November 2020

Important Notes on Precautions of Bogus Voice Message Phone Calls, Fake E-mails, Fraudulent Websites and Fraudulent SMS messages

Nanyang Commercial Bank ("NCB") would like to remind its customers to stay vigilant to voice message phone calls purportedly from NCB, fake e-mails, fraudulent websites and fraudulent SMS messages, etc. Customers are advised to protect their personal information at all times.

In this regard, NCB wishes to alert its customers to the following important notes:

1. NCB will not require customers to provide sensitive personal information (including login and one-time passwords) through phone calls, emails or SMS messages. Customers should not disclose their personal information to any suspicious caller or third party.

2. NCB will not notify customers of any irregularities or suspension of their bank or credit accounts, and request customers to input their personal information or contact bank staff for identity verification through any pre-recorded voice messages, e-mails or SMS messages. Customers are also reminded not to rely solely on the incoming call display, e-mail address, website address, SMS message or message content to identify the caller/sender.

3. Customers who are suspicious about the identities of the callers should request for the callers' contact numbers and names, etc for verification and should not disclose their personal information during the process.

4. If customers would like to verify any phone calls, e-mails, website addresses or SMS messages purporting to be initiated by or

related to NCB, they should call NCB Customer Service Hotlines at (852) 2622 2633 (press "0" after language selection) or visit any of our branches for enquiry.

5. When accessing the Internet Banking or Mobile Banking Service, customers should type the website of NCB (www.ncb.com.hk) directly into the address bar of the browser. Customers should not log into the Internet Banking or Mobile Banking through any hyperlinks embedded in emails of unknown sources.

For the security information of Internet Banking, please browse http://www.ncb.com.hk/nanyang_bank/resource/si_en.pdf .
If customers are concerned that they may have disclosed their personal information to any suspicious person, they should immediately call NCB Customer Service Hotlines at (852) 2622 2633 (press "0" after language selection) or visit any of our branches for enquiry, or directly contact the Hong Kong Police Force.

If customers do not wish to receive telemarketing calls from NCB, they may exercise their opt-out right by calling NCB Customer Service Hotlines at (852) 2622 2633 (press "0" after language selection) or visiting any of our branches.

Please visit the website of the Hong Kong Monetary Authority https://www.hkma.gov.hk/eng/smart-consumers/beware-of-fraudsters/ to watch the promotional video and relevant materials to learn more about how to against fraudsters.

A copy of the "Alert on Bogus Voice Message Phone Calls, Fake E-mails, Fraudulent Websites and Fraudulent SMS messages" is attached for your reference.

Nanyang Commercial Bank, Limited

NCB 南洋商業銀行

Alert on Bogus Voice Message Phone Calls, Fake E-mails, Fraudulent Websites and Fraudulent SMS messages

Scenario 1: Preventive measures against fraud

Do

✓	Request for the callers' contact numbers and names, etc for verification in case of suspicious calls
✓	Call NCB Customer Service Hotlines or visit any of our branches for verifying the authenticity of phone calls, e-mails, website addresses or SMS messages
✓	Type the website of NCB directly into the address bar of the browser for access to the Internet Banking Service
✓	Stay vigilant to anything abnormal (e.g. request for inputting your credit card number, expiry date or verification code on the back of credit card, one-time password or personal data) during login to NCB's website/Internet Banking

Don't

×	Disclose sensitive personal information (in particular the login and one-time passwords) to third party
×	Rely solely on the incoming call display, e-mail address, website address, SMS message or message content to identify the caller/sender
×	Log into the Internet Banking and Mobile Banking through any hyperlinks embedded in emails of unknown sources

Scenario 2: Follow-up action in case of disclosure of personal information to any suspicious person

Do

✓	Contact our staff by calling NCB's Customer Service Hotline or visiting any of our branches immediately
✓	Stay calm and contact the Hong Kong Police Force as soon as possible

Don't

×	Attempt to handle the case on your own and delay contact with our bank staff or report to the Hong Kong Police Force

懷疑被騙

請即打
防騙易諮詢熱線

反詐騙協調中心

ADCC
Anti-Deception Coordination Centre
反詐騙協調中心

ANTI-SCAM
防騙易
18222

提防電騙

1 預錄語音

騙徒以預錄語音致電市民，聲稱為速遞公司、銀行、政府部門或其他機構等，然後要求市民按鍵選擇收聽語言

懷疑被騙
請即致電
18222

2 聲稱市民涉及刑事案件

市民被轉駁至假冒的內地執法人員，該騙徒聲稱市民在內地犯法，需要提供其網上銀行資料作快速審查，以協助其洗脫嫌疑。過程中，騙徒能夠向受害人展示其相片、姓名及身份證等個人資料

3 操控網上理財戶口及轉走存款

騙徒會要求受害人下載應用程式或要求受害人到偽冒網站，並在程式或網站輸入網上銀行資料。受害人最終被轉走戶口內所有存款

陌生來電 即刻收線
同你講錢

ADCC
Anti-Deception Coordination Centre
反詐騙協調中心

ANTI-SCAM 防騙易
18222

ADCC

Anti-Deception Coordination Centre

反詐騙協調中心

防騙易諮詢熱線 18222

核實來電 提防電騙

如有懷疑:

請致電 18222

聯絡 反詐騙協調中心

如遇到緊急事故，請立即致電 999

香港特別行政區政府
香港警務處

www.police.gov.hk/adcc/

Beware of Telephone Deception by "Pretending Officials"

Don't disclose your online banking accounts and passwords

ANTI-SCAM 防騙易
18222

HELPFUL TIPS!

Latest Tricks

1. Request for online banking accounts and passwords

The swindlers would request the victims to provide online banking accounts and passwords

2. Request to access the fake website provided by the swindlers

The swindlers would provide a link to a fake website and request the victims to input their online banking accounts and passwords

3. Request to download suspicious mobile applications

The swindlers would request the victims to download mobile applications and ask them to input their online banking accounts and passwords

騙愛玩家呃到埋身

行騙伎倆

- 假肖像
- 假甜言蜜語
- 假投資應用程式

即掃QR Code
同我展開激情對話！

18222
www.adcc.gov.hk

ADCC
Anti-Deception Coordination Centre
反詐騙協調中心

「網戀投資騙案」三步曲

1 搭訕

騙徒扮成「高富帥」透過社交媒體或交友程式向受害人搭訕。繼而自稱是投資達人，並向受害人展示自己生活無憂的相片，以降低受害人的戒心。

2 網戀投資

騙徒開始對受害人甜言蜜語。當成功令受害人以為自己是網上情人後，便向受害人推介一些虛假的投資應用程式，並聲稱可提供內幕投資貼士，受害人於是下載程式，之後依從騙徒指示將投資金額存入騙徒提供的個人銀行戶口或虛擬貨幣錢包。

3 「贏粒糖輸間廠」

受害人依照騙徒的投資貼士在投資應用程式內投資。最初，騙徒會令受害人嚐到甜頭（獲利），使其放下戒心。受害人加大投資金額，但最後發覺根本不能取回投資金額和利潤。

懷疑受騙
即打18222
www.adcc.gov.hk

ADCC
Anti-Deception Coordination Centre
反詐騙協調中心

電騙之王 呃到埋身

行騙伎倆

- 假冒執法人員
- 製造恐慌「先嚇你，後幫你」
- 展示個人資料換取信任

而家你犯咗法！

即掃QR Code同你化解

18222

www.adcc.gov.hk

ADCC
Anti-Deception Coordination Centre
反詐騙協調中心

「假冒官員電話騙案」三步曲

1 預錄語音

騙徒以預錄語音致電市民，聲稱為速遞公司、銀行、政府部門或其他機構等，然後要求市民按鍵選擇收聽語音。

2 聲稱市民涉及刑事案件

市民被轉駁至假冒的內地執法人員，該騙徒聲稱市民在內地犯法，需要提供其網上銀行資料作快速審查，以協助其洗脫嫌疑。過程中，騙徒能夠向受害人展示其相片、姓名及身份證等個人資料。

3 操控網上理財戶口及轉走存款

騙徒會要求受害人下載應用程式或要求受害人到偽冒網站，並在程式或網站輸入網上銀行資料。受害人最終被轉走戶口內所有存款。

懷疑受騙

即打 18222

www.adcc.gov.hk

ADCC
Anti-Deception Coordination Centre
反詐騙協調中心

假工祭司 呃到埋身

大把筍工 俾你揀

即掃QR CODE

18222

www.adcc.gov.hk

ADCC
Anti-Deception Coordination Centre
反詐騙協調中心

「匯款員式求職騙案」三步曲

1 「高薪厚職」作招徠

騙徒在社交平台或網站刊登招聘廣告，聘請專人協助外國公司轉移資金到香港，並以「合法」、「搵快錢」、「彈性工作時間」和「高薪厚職」等字眼作招徠。

2 騙取受害人的資料借貸

受害人按招聘廣告的聯絡方法以社交媒體或即時通訊軟件聯絡騙徒。對話中，騙徒指示受害人傳送身份證、住址證明、銀行卡或月結單的副本。之後，騙徒用上述資料以受害人的名義向銀行或財務機構借貸。

3 誘騙受害人交出貸款

其後，貸款轉帳到受害人的銀行戶口，騙徒向受害人訛稱該筆款項是外國公司的資金，並要求受害人交出款項。騙徒取得款項後便逃之夭夭，而受害人則負上債務。

ADCC
Anti-Deception Coordination Centre
反詐騙協調中心

懷疑受騙 即打18222

www.adcc.gov.hk

釣魚特工 呃到埋身

你個銀行戶口有問題
即掃QR CODE檢查戶口設定

18222
www.adcc.gov.hk

ADCC
Anti-Deception Coordination Centre
反詐騙協調中心

「網絡釣魚騙案」三步曲

1 設置釣魚網站

黑客仿照政府部門、銀行、網上付款服務商、網上零售商等機構的網站，並製作一些外觀一樣的釣魚網站。無論如何相似，偽冒網站的域名和真正的網站必會有所不同，偽冒網站的功能很多時也不齊全。

2 向大眾發放釣魚訊息

黑客發放偽裝由上述機構發出的電郵或電話短訊(SMS)。這些假電郵及短訊的行文及格式都和官方的電郵及短訊非常相似，內容一般是指機構發現了和受害人相關的異常情況(例如是發現受害人的網上銀行戶口新增了一名登記收款人)，以引誘受害人按動附上的假連結作出修正。

3 受害人被引導至虛假網站

受害人按動假連結進入釣魚網站後被要求登入網站。受害人輸入其個人、信用卡或網上銀行戶口資料。騙徒掌握以上資料後，會直接從受害人的銀行戶口或信用卡竊取金錢。

懷疑受騙
即打 18222
www.adcc.gov.hk

ADCC
Anti-Deception Coordination Centre
反詐騙協調中心

虛App神棍 狂嗰億金

防騙易熱線
18222
www.adcc.gov.hk

ADCC
Anti-Deception Coordination Centre
反詐騙協調中心

「網上投資騙案」三步曲

1 利用社交媒體結識受害人

騙徒利用社交媒體接觸受害人，與其混熟後，表示自己是投資達人。

2 誘騙受害人進行假投資

騙徒向受害人推介虛假的投資應用程式供其下載，並聲稱掌握程式的買賣規律。受害人下載該程式後，騙徒便教受害人聯絡程式的客戶服務員，以安排開戶。受害人之後按指示將款項或加密貨幣存入指定的個人銀行賬戶或電子錢包，並在程式進行買賣。

3 受害人獲得甜頭後加注 最後血本無歸

起初，騙徒讓受害人獲利，將利潤存入受害人的銀行賬戶，以獲取信任。受害人加大投資，但其後向客服申請取回本金及利潤時，卻被不同藉口拖延，或被要求存入更多錢方能取回款項。受害人最後血本無歸。

懷疑受騙
即打 18222
www.adcc.gov.hk

ADCC
Anti-Deception Coordination Centre
反詐騙協調中心

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

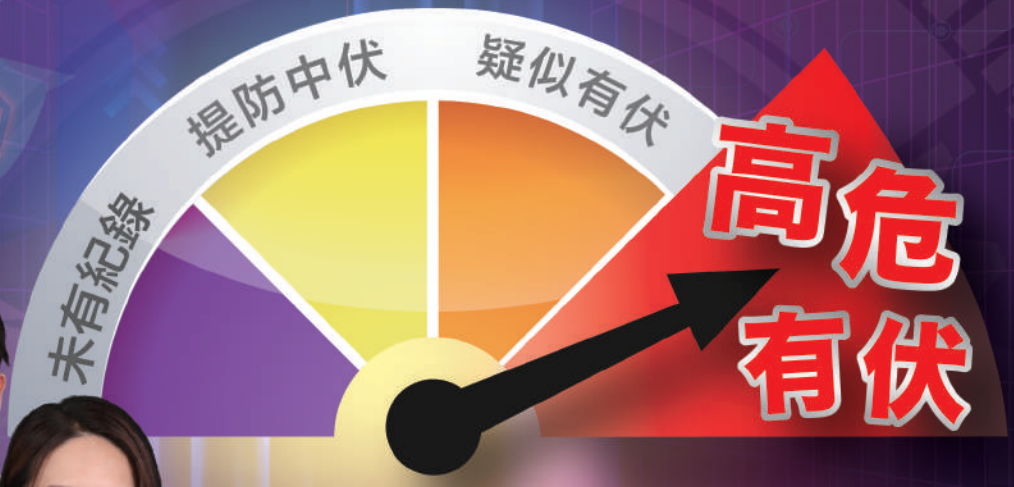
HONG KONG MONETARY AUTHORITY
香港金融管理局

陌生來電　可疑網店　筍工招聘　白撞訊息　必賺投資

係咪呃緊你？Check 吓

防騙視伏器

即上 CyberDefender.hk



輸入資料，揭穿**詐騙**陷阱！

一站式詐騙陷阱搜尋器

電話號碼
平台用戶名稱
社交帳號
網址
收款賬號
電郵地址
IP 地址

網頁　Facebook　Instagram　YouTube

CYBER DEFENDER 守網者


懷疑受騙　即打18222
寂寞
網戀
恐懼
來電靠嚇
貪心
瘋投快搵機
無知
刷單圈套
騙局誘惑
捉心理騙局
誘惑到你萬劫不復！
ADCC
Anti-Deception Coordination Centre
反詐騙協調中心