Reducing the Risk of Corporate Account Takeover

A vast majority of cyber threats begin with the thieves compromising the computers of Business Account Holders. Perpetrators often monitor the customer's email messages and other activities for days or weeks prior to committing the crime. Businesses are most vulnerable to this kind of theft just before a holiday when key employees are often on vacation. Another risk period is on a day the Business office is relocating or installing new computer equipment. It is important and necessary to follow established security practices. Below are examples of deceptive ways criminals contact account holders:

- The FDIC does NOT directly contact bank customers (especially related to ACH and Wire transactions, account suspension, or security alerts), nor does the FDIC request bank customers to install software upgrades. Such messages should be treated as fraudulent and the account holder should permanently delete them and not click on any links.
- Messages or inquiries from the Internal Revenue Service, Better Business Bureau, NACHA, and almost any other organization asking the Business to install software, provide account information or access credentials is probably fraudulent and should be verified before any files are opened, software is installed, or information is provided.
- Phone calls and text message requesting sensitive information are likely fraudulent. If in doubt, account holders should contact the organization at a phone number obtained from a different source (such as the number they have on file, that is on their most recent statement, or that is from the organization's website). Account holders should not call phone numbers (even with local prefixes) that are listed in the suspicious email or text message.

Here are some ways to reduce your risk of theft:

- Provide continuous communication and education to employees using online banking systems. Providing enhanced security awareness training will help ensure employees understand the security risks related to their duties;
- Update anti-virus and anti-malware programs frequently;
- Update, on a regular basis, all computer software to protect against new security vulnerabilities (patch management practices);
- Communicate to employees that passwords should be strong and should not be stored on the device used to access online banking;
- Adhere to dual control procedures;
- Use separate devices to originate and transmit wire/ACH instructions;
- Transmit wire transfer and ACH instructions via a dedicated and isolated device;
- Practice ongoing account monitoring and reconciliation, especially near the end of the day;
- Adopt advanced security measures by working with consultants or dedicated IT staff; and
- Utilize resources provided by trade organizations and agencies that specialize in helping small businesses. See Appendix A for a list of resources.

To be prepared should such fraud occur, business should prepare an incident response plan. Each business is unique and should prepare its own incident response plan. A general template should include:

- The direct contact number of key bank employees (including after hours numbers);
- Steps the business should consider to limit further unauthorized transactions, such as:
    - Changing passwords;
    - Disconnecting computers used for internet banking; and
    - Requesting a temporary hold on all other transactions until out-of-band confirmations can be made;
- Information the business will provide to assist the bank in recovering their money;
- Contacting their insurance carrier; and
- Working with computer forensic specialists and law enforcement to review appropriate equipment.

Thank you for taking the time to review this important information. Please feel free to contact us at Basile State Bank with any questions or concerns.

Basile State Bank 337-432-6646

Appendix A: Resources for Business Account Holders

- The Better Business Bureau's website on Data Security Made Simpler: http://www.bbb.org/data-security;
- The Small Business Administration's (SBA) website on Protecting and Securing Customer Information:

http://community.sba.gov/community/blogs/community-blogs/business-law-advisor/how-small-businesses-can-protect-and-secure-customer-information;

- The Federal Trade Commission's (FTC) interactive business guide for protecting data: http://www.ftc.gov/bcp/edu/multimedia/interactive/infosecurity/index.html;
- The National Institute of Standards and Technology's (NIST) Fundamentals of Information Security for Small Businesses: http://csrc.nist.gov/publications/nistir/ir7621/nistir-7621.pdf;
- The jointly issued "Fraud Advisory for Businesses: Corporate Account Takeover" from the U.S. Secret Service, FBI, IC3, and FS-ISAC available on the IC3 website (http://www.ic3.gov/media/2010/CorporateAccountTakeOver.pdf) or the FS-ISAC website (http://www.fsisac.com/files/public/db/p265.pdf); and
- NACHA – The Electronic Payments Association's website has numerous articles regarding Corporate Account Takeover for both financial institutions and banking customers: http://www.nacha.org/c/Corporate_Account_Takeover_Resource_Center.cfm .