Frequently Asked Question

Internet Banking Online Security

Click on questions below to search through FAQ

Contents

Security Online

1. Multi-layer logon verification

Your financial information is protected by a sophisticated combination of a unique Username and Password, and a one-time Security Code generated by your Security Token.

Transaction verification

When you transfer money online, HSBC prompts you for the Security Code generated by your Security Token. This ensures that only you can authorise payment and transfer requests.

128-bit encryption

HSBC uses the highest level of encryption for information transmitted during an Internet Banking session

Automatic 'Time-out' feature

As a security measure, your Internet Banking session will automatically shut-down or time-out, out after a period of not being used. You should always close your Internet Banking session when you have finished.

2. How does HSBC ensure Internet Banking security?

HSBC follows industry best practice to ensure our Internet Banking is safe and secure. These include:

- Secure 128-bit encryption (the highest available) for all information transmitted during an Internet Banking session.
- Each Internet Banking User has a unique Username and Password, and is issued with a Security Token - which generates a constantly changing Security Code that must be input every time you logon to Internet Banking and to transfer money to third party accounts.
- An automatic time-out feature that will end your Internet Banking session after a period of not being used.

3. What is my role in security?

You also have a role to play in security. You should adopt the following measures to ensure your Internet Banking is safe and secure:

- Ensure your computer is protected with the latest anti-virus and firewall protection software at all times. Download updates regularly to ensure you have the latest protection. Click Here to Learn More
- Choose a Password that is memorable to you but not easy to guess by someone else. Passwords that contain combinations of alpha and numeric characters are generally harder to guess (e.g. a7g3cy91).
- Do not choose a Password that you use for other services. Your Password should be unique to Internet Banking.
- Change your Internet Banking Password on a regular basis.
- Never disclose your Internet Banking Password to anyone. A member of HSBC will never ask you for your Password.
- Do not write your Internet Banking Username together with your Password. Do not write your Password in a recognisable format and never leave your logon details with your Security Token.
- Disable functionality on your computer or browsers that remembers logon details.
- Exercise care not to lose your token. If your Token is missing, immediately contact us on 800 1234 or (230) 403 0750 to disable it.

If you suspect someone may have obtained access to your Internet Banking details, logon to Internet Banking to change your Password. Call us on 800 1234 or (230) 403 0750 for assistance.

4. What is the HSBC Security Token?

The HSBC Security Token is a small, key-ring size, digital code generator provided to Internet Banking customers. Once activated, you will need to use the Security Token to generate Security Codes, which are required when you log on and transact on Internet Banking.

Why has HSBC selected the Security Token solution rather than other security measures?

The Security Token solution has been selected by HSBC as the technology that best meets our customers' need for flexibility and portability, and our business volume requirements. The Security Token meets industry best practices for Two-Factor Authentication standards, while providing the following benefits to you:

- The Security Token itself generates the Security Code. As there is no dependency on a third party for Security Code generation or transmission, our customers do not need to rely on another party's service standard to access Internet Banking.
- The generation of the Security Code is not dependent on capacity constraints, signal availability or the geographical location of our customers.
- The Security Token is small, light and portable. It can be used on Internet-enabled terminals and does not require any downloads, setups or system adjustments.

5. Top Tips to Protect Yourself from Frauds & Email Scams

- Do not forward or reply directly to any emails that ask you to provide personal information. Report to us immediately if any.
- Avoid using public computers; instead use your own computer to read personal emails.
- HSBC will not provide any hyperlinks to HSBC Internet Banking Logon page in our emails.
- If you receive any Email from unrecognized source, you should delete it without opening it. You should also be able to activate a spam filter, which will automatically route all such mail to a separate inbox. Deleting unwanted spam without reading it will also protect you from most phishing e-mails.
- Be aware that there are fake websites designed to trick you and collect your personal information. Sometimes links to such websites are contained in e-mail messages purporting to come financial institutions or other reputable organisations. Never follow a link contained in an e-mail - even if it appears to come from your bank.

Disclaimer: This document is for information purposes only.

Issued by The Hongkong and Shanghai Banking Corporation Limited in November 2018 .Incorporated in the Hong Kong SAR with limited liability.