恒生銀行
HANG SENG BANK

Major Tips On Protection Of Your Computers And Mobile Phones

(a) Passcodes for mobile phones
– Set a passcode for your mobile phone that is difficult to guess and different from other services. Activate the auto-lock function.

(b) 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.

(c) Beware of computer viruses
– Your phone device is important to receive transaction notification or One-time Password (OTP) from the bank during online banking or online purchase with your cards.
– Do not enter personal information (e.g. ID card/passport number) and credit card information together in mobile Apps unless you are absolutely sure this is verified in an alternate channel. This could be a phishing attack (Please see the picture below).
– Install and update promptly your security. Do not browse suspicious websites or click on the hyperlinks and attachments in suspicious emails/SMS messages. Download and upgrade your Apps from official App stores or reliable sources only.

(d) 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. Avoid using public computers or public WiFi for internet banking services.

* Jailbreaking is the process of removing hardware restrictions imposed by iOS, Apple's operating system, on devices running it through the use of software exploits.
** Rooting is the process of allowing users of smartphones, tablets and other devices running the Android mobile operating system to attain privileged control (known as root access) over various Android subsystems.