Best Practices for Online and Mobile Banking Users

Note to Customer

In this increasingly connected world, consumers must take proactive steps to safeguard their data. Channels (such as online and mobile banking) and tools (such as social networks) have become a part of our daily landscape. Due to increased risk of personal data being compromised and also increased probability for fraudulent transactions from these added conveniences, consumers should take the time to review the following recommendations for risk mitigation:

1. Be vigilant in reviewing your financial statements and monitoring your transactions. Develop the good habit of monitoring your financial accounts (e.g. bank, credit card, retirement etc.) at least weekly through online, mobile, voice banking or the ATM.
2. Never leave your computer, tablet or mobile phone unattended when using any Internet banking, mobile banking or other financial services.
3. After you have completed your Internet or mobile banking session, it is good practice to log off to ensure that the session is completed.
4. It is also good practice to lock your computer or mobile device whenever you plan to leave it unattended.
5. Never use publicly available information to create your password. Examples to avoid are common names or phrases, birthdates, social security numbers, etc. And of course, it goes without saying that you should never reveal your password to anyone.
6. Change your passwords frequently. Establish a routine where you change your password every few weeks to reduce the risk of a compromised account.
7. Avoid using password managers. Even though they may be convenient, password managers create a habit of not changing your passwords regularly and therefore make it easy to forget your passwords over time.
8. Never click on links or applications that you receive in e-mail, as those are common ways viruses, malware and malicious software are installed. If you get an e-mail with links purporting to be from your financial institution, please visit your financial institution's main website through your browser or call your financial institution to verify legitimacy.
9. Keep your passwords/pin confidential. Under no circumstance will you be asked to provide it to your financial institution.
10. While using the Internet, verify use of a secure session ("https://" and not "http://") in your browser's address bar. This is your indication that the data being transmitted between your browser and your financial institution's systems is securely encrypted.
11. Install anti-virus and anti-malware software. There are many good applications available for both your computer and your mobile device. Some are even free. Also, remember to keep these products updated regularly so they can be most effective.
12. If you have a mobile device such as a Smart phone or tablet, ensure that you install software capable of remotely wiping the device should it get stolen or lost.
13. The minute you suspect that your device is lost or stolen, notify your mobile carrier and suspend your service.

14. Install mobile software only from the Android Market or the Apple App Store and never a 3rd party site. Android users should read the permissions requested by the application carefully and determine whether the permissions coincide with the alleged function of the application.
15. Do not "jailbreak" your iPhone or "root" your Android to avoid unintentionally opening "backdoors" for malicious software.
16. Turn off wireless device services such as Wi-Fi, Bluetooth and GPS when they are not being used.
17. Avoid using unsecured public wireless connections. If you must, then use VPN software to provide a secure "tunnel" within which to work.
18. Be aware of the types of information that you post to social networking sites. Ensure you know who your "friends" are on such sites and do not accept "friend" requests from unverified parties. Statistics show that users of such sites experience a higher incidence of fraud. Use privacy settings on social networking sites to control who is able to access your personal information.
19. If your Internet and mobile banking service has extensive alerts available for your use, be sure to take advantage of these alerts. Once you set up the alerts you need, your financial institution's systems will notify you of activity on your accounts.
20. Checks and your financial statements all have your private financial information on them. Request electronic statements and use online bill pay whenever possible to reduce the paper trail and the risk of your account information being compromised.

If you suspect fraudulent activity or have doubts about the authenticity of a site or communication you have received via any medium, please call New Jersey Community Bank at 732-431-2265.