SAFEGUARD YOURSELF AGAINST ONLINE SCAMS

In conjunction with Polis Diraja Malaysia's campaign against online scams, here are some online security tips to safeguard yourself.

What is Phishing?

Phishing is a type of online scam where fraudsters pose as legitimate organisations to solicit user data such as personal details, login credentials and credit card numbers. The fraudsters may also deploy malicious software on the victim's device through suspicious links shared via email or SMS. The fraudsters can use the data collected to commit identity theft, unauthorised purchases or stealing of funds.

What you should do?

- Never disclose your banking details such as your username and password, or your OTP to anyone via unsolicited calls, emails or third-party websites that are not owned by Citi.
- Never click on suspicious links as it may lead you to a phishing website to trick you into divulging sensitive personal details or banking credentials.
- Contact Citi immediately if you may have provided your details to the scammer, or if you know that your username and password have been compromised.
- Always enter Citibank's web address "www.citibank.com.my" or "www.citigold.com.my" directly into your browser's address bar before you log in to ensure that you are on the legitimate Citibank website.
- Learn more online security tips at www.citibank.com.my/security
- If you suspect you've been sent a fraudulent email, contact our CitiPhone at 03-2383 0000 immediately or alternatively you can login to Citibank Online and chat with our 24/7 e-chat agent or forward the entire phishing email as an attachment to spoof@citicorp.com