其他常見的詐騙攻擊方式

語音釣魚和電話詐騙

電話詐騙，或稱語音釣魚，是指詐騙者假冒成您的銀行或其他可信任的機構來進行電話詐騙。以現時的人工智能技術，只需擷取你五秒鐘的對話，騙徒便能以深度偽造技術，模擬你的聲音來創造不同對話。騙徒甚至可能讓來電顯示成您認識且信任的號碼或偽冒您的認識的聲音以要求將資金轉移到另一個賬戶。此被稱為改號欺詐，其對話內容聽起來可能非常真實可信，詐騙者甚至可能已經掌握了一些有關您的個人資訊，如賬戶號碼或地址。如果您覺得有任何不妥，或察覺有異，請不要猶疑，立即掛斷電話。

您可以反過來致電您所知的機構電話號碼，例如您銀行卡背面的電話號碼，以核實來電的真偽。

但請留意，騙徒可能繼續保持通話線路連通，甚至偽造撥號的音效，讓您誤以為真。因此，請使用另一部手機，或相隔至少30秒後才致電。

常見的例子包括：

- 「您的銀行」通知您的賬戶出現風險，需要將您的資金轉移到另一個賬戶，以確保安全。
- 「您的銀行」需要您的協助來調查詐欺事件。
- 您的網絡或電訊供應商致電給您，替您解決您從沒有報告過的問題。

銀行可以根據您的要求轉賬，但絕不會因此索取您的密碼、PIN碼、任何一次性密碼或安全代碼。

入侵賬戶欺詐

騙徒可能以偽冒的電話號碼致電給您，例如顯示為恒生電話銀行或其所偽冒公司的電話號碼。騙徒往往對公司的運作相當熟悉，會引導您進行您所預期的流程，例如驗證程序，以搏取您的信任。

接著，他們將以各種方法來騙取您的安全資訊，例如使用者名稱、密碼、安全代碼。騙徒隨後可以使用這些資訊，成功入侵您的賬戶，並將您的資金轉走。

請謹記：

- 恒生不會要求您提供卡片PIN碼、密碼或安全代碼。
- 不要向任何人透露安全代碼。
- 恒生絕不會要求您將資金轉移到任何安全賬戶。