*TRAINING FOR AMERICAN MOMENTUM BANK CLIENTS*

# Corporate Account Takeover & Information Security Awareness

AMERICAN MOMENTUM BANK

The information contained in this session may contain privileged and confidential information.

This presentation is for information purposes only. Before acting on any ideas presented in this session; security, legal, technical, and reputational risks should be independently evaluated considering the unique factual circumstances surrounding each institution.

No computer system can provide absolute security under all conditions.

Any views or opinions presented do not necessarily state or reflect those of **American Momentum Bank** or any other entity.

# What will be covered?

- What is Corporate Account Takeover (CAT)?
- How does it work?
- Statistics
- Current trend examples
- What can we do to protect?
- What can businesses do to protect?

# What is Corporate Account Takeover?

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*, malware 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 begin monitoring the accounts
- Victim logs on to their Online Banking
- 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)
  - E-mail
  - 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 5 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.
- 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 (user names, 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.

# E-mail Usage Continued…

- Some experts feel e-mail is the biggest security threat of all.
- The fastest, most-effective method of spreading malicious code to the largest number of users.
- 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 we can do to PROTECT?

- Provide Security Awareness Training for our employees and clients.
- Review our contracts. Make sure that both parties understand their roles and responsibilities .
- Make sure our clients are aware of basic online security standards.
- Stay informed. Attend webinars/seminars and other user group meetings.
- Develop a layered security approach

# Layered Security

**Layered Security Approach**

- **Monitoring of IP addresses**
- **New user controls – Administrator can create a new user; bank must activate user.**
- **Dual control processing of files on separate devices – recommended**
- **Fax or out of band confirmation**
- **Secure browser key**
- **Pattern recognition software**

# 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 and maintain real-time anti-virus, anti-spyware, desktop firewall, malware detection and 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

# What can Businesses do to Protect?

- Do not open attachments from suspicious e-mails
- Do not use public Internet access points when working on confidential matters
- Reconcile accounts daily
- Note any changes in the performance of your computer
  - Dramatic loss of speed, computer locks up, unexpected rebooting, unusual pop-ups, etc.
- Make sure that your employees know how and to whom to report suspicious activity to at your company and the Bank

<u>Contact the Bank if you:</u>

>Suspect a fraudulent transaction

>If you are trying to process an online wire or ACH batch and you receive a maintenance page.

>If you receive an e-mail claiming to be from the bank and it is requesting personal/company information.