Internet and Mobile Banking Security Tips and Precautions

Table of Contents

1. YOUR ROLES AND RESPONSIBILITIES

While we strive to do our utmost to protect your online transactions, as an end-user, you too have a role to play in ensuring the security of your account. Please use the following checklist to assist us in protecting you.

- Ensure all your personal computers (PCs), mobile devices, operating systems and Internet browsers which are used for online banking are regularly updated with the latest software.
- Notify us immediately if you notice any doubtful log-ins on your log-in history.
- Protect your PIN, User ID by keeping them confidential at all times. Keep your Token in a secured place.
- Always log off when you are done with the online session and do not keep it unattended.
- Report the loss of your Token to us immediately.
- Update us of any change of your particulars (i.e. Mobile Number and Contact Details).
- Install Anti-Virus Software on your Computer and Mobile Device.
- Do not disclose your sensitive information to suspicious websites

- Ensure that you are banking with us on our official website. A click on the padlock icon in your web browser should show you the certificate issued by the website's owner.
- Download our Mobile Banking application from trusted sources such as the App Store and GooglePlay. This will significantly reduce the risk of downloading mobile Trojan programmes.
- Do not modify, 'hack' or 'jailbreak' your mobile device as it will become more vulnerable to virus and malicious software attacks.
- Report the loss of your mobile device to your service provider as soon as possible.

2. COMPLAINTS AND DISPUTES HANDLING PROCEDURES

We aim to serve you better. We welcome and cherish your feedback.

If you wish to lodge a complaint, please email us at customer_complaint@sg.icbc.com.cn or call us at 6369 5588.

Upon receipt of your complaint through e-mail or by mail, we will send you an acknowledgement e-mail within 2 business days.

Thereafter, we will investigate your complaint with the relevant department and officers-in-charge. An official explanation will be issued to you within 20 business days after receipt of complaint.

The following questions, if answered, would aid us greatly in resolving your complaint in an expeditious manner:

(a) Are you an existing customer of the Bank?
(b) Are you an individual or corporate customer?
(c) Name of Complainant (& Corporate Name if applicable)
(d) Account Number! NRIC! Passport No.! Employment Pass
(e) Contact details for communication (Telephone No.! Mobile No.! Email Address)
(f) Details pertaining to complaint or query.

3. TIPS TO PROTECT YOURSELF

A. ON THE INTERNET

- Set your anti-virus, anti-spyware and operating system to perform automatic updates daily.
- Secure your Internet connection and computer with a personal firewall.
- Lock down your wireless network at least with a WPA level protection, and WPA-2 whenever possible
- Avoid using the same password for all of your web based accounts (i.e. e-mails, shopping websites and/or social media).
- Use a strong password. It should not contain information related to you as such information may have been published elsewhere by you on the internet, and gathered by potential attackers.
- Memorise your passwords and PIN. Do not record them anywhere, or store or retain them in your Internet browser.
- Change your passwords and PIN regularly, or when there is any suspicion that it has been compromised.
- Do not click on links from e-mails or download any attachments therein if it is from an unknown sender or sources.
- You should not perform online transactions on PCs which are accessible to the public or compromised.
- Regularly backup all critical data and encrypt these data with (at least) 128-bit encryption.
- Restrict access to your social networking profile and keep your personal information private.
- Disable printer and file sharing when your PC is connected to the Internet.
- Always make sure that the online merchant you are dealing with is reliable. They are typically certified with trust labels (e.g. TrustSG, Truste or VeriSign).
- Check if the website you are surfing has SSL protection before you transmit any sensitive data to them. This is usually shown if the website begins with a https://.
- Do not send your credit card information over the e-mail even when you are contacted by a reliable merchant.

B. ON YOUR COMPUTERS AND MOBILE DEVICES

- Lock your PC screen when you step away from it, or configure a password-protected screensaver to be activated after a preset period of inactivity.

- Mitigate your losses when you lose your Mobile Device. Ensure that it has a pass code and its "Erase Data" function is on. This function will erase all data after several invalid password attempts so that your sensitive data will not be compromised if and when it is lost or stolen.
- Report your lost or stolen Mobile Device to your service provider as soon as possible so they can terminate your service immediately.
- Beware of "Free Games" or "Free Apps" as they may be mobile Trojan programmes. Ensure that such apps are scanned for viruses or published from a reliable source before you download them.

C. AT THE ATM

- Do not write down your PIN number and store it along with your ATM, debit or credit cards.
- Never disclose your PIN to anyone.
- Observe the ATM and see if there are any suspicious devices. If the ATM seems to be abnormal, stop your transaction and use another ATM.
- Don't leave your ATM card unattended. Take care of it as you would for your wallet and cash.
- When entering your PIN at the ATM, use your free hand, wallet or purse to shield your keying hand. You should check the mirror to ensure that there is no one looking over your shoulder.

D. AGAINST FRAUD

- Always shred unwanted receipts, bank statements, application forms and other official letters before they go to the trash. Fraudsters may attempt to use information contained on those documents to assume your identity.
- If you ever need to provide your sensitive information to an employee of the Bank, make sure that you are the one initiating the call. You should also check that you are calling our official hotline shown on our website.
- Avoid providing sensitive information to strangers over the phone or e-mail.
- Check your credit card bills and bank statements every month (and especially after an overseas trip) to see if there are any suspicious charges. Notify your bank immediately if you notice any discrepancies.