# 教育局
# 人工智能素養與守護學生網絡安全網上研討會-小學

## 網上銀行保安措施簡介

趙紫瑋
總經理
香港金融管理局

2026年10月8日

# 網銀安全ABCD

- 一套全方位措施，用以防範越趨複雜的網絡詐騙手法，並提升網絡安全防護意識。

## App內認證

- 讓客戶預設使用綁定流動裝置以認證高風險網上銀行交易，不再使用短訊一次性密碼。
- 客戶綁定或重新綁定其流動裝置時，須通過較嚴謹的身份驗證方法進行認證。

## Bye bye高危功能

- 允許客戶選擇停用高風險網上銀行功能，包括網上新增收款人及網上提高轉帳限額。

## Cancel可疑轉帳

- 進一步增強「可疑帳號警示」機制下顯示的警示的有效性，包括要求「高危」警示最少顯示 10 秒。

## Deepfake偵測

- 加強銀行偵測及抵禦Deepfake相關作案手法的能力。

# 新興詐騙手法 (1/2) — 信用卡詐騙

- 騙徒利用早前收集的信用卡資料，對新推出的 iPhone 18 Pro 進行預訂。

資料來源：香港經濟日報

資料來源：香港 01

資料來源：
星島日報

# 客戶防騙意識 (1/2) — 信用卡詐騙

銀行不會透過短訊或電郵超連結，引領客戶到其網站或流動應用程式進行交易，更不會透過超連結要求客戶提供任何敏感的個人資料（包括登入密碼和一次性密碼）。

在提供個人及信用卡資料作授權交易前，應仔細確認商戶的真實性及網頁真偽。

時刻留意電郵、手機短訊等收到的銀行通訊，不時查閱信用卡交易紀錄及核對月結單。

如發現可疑或未經授權交易，不論牽涉金額多少，應立即通知發卡銀行。

# 新興詐騙手法 (2/2) — 惡意程式詐騙

1

誘騙受害人下載
惡意程式

2

3

4

利用所獲取的登入資料
進行未經授權交易

獲取信用卡
資料

截取短訊
一次性密碼

# 客戶防騙意識 (2/2) — 惡意程式詐騙

## 惡意程式騙案的潛在風險

洩露敏感的個人資料

蒙受財務損失

## 如何提防惡意程式詐騙

- **銀行網址及流動應用程式（App）**：應透過輸入銀行網址或銀行App登入。切勿透過電郵或網上超連結、附件登入或提供個人資料（包括密碼）。
- **只透過官方應用程式商店下載程式**：避免經非官方渠道，例如社交媒體連結、陌生人提供的檔案或不明來源的APK安裝。
- **切勿隨意點擊超連結**：切勿點擊來歷不明的超連結，尤其是短訊或電郵中的超連結。
- **小心附件**：切勿隨意開啟來歷不明的電郵或短訊附件。
- **核實發件人身分**：如收到訊息要求提供個人資料或密碼，應先核實發件人的身分。可透過官方電話或網站查詢，切勿直接回覆或跟隨訊息內的指示。

# 公眾教育

- 為提高公眾的防騙意識以及對「網銀安全ABCD」措施的認識，金管局推出一系列的公眾教育活動，包括社交媒體帖文及動畫歌曲：

*網銀安全家族*

*網銀安全家族動畫歌曲*

YouTube: https://youtu.be/F6U72lbuqnA