Online Banking
Security Procedures

Required Security Procedures - Business Online Banking Customers
Recommended Security Procedures - All Other Online Banking Customers

1. Installation of a security software suite that includes antivirus, anti-spyware, malware, and adware detection from a reputable vendor. You must keep the software up-to-date through an automatic update feature and configure it to perform recurring, automated complete system scans on a routine basis. This will help to protect a computer against known viruses, malware, and adware but you are advised that many viruses, malware, and adware programs are undetectable by antivirus software.
2. A firewall must be enabled at all times.
3. Restrictions and controls of user names and passwords. User names and passwords should not be shared, but should be protected and securely maintained. Allowing multiple access and failure to secure user names and passwords creates risks of identity theft and unauthorized access.
4. Frequent changing of passwords on a regular basis (at least every 90 days).
5. Creation of strong passwords that include a combination of mixed case letters, numbers, and special characters.
6. Daily review of your bank transaction histories. You must immediately report to the Bank any suspicious activity in your accounts. There is a limited recovery window and a rapid response may prevent additional losses.

Recommended Security Procedures - All Online Banking Customers

1. Routinely install all new software and hardware patches or use the automatic update feature when available. Ensure all your software, including its operating system and application software, are updated.
2. Be suspicious of unsolicited phone calls, visits, or email messages asking for sensitive information, offering deals that are “too good to be true”, or compensating you for assisting someone with moving funds.
3. Never reveal personal or financial information in email, and never respond to email solicitations or hyperlinks for this information.
4. Visit web sites by manually typing the URL into the browser’s address bar instead of clicking on a link in an email.
5. Never send sensitive information over the Internet before checking a web site's security (Verify “https:”).
6. Pay attention to the URL of a web site. Malicious web sites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net).
7. Verify any suspicious email or information request by contacting the company directly.

8. Do not use contact information provided on a website connected to a request; instead, check previous statements for contact information.
9. Check for known "Phishing" sites with groups such as the Anti-Phishing Working Group (http://www.antiphishing.org).
10. Immediately report suspected fraudulent activity to us and the proper authorities.
11. Strongly consider initiating ACH and wire transfers under dual control, with a transaction originator and a separate transaction authorizer.
12. Consider establishing daily transaction limits for all online transactions.
13. Whenever possible, do not use an unsecured wireless network for financial transactions.
14. Be cautious when accessing bank, brokerage, or other financial institution information at Internet cafes, public libraries, hotel business centers, or other public shared computers. If possible, be sure to clear browsing history, cookies, and temporary internet files as personal information can be retained in these shared systems.

PLEASE NOTE

These Security Procedures are for information purposes and are not intended to provide legal advice. This guidance should not be considered an exhaustive list of actions. Security threats change constantly. It is your responsibility to thoroughly investigate, implement, and update appropriate security protocols. You should engage professional technical advice to assure proper implementation of security procedures on an ongoing basis.