating fraudulent activities requires not only the efforts of Police and relevant organisations, but also the active participation of the public. To encourage public participation, a third new feature – the "Public Intelligence Platform" – is introduced to the Scameter+. Through this platform, the public can provide information on suspicious telephone numbers or websites directly to Police, who will analyse the reports with AI and conduct risk assessment on the information submitted. Police will further verify such information to ensure the accuracy of the scam database.

Last year, a victim received an unsolicited message from a scammer who claimed to be an investment expert and lured the victim to invest in cryptocurrency. Feeling interested, the victim was scammed and transferred HK$18 million in total to nine local bank accounts between May 2023 and February 2024. Police investigation revealed that out of the nine bank accounts provided by the scammer, six were involved in earlier scams and had been indexed in the Scameter database. If the victim had checked Scameter before making the transfers, loss could have been prevented.

Another victim came across an online advertisement posted by a scammer who impersonated a local stock commentator using the latter's stolen photos. Falling prey to the scam, the victim joined the scammer's investment group, downloaded a bogus mobile app and created an investment account therein. Not suspecting a thing, the victim transferred a total of HK$500,000 to the app but her funds were soon frozen. The victim only realised she was scammed after checking Scameter, and thus made a Police report.

To protect you and your children, we strongly recommend you to download and update the Scameter+[1] and enable the functions so as to minimise the risk of being scammed. For more information on cybersecurity and enhancing your children's ability to recognise online pitfalls, please visit the official website of CyberDefender (https://CyberDefender.hk).

Cyber Security and Technology Crime Bureau
Hong Kong Police Force

[1] The public can download the upgraded version of Scameter+ for free from the Apple App Store, Google Play Store and Huawei AppGallery.