

Business Electronic Banking Safety Best Practices

- The **best protection against fraud is to conduct all online banking activities on a stand-alone, locked down computer** that does not have access to email or websites other than your online banking sites.
- **Be suspicious of emails** sent from a financial institution, government office or other agency where the sender is requesting account information, account verification, or banking access credentials such as usernames, passwords, PIN codes, or similar information. Opening attachments or clicking on web links can expose your computer to malicious codes intended to hijack your banking information.
- **Never share username** and/or password information for online services with third party providers.
- **Install a dedicated, regularly maintained firewall**, especially if you have broadband, cable or DSL access to the internet. The firewall will limit the potential for unauthorized access to your network and computers.
- **Install commercial anti-virus and desktop firewall software** on all computers. Free software may not always provide protection against recent threats like an industry standard product will.
- Maintain and **update your anti-virus and security protection** software regularly.
- **Maintain operating system and key application updates** regularly - most offer automatic update options.
- **Install** spyware detection programs.
- **Clear the browser cache** before starting an online banking session to eliminate copies of the web pages that may have been stored in your hard drive - instructions for doing this can be found in your browser's preferences menu.
- **Create a safe password for your online banking credentials** - make sure it is at least 10 characters in length and includes a combination of numbers, mixed case letters and special characters.
- **Prohibit the use of "shared" usernames** and passwords for online banking access. Require individual user accounts for each employee.
- Use a **different password for each website** that is accessed and change the passwords a few times each year.
- **Limit the access rights** of additional users accessing your business accounts online to prevent possible downloading of malware or viruses.
- **Use secure hiring practices, including background checks**, for employees who will have access to important data and online banking.
- **Review the activity of your online banking administrators and employees.**
- Consider hiring qualified third parties to conduct **audits and risk assessments** of your data security.
- **Verify the online banking session is secure** by looking for the https (not http) in the browser.
- **Never save your username and password** for automatic login to your online banking session.

- **Never leave a computer unattended**, especially when using online banking or investment services.
- **Close all other applications** and browser windows before initiating online banking.
- **Never access your bank account information publicly** - internet cafes, public libraries, or other publicly accessible computers - unauthorized software may have been installed to capture account access information.
- **Make backup copies of important business information.**
- **Control physical access** to your computers and network equipment.
- **Always notify your bank immediately** if you feel your account information has been compromised in any way. This is especially important when suspicious account activity includes ACH or wire transactions - there is a limited recovery window for these types of transactions.
- **Understand and use the Bank's security features** including multi-factor authentication, dual control for ACH and wire transfer processing, limit access for users within each company and separate user account for an administrator.
- **Share these best practices** with others who work in your business and **train employees in data security.**
- **Continue to educate yourself and your staff on data security.**
Some current information can be found at the websites of the Federal Communications Commission: <http://www.fcc.gov/cyberforsmallbiz> and the Department of Homeland Security: http://www.dhs.gov/sites/default/files/publications/FCC%20Cybersecurity%20Planning%20Guide_1.pdf