MAJOR TIPS ON PROTECTION OF YOUR COMPUTERS AND MOBILE PHONES

PASSWORDS

Set difficult-to-guess passwords for your computer and mobile phone. Activate the auto-lock function.

SECURE SYSTEMS AND SOFTWARE

Use the latest versions of operating system, Internet banking App and browser. Do not jailbreak or root your mobile phone or tablet.

BEWARE OF COMPUTER VIRUSES

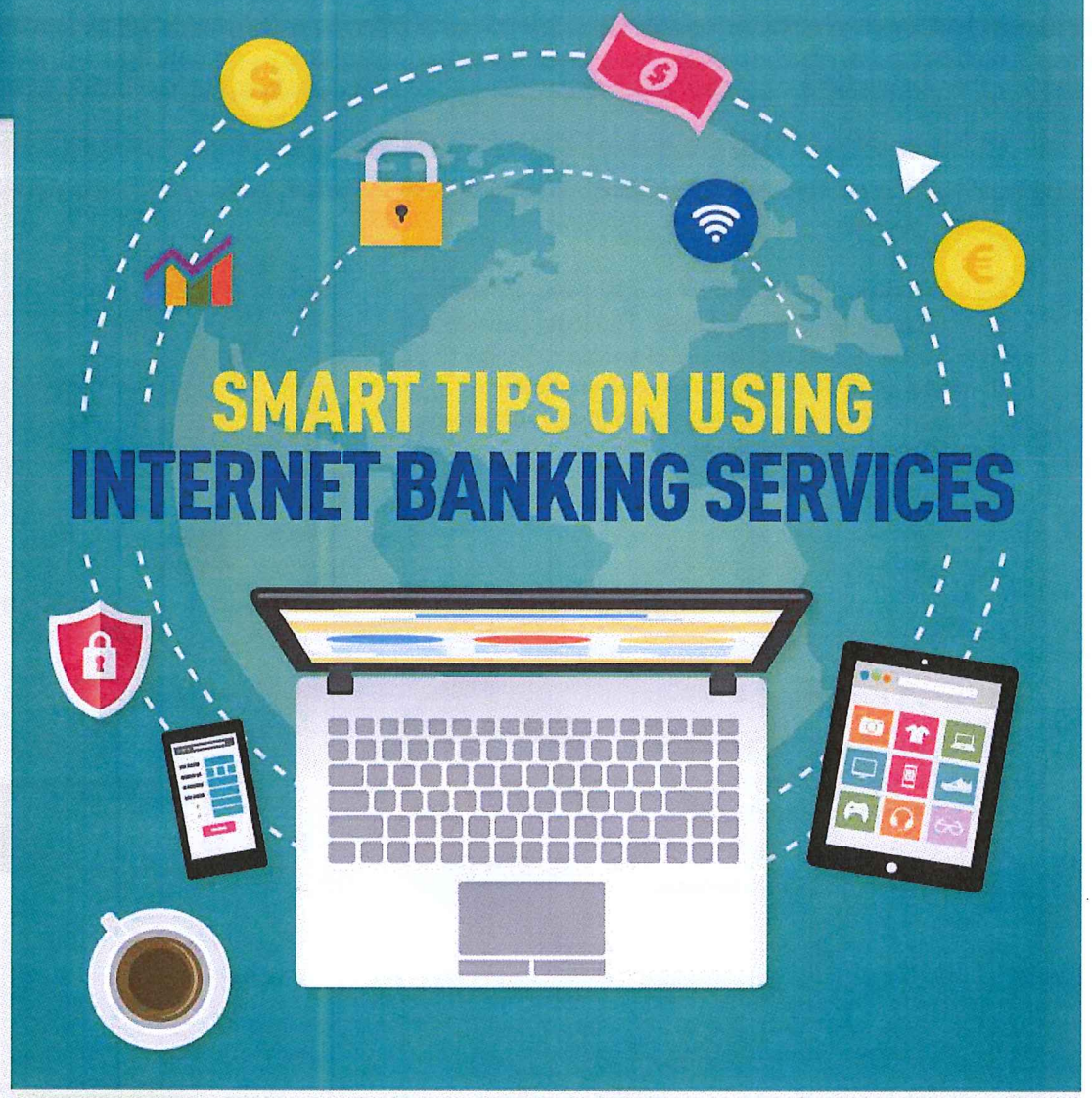
Install and update promptly your security software. Do not download or open doubtful files, browse suspicious websites, or click on the hyperlinks and attachments in questionable sources (e.g. emails, instant messaging, SMS messages, QR codes). Download and upgrade your Apps from official App Stores or reliable sources only.

NETWORK FUNCTIONS

Disable any wireless network functions (e.g. Wi-Fi, Bluetooth, NFC) not in use. Choose encrypted networks when using Wi-Fi and remove any unnecessary Wi-Fi connection settings.

Reference: The Government's Cyber Security Information Portal (http://www.cybersecurity.hk)

12/2015



SMART TIPS ON USING INTERNET BANKING SERVICES

Published by

HONG KONG MONETARY AUTHORITY
香港金融管理局

Supported by

MAJOR SAFETY TIPS ON USING INTERNET BANKING SERVICES

LOGIN PASSWORDS

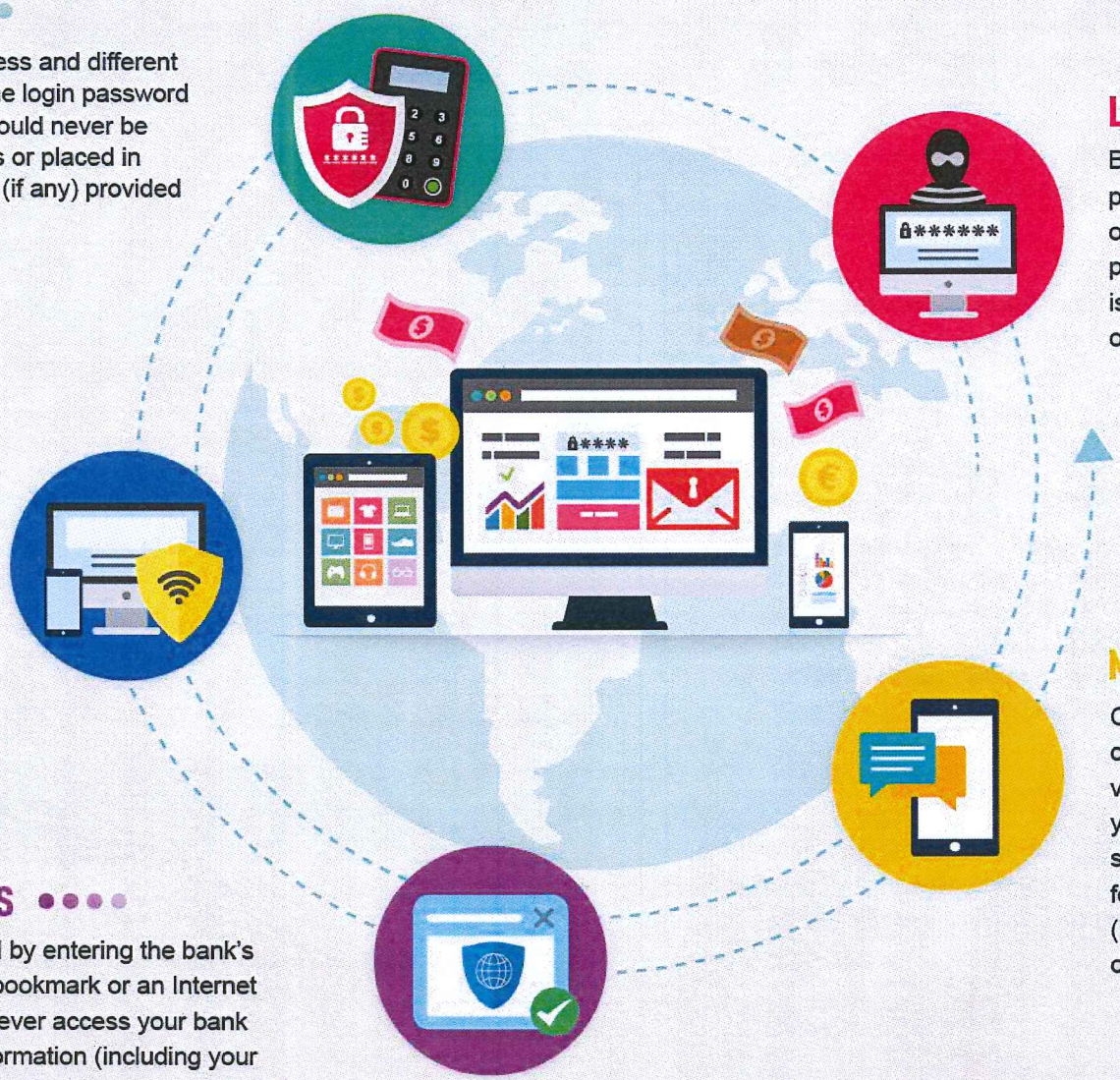
Set a password that is difficult to guess and different from the ones for other services. The login password should be changed regularly and should never be stored on computers, mobile phones or placed in plain sight. Keep the security token (if any) provided by your bank at a safe place.

COMPUTERS AND MOBILE PHONES

Protect your computer and mobile phone for logging into your Internet banking. Avoid using public computers or public Wi-Fi to access Internet banking services.

BANK WEBSITES AND APPS

Internet banking should be accessed by entering the bank's website address directly, or using a bookmark or an Internet banking mobile application (App). Never access your bank website or provide your personal information (including your password) through any hyperlinks or attachments embedded in emails or from websites.



LOGIN PROCESS

Beware of any unusual login screen or process (e.g. a suspicious pop-up window or request for providing additional personal information) and whether anyone is trying to peek at your password. Log out immediately after use.

MESSAGES FROM BANKS

Check your bank's SMS messages and other messages in a timely manner and verify your transaction records. Inform your bank immediately in case of any suspicious situations. Banks will not ask for any sensitive personal information (including passwords) through phone calls or emails.

SMART TIPS ON USING AUTOMATED TELLER MACHINES

Published by

HONG KONG MONETARY AUTHORITY
香港金融管理局

Supported by

THE HONG KONG ASSOCIATION OF BANKS
香港銀行公會

HKCERT

Jetco

cybersecurity.hk
Office of the Government Chief Information Officer

MAJOR SAFETY TIPS ON USING ATMs

ATM CARDS AND PASSWORDS

Keep your Automated Teller Machine (ATM) card safe. Set a password that is difficult to guess and different from the ones for other services. Change your password regularly. Do not keep your ATM card and password together.

ATMs

Beware of anything unusual about the card insertion slot, keypad and keypad cover (e.g. whether any suspicious device is installed). Cover the keypad with your hand when entering your password and check whether anyone is trying to peek at your password.

HANDLING YOUR CASH WITHDRAWALS

Count the banknotes immediately after each cash withdrawal. Do not take away any banknotes at the cash dispenser or ATM card at the card insertion slot left behind by someone else. Let the banknotes or ATM card return to the ATM automatically.

OVERSEAS CASH WITHDRAWALS

If you intend to withdraw cash from overseas ATMs, check with your bank whether your intended overseas destination can support cash withdrawal using your ATM card. You should also activate the overseas ATM cash withdrawal function in advance and set a prudent overseas ATM cash withdrawal limit and an activation period.

MESSAGES FROM BANKS

Check the transaction records provided by your bank in a timely manner. Inform your bank immediately if you lose your ATM card, or in case of any suspicious transactions or situations. Banks will not ask for any sensitive personal information (including passwords) through phone calls or emails.

12/2015