WATCH OUT FOR THESE SCAMS

Phishing scam
In a phishing scam, a target comes across an advertisement – put up by what he/she thinks is a legitimate entity, like a government organisation or bank – on websites or social media platforms like Carousell, Facebook or TikTok. These ads often display offers that are too good to be true. Enticed, the target gets in touch with the scammer using the contact details provided in the ad. The scammer will then send the target a link (usually via messaging platforms like WhatsApp, Telegram or SMS) and request that the target enters his/her banking credentials at that website.

The site is actually a spoofed one that is designed to appear legitimate; in fact, the scammer uses it to steal the target's information. The target only realises that he/she has been scammed when unauthorised transactions are made using his/her bank accounts.

Fake friend scam
Got a call from an unknown number – and had the other party ask you to guess who he/she is? This is how 'fake friend' scammers lure targets into their traps. Once the target suggests a name, the scammer will assume that identity and ask the target to replace his/her number in the target's contact list. At other times, such scammers may pretend to be a long-lost friend and ask for urgent financial assistance.

WAYS TO PROTECT YOURSELF

Scammers prey on their targets' emotions. They may try to intimidate, create false urgency or

make you feel like you are missing out. Be vigilant and adopt protective measures.

Got an unsolicited direct message – or one where the sender claims to know you – via social media?	Always **verify the identity** of the sender. If the sender is purportedly an organisation, call their hotline number to check. If in doubt, get a second opinion from a trusted friend or family member.
Came across an online deal that seems too good to be true?	Always **check the credibility** of online sellers by reading reviews of their services. Make purchases only from reputable merchants.
Received a link from a seller through a social messaging platform, and asked to access it to share sensitive information or make payment?	**Do not key in your banking credentials** into – or make payment through – unverified webpages. These include webpages that you access through links sent to you via social messaging platforms (e.g. WhatsApp, Telegram).
Prompted to authorise a suspicious payment or received a transaction notification for a purchase you did not make?	● **Never authorise a transaction** (including login requests) unless you know its purpose. ● To receive timely notifications, ensure your contact details in our records are up to date. Always read the notifications we send you carefully. Notify us immediately if you see a transaction you did not make. ● Consider **setting a lower daily transaction limit** – this stops large sums of money from leaving your account(s) without your authorisation.