CREDIT SUISSE

Credit Suisse
Private Banking Asia Pacific
In-App Security Tips
June 2016

General Information

Credit Suisse employs various security practices and measures in order to protect the confidential information of its clients, including ensuring that the apps' data remain encrypted and intact throughout your authenticated session. In the event of interference or connection disruption, your connection is terminated and any non-submitted/incomplete order instructions will be abandoned.

Further to the efforts undertaken by Credit Suisse, end users play an essential role in safeguarding against risks such as those related to virus attacks, unauthorized access and fraudulent online transactions. The following security tips are in addition to the important obligations owed to Credit Suisse (e.g. for log in credentials to be kept confidential, secure and personal to each user at all times, and for the risk of their having been compromised to be reported to Credit Suisse); please refer to the terms of the legal agreements governing the use of the apps.

We strongly recommend that you review in detail and adhere to the following recommended security practices:

Configure mobile electronic devices/personal computers securely

- Enable Auto-Lock and Passcode/Touch ID protection on Apple mobile electronic devices.
- Enable remote wipe.
- Do not make modifications to your mobile electronic device not authorized by the operating system's issuer and the device's manufacturer (often called "jailbreaking").
- Avoid auto-complete features which remember user names or passwords.
- Disable any wireless network functions (e.g. Bluetooth, Wi-Fi and NFC) when you are not using them.
- Update your mobile electronic device or personal computer's operating system promptly by selecting the automatic update option for this purpose.
- Install anti-virus, anti-spyware and firewall software from a reputable provider and promptly update these with security patches or newer versions on an ongoing basis.
- Connect only to secure/encrypted networks (i.e. avoid public Wi-Fi to access the apps) and remove any unnecessary Wi-Fi connection settings.
- Back up any critical data you may hold upon your mobile electronic device or personal computer. Consider the use of encryption technology to protect any highly sensitive data being maintained.
- Remove file and printer sharing features in personal computers and mobile electronic devices, particularly when connected to the internet.

Install/use the apps only from trusted sources

- Use only official apps from Credit Suisse for banking with us.
- Download apps only from official app store (i.e. Apple App Store).
- Always either type in the website address for the app within the web browser or bookmark the genuine website for subsequent access.
- Check the authenticity of the website by comparing the website address (URL) and Credit Suisse's name in its digital certificate (available to view by clicking on the padlock or key icon shown in the web browser) before entering your log-in credentials.
- Beware of any unusual login screens or process (e.g. a suspicious pop-up window or request to provide additional personal information).

Phishing Attempts

- Avoid replying to emails which may lure you to websites that look very similar to those of Credit Suisse and avoid tapping/clicking on suspicious links, attachments or embedded images within such emails. By requesting your log-in credentials, unauthorized persons may be able to access your login data in your guise.
- Credit Suisse will not ask for any sensitive personal information (including passwords) via phone/email or send you emails with embedded hyperlinks to the apps.

Additionally, when accessing the apps via the internet

- Only use the recommended web browsers to ensure your online session is protected by more up-to-date security features.
- Always clear and permanently delete your browser cache and history when you finish your online session so that your account information is removed.

Password Management

- Ensure that any passwords are strong and difficult to guess. We advise that passwords should contain at least 8 characters, combining uppercase letters, lowercase letters, numbers and symbols, whilst avoiding common words, names or repeated, or sequences of, characters.
- Always change your password on a regular basis.
- Keep your device and app passcodes, user names, passwords, security device(s), personal details and other confidential data confidential, secure, and personal to yourself at all times (i.e. never store on computers, mobile phones or keep in plain sight), and immediately report to Credit Suisse the risk of their having been compromised.
- Be aware when using “Remember your password” browser programs as these have varying degrees of security protecting your password information, and anyone with access to the computer may be able to retrieve all saved passwords and information.
- Never click “yes” to “Remember your password” options on public computers.

Exercise caution in public

- Never leave your mobile electronic device or personal computer unattended when logged in to the app.
- Immediately report the loss or theft of your mobile electronic device or personal computer to the police and also to your telecommunications provider for the mobile electronic device.
- Be aware of the people around you to avoid anyone overseeing you (”shoulder surfing”) when entering your passcodes, passwords or using the app; i.e. do not disclose confidential information in public.

Furthermore

- Do not use a public or shared personal computer or mobile electronic device when accessing the apps or to perform any transactions.
- Always verify the date and time of your last login session. The date and time of your last login is displayed at the top of the screen shown after successfully logging in to the app.
- Always log out of the app when you are no longer using it.
- Promptly check the notifications (i.e. SMS messages and other notifications) and account statements provided to you by Credit Suisse for any unauthorized transactions, and if any, report them immediately to Credit Suisse.
- Do not download or open attachments/files or click on hyperlinks or browse suspicious websites within emails, instant messages, SMS messages or codes from strangers or from known contacts which are nevertheless suspicious.
- Delete any junk or chain emails that you receive.
- Do not disclose personal, financial or account information/details to little-known or suspect websites or e-mail addresses or otherwise.

Information

Please contact your Relationship Manager or our Customer Care Center without delay should you:

- Notice any unusual or suspicious transactions on your account or observations (e.g. suspicious pop-up screens or abnormal login steps).
- Suspect that any of your log in credentials have been compromised.

Our Customer Care Center can be contacted as follows:

Phone: +65 6212 6000 (Singapore) or +852 3407 8188 (Hong Kong)
Email: apac.app@credit-suisse.com