INFORMATION SECURITY RECOMMENDATIONS

At SHB, we strive to deliver the most secure and convenient online banking services for our customers. As part of our effort to maintain the highest level of security on our site and for our internet banking users, we ask that you read and be aware of the below information for your own safety.

Principle 1: Set password and secure password

Customers should follow these recommendations in order to avoid unfortunate events that might happen:

How to set password:

- Password must contain upper case letters, lower case letters, numbers and special characters.
- Password must be at least 8 characters long.
- Do not attempt to use passwords like names, phone numbers, birth dates etc and other private information or words contained in dictionaries.

How to secure password:

- Customers should secure usernames and passwords; never disclose internet login details to anyone.
- Regularly change password.
- Do not write them down.
- Do not share password with anyone.
- Avoid to use the same password for different services.
- Inform SHB immediately if you find out that your password is disclosed or used by someone else.

Principle 2: How to secure authentication token

Customers secure authentication token (eSecure card, USB token with digital signature, password storage device), do not share or disclose information to others.

- Do not take photo, save picture of eSecure card to mobile phone, computer
- Do not share USB token digital signature with others.

Principle 3: How to use web browser

Customers should not allow web browser to save username and password.

Principle 4: Log out from Internet Banking when you are not using it

When leaving your computer, you should close the transaction window that is being performed by clicking on LOG OUT on the screen and lock the computer.

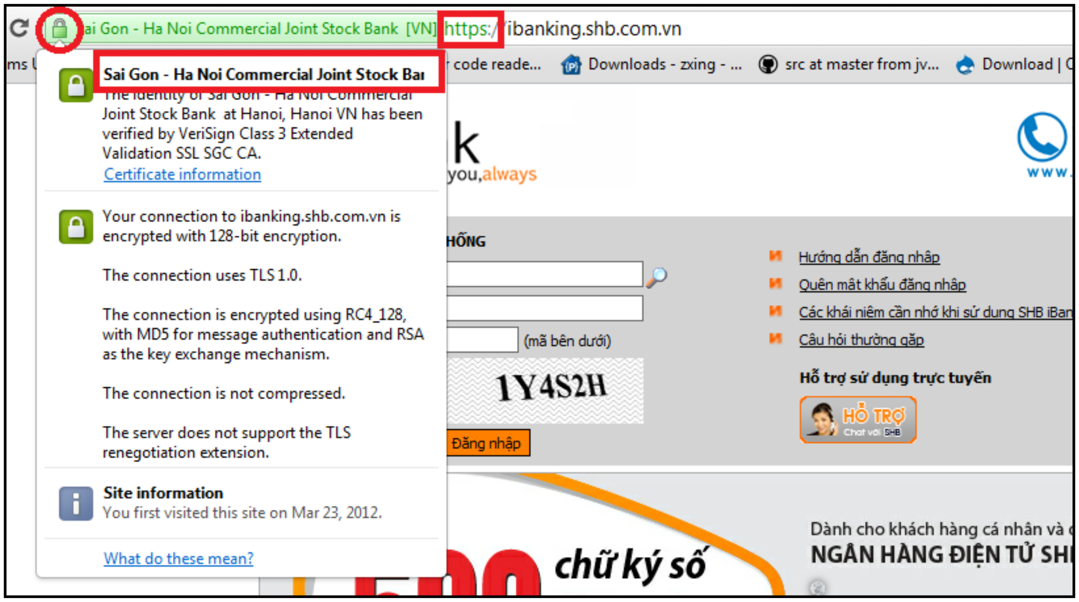
Principle 5: Access to the right website of SHB online banking

Criminals use a fraudulent website with the interface that is identical to the authentic website in order to gain access to user's account and its sensitive information so they can use these information to do financial damage or ruin prestige of customers. To ensure the safety of your transaction information, customers should follow the following recommendations:

- Always type the website address on searching toolbar: http://ibanking.shb.com.vn
- Do not sign in your account information on any other website.
- Be alert when using public computer, public wifi in coffee shops, shopping centers, bookstores etc to access the internet banking because those environments are not safe and sensitive information like username, password, PIN code of customers can be stolen.
- Check the lock symbol and certificate of the website as follow:
    - A safe transaction is a transaction having URL address starting with http:// or having lock symbol appear on the performing window of the customer.
    - In the authentic website of SHB online banking, when customers access, a green line will appear and confirm that the website is encrypted with SSL method. Other connections are also encrypted to avoid being eavesdropped. When clicking the green line mentioned above, a window will pop up below certifying that the website is under control of Saigon Hanoi Commercial Joint Stock Bank.
    - Websites that do not guarantee one of the above conditions can be fake websites, please stop the transaction and contact 24/7 free hotline - Tel: 1800 5888 56.

Authentic Website of SHB with distinctive features

○



Sai Gon - Ha Noi Commercial Joint Stock Bai

The identity of Sai Gon - Ha Noi Commercial Joint Stock Bank at Hanoi, Hanoi VN has been verified by VeriSign Class 3 Extended Validation SSL SGC CA.

[Certificate information]

Your connection to ibanking.shb.com.vn is encrypted with 128-bit encryption.

The connection uses TLS 1.0.

The connection is encrypted using RC4_128, with MD5 for message authentication and RSA as the key exchange mechanism.

The connection is not compressed.

The server does not support the TLS renegotiation extension.

Site information

You first visited this site on Mar 23, 2012.

What do these mean?

Principle 6: Contact SHB immediately when:

- When you encounter errors and incidents while using the service; free hotline service 24/7 - Tel: 1800 5888 56.
- When you use Internet Banking with SMS authentication and lost your mobile or use eSecure authentication and lost Token, please contact hotline 24/7 – Tel: 1800588856 or go to the nearest transaction point to inform and demand to deactivate your authentication method.
- Contact SHB immediately if you receive a suspicious email or a call from someone asking you to provide your login information. DO NOT follow those requirements even if it seems to be from SHB because SHB will never ask you to reveal your password, PIN code or security code over the phone or via email.

Principle 7: Follow SHB's recommendations about installing software

To secure online transaction with the bank, you need to:

- Ensure that your computer has windows repair program and is updated to the latest version from the vendor.
- Install anti-virus, malware, rootkit programs on the computer because some security issues cannot be guaranteed by an operating system of personal computers. Personal computers are easily infected with virus, malware, spyware, rootkit etc from the internet if they are not installed sufficient anti-virus programs. You should install commercial version of prestigious brands in this field such as: Symantec, Kaspersky, McAfee, AVG etc, or use the free software of Microsoft "Microsoft Security Essential" that can be downloaded directly from its website http://www.microsoft.com.
- Use personal firewall, intrusion detection program are two effective methods that help you notice and prevent cyber attack or illegal access from unwanted subjects. You can use common programs, for example: Zone Alarm, Patriot etc.
- You should only use legal programs and not download programs from illegal websites on the internet and install them on your personal computer. Do not open files sent from anonymous emails and use anti-virus programs to scan files before opening.
- Do not use jailbreak mobile devices to download and use Internet Banking app, OPT creating software and other software belonging to E-banking system.

Principle 8: Choose authentication method

- Choose authentication methods having high safety/security to suit your needs for transaction limit on E-banking (authentication methods via SMS, by eSecure or digital signature, etc.)