

Online Banking Security Tips

Boston Private Bank & Trust Company takes great care to safeguard the security of your online banking transactions with us. As our customer, we believe you also have a stake in securing your online banking experience. There are two important roles that you can provide to help protect your confidential information and prevent online fraud and identity theft – the security of your computer and the security practices you adopt for online banking. The suggested guidelines below will help to secure your computer and online banking habits from potential viruses, worms, and malicious e-mail to reduce the risk of online fraud and identity theft. If you have questions on any of these tips, please contact your Private Banker at (617) 912-1900.

Computer Security

Secure your computer with the following practices to help prevent online threats such as viruses, worms, and spyware:

1. Use current versions of the operating system and applications on your computer and ensure that security patches are up-to-date. Most major software companies regularly release updates or patches to their software or operating systems to repair security problems. Some companies, such as Microsoft, offer you the ability to automatically receive these updates. All other vendor software updates can typically be found on their website.
2. Ensure that your computer has anti-virus and anti-spyware protection and make sure these programs are updated regularly. Keeping these programs up-to-date helps protect you from current virus threats and spyware used to gather confidential information such as passwords, credit card numbers and social security numbers. Also, scan your computer for viruses and spyware at least once per month.

If you currently do not have an anti-virus program installed on your PC, please visit these popular anti-virus vendor sites below:

www.symantec.com

www.mcafee.com

www.trendmicro.com

3. Use a personal firewall to prevent intruders from compromising your computer. Every computer system connected to the internet is at risk of an attack by an unauthorized intruder. Personal firewalls serve as a protective barrier between your computer, the internet and this risk. Personal firewalls can be either hardware or software and are a big part of improving the security on your computer.

BOSTON PRIVATE BANK
& **TRUST COMPANY**

Member
FDIC

www.bostonprivatebank.com



4. If you use wireless networking, secure the network with the following practices to reduce the risk of being hacked by a wireless intruder:

- Ensure wireless encryption is enabled and the encryption level selection is at least 128-bit encryption which provides a stronger encryption level.
- Change the default administrator ID and/or password provided by your wireless equipment (e.g. wireless router) manufacturer.
- Change the default wireless network name provided by your wireless equipment manufacturer so a hacker can't use the default to try to access your network. Select a name that is equivalent to a strong password.
- Consider the option that disables the broadcast of your wireless network name over the air at regular intervals. Broadcasting the name is unnecessary and increases the likelihood that an unwelcome neighbor or hacker will try to log in to your network. Also consider the option to limit access to your wireless network to only your computer device(s). Consult your wireless equipment manufacturer for assistance on how to select these options.
- Beware that connecting to an unprotected network may result in an intruder gaining unauthorized access to your computer. It is possible for someone to monitor your internet connection and even record your password(s).

5. Do not download or run software from unknown sources. This applies both to software available on the Internet and sent via e-mail. Installing software from unknown sources increases the probability of installing malicious code or accepting computer viruses. Also, exercise caution when trading files with other users as these may also contain software.

6. Power off your computer when it is not in use.

Online Security

Adopt the following practices to help protect your online banking and confidential information from fraud and identity theft:

1. Use strong password construction by adopting the following principles:

- At least eight (8) characters in length if application allows.
- Contains at least one upper and one lower case alpha character (e.g., a-z, A-Z).
- Contains at least one digit and one special character if supported.
- Is not a word in a standard dictionary (English or foreign) or publicly known slang, dialect or jargon.
- Is not based on personal information, family names, pet names, the Bank's name or geographic location, etc.
- Does not contain ascending or descending characters, digits (e.g., abcd, 4321), repeating characters, or digits (e.g. aaaa, 3434).

- Try to create a password that can be easily remembered. One technique is to create a password based on a phrase. For example, the phrase might be “This May Be One Way To Remember” and the password could be “TmB1w2R!”.
2. Change your password regularly, at least every 45 days.
 3. Never share your password with anyone.
 4. Never write your password down or store it online.
 5. Use a different password for each online system you access.
 6. Never use the “remember my ID and password” option on your computer.
 7. Use your own computer when accessing online banking systems and never leave it unattended during an online banking session. Internet kiosks, cyber cafes, and other public use computers are not as secure as your own computer and should not be used to access personal financial information.
 8. Practice safe browsing:
 - Do not download freeware or shareware; these programs often contain spyware or malicious applications.
 - Do not click on links or buttons in pop-up advertisement windows.
 - Use a pop-up blocker.
 9. Conduct financial transactions only with trusted and secure sites. When shopping or banking online, it is important to make sure you are utilizing a secure connection. You can check for a secure site by looking at the web site address. Look for an “s” to follow http (i.e. https://). Also, many web browsers show an image of a padlock to indicate a secure connection. You can verify secure sites by “double-clicking” on the padlock icon located at the bottom of your browser application and reading the site info in the box that appears.
 10. Always log off of your on-line banking session and close your browser.

E-Mail Security

E-mail over the Internet is inherently unsecured. Adopt the following practices to help minimize the risk of being the victim of fraudulent e-mail scams.

1. Boston Private Bank provides Secure Mail, a secure encrypted e-mail service, to communicate confidential e-mail information between the Bank and its clients.
 - When communicating confidential e-mail to us, such as account numbers and social security numbers, always use Secure Mail service. Never communicate confidential information via normal Internet e-mail.
 - Boston Private Bank will always utilize Secure Mail when communicating confidential e-mail information to you.

- In addition to Secure Mail, you may also communicate confidential information to us by phone to your Bank representative, by mail, via our online banking secure messaging feature, or visit one of our offices.
 - To learn how to use our Secure Mail Service, please visit our website www.bostonprivatebank.com and click on the “Secure Mail” link at the bottom of our homepage.
2. Do not open e-mail or attachments from unknown senders, especially executable attachments.
 3. Be aware of e-mail scams and phishing. Phishing is an e-mail that falsely claims to come from a known sender. It typically provides a link to a phony website where you are asked to supply your confidential information. Never respond to unsolicited e-mail asking for confidential information. Avoid clicking on links provided in emails. It is better to type the address directly into your browser’s address bar.
 4. Use e-mail filtering software to screen for unsolicited email (spam). Consider installing a software tool that will assist in filtering spam from your email in-box. These tools can help reduce the likelihood of a virus or worm installing a malicious program on your computer or receiving e-mail phishing attempts.

BOSTON PRIVATE BANK
& TRUST COMPANY

Member
FDIC

www.bostonprivatebank.com

