FINEXUS®

SECURITY ALERT

INTRODUCTION

Finexus Cards Sdn Bhd ("FINEXUS") is committed to ensuring that all transactions performed online is secure, safe and confidential. We have made it a point to reinforce our systems with safeguards to preserve a secure environment for you to carry out your transactions and now wish to provide you with safety precautions that are practical, effective and in certain instances obligatory for online and overseas usage of your card.

PROTECT YOURSELF

In addition to our security measures you also play an important role in safeguarding your transactions made through your computer and mobile devices. We recommend that you do the things as listed below:

1. Install anti-virus and anti-malware

   Protect your devices from virus and malware by installing anti-virus and anti-malware software. To maximise your protection, update them regularly to make sure you always have the latest virus definition.

2. Avoid rooting or jailbreaking your mobile devices

   You will be disallowed to use a rooted or jailbroken device as they are more vulnerable to fraudulent attacks. A rooted or jailbroken device has minimal security, making it easier for a fraudster to gain access to your personal details and other information stored or transmitted through your device.

3. Install anti-spyware software

   Spyware is a general term for hidden programs on your computer/mobile devices that track what you are doing on your computer/mobile devices. Spyware is often bundled together with file sharing, email virus checking or browser accelerator programs, and is installed on your computer/mobile devices without your knowledge to intercept information about you and your computer/mobile devices. The type of information gathered can include personal Internet usage, and in some instances, confidential data such as passwords. You can download and run a specialist program designed to help identify and remove threats from spyware. Like an anti-virus program, it also needs to be regularly updated in order to recognise the latest threats.

4. Keep your browser and operating system up-to-date

   From time to time security weaknesses or bugs are found in browsers and operating systems. Usually 'Service Packs' are issued by the software company to make sure these are fixed as quickly as possible.

You should make regular checks on your software vendor's website and apply any new security patches as soon as possible to ensure you have the most updated security features available.

5. Avoid running programs or opening email attachments from any source you do not know or trust

You should not install software or download any files from websites (e.g. programmes, games, and screensavers) that you aren't completely sure about. We also recommend that you scan all email attachments for viruses and avoid opening any from people or organisations that you do not know or trust. However, some viruses may forward infected emails to everyone in an address book, therefore you can also get an infected attachment from someone you know. If you are not sure what is in the attachment, do not open it.

6. Be cautious when using public or shared computers/networks

If you access your accounts using a computer in a cyber café, a library or your workplace, try to ensure the computer has the latest antivirus, firewall, antispyware and browser software installed. Although Wi-Fi is a convenient way for you to access the Internet, it is not advisable to access your account via Wi-Fi connection especially in public places like airports, hotels or shopping malls.

7. Be proactive

You should regularly be kept informed of your accounts by checking all transaction alerts in a timely manner and to check account balances on a regular basis to detect any unauthorised transaction, error or discrepancy and to report the same to FINEXUS in the event any unauthorised transaction, error or discrepancy is detected.

TYPES OF THREAT

Protect yourself from becoming a victim of online fraud. Listed here are the four major types of threat:

1. Computer Viruses

Computer viruses are malicious software which are also known as malware that infect computer devices and perform harmful activities. It can be viruses, Trojans and spyware to “PC Optimization” programs that harm your devices, interfering with the system's operations, corrupting data, logging user's keystrokes and stealing private information.

2. Phishing Scam

“Phishing” is a type of identity theft where criminals blast emails to mass audience purportedly from FINEXUS in their malicious attempt to bait user into fake websites. It usually comes with a link that the user can click on which will direct the unsuspecting victim to a fake website and the user will be asked to disclose confidential or financial information, passwords, and credit card numbers along with highly confidential information. More often than not, the emails may imply a sense of urgency or serious

consequences should the user did not respond to it. For example, it could be worded in such a manner that if no action is taken, the account will be suspended.

3. Phone Scam

This comes in the form of the phony disguises as a FINEXUS staff, any Card Brands like Visa & Mastercard, Bank Negara Malaysia or someone you can trust who calls you. The victim is usually informed of some irregularities with the account in question and action needed to be taken immediately. Usually the user will be "alerted" of "missing money" or that the user's account has been compromised by possible scams by the phony. To rectify user's losses or to prevent the "scams", the phony will instruct the user to perform an online transaction to a third-party account.

4. SMS Scam

These are fraudulent SMS sent to user victims informing them that they have won a cash prize or requiring them to call a given number to confirm on a transaction involving the user's credit card or account information. To claim the prize, the victim is told to transfer a certain amount of money to a third-party account or open an internet banking account at the ATM. The victim is tricked into divulging the registered User ID and Password to the fraudster. Having done as instructed, the victim has unknowingly given the fraudster access to their banking account.

What should you do?

- Do not click on adware or suspicious URL sent through SMS/Messaging services.
- Do not use public Wi-Fi networks that are suspicious for online transactions.
- Do not save your login details on a public computer.
- Do not respond to suspicious emails or SMS content from suspicious links or unsolicited senders seeking personal or confidential information.
- Do not respond to a request seeking for you to validate or verify your personal and confidential information.
- Do not respond to any SMS or call from an unknown person asking details of any transaction.
- Do not respond to any call from a person claiming to be from Bank Negara Malaysia. Their officers will never call to ask you about an online transaction.
- Clear your cache (information stored in your computer or mobile application memory) each time you log out.
- Change your password frequently. If you think your password has been compromised, contact us to reset your password.
- Avoid downloading free programs. These may incorporate hacker-friendly software.
- Install anti-virus or anti-malware software.
- Refrain from rooting or jailbreaking your mobile devices as this could compromise its security features.

Take note that on principle, we would NEVER ask you to validate personal or confidential information via e-mail. If for some reason you have entered sensitive information after clicking on a link or if you suspect that you've been a victim of fraud, please contact FINEXUS immediately.

CARD FRAUD PREVENTION TIPS

1. Receiving Card
   - ALWAYS check that the card received is under your name and the sealed package is not compromised. Immediately contact FINEXUS if the card is not yours or if the seal has been tampered with.
   - SIGN on the signature panel at the back of your card immediately, using non-erasable ballpoint pen.
   - REMEMBER to thoroughly destroy your expired / unusable card by cutting it in half across the magnetic stripe and/or chip.

2. Managing Card
   - KEEP your card in a secured place and ensure that it is in your possession at all times.
   - DO NOT leave your card unattended even in the privacy of your home / office.
   - TRY not to leave your card in your vehicle when you are at public places to avoid theft or it being switched with another invalid card. However, if this is unavoidable, once returned to your vehicle;
     - Check for any sign of vehicle being broken into and/or;
     - Ensure the card is not missing and/or
     - Ensure the card is yours and does not belong to someone else.
   - TRY to carry your card separately from your wallet / purse.
   - DO NOT carry cards that are not needed.
   - NEVER lend your card or allow others to use your card. (CARDS ARE NOT TRANSFERABLE!)
   - KEEP a record of your card numbers, expiration dates and the contact number / address of each bank in a secure place.

3. Managing PIN & Personal Details
   - DO memorize your PIN and destroy the slip immediately.
   - Immediately go to the ATM and change your PIN, while ensuring no one is observing.
   - DO NOT create PIN that is sequential, repetitive and obvious (such as date of birth, identity card number, etc.)
   - DO NOT write your PIN on your card, anywhere near it or unsecured places.
   - NEVER disclose your PIN (or username, password, security questions/answers, etc) to others.
   - AVOID using the same PIN for every card.
   - CHANGE your PIN periodically for precaution.

4. Retail Usage
   - ENSURE your card is always within your sight while making a transaction.
   - CHECK all purchase details on sales receipt before signing it. Draw a line through blank space above the total or circle the purchase amount.
   - DO NOT sign a blank receipt.
   - ALWAYS mark void on an incorrect receipt and destroy it before you sign a new one and ENSURE the merchant also voids that specific transaction through the card machine as well.
   - ENSURE that it is your card and not someone else's that is returned to you immediately after the purchase transaction.
   - ALWAYS keep your receipt for future reference.

5. Online Usage
   - NEVER provide your card details on website that is unsecured or unreliable.
   - NEVER provide your card details online unless you are making a purchase.
   - AVOID using public computers to make online purchase. If you do, please remember to log off and quit browser after you have finished.
   - AVOID using the same username and password for everything.
   - ALWAYS print or save the confirmation page and receipt of your purchase.
   - PROTECT your card CVV (Card Verification Value) / CVC (Card Verification Code). CVV/CVC is a three-digit security code that is placed on the back of your card. Most online, phone, or mail-order purchases requires you to give this code before the transaction goes through, so make sure to keep it confidential.
   - Ensure you provide us with the latest mobile number so that we can deliver One-Time Password (OTP) to you so that we can make your online payment securely.

6. Managing Statements & Related Documents
   - CHECK your card statement promptly and report immediately on any transactions that you do not recognize or did not authorize.
   - SHRED any document with your card number and details stated on them before discarding.
   - KEEP FINEXUS updated with your latest contact number and/or email address to allow FINEXUS to perform verification of unusual or suspicious transactions. Notify FINEXUS on your change of mailing address too.

7. Scams
   - NEVER respond to email, website or phone inquiry is that request you to provide your card details or ask you to go to a website to verify card or personal details. These are called “Phishing” scams.
   - DO NOT provide your card details over the phone unless you have validated the company or individual you are speaking with.

CUSTOMER OBLIGATIONS FOR ONLINE AND OVERSEAS CARD USAGE TO PREVENT UNAUTHORISED TRANSACTIONS

We shall at all times and to the best of our ability, endeavour to ensure that all online and overseas card usage and transactions which are made on the mobile application or website of FINEXUS are secure. We employ in our authentication process the use of individual security devices and distinct pass codes including but not limited to usernames, PINs and passwords. These will act as a key to access your relevant account.

To ensure the integrity of these pass codes and security devices, you are under an obligation to maintain its confidentiality by not sharing it or making it accessible to any other person and to take all reasonable endeavours to maintain its security which may include, memorising the usernames, PINs and passwords, changing your password regularly and signing of before visiting any other Internet sites.

In the event of a security breach of any pass codes, loss of your security device, loss of your card, the occurrence of any unauthorized transactions that you have become aware of or ay unauthorised transactions having transpired as a result of a lost, stolen or misused security device or pass code, you are under a mandatory obligation to report any of the incidences aforementioned to FINEXUS as soon as reasonably practicable.

When performing online transaction(s) you should ensure the trustworthiness of the respective website before you input your card details on to the respective website and for overseas transaction(s) before your card is swiped at the debit card terminal of any vendor, you are to ensure that no external devices are attached to the terminal in order to prevent your card from being cloned by theft of your magnetic strip that contains your card information.

In the event you fail to carry out the mandatory obligation to report to FINEXUS as soon as reasonably practicable, FINEXUS will block and prevent any further transactions being carried out on your card. In which case you shall be liable for the amount in monetary value transacted for such unauthorised transaction deemed as a fraudulent or a disputed transaction. Notwithstanding this proviso, FINEXUS shall have the sole discretion to determine your liability in the event of the occurrence of an unauthorised transaction for online and overseas card usage.