Tips

Log-On Safely

- Always enter website address "www.finexuscards.com" directly into your browser address bar before you login to ensure that you are on the legitimate website.
- DO NOT disclose your user name or your password to anybody or on any third party websites. Ensure the chosen image is of your choice prior to completing your log-in process.
- Check that the website address changes from http:// to https:// once you are on the login page. Also, look out for a security icon that looks like a lock or key, which normally appears at the bottom of the webpage or next to the URL bar (depending on the browser used), when authentication and encryption is expected.
- Always click 'log out' when you have finished your session. Do not close your browser window or leave your browser / computer unattended without logging out.
- Update your new contact details immediately with us. This will enable us to contact you in a timely manner if we detect unusual transactions.
- Do not proceed if you encounter a request for information not normally requested for and/or if the online experience differs from previously. Contact us immediately if you encounter such incidences.
- If you are the target of SMS, email or phone call flooding, be cautious and check for any fraudulent activity in your card account.

How to Protect Your Username and Password and other Authentication Credentials

- Your log-in password should be at least 8 alphanumeric characters and case sensitive. The password or PIN that you selected should not be based on the username, personal telephone number, birthday or other personal information.
- You should memorise your ATM/Telephone PIN (T-PIN), online username and password and not record it anywhere, including in your mobile.
- You should not deliberately disclose your username and password to anyone via unsolicited emails or any other channels. We will never request for your online username or your password..
- Ensure that no one is watching you while you key in your username, password, ATM PIN, T-PIN or any other sensitive information.
- You should NOT reveal your ATM/T-PIN, username, password or other authentication credentials such as One-Time PIN (OTP) to anyone regardless who they claim to be attached to.

Protecting Your Computer

- Do not select the option to auto save on browsers for storing or retaining username and password. Make sure your computer's operating system and browser software is updated with the latest security patches.
- Configure a personal firewall and install the latest anti-virus software to help prevent unauthorized access to your home computer, particularly when they are linked via

broadband connections, digital subscriber lines or cable modems. Be sure to update the anti-virus and firewall products with the latest security patches on a regular basis.

- Clear your browser's cache and history after each session so that your account information is removed, especially if you are using a shared computer.
- If you are using a Windows operating system, ensure File & Print sharing is disabled while online, particularly if you are linked to the internet via any broadband connection, digital subscriber lines or cable modems.
- Make regular backups of critical data.
- Consider the use of encryption technology to protect highly sensitive data.
- Do not open any suspicious or unsolicited emails; delete them.
- Do not click on any links or open any attached files found in spam emails/SMS.
- Do not give your personal and financial information over the telephone to unverified callers.
- Never enter your internet account details on a website that you are not sure is genuine.

Wireless Networks

- You should set a strong password and encryption for your wireless point. This will prevent unauthorised users from accessing and using your wireless connection.
- Disable broadcasting of your network name (SSID-Service Set Identifier) to prevent casual surfers from detecting and connecting to your wireless network.
- You should use encryption on data transmission to protect your wireless network.
- You should allow only registered machines for your wireless network.

Beware Of Scam Emails

- Fraudulent (a.k.a. spoofing, impostor, or phishing) e-mails appear to be sent from a legitimate source. However, these fraudulent emails attempt to trick you into providing sensitive personal information either on the spot (e.g. by replying to the e-mail) or by including links to a fake website that will attempt to get you to disclose personal data or login credentials. Do not disclose personal, financial or credit card information to little known or suspect websites. We or regulators will never send emails, Facebook messages, or tweets asking for identity confirmation or security details. In case of any uncertainty, contact us immediately via + **03- 8318 3100**.
- Do not open email attachments from strangers or install software or run programs of an unknown origin.
- We only send out ‘NOTICE’ emails or emails requesting you to contact due to whatever so ever reasons.

Beware Of Spyware

- Spyware is a piece of software installed in your computer that collects information about you and your internet traffic. It is stored in your PC (with/without your consent) when you download certain software, games, screensavers, etc from the web. It usually claims to be able to improve your computer's performance.
- Spyware can be used maliciously to gain access to your passwords, usernames, card numbers and internet browsing history. They can also be used to scan files on your hard

drive and slow down your computer by consuming system resources leading to system instability or a crash.

Beware Of Embedded Link

- Cyber criminals may use embedded links to trick you into clicking on them to upload malware to your computer or network, and to collect your personal or confidential information. Instead of clicking an embedded link, copy and paste the URL directly into your web-browser.