Edmonton State Bank

Corporate Account Takeover & Information Security Awareness

What will be covered?

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

What is corporate account takeover?

- Corporate Account Takeover is a form of business identity theft where cyber thieves gain control of a business' bank account by stealing employee passwords and other valid credentials. Thieves can then initiate fraudulent wire and ACH transactions to accounts controlled by the thieves.

What is 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.

Malware usage

- Domestic and International Wire Transfers
- Business to Business ACH payments
- Online Bill Pay and electronic payroll payments

How does malware work?

- Criminals target victims by scams
- Victim unknowingly installs software by clicking on a link or visiting an infected Internet site.
- Fraudsters begin monitoring 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.

Malware statistics

Where does malware come from?

- Malicious websites (including social networking sites)
- Email
- P2P downloads
- Ads from popular web sites

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 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 email
  - 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

Email Usage

- 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.

Email Usage

- Some experts feel email 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 email waste:
  - Electronic greeting cards
  - Chain letters
  - Jokes and graphics
  - Spam and junk email

What can we do to protect?

- Provide security awareness training for our employees and clients
- Review our contracts, make sure 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

- Monitoring IP addresses
- New user controls – Administrator can create a new user; bank must activate user
- Dual control processing of files on separate devices
- 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 networks
- Limit administrative rights
  - Do not allow employees to install any software without receiving approval

Business protection

- Install and maintain real-time anti-virus, anti-spyware, desktop firewall, malware detection and removal software.
  - Use these tools regularly to scan your computers, allow for automatic updates and scheduled scans

Business protection

- 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
- Do not open attachments from suspicious emails
- Do not use public internet access points when working on confidential matters
- Reconcile accounts daily
- Note any changes in the performance of your computer

Business protection

- Make sure that your employees know how and to whom to report suspicious activity to at your company and the Bank
- Contact the Bank if you:
  - 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 email claiming to be from the bank and it is requesting personal / company information.