First American Bank

Ca$hTrac

Security Best Practices

First American Bank would like to make you aware of some "Best Practice Techniques" that may help prevent unauthorized access through Online Banking to your accounts. It is your responsibility to keep your computer free of malicious programs. You would be liable for any financial losses should your operating system become infected and allow a perpetrator to take over your machine For more detailed guidance, we suggest you visit the official FBI website at http://www.fbi.gov/.

BEST PRACTICE TECHNIQUES

- Ultimately the best way to insulate your business against fraudulent online banking transactions is to use a dedicated PC that is not used for other online activity. Implement white listing methods to prevent the system from going to any site/address that does not have a documented business need. This would include, web browsing, social networking and most importantly email.

- Install a security software suite that includes anti-virus, anti-spyware, malware and adware detection, from a reputable vendor. 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.

- Ensure that the anti-virus and security software and mechanisms are installed on all computer workstations and laptops that are used for online banking and payments. This would include personal home computers if they are used to access your commercial online banking system.

- Install a firewall on your computer which will block unauthorized access.

- Implement block/black lists and enforce them on the network perimeter.

- Monitor log files, especially proxy server logs, for unauthorized/suspicious Internet connections coming to and leaving the network.

- Run a virus scan on all emails at the Network level and not from the desktop. Once an infected email is opened from your desktop, it's too late.

- Never click on a URL within an email. A better practice is to enter the URL yourself.
- Monitor and reconcile your accounts daily. Keep all account information secure.
- Never leave your PC unattended when logged into a secure site. Set the computer to automatically lock after a set period of inactivity, e.g. 15 minutes.
- Protect your passwords. *Never have password information written down.*
- Do not share user IDs.
- Do not allow your computer or web browser to save your login names or passwords.
- Always use dual control when processing any payment entries. One individual to initiate the entry and a second individual to approve the entry.
- Be aware of changes to the look of your online banking login screens. If the screens are unfamiliar or you are prompted multiple times for a security code, contact us immediately.
- Utilize a security expert to test your network or run security software that will aid you in closing known vulnerabilities.
- Educate users on good cyber security practices to include how to avoid having malware installed on a computer.
- Be suspicious of emails and text messages purporting to come from First American Bank or government agencies requesting verification of information. Do not click on any links provided, always type in www.firstambank.com in your internet browser bar to access our site.

For more information,
please visit our website at **www.FirstAmBank.com**
or call us at **847-952-3701**.

FIRST AMERICAN BANK