HongLeong Bank

DUITSMART

A Better Future for all Malaysians

COMMON SCAMS

Most of us have come across financial scam cases in the news or on social media.

But how much do you really know?

Here's a mini guide
on the latest tactics, to help you prepare and protect yourself.

The Macau Scam

Spot the signs

- You receive a call from someone claiming to be an officer of the bank / police / other authority.
- The caller has "evidence" that you committed a crime e.g. money laundering, drug trafficking, hit-and-run.
- You are asked to keep the investigation secret, not to inform the bank or others including your family.
- You are instructed to deposit your money with authorities for investigation of illegal transactions, with assurance that all funds will be returned when your case is cleared.
- There are threats to freeze your accounts, or arrest and court action if you do not cooperate.

The TAC Scam

Spot the signs

- You receive a call from someone who claims their TAC SMS was wrongly sent to you.
- The caller may sound very polite or apologetic, asking you to give them the code received in order to complete an urgent transaction.
- As excuses, the caller may claim to have recently switched mobile numbers, or that their family mistakenly used the wrong number.
- The caller promises to correct the error after the transaction is done.

Note:
TAC is the 6-digit Transaction Authorisation Code required to confirm and complete your online transactions.

The Phishing Scam

Spot the signs

- You receive an SMS / email that claims to be from your bank / other authorities.
- Message directs you to click a link that opens a fake website.
- You are asked to update your personal information or banking / online login details.
- Threats to close or suspend your accounts if you do not respond as instructed.

REMEMBER

- The bank will never request personal / banking information or confirmation of details via SMS, messaging app, email or social media.

REMEMBER

- If you receive this kind of call, hang up immediately and do not transfer the money requested.
- If you are told your bank account is linked to a crime, go to the bank directly for confirmation.
- Stay alert even if the caller's phone number appears correct, or you are promised "receipts" for your transactions.

REMEMBER

- TAC is always sent to the mobile number registered with the bank and tied to your account, so it cannot be "wrongly" sent. Never share your TAC with anyone else.

- Be careful when you click on links received from unsolicited SMS / email.
- Always type the online banking web address (www.hongleongconnect.my) into your browser to enter the bank's official platform, and only enter your password / log in if you see the Security Picture you selected during registration.

Good Security Habits

for Everyone

Never share your online banking login details (i.e. username & password) or TAC with anyone,

even if the party requesting such information claims to be from a bank, Bank Negara Malaysia or other authorities.

Create a strong online banking password that uses a combination of alphabets, numbers and symbols, and change it regularly.

Check your transaction alerts promptly, and monitor account balances and statements on a regular basis.

If you detect unauthorised transactions or discrepancies, report it to your bank immediately.

For more ways to DuitSmart and get in better financial shape,
go to www.hlb.com.my/duitsmart