



Figures from the FBI's Internet Crime Complaint Center (IC3) show the cost of Internet fraud is significant and growing with the current trend of targeting businesses and public agencies. For this reason, FirstBank offers the following tips originally issued by the FBI, FS/ISAC and NACHA to aid you in protecting your banking transactions from fraud and compromise.

1. Initiate ACH and wire transfer payments under dual control.
2. Ensure that all anti-virus and security software and mechanisms for all networks and personal computers used for Internet Banking are robust and up-to-date.
3. Install a dedicated, actively managed firewall to limit the potential of unauthorized access to the network or company's computers.
4. Restrict functions for computer workstations that are used for online banking and payments. If a computer is used for online banking functions, do not use it to browse the Internet, social networking or email.
5. If possible, conduct online banking and payments activity from a dedicated computer that is not connected to an internal network.
6. Monitor and reconcile accounts daily.
7. Perform out of band authorization of high value transactions via fax or phone .
8. Limit administrative rights on users' workstations to help prevent the inadvertent downloading of malware or other viruses.
9. Prohibit the use of shared usernames and passwords for online banking systems.
10. Use strong passwords to deter less sophisticated attacks and change the password a few times a year.
11. Never leave a computer unattended while using an online banking service.
12. Always logoff online banking when your business is complete. Simply closing the browser does not terminate the online banking session.
13. Use a unique password for online banking and never use this password on other sites such as social networking sites.

Report Internet crimes at www.ic3.gov.

Visit www.onguardonline.gov for additional advice and details.