Corporate Account Takeover

Takeover is an evolving electronic crime typically involving the exploitation of businesses of all sizes, especially those with limited computer safeguards and minimal or no disbursement controls for use with their bank's online business banking system. These businesses are vulnerable to theft when cyber thieves gain access to its computer system to steal confidential banking information in order to impersonate the business and send unauthorized wire and ACH transactions to accounts controlled by the thieves. Municipalities, school districts, large nonprofit organizations, corporate businesses, and any customers that perform electronic transfers are potential targets. Losses from this form of cyber-crime range from the tens of thousands to the millions with most of these thefts not fully recovered. These thefts have affected both large and small banks.

This type of cyber-crime is a technologically advanced form of electronic theft. Malicious software, which is available over the Internet, automates many elements of the crime including circumventing one-time passwords, authentication tokens, and other forms of multi-factor authentication. Awareness of online threats and education about common account takeover methods are helpful measures to protect against these threats. However, due to the dependence of banks on sound computer and disbursement controls of its customers, there is no single measure to stop these thefts entirely. Multiple controls or a "layered security" approach is required.

BASIC ONLINE SECURITY PRACTICES

o Education is Key – Train your employees
o Secure your computer and networks
o Limit Administrative Rights – Do not allow employees to install any software without receiving prior approval.
o Install and Maintain Spam Filters
o Surf the Internet carefully
o Install & maintain real-time anti-virus & anti-spyware desktop firewall & malware detection & removal software. Use these tools regularly to scan your computer. Allow for automatic updates and scheduled scans.
o Install routers and firewalls to prevent unauthorized access to your computer or network.
o Change the default passwords on all network devices.
o Install security updates (patches) to operating systems and all applications as they become available.

o Block Pop-Ups
o Use strong password policies
o Do not open attachments from e-mail -Be on the alert for suspicious email
o Do not use public Internet access points
o Monitor and Reconcile Bank Accounts Daily, especially near the end of the day
o Note any changes in the performance of your computer Dramatic loss of speed, computer locks up, unexpected rebooting, unusual popups, etc.
o Make sure that your employees know how and to whom to report suspicious activity to at your Company & the Bank

Contact the Bank if you:

– Suspect a Fraudulent Transaction
– If you are trying to process an Online Wire or ACH Batch & you receive a maintenance page.
– If you receive an email claiming to be from the Bank and it is requesting personal/company information

Incident Response Plans
Since each business is unique, customers should write their own incident response plan. A general template would include:

1. The direct contact numbers of key bank employees (including after hour numbers);
2. Steps the account holder should consider limiting further unauthorized transactions, such as:

o Changing passwords;
o Disconnecting computers used for Internet banking; and
o Requesting a temporary hold on all other transactions until out-of-band confirmations can be made;

3. Information the account holder will provide to assist the bank in recovering their money;
4. Contacting their insurance carrier; and
5. Working with computer forensic specialists and law enforcement to review appropriate equipment.

Resources for Business Account Holders

1. The Better Business Bureau's website on Data Security Made Simpler:
http://www.bbb.org/datasecurity
2. The Small Business Administration's (SBA) website on Protecting and Securing Customer Information:
http://community.sba.gov/community/blogs/community-blogs/business-law-advisor/howsmallbusinesses-
can-protect-and-secure-customer-information
3. The Federal Trade Commission's (FTC) interactive business guide for protecting data:
http://www.ftc.gov/bcp/edu/multimedia/interactive/infosecurity/index.html
4. 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
5. 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
6. 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