User Guide and Safety Tips for Personal Internet Banking

I. User guide for personal Internet Banking

Thank you for choosing to apply for our personal Internet Banking service. You can log in and use our personal Internet Banking with your Internet banking user ID, login password, and token. If there are any changes to the features and services of personal Internet Banking, we will release a notice on our official website. Please pay attention to the relevant notice information.

1. How to complete the first login of personal Internet Banking?

If you have activated our personal Internet Banking and obtained a token, please follow the following process to complete the first login of personal Internet Banking:

1) Log in to our official website (www.ocbc.com.cn) and select "Personal Banking" or “Line Switching” from the login drop-down box on the right side of the homepage;

2) On the personal Internet Banking login page, enter the Internet banking user ID, initial password, and page verification code according to the prompts on the page, and click "Login";

3) Please follow the prompts on the newly pop-up page to obtain and enter a 6-digit Token OTP through your token, and click "OK";

4) Enter the " Terms and Conditions Governing Electronic Banking Services （for Personal Customer） ", "Authorization for Handling of Personal Information and Notification", "Separate Consent Authorization for Handling of Sensitive Personal Information", and "Separate Consent Authorization for Providing Personal Information Outside of the Country" pages. Please carefully read and verify the mobile phone number at the bottom of the page. After confirming it is correct please check the box to confirm and click "Agree"; Enter the “Change Login Password” page, follow the prompts on the page to enter the initial password, new password, confirm the new password, and click on "Obtain Token OTP";

5) Please follow the prompts on the pop-up page to obtain and enter a 6-digit Token OTP through your token, and click "OK";

6) The Token OTP will automatically be displayed on the personal Internet Banking “Change Login Password” page. Click "OK" and the page will prompt that the password has been successfully changed, thus completing the first login.

2. What should be noted when using the initial password for personal Internet Banking?

1) When you successfully apply for our personal Internet Banking at our branch, you can set your initial password for personal Internet Banking.

2) This password is valid for 15 days from the date of issuance. Please log in to personal Internet Banking in a timely manner and set a new Internet banking login password. If the password is not used after the expiration date, you can reset your password through personal Internet Banking or come to our personal banking branch in person with your valid identity certificate for password resetting.

3. What should be noted when using personal Internet Banking token?

If you have any questions during the process of using your personal Internet Banking token, please log in to our official website (www.ocbc.com.cn), select “Personal Banking” from the drop-down box on the right side of the homepage to

enter the personal Internet Banking login page and then click “Token User Guide” on the lower left of the login page for help. If the personal Internet Banking login page cannot be opened, you can click "Line Switching" under "Personal Banking" in the electronic banking login drop-down box on the right side of the homepage.

4. What features and services does personal Internet Banking provide?

1) Overview of assets & liabilities

2) Transfer

3) Time deposit and call deposit transactions

4) To purchase structured deposit products

5) To change and reset login password

6) To inquire loan information

7) To know our latest products and services

5. If you encounter problems during operation, how can you contact us?

Please call our customer service hotline: 40089 40089 (China’s mainland); +86 755 2583 3688 (Hong Kong, Macao, Taiwan and overseas). The business hours of manual service are 7:30-22:00.

II. Security tips for personal Internet Banking

To protect the security of your funds, our bank is committed to providing you with secure Internet banking services and continuously improving the security of the Internet banking system. Our bank adopts end-to-end encryption of all Internet banking transactions, meaning that data will be encrypted from the client end and decrypted at the bank end, and the transmission process is under full encryption protection.

Customers must ensure the security of their terminals and user information to safely access Internet banking services. If the client terminal is implanted with malicious programs, there is still a risk of tampering with transaction information, and the corresponding risks of fund theft will be borne by the customers. So please pay attention to the security protection of client terminals and user information.

The following security tips are for reference only, and our bank is not responsible for the accuracy and completeness of these network security related tips. Please consult with information security experts for details.

1.Make sure you are visiting our official website

Counterfeit websites that attempt phishing often use the Bank's official logo, images, and design style, which are very difficult to recognize and differentiate simply from the content of the webpage. It is suggested to identify in the following ways:

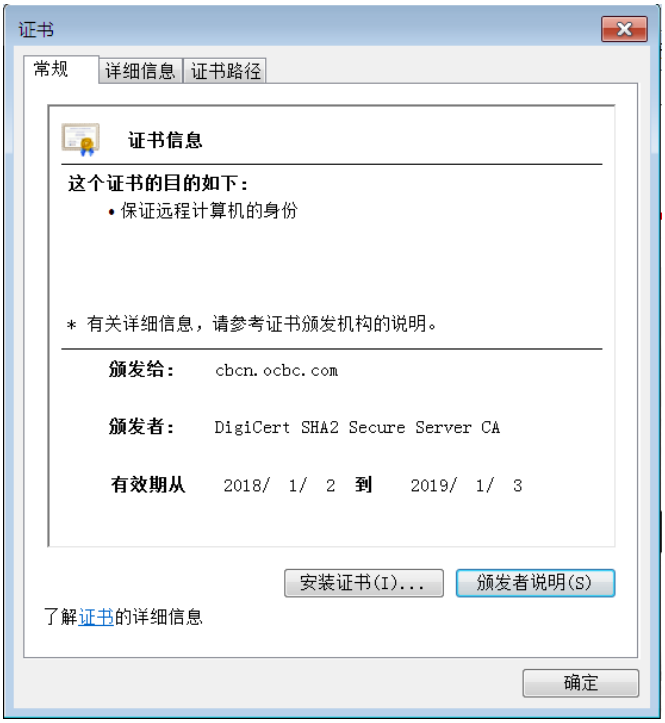
1) Confirm the right URLs. Our personal Internet Banking address is

   www.ocbc.com.cn

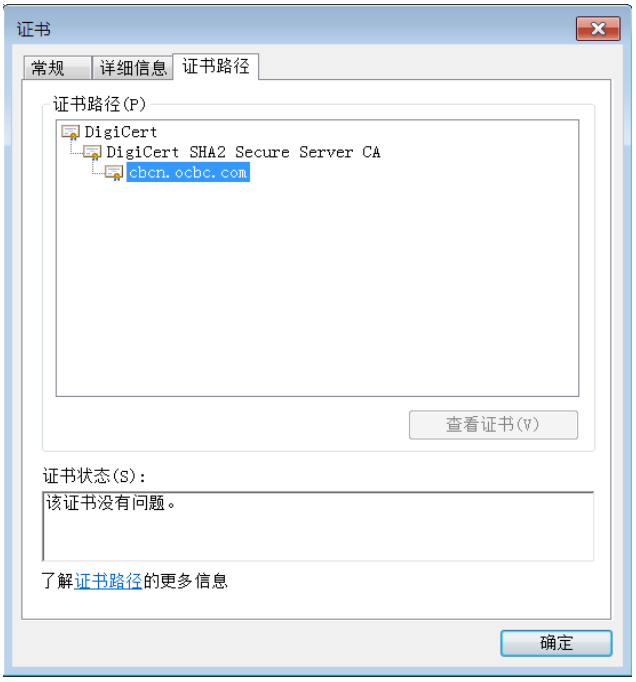
2) Verify the SSL certificate of the website as follows:

- Click on the 'padlock' icon next to the address bar

- Click on “View Certificate”
- Verify that the certificate is issued to the domain name cbcn.ocbc.com
- Verify that the certificate is issued by “DigiCert”



- Click on the “Certificate Path” tab
- Verify that the certificate status is “There is no problem with this certificate”



2. Warnings or error prompts about website certificate

What should you do when you see a warning or error prompt related to a website certificate:

1) SSL (Secure Sockets Layer) and its upgraded version TLS (Transport Layer Security) is a security protocol that provides security and data integrity for network communication. It is a technology used for secure encryption between bank servers and client browsers in Internet banking. This connection ensures that all data between the bank's network server and browser remains confidential and secure. SSL/TLS is an industry standard used by banks to protect online transactions between us and our customers.

2) This secure connection assigns an encryption key in the form of a certificate. If you see any certificate warnings or certificate errors when logging into the Internet banking, please immediately log out and notify the bank.

3) Our bank is committed to providing customers with the highest level of security protection. Please ensure that your computer supports TLS1.2 transport layer security protocol, otherwise you will not be able to log in to Internet banking.

3. Protect your computer

1) Install antivirus, antispyware, and firewall software to protect your personal computer from hacker attacks, virus attacks, and attacks from other malicious programs such as Trojans. When connected through broadband, digital subscriber line, or cable modem, your computer is particularly vulnerable to attacks. Installing this security software will prevent and detect unauthorized access to your computer.

2) Disabling the “File and Printer Network Sharing” feature in the system can prevent illegal external control of and intrusion into your computer. This feature can be disabled by selecting 'Network' in the control panel and clicking “File and Printer Sharing”.

3) Do not log in to your Internet banking or perform any financial transactions on public/shared personal computers (such as those in internet cafes).

4) Do not download any programs without knowing the website's reputation.

5) Suspected viruses can be distributed and disguised as email attachments, so do not open attachments in emails from unknown senders.

6) Update your anti-virus, anti-spyware and firewall programs regularly by using security patches or downloading the latest version.

7) Delete files and information shared on your printer, especially when you access the Internet through a cable modem, broadband connection, or other similar settings.

8) Consider using data encryption technology to protect sensitive data.

9) Do not install or run any programs from unknown sources.

10) Do not use any computers and drivers that you do not trust (such as thumb drive and portable drive).

11) After logging into Internet banking, please make sure you've logged out before leaving your seat.

4. Protect your Internet banking user ID and login password

1) Do not disclose your Internet banking user ID or login password to anyone. If you suspect that someone has obtained your Internet banking login password, please immediately change it, or reset it through "Forget Password" on the personal Internet Banking login page.

2) Try not to use the same numbers or letters in the same order for Internet banking user ID and login password.

3) Try not to use the same password as other accounts, such as email password, QQ password, mobile phone password.

4) When setting the login password, please try to use both uppercase and lowercase letters and numbers, preferably including symbols.

5) Try not to use easily recognizable numbers as login passwords, such as phone numbers and birthdays.

6) Try to change the login password as often as possible by using "Change Login Password".

7) Keep your login password in mind and do not leave any physical records. If you forget your login password, please reset through the "Forget Password" on the personal Internet Banking login page.

8) Check and confirm that your computer browser will not store your login password. If you are using Microsoft Internet Explorer, please ensure that the browser's' “auto completion” function is disabled.

9) Bank staff will never inquire about your Internet banking user ID or login password. If you receive similar phone calls, text messages, or emails inquiring about your password information, please do not reply.

10) Do not entrust your Internet banking account to your relationship manager for purchasing our products on your behalf. If your relationship manager has to introduce products during your purchasing of our structured deposits and other products through Internet banking, you will need to go to the counter for audio and video recording before making the purchase.

11) Regularly clear the cache of your computer browser to ensure that your account information can be permanently deleted from the system records.

- Take the following steps to clear cache in Microsoft Internet Explorer, for reference only:

- Click “Tools”
- Select the “Internet” option
- Click “General”
- Select “Temporary Internet Files” and click “Delete Files”
- Click “Finish”

- Take the following steps to clear cache in Mozilla Firefox, for reference only:

- Click on "Tools" in the upper right corner of the browser ->"Clear Recent History" to open the “Clear History” window
- Select “All” for “Schedule a time to clear history”
- Click on “Details”, check “Browse, Download History”, “Forms & Search History”, “Cookies”, “Caching”, and “Active Logged in Sessions”
- Click “Clear Now”

5. Protect your password device (including tokens and registered mobile phone numbers)

1) Do not give your password device to anyone to keep, use or tamper with it.

2) Do not place your password device in an insecure place. When not in use, it should be properly stored.

3) Do not disclose your token serial number to anyone.

4) Do not disclose the Token OTP or SMS OTP (one-time password) to anyone, and do not enter it into any system other than our Internet banking.

5) If you have lost your password device, please bring your valid identity certificate to our branch in person to replace

a new token, or call our customer service hotline to apply for suspension of Internet banking.

6. Email and other protective measures

1) To prevent online fraud, please be cautious of the following:

- Any unknown email address
- Any unknown icon or image that may mislead you to a website or email address
- Any forged domain name appearing on the website of a bank or other financial institution
- Any links to forged websites
- Any table forms that appear in emails; or
- Any other attempts trying to mislead you to provide personal details, such as your Internet banking user ID and login password, account password, or any other sensitive information
- Other online scams

2) Never access our Internet banking through any link in the email.

3) When logging into our Internet banking, please enter our website by typing our domain name (www.ocbc.com.cn) through your browser. Please take necessary measures to prevent fraud and do not access our website through any other links. If you have any doubts, please call the customer service hotline to contact us.

4) It is recommended that you regularly delete spam and any emails of unknown origin. Do not open the mail sent to you by strangers.

5) If you find or think that there are any fraudulent emails or fraudulent websites directed at you, other customers of the bank, our bank or our group, please contact us immediately by calling our customer service hotline.

7. How to prevent "phishing"?

Phishing emails often use domains, logos, and images similar to those of our bank, which can easily cause confusion. If you receive an email requesting your account information in the name of our bank for security upgrade purposes, please do not reply. We would like to remind our customers and the public that our official domain name is www.ocbc.com.cn, and please be particularly alert to any websites that are similar to our domain.

If you have visited any such website or received any email, text message (SMS), or instant message (IM) from an unknown sender instructing you to disclose or submit sensitive information about your bank account, Internet banking user ID, login password, etc., do not reply and please immediately call our customer service hotline to notify us.

We will not ask customers for their personal information by email, short message (SMS), instant message (IM) and other forms, nor will we instruct customers to conduct specific transaction operations, nor will we advise customers to enter any other web pages than ours. Our bank always regards protecting your information security as our top priority.