Types of Fraud

Phishing Scams

Phishing occurs when fraudsters pose as trusted organizations and send out thousands of fraudulent emails to random email addresses.

These emails usually contain a link to a look-alike website to mislead customers into entering sensitive financial information such as their account number and PIN. This will enable the fraudsters to capture the customer's account information to access the customer's bank accounts.

- If you suspect you've been sent a fraudulent email, ignore the email and contact us at + **03-8318 3100** immediately.
- Do not input any sensitive information that might help provide access to your accounts, even if the website appears legitimate.
- FINEXUS Cards will **NEVER** send emails to customers to verify confidential, personal or account information.

Pretext Calling

Pretext calling is defined as a deceptive means of obtaining personal information and unauthorised disclosure of customer financial information. Fraudsters may pretend as bank officers to obtain your account number or card number and other information required. Upon obtaining such information, the fraudsters may call us posing as you, using the information stolen to take over your identity in order to perform transactions using your card account.

Another form of pretext calling is when fraudsters request victims to confirm transactions that were purportedly made on victims' cards. When victims inform fraudsters that they do not have such cards, the victims are provided with a fake Bank Negara Malaysia telephone number in order to lodge a report. Upon calling, the fraudsters will request for victims' personal information which will subsequently be used for fraudulent activities.

Be aware that Bank Negara Malaysia will never request for your personal or financial information through SMS or telephone calls and will never ask anyone to transfer money to any third party account.

- Monitor and pay attention to your regular card account to ensure your transactions are accurate.
- Do not share personal information, such as account numbers, passwords, National Registration Identity Card (NRIC) number and other personal information over the telephone, email, SMS or internet, unless you know who you are dealing with.
- Store your personal information in a safe place and shred your old card receipts, ATM receipts, old account statements, and any other correspondences prior to disposing them.

Pharming

Pharming is a scamming practice in which a malicious code is installed on a personal computer or server, misdirecting users to fraudulent websites without their knowledge or consent.

Pharming can be conducted either by changing the host file on a victim's computer by exploitation of a vulnerability in DNS server software.

- If you access websites which requires your personal information, ensure the website address has https:// in its URL.

Keylogging

This is a form of online fraud where the keys inputted on a keyboard are captured, typically in a covert manner so that the person using the keyboard is unaware that their actions are being monitored.

- Install anti-spyware applications which are able to detect and disable/cleanse keylogging softwares.

- Keylogging on **ATM** has been known as overlaying a keyboard ATMs pinpad to capture people's PINs. The device is designed to look like an integrated part of the ATM so that bank customers are unaware of its presence.

- If you notice any "unauthorized" devices or objects fixed to the ATM, do not use the ATM machine If you notice anything strange at the ATM, leave immediately. If you have already started a transaction, cancel it and leave immediately.

- **Interactive Voice Response (IVR)** keylogging on mobile phone has been known in the market for a number of years. The main purpose of such spyware is to capture and transmit information including email, sms and keystrokes on the cell phone without the user of the phone being aware of it.

Think before downloading applications. Review the privacy policy and understand what data (location, access to your social networks) an application can access on your device before you download it.

If you did not expect any message or connection attempt to your mobile device, take precaution by declining the connection as this may be an attempt to send a malicious program to your mobile device. Always decline such attempts in connection when in doubt.

SMS Spoofing

SMS spoofing uses the short message service (SMS) to set who the message appears to come from by replacing the originating mobile number (sender ID) with alphanumeric text. Spoofing has both legitimate uses (setting the company name from which the message is being sent, setting your own mobile number, or a product name) and illegitimate uses (such as impersonating another person, company or product).

Telephone Tapping

Telephone tapping is the unauthorized monitoring of telephone and Internet conversations and/or key tone by a third party. Phone Tapping is possible on a public switched telephone network and can be difficult to detect. To minimize the risk, consider disabling your mobile phone's Bluetooth connection to prevent any unauthorized access to signal sent from and to your phone.