Security Notice

Your security is our top priority!

Bank of China New York Branch uses a variety of security tools to keep your information safe. However, there are many safeguards that you can employ to further ensure the security of your information.

You should note that while we may contact you to discuss your account, we will never ask you to provide your login credentials over the phone or via email. We will never ask you for confidential information through email or regular mail. Do not provide any account or security information to anyone, unless you initiate a request with Bank of China.

Below is some information on how you can keep your account and sensitive personal information safe:

Avoid Social Engineering or "Phishing" Scams

Fraudsters may attempt to steal your personal or financial information through a variety of fraudulent techniques, including impersonating a bank employee on the phone or via email, with the intent of deceiving you into disclosing sensitive information, such as account numbers, your Social Security Number or online credentials. Often, these attempts may direct you to a "spoof" website that closely resembles a real website where you might be asked to provide sensitive information.

For the most recent scam alerts, visit the Federal Trade Commission, Consumer Information Scam Alerts page (https://www.consumer.ftc.gov/features/scam-alerts).

How to Prevent Phishing

Protect Your Personal Information

- Keep your personal and financial information protected. Never give out sensitive personal or financial information, such as your password or PIN via text message, email or phone.
- Do not disclose your personal information such as ID number, passport information, account number or other sensitive information to any suspicious or unverified person or website.
- Do not use personal information as your Access ID, Username or Password.
- Create difficult passwords that include letters and numbers, upper and lowercase letters, and special characters.
- Change your online banking login password regularly and do not write down your user ID and password on paper.

- Never share security question information such as pet names, schools you attended, birthdays or names of relatives.

Practice Proper Security Measures

- Avoid using public computers or public WiFi connections to access your Internet Banking.
- Always secure physical access to your computers or other devices.
- Be suspicious of any email with urgent requests for personal financial information, such as a threat of account closure if you fail to respond with sensitive information.
- Be careful of emails that are not personalized and may contain spelling errors, awkward syntax and phrasing, or poor visual design.
- Be careful of emails or pop-up windows telling you there is a problem requiring someone to remotely access your computer.
- Be careful of emails telling you not to call the bank and to only reply to the email.
- Instead of using links in an email to access a webpage, use bookmarks or paste the website address into the browser window directly. Make sure that "https" appears in the window to ensure proper encryption.

Be Aware of Your Account Activity

- Do not complete forms in email messages, such as customer service surveys, that ask for personal financial information in return for some financial benefit. Bank of China will never ask for information in this manner.
- Never agree to cash checks for strangers or otherwise act as a third party.
- Keep your contact information updated so we can get in touch with you as quickly as possible if we detect a potential fraud issue.
- Regularly log on to your online accounts and check your bank statements to ensure that all transactions are legitimate.
- Call Bank of China at (212) 935-3101 to confirm or verify any changes to your accounts.

In addition, you may want to visit our Security Alert page for a list of scams of which the bank is currently aware.

Protect Your Computer Against Malware

Malware, or malicious software, includes various programs known as viruses and spyware that are designed to infect your computer and then steal personal sensitive information.

How to Protect Your Computer

- Ensure that your browser is up-to-date and security patches are applied.
- Make sure your home computer has the most current anti-virus software.
- Avoid downloads from file sharing or social networking sites.
- Avoid downloads or email attachments from strangers.

- Do not click on suspicious pop-up ads, especially those asking for sensitive information.

User Guide

Points to Keep in Mind When Using Internet banking:

Do not access your online banking in public places such as an internet café or public library; unfamiliar computers may be installed with malicious monitoring programs to track your username and password. Moreover, your keyboard operation may be open to the stealthy observation of strangers.

When you login to online banking, please examine carefully the Previous Logon Time on the welcome page and make sure that it complies with your recollection of your last login time to avoid being confused or cheated by malicious email or website.

Please make sure the website address is correct before you login to the online banking system with the website address stored in the Favorites folder of your Internet Explorer.

How to identify fake or malicious websites: malicious emails or websites use different disguises to make them look legitimate. These disguises include: i) using the images of the genuine website ii) redirecting customers to the genuine website, and intercepting customers' data flow through the fake website during the communication between the customer and the bank iii) using a similar domain name which may be falsely recognized as the domain name of the genuine bank website.

Every time you finish with online banking, please always choose Exit on the top right-hand corner of the system and then close the browser.

If you need to leave your computer for any reason, please log out of online banking, by clicking Exit on the top right-hand corner of the system.

Please set a password for your computer to secure the information.

Please check your account balance before and after you finish the online transactions. Moreover, we suggest that you check your accounts regularly. If you have any trouble or discover any abnormal situation, please contact us through our customer service hotline.

What If I Suspect I Have Been a Victim of Fraud?

IF YOU SUSPECT YOU MAY BE THE VICTIM OF FRAUDULENT ACTIVITY CALL US AT (212) 935-3101

Bank of China will update this Security Notice periodically in an effort to follow best practices. Please read this security notice often to stay current with our latest security policies.