KEEP YOUR PERSONAL DIGITAL KEYS SAFE

HONG KONG MONETARY AUTHORITY
香港金融管理局

www.hkma.gov.hk

2878 8196

HKMA

HKMAGOVHK

HKMAGOVHK

鳴謝: 香港銀行公會
Acknowledgement: The Hong Kong Association of Banks

What are Personal Digital Keys?

In the digital world, account login credentials and personal information are your personal digital keys. They are as important as the keys to your home, and should be well protected. If such information is stolen by fraudsters, they may disguise you to log into your Internet/mobile banking or e-wallet (collectively known as "digital financial services" thereafter) accounts, resulting in financial loss. Remember to **keep your personal digital keys safe!**

Examples of personal digital keys:

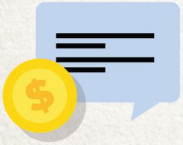
Smart Tips on Protection of Personal Digital Keys

When submitting your personal information online, for example during online shopping, ensure the website is reliable.

Do not use unknown Wi-Fi or public computer to access Internet/mobile banking and e-wallet services.

Properly protect your computers or mobile phones used for performing online transactions (including digital financial services).

Remember to delete all information in a mobile phone before changing your phone.



Pay attention to alert messages from your bank. If you ignore them, you may not be aware even when your account is hacked.

Passwords should be hard to guess and should be changed regularly. Do not use the same password for all accounts of digital financial services.

Contact the bank or digital financial service provider if you suspect that personal information has been stolen.

Major Tips on Protection of Your Computers and Mobile Phones

Passwords

Set hard-to-guess passwords for your computer and mobile phone and change the passwords periodically. Use different passwords across various devices and online services. Do not share your passwords with others. Activate the auto-lock function on your computer and mobile phone.

Secure systems and software

Use the latest versions of operating system, Internet/mobile banking and e-wallet mobile applications (Apps) and browser. Do not jailbreak or root your mobile phone or tablet. Download and upgrade your Apps from official App Stores or reliable sources only. Install and update promptly the latest security software and security patches. Back up important data.

Beware of malicious software programme

Think Before You Click – Do not download or open suspicious files, browse suspicious websites, or click on the hyperlinks and attachments from questionable sources (e.g. emails, instant messaging, SMS messages and QR codes).

Always stay alert and beware of fraudsters who disguise themselves as reputable business websites or persons, establish fraudulent websites or emails that look like the official ones, or trick users into clicking on hyperlinks or attachments or in other format so as to steal users' personal information. When in doubt, you should type the correct website address in your browser and avoid clicking suspicious hyperlinks.

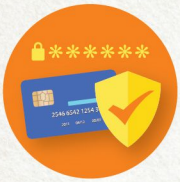
Network functions

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

Major Safety Tips on Using Digital Financial Services

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.



Login credentials

Set a password that is difficult to guess and different from the ones for other online services. The login password should be changed regularly and should never be stored on computers, mobile phones, placed in plain sight or be disclosed casually to third party Apps.

Use two-factor authentication for accessing digital financial services accounts if possible and seek to understand the operations. Protect your devices used for two-factor authentication (e.g. security tokens or mobile phones).

Payments and funds transfers

Carefully check payee information (e.g. mobile phone numbers, emails, account numbers and payee names) before confirming payments and funds transfers. Set appropriate transaction limits.

Computers and mobile phones

Protect your computer and mobile phone for logging into the digital financial services accounts. Avoid using public computers or public Wi-Fi to access those services. Avoid using others' devices to login to digital financial services accounts, or share your devices with others.

Digital financial service website and Apps

Digital financial services should be accessed by entering the respective service provider's website address directly, or using a bookmark or the related mobile App. Never login or provide your personal information (including your login credentials, credit card credentials and one-time passwords) through unexpected or suspicious websites, any hyperlinks or attachments embedded in emails or from websites.

Messages from banks

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

SECURITY PRECAUTIONS OF BUSINESS CUSTOMERS

Companies have to remind employees on how to identify phishing emails and not to share their job duties and organisational structures on social media to prevent misuse of the data for deception. Apply appropriate controls to users' access to business systems. Deploy encryption to protect your business and customer data.

Be mindful of requests to change beneficiary information or unusual and urgent payment requests received via emails or phone calls. Immediately validate any suspicious request by contacting your key business contact or the company's senior management using the usual contact number. Do not amend payment information unless you are certain that it is legitimate.

12/2019