

FAQ

What is TLS ("Transport Layer Security") encryption?

- Our Internet Services have adopted TLS encryption (TLS v1.2 or above), one of the online security standards for commercial application. All data transmitted via the Internet Services are protected by this technology to ensure data security.

What precautions should I take when I set up my password or login information?

- Do not use your date of birth, ID / passport number, telephone number or any combinations of your English name as your password or login information.
- Do not use 3 or more consecutive identical alphabets or digits, e.g. "333", "bbb" etc.
- Do not use sequential alphabets or digits, e.g. "123", "abc", etc.
- Do not use your user name / login ID as your password.
- Do not use the same passwords for accessing other services (for example, connection to the internet or accessing other websites).

How often should I change my password?

- You are advised to change your password regularly. If you have not changed your password over certain period of time, our system will remind you automatically.

How can I protect my personal information?

- You may be asked to provide personal information (such as your ID / passport number and date of birth) as additional identity verification when you use the internet banking service. Be vigilant and do not casually disclose your personal information to anyone. You should also keep documents (such as letters and bank statements) which carry your personal information in a proper and secured manner.

Why should I update my operating systems and browsers regularly?

- It helps to fix security problems of the operating systems or web browsers if you update and download "patches" provided by software vendors regularly. This helps to prevent your computer from virus attacks or unauthorised access from hackers.

How can I set up the security settings of Wireless LAN?

- Do not place the Access Point ("AP") too close to doors and windows to avoid data captured and decrypted by any third party.
- Take appropriate security measures to protect the Wireless LAN. Do not disclose the security setting of your wireless network to any third party.

Precautionary measures for using internet?

- Encrypt your data if you have to keep your personal information in an electronic storage medium to prevent unauthorised access or use by third parties.
- Do not save or keep your password in your browser and disable the "Auto-Complete" setting to prevent third parties from accessing your information via the browser.
- Disable the "File and Printer Sharing" function of the Windows system and set up proper access permissions of your computer to prevent unauthorised access to your data by third parties via the network.
- Do not download or install illegal or unknown softwares to prevent infection from computer virus or Trojan programmes. Remember to scan for virus before opening any files from external sources.

Where can I obtain more information on precautionary measures for Internet Banking and ATM Services?

- Hong Kong Monetary Authority – –SMART TIPS Beware of Fraudsters!
https://www.hkma.gov.hk/gb_chi/smart-consumers/beware-of-fraudsters/
- Hong Kong Monetary Authority – SMART TIPS ON USING INTERNET BANKING SERVICES

<https://www.hkma.gov.hk/eng/smart-consumers/internet-banking/#using-internet-banking-services>

- Hong Kong Monetary Authority – SMART TIPS ON USING AUTOMATED TELLER MACHINES

<https://www.hkma.gov.hk/eng/smart-consumers/atms/>

- The Hong Kong Association of Banks “Smart Consumer Security Tips”

<https://www.hkab.org.hk/en/useful-information/smart-consumer#security-tips>

- Hong Kong Police Introduction to Cyber Security and Technology Crime

https://www.police.gov.hk/ppp_en/04_crime_matters/tcd/

- Office of the Government Chief Information officer – “The InfoSec Web Site”

<https://www.infosec.gov.hk/en/>

- The Hong Kong Association of Banks “Enhancement on security measures to safeguard customers against malware scams”

<https://www.hkab.org.hk/tc/news/press-release/292>