Recommendations to Business Customers to Prevent Corporate Account Takeovers

Corporate Account Takeover is a form of corporate identity theft where a business' online credentials are stolen by malware. Criminal entities can then initiate fraudulent banking activity.

Attacks today are typically perpetrated quietly by the introduction of malware through a simple email or infected website. For a business that has low resistance to such methods of attack, the malware introduced onto its system may remain undetected for weeks or even months.

Account Controls:

Create a secure financial environment by dedicating one computer exclusively for online banking and cash management activity.

- Dual Control – One user uploads or enters the ACH file information. Another user must approve the file for release. . (Cross Keys Bank can assist you with setting up this additional form of security; it requires two different users to approve all ACH Transactions).
- Security Tokens – Cross Keys incorporates Multifactor Authentication for Cash Management Customers. This includes Security Questions and RSA Tokens. Keeping these items secure will provide another layer of protection.
- Reconciliation of all banking transactions on a daily basis.
- Report Suspicious Activity - Ongoing monitoring and timely reporting of suspicious activity are crucial to deterring or recovering from these frauds.

An employee whose computer becomes infected can infect the entire network. For example, if an employee takes a laptop home and accidentally downloads credential-stealing malware, criminals could gain access to the business's entire network when the employee connects again at work.

Employ best practices to secure computer systems in your business including but not limited to:

- Be suspicious of e-mails purporting to be from a financial institution, government department or other agency requesting account information, account verification or banking access credentials such as usernames, passwords, PIN codes and similar information. Opening file attachments or clicking on web links in suspicious emails could expose the system to malicious code that could hijack their computer.
- Install a dedicated, actively managed firewall, especially if they have a broadband or dedicated connection to the Internet, such as DSL or cable. A firewall limits the potential for unauthorized access to a network and computers.
- Create a strong password with at least 10 characters that include a combination of mixed case letters, numbers and special characters.

- Prohibit the use of "shared" usernames and passwords for online banking systems. Use a different password for each website that is accessed.
- Change the password a few times each year.
- Never share username and password information for Online Services with third-party providers. (Password Program)
- Limit administrative rights on users' workstations to help prevent the inadvertent downloading of malware or other viruses.
- Install commercial anti-virus, anti-malware and desktop firewall software on all computer systems. Free software may not provide protection against the latest threats compared with an industry standard product.
- Ensure virus protection and security software are updated regularly.
- Ensure computers are patched regularly particularly operating system and key application with security patches. It may be possible to sign up for automatic updates for the operating system and many applications.
- Install Spyware detection programs.
- Clear the browser cache before starting an Online Banking session in order to eliminate copies of web pages that have been stored on the hard drive. How the cache is cleared will depend on the browser and version. This function is generally found in the browser's preferences menu.
- Verify use of a secure session (**https** not http) in the browser for all online banking.
- Avoid using an automatic login features that save usernames and passwords for online banking.
- Never leave a computer unattended while using any online banking or investing service.
- Never access bank, brokerage or other financial services information at Internet cafes, public libraries, etc. Unauthorized software may have been installed to trap account number and sign on information leaving the customer vulnerable to possible fraud.
- Familiarize yourself with the institution's account agreement and with the customer's liability for fraud under the agreement and the Uniform Commercial Code as adopted in the jurisdiction.

Block access to unnecessary or high-risk websites. At a minimum, a business should prevent access to websites that employees should not visit during work hours. Common sites that carry high-risk include adult entertainment, online gaming, social networking and personal email.

Remember the analogy: An unsecure computer is the same as an unlocked house. If you fail to lock your house, then you have a significant chance of losing your valuables.

For more information please review [NACHA's Corporate Account Takeover Resource Center]