



Recommendations to Help Protect your Organization against Funds Transfer Fraud

In the last several months the online criminal world has shifted from primarily targeting individuals to an escalated increase in targeting corporations. Law enforcement agencies are all reporting an increase in funds transfer fraud involving capture of valid online banking credentials belonging to small and medium sized businesses.

Usually the compromise of the online banking credentials is done via a “spear phishing” e-mail which directly names the recipient correctly and contains either an infected file or a link to an infectious Web site. Once the user opens the attachment, or clicks the link to open the Web site, malware is installed on the user’s computer which consists of a keystroke logger, which gathers the user’s corporate online banking credentials.

Six figure losses are common as electronic payments from your accounts are sent to “money mules”, who then wire transfer the funds out of the country.

Below you will find some recommendations to help you protect your organization against Funds Transfer Fraud.

Account controls:

- **Reconcile all banking transactions on a daily basis.**
- **Initiate ACH and wire transfer payments under dual control.**

Employ Best Practices to secure computer systems including but not limited to:

- **Perform all online banking activities from a stand-alone, hardened and completely locked down computer system from which e-mail and Web browsing are not possible.**
- **Be suspicious of e-mails claiming to be from a financial institution, government department or other agency requesting information, account verification, password, PIN codes and similar information.**

- **Opening file attachments of suspicious mail or clicking on web links could expose your system to malicious code that could hijack your computer.**
- **Install a dedicated, managed firewall, especially if you have a broadband or dedicated connection to the Internet.**
- **Create a strong password that includes a combination of mixed letters and numbers.**
- **Prohibit the use of “shared” usernames and passwords for online banking.**
- **Require the use of a different password for each website accessed.**
- **Change passwords several times a year.**
- **Limit administrative rights.**
- **Install commercial anti-virus and desktop firewall software on all computer systems. Free software may not provide the protection needed that an industry standard product can.**
- **Ensure that virus protection and security software are updated regularly.**
- **Consider installing spyware detection programs.**
- **Clear your browser cache before starting an online banking session. This will eliminate copies of web pages that have been stored on the hard drive.**
- **Verify that you are using a secure session (https not http) in the browser.**
- **Do not use automatic login features that save usernames and passwords for online banking.**
- **Do not leave a computer unattended while using online banking.**
- **Do not access your online banking at Internet Cafes, public libraries etc.**
- **Sign up for Restricted IP Address Service with your financial institution. This service limits communication to only approved IP addresses.**
- **Insist that your financial institution utilize old-fashioned physical controls for verification of originated files.**

Bank Where  Live

5999 Delaware P.O. Box 26017 Beaumont, TX 77720-6017 | 409.861.7200 1.866.427.9306

communitybankoftx.com Member FDIC  Equal Housing Lender