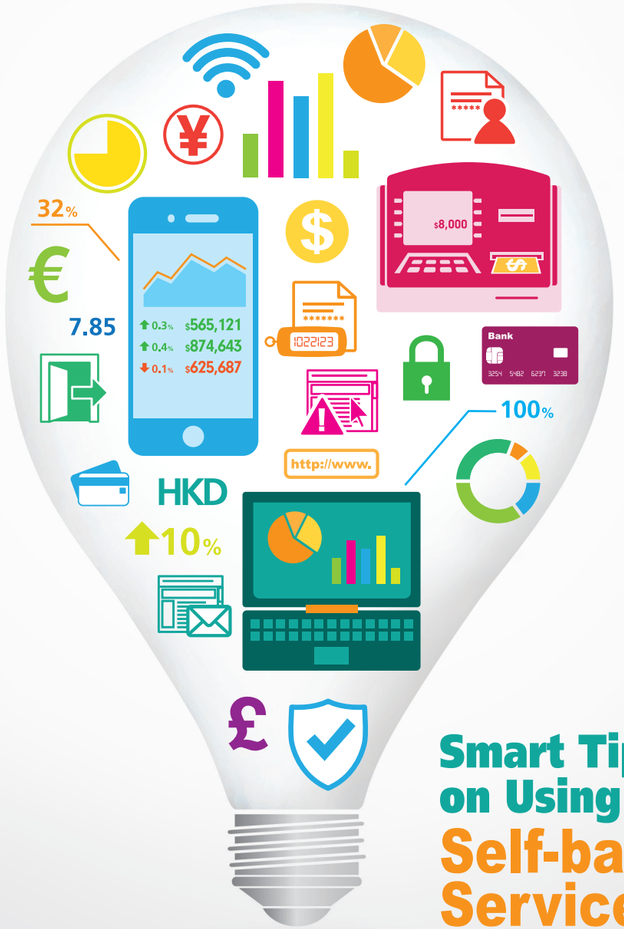
HONG KONG MONETARY AUTHORITY
香港金融管理局



Smart Tips on Using Self-banking Services

Internet Banking

Dos

Ensure your login information (including login name and password) and the security token provided by your bank (if any) are kept in a safe place, and change your password regularly.

Ensure the device through which you bank on-line (like your desktop or tablet personal computer) is password protected, and has enabled the auto-update feature for your computer's operating system, as well as a proper firewall, anti-virus and internet security software, to reduce the risk of your device being compromised.

http://www. If you encounter any suspicious situations when logging into your internet bank account (for example, your computer responds extraordinarily slowly, the login procedure is awkward, or you are required to key in additional information), you should stop the login and inform the bank immediately.

Be aware of fake bank websites and purported bank emails. To ensure a secure connection to the bank's website, always type your bank website address into the browser yourself, or bookmark your bank's genuine website address in your computer. If you suspect you have provided personal information or conducted transactions through a suspicious bank website or a purported bank email, you should immediately inform the bank and the police.

Log out properly and close the browser each time after using internet banking to prevent the leakage of your personal information.

Don'ts

Never disclose the login information of your internet bank account to anyone.

Never keep a record of the login information of your internet bank account together with the security token provided by your bank (if any).

Never access your internet bank account through public computers (such as computers available in cyber cafés, public libraries, public transport or airports) or public WIFI.

Never access your bank website through any hyperlink in emails or SMS, or a website address shown in a suspicious pop-up window or internet browser. Banks never issue emails with hyperlinks to transaction webpages, nor will they ask for sensitive information like your internet bank account and personal information (including the login password or one-time password) by email, phone or person.

Website: www.hkma.gov.hk Telephone: 2878 8196

Automatic Teller Machines (ATMs)

Dos

Ensure your ATM card and password are kept in a safe place. Change your password regularly.

Cover the keypad with your hand when entering your password and make sure no one is looking over your shoulder or next to you.

Before using an ATM, check the keypad cover has not been removed or tampered with. If you notice any suspicious devices or cameras around the ATM, for example, near the card slot or on the upper part of the ATM, do not use the machine and immediately report the matter to the bank or the police.

Report to your bank immediately in case of any card loss.

Count the banknotes immediately after each cash withdrawal.

Don'ts

Never disclose your ATM card password to anyone.

Never write down your password on the front or back of your ATM card. Do not keep a record of your password in your wallet.

Avoid using your mobile phone or listening to music when withdrawing cash from an ATM as you may be distracted and leave the banknotes unattended at the ATM. Contact the bank immediately if any banknotes are left at an ATM.

Do not remove banknotes left at an ATM dispenser by another person. The banknotes will be automatically returned to the ATM after a designated period of time. It is a criminal offence to steal the cash left unattended in an ATM by another person.

Chip-based Technology

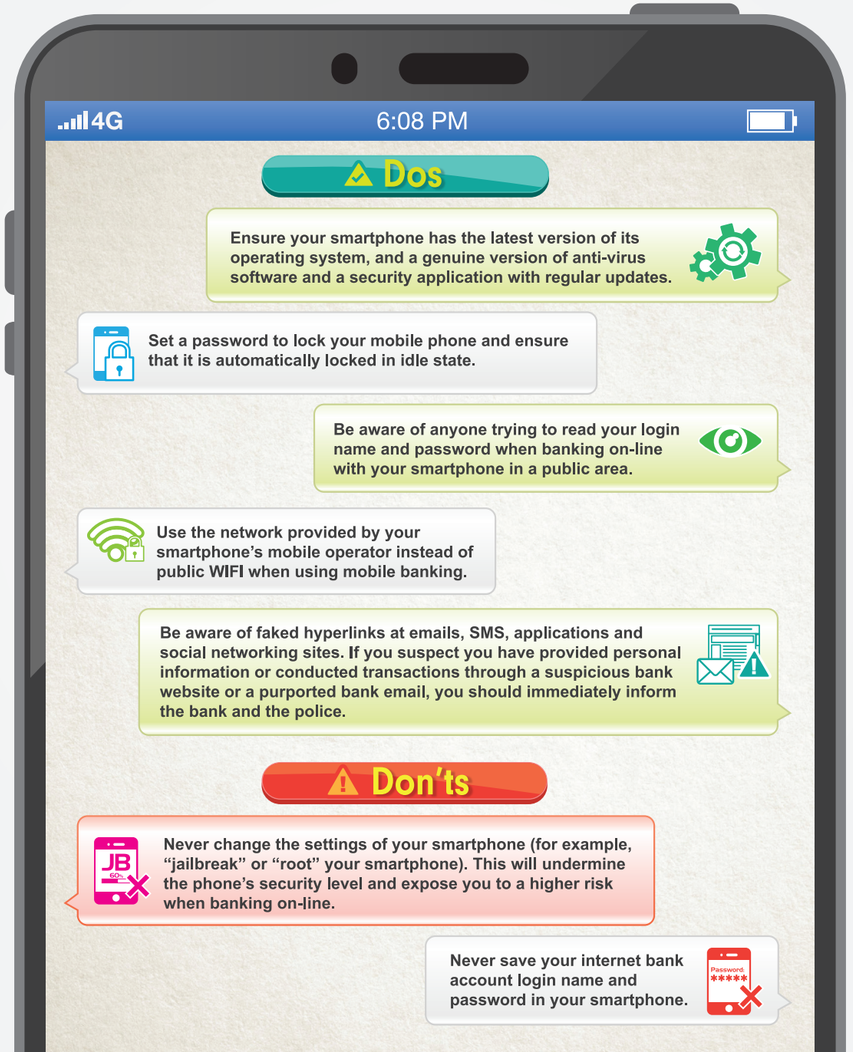
In 2011, the HKMA required banks to adopt chip-based technology to strengthen the security control of ATMs and ATM cards. This technology makes it more difficult to steal card data and produce counterfeit cards for unlawful use in Hong Kong. Upgrading ATMs with the chip-based technology has been completed and banks are replacing customer cards in phases until 2015.

Reminder on Overseas Cash Withdrawal

To prevent unlawful cash withdrawals at ATMs outside Hong Kong through the use of counterfeit cards, the overseas cash withdrawal function of all ATM cards (including debit cards and credit cards) is pre-set to "deactivate". If you intend to withdraw cash from overseas ATMs, you should:

- **activate the overseas ATM cash withdrawal function** in advance of your travel, either through ATMs in Hong Kong, internet banking, phone banking or bank branches;
- **set the overseas ATM cash withdrawal limit** (which can be lower than the amount set for Hong Kong), and the effective and expiry dates of the activation period according to your needs; and
- if necessary, check with your bank whether the **ATM network(s) in your destination can support your ATM card**.

Mobile Banking



Dos

Ensure your smartphone has the latest version of its operating system, and a genuine version of anti-virus software and a security application with regular updates.

Set a password to lock your mobile phone and ensure that it is automatically locked in idle state.

Be aware of anyone trying to read your login name and password when banking on-line with your smartphone in a public area.

Use the network provided by your smartphone's mobile operator instead of public WIFI when using mobile banking.

Be aware of faked hyperlinks at emails, SMS, applications and social networking sites. If you suspect you have provided personal information or conducted transactions through a suspicious bank website or a purported bank email, you should immediately inform the bank and the police.

Don'ts

Never change the settings of your smartphone (for example, "jailbreak" or "root" your smartphone). This will undermine the phone's security level and expose you to a higher risk when banking on-line.

Never save your internet bank account login name and password in your smartphone.