

要保護您的資金關鍵盡在您手中

The power to protect your money is in your hands

要保護辛苦賺來的金錢，便要掌握最新的防騙資訊，讓您可及時發現並防範詐騙。
Protect your hard-earned money from scams!

Equip yourself with the most updated knowledge to spot and stop scams.

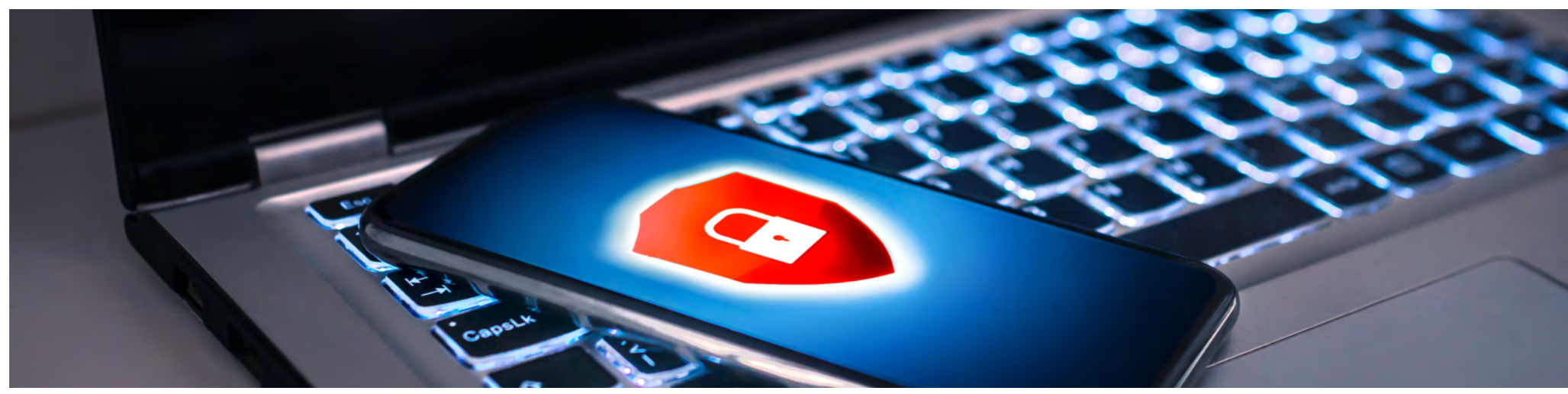
想知道如何開始？請細心閱讀並謹記以下貼士，以免墜入3種常見的騙局：
惡意軟件、釣魚程式及偽冒政府官員。

Not sure where to start? Read the tips below to protect yourself from 3 common scams – malware, phishing and government impersonation.

提防這些騙局 WATCH OUT FOR THESE SCAMS

以下是3種常見騙局，您必需隨時保持警惕以保護您的財產。

Here are 3 scams you should know about and the ways to protect yourself from them.



惡意軟件 Malware threats

惡意軟件是一種騙徒故意編寫的軟件，用以入侵電腦和手提電話以圖做出犯法之行為。如您的裝置被惡意程式入侵，即有機會被騙徒遙距控制，並竊取您的個人資料。

Malware is a type of malicious software that scammers use to infect computers and mobile devices in order to carry out criminal activities. Once infected, the devices can be accessed remotely by scammers and confidential data like your login credentials may be stolen.

如何保護自己 How to protect yourself:

- 避免安裝或運行來歷不明的軟件或程式
Avoid installing software or running programs from unknown sources
- 不要打開未經認證的電郵、WhatsApp訊息或任何社交媒體內的附件或連結或掃描二維碼
Do not open attachments and links – or scan QR codes – from unsolicited emails and WhatsApp messages, and social media platforms
- 使用可信的防毒軟件來保護您的裝置
Keep your devices secure by using trusted anti-virus solutions
- 切勿將您的登入資料儲存於您的網絡瀏覽器或裝置中
Never store your online banking login credentials in your web browsers or devices



釣魚程式詐騙 Phishing scams

釣魚程式詐騙是指詐騙者透過冒充他人或提供某些東西作交換，以欺騙您分享您的重要資訊。

Phishing scams are those where scammers trick you into sharing confidential information by pretending to be someone they are not or offering something in exchange.

如何保護自己 How to protect yourself:

- 對於回報過高而又不切實際的交易持懷疑態度
Be sceptical of deals that seem too good to be true
- 對未經驗證的網站提示，不要提供您的個人或銀行資料
Do not provide your personal and/or banking details when prompted by unverified websites
- 為您的銀行帳戶及信用卡啟動交易提醒
Enable transaction alerts for your bank account(s) and credit card(s)



偽冒政府官員 Government impersonation

提防詐騙者冒充政府官員，尤其是警察或法院官員，他們經常會使用恐嚇性的技巧來誘騙您透露您的個人資料。

Beware of scammers posing as government officials, such as police officers and court officials. They often use scare tactics to convince you into disclosing your personal details.

如何保護自己 How to protect yourself:

- 不要因一時受壓或恐懼而做出倉促決定
Do not give in to pressure and let fear rush you into making hasty decisions
- 如來電者未能清晰或明確說出自己的身分，請立即結束通話
End a call immediately if the caller is unable to properly identify himself/herself
- 如任何時候，對於任何訊息或請求有懷疑，請務必透過官方網站核實其真偽性
Always verify the authenticity of any information shared with you, or requests made to you, by contacting the organisation through their official website or hotline

謹記以下的防騙貼士： REMEMBER THESE ANTI-SCAM TIPS



切勿向其他人透露
戶口及個人資料

Never share your banking
credentials with anyone



務必檢查您瀏覽的網站為
官方網站

Always check that the
websites you browse are
official ones



確保我們有您最新的
聯絡資料以便您可以及時
收到銀行提醒

Ensure that your contact
details are up to date in our
records so you can receive
timely banking alerts

如懷疑遇到任何詐騙，請致電司法警察局「防詐騙查詢熱線8800 7777」求助。
If you encounter any scams, please call the Judiciary Police “Anti-Fraud Enquiry Hotline 8800 7777” and let others know promptly.

如您有任何懷疑或異常情況，請即致電我們的客戶服務熱線2832 2222，盡快與本行查詢並核實真偽。

If you suspect that you have encountered a fraud case, please call our customer service hotline at 2832 2222 and verify the authenticity of the text message or email.

華僑銀行（澳門）股份有限公司

OCBC Bank (Macau) Limited

ocbc.com.mo



OCBC Macau



OCBC | 搜尋



華僑銀行澳門 | 搜尋

保安提示 Security Alert :

本行絕不會透過電郵或電郵中之超連結要求客戶核實個人及/或戶口資料。客戶應透過華僑銀行之官方網站與本行聯絡，而非透過此等電郵或超連結。

OCBC Bank will never ask out customers to provide or validate their personal and/or account related information by emails or through any hyperlinks embedded in such email. The Bank will not send out emails with embedded links. Customers should contact us via our official website.

若閣下不欲收取本行之電子宣傳郵件，請以書面形式知會本行，內容請註明「拒收電子推廣訊息」，列明閣下之賬戶/信用卡名稱及號碼，並以留存本行印鑑簽署後，交予各華僑銀行分行或寄回澳門郵箱3087號。此服務不收取任何費用。

Should you want to unsubscribe any electronic marketing messages from the Bank, please inform us via written requests on “unsubscribe e-marketing messages”. In the request, your bank/credit card account and account no. should be indicated, together with your signature (the one registered at the Bank). You may submit the request to our branches or mail it to Macau P.O. Box no. 3087. This service will not incur any cost.

請勿回覆此電郵 Please do not reply this email.