MOBILE BANKING SECURITY TIPS

Boston Private takes great care to safeguard the security of your non-public personal information.

As more people use their smartphones to manage bank accounts, new potential security risks arise. Through the security of your mobile device and the security practices you adopt for mobile banking, you can help mitigate the risk of online fraud, identity theft and protect your confidential information. The following are security tips and best practices to keep in mind when accessing your online banking account via a mobile device.

1. PASSWORD-PROTECT AND AUTO-LOCK YOUR PHONE
   In addition to the Online Banking application, your mobile device itself should be protected with a password to ensure that no one but you will be able to access your accounts. It is also recommended that you set your phone to auto-lock after a set number of minutes.

2. AVOID STORING CONFIDENTIAL INFORMATION ON YOUR MOBILE DEVICE
   Be cautious about what information you store on your mobile device. Saving your passwords on the device is not recommended. Regularly delete text messages and old calendar entries, clear your browser history, and delete files from your phone. In addition, be sure to clear sensitive information prior to disposing of, recycling, selling or giving away your mobile device.

3. TEXT MESSAGING
   Text messages are not secure and may be intercepted, which is why you should never send personal, identifying, or confidential information via text message.

4. DOWNLOADING APPLICATIONS
   Smartphone applications (apps) may contain malicious content. Be sure to check for a website certificate before downloading apps or files to your mobile device. Read carefully the application's privacy policy to be aware of what they are doing with your private information.

5. MOBILE DEVICE PERFORMANCE
   If you download an app and your phone starts performing differently (e.g., responding more slowly to commands or draining its battery more quickly), it could be a sign of malicious code, and it is probably best to take your device to your carrier.

6. REVIEW AND UTILIZE THE SECURITY OPTIONS AVAILABLE ON YOUR DEVICE
   Consider additional measures such as security software and antivirus solutions. Refer to your phone's user manual or contact your mobile carrier for more information on these features. Also, be sure to check for and download available software updates regularly on your phone, as these updates may include fixes to any security flaws.

7. PUBLIC WI-FI AND BLUETOOTH CONNECTION
   Do not connect to unsecured Wi-Fi when accessing Online Banking from your mobile device. Most smartphones and tablets can use both wireless Internet and a mobile provider's cellular network. Avoid using Bluetooth in public places to prevent attackers from taking advantage of that connection by obtaining information, or downloading malicious code to your mobile device.

8. LOG OUT COMPLETELY
   Be sure to log out completely every time you finish a mobile banking session. This will prevent someone from having easy access to your information if they get hold of your phone/mobile device.

9. INFORM YOUR SERVICE PROVIDER IF YOUR MOBILE DEVICE IS LOST OR STOLEN
   If your phone is lost or stolen, notify your service provider immediately so they can disable your device and reduce the risk of information being accessed. You may also want to consider logging into Online Banking from a computer to change your password for additional security of your data. Some mobile devices allow you to remotely wipe your personal data and restore your device to its factory state. Find out if your device has this option, and write down the steps for remotely wiping your device in case it's ever lost or stolen.

BOSTON PRIVATE STANDARD SECURITY CONTROLS FOR BUSINESS CLIENTS

For business accounts, we have established the following standard Mobile Banking security controls:

CLIENT VALIDATION, VERIFICATION AND LOGIN

Before clients can use Mobile Banking, they must have an active Online Banking enrollment.

If you are a client who has access to cash management functions (Approve ACH/Wire transactions), you will be required to use a hardware token. The hardware token is a small device that fits on a key ring and generates a random security code by pressing the button on the face of the token (35 seconds display time). Security token code will be required to access the "My ACH/Wires" tab to approve pending transactions.

DUAL-FACTOR AUTHENTICATION AT LOGIN

The Online Banking environment stores login and session statistics for all Online Banking clients. This information allows us to build a pre-login and post-login profile for each client, which can then identify unusual transactions or behavior based on the client's profile. Any activity that deviates from the client's historical profile is scored from based on the differences in behavior, with a high score at login indicating the highest difference in behavior. Having a high score can trigger the dual-factor authentica¬tion at login as described below. Dual factor authentication adds an extra layer of security by taking something the user knows (Access ID and passcode) and combining it with an additional form of authentication such as IP address or security challenge questions. If your score at login is high as noted above, in addition to Access ID and passcode, Clients without access to cash management functions (ACH/Wire) have the option of correctly answering two of the three security challenge questions originally selected at enrollment, or requesting a one-time use PIN to be sent to your e-mail address on file. Clients with cash management functions that have a high score at login will be required to enter a random security code generated from the token in addition to the Access ID and passcode.

DUAL-FACTOR AUTHENTICATION FOR CLIENTS WITH CASH MANAGEMENT FUNCTIONS (APPROVE ACH/WIRE PAYMENTS)

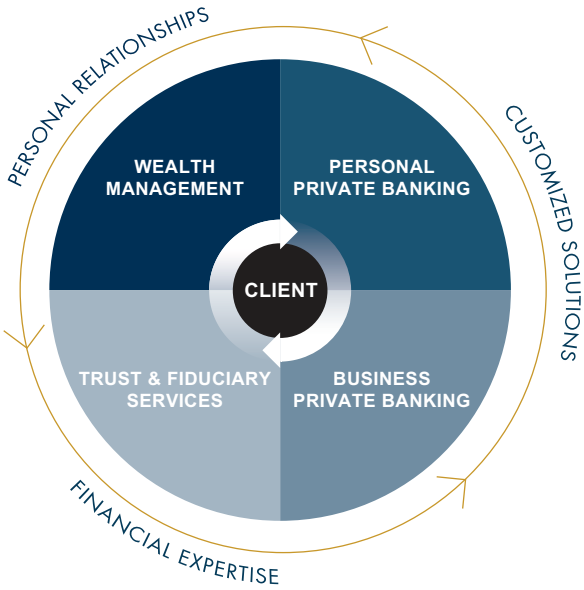
Authorized Clients will be required to enter a random number generated from the token in the My ACH/Wires tab to access the ACH/Wire payment Approval tabs (screens).

ABOUT BOSTON PRIVATE

Boston Private is a leading wealth management, trust, and private banking company with a national presence. Headquartered in Boston, we serve clients from our offices located in the major markets of Boston, San Francisco, San Jose, Los Angeles and Palm Beach.

We're committed to building a trusted relationship with each client and have the broad expertise to create comprehensive, custom solutions for their personal and business needs that are often interconnected.

As wealth creators, our clients value having one trusted resource that can help them address all of their wealth management, trust, and private banking needs.



BOSTON PRIVATE
WEALTH ▫ TRUST ▫ PRIVATE BANKING

V020817