What is Corporate Account Takeover?

Corporate Account Takeover(CATO) is a fast growing electronic crime where thieves typically use some form of malware to obtain login credentials to Corporate Online Banking accounts and fraudulently transfer funds from the account(s).

Malware- Short for malicious software, is software designed to infiltrate a computer system without the owner's informed consent.

Malware includes computer viruses, worms, Trojan horses, spyware, dishonest adware, **crimeware**, most **rootkits**, and other malicious and unwanted software. Domestic and International Wire Transfers, Business-to-Business ACH Payments, Online Bill Pay and electronic payroll payments have all been used to commit this crime.

How does it work?

Criminals target victims by scams. Victim unknowingly installs software by clicking on a link or visiting an infected Internet site. Fraudsters began monitoring the accounts. The victim logs on to their Online Banking and fraudsters collect login credentials. Fraudsters wait for the right time and then depending on your controls – they login after hours or if you are utilizing a token they wait until you enter your code and then they hijack the session and send you a message that Online Banking is temporarily unavailable.

Statistics- Where does it come from?

Malicious websites (including Social Networking sites)

Email

P2P Downloads (e.g. LimeWire)

Ads from popular web sites

Web-borne infections:

According to researchers in the first quarter of 2011, 76% of web resources used to spread malicious programs were found in five countries worldwide ~ United States, Russian Federation, Netherlands, China, & Ukraine.

Rogue Software/Scareware

Form of malware that deceives or misleads users into paying for the fake or simulated removal of malware. This has become a growing and serious security threat in desktop computing.

Mainly relies on social engineering in order to defeat the security software.

Most have a **Trojan Horse** component, which users are misled into installing.

Browser plug-in (typically toolbar).

Image, screensaver or ZIP file attached to an e-mail.

Multimedia codec required to play a video clip.

Software shared on peer-to-peer networks

A free online malware scanning service

Phishing

Criminally fraudulent process of attempting to acquire sensitive information (usernames, passwords, credit card details) by masquerading as a trustworthy entity in an electronic communication.

Commonly used means:

Social web sites

Auction sites

Online payment processors

IT administrators

E-mail Usage

CAUTION!

What may be relied upon today as an indication that an email is authentic may become unreliable as electronic crimes evolve. This is why it is important to stay abreast of changing security trends. Some experts feel e-mail is the biggest security threat of all.

It's the fastest, most-effective method of spreading malicious code to the largest number of users. It's also a large source of wasted technology resources.

Examples of corporate e-mail waste:

Electronic Greeting Cards

Chain Letters

Jokes and graphics

Spam and junk e-mail

What can Businesses do to Protect?

Education is Key – Train your employees

Secure your computer and networks

Limit Administrative Rights -Do not allow employees to install any software without receiving prior approval.

Install and Maintain Spam Filters

Surf the Internet carefully

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.

Install routers and firewalls to prevent unauthorized access to your computer or network. Change the default passwords on all network devices.

Install security updates to operating systems and all applications as they become available.

Block Pop-Ups

Do not open attachments from e-mail -Be on the alert for suspicious emails.

Do not use public Internet access points

Reconcile Accounts Daily

Note any changes in the performance of your computer-

Dramatic loss of speed

Computer locks up

Unexpected rebooting

Unusual popups

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.

Bank Contact Information:

Leigh Ann Ulmer
318-435-7535 ext 126 or

Jessica Johnston
318-435-7535 ext 125