PROTECT YOUR ACCOUNTS

CORPORATE CUSTOMER ACCOUNT TAKEOVER & INFORMATION SECURITY

2024

First American Bank AND TRUST

A BANKING TRADITION SINCE 1910

Security Awareness Training

- **What is Corporate Account Takeover (CATO)?**
- **How does it work?**
- **Types of Security Threats & Countermeasures**
  - Malware
  - Viruses
  - Spyware
  - Rogue Software/Scareware
  - Phishing
  - E-mail Usage
  - Hoaxes
- **Where does it come from?**
- **What can Businesses do to PROTECT!**
- **Communication**
- **Tips for Mobile Banking Security NEW**

WHAT IS CORPORATE ACCOUNT TAKEOVER (CATO)

Corporate Account Takeover 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).

CATO is a form of corporate 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.

Businesses with limited or no internal computer safeguards and disbursement controls for use with the financial institution's online banking system are vulnerable to theft when cyber thieves gain access to their computer systems, typically through malicious software (malware).

Malware can infect your computer system not just through infected documents attached to an email, but also simply when an infected website is visited. Businesses across the United States have suffered large financial losses over the last few years from these thefts. 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, 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.

TYPES OF SECURITY THREATS & COUNTERMEASURES

- **MALWARE**

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.

- **VIRUSES**

Viruses are computer programs that can copy themselves and infect a computer. The term "virus" is also commonly, but incorrectly used to refer to other types of malware, adware, and spyware programs that do not have the reproductive ability. Some viruses try to avoid detection by killing the tasks associated with antivirus software before it can detect them.

- **SPYWARE**

Spyware is a type of malware that is installed on computers and collects little bits of information at a time about users without their knowledge. The presence of spyware is typically hidden from the user, and can be difficult to detect. It can install additional software, redirecting Web browser, changing computer settings, including different home pages, and/or loss of Internet.

TYPES OF SECURITY THREATS & COUNTERMEASURES

- **ROGUE SOFTWARE/SCAREWARE**

Rogue Software/Scareware is a form of malware that deceives or misleads users into paying for the fake or simulated removal of malware. It has become a growing and serious security threat in desktop computing. It 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 codes required to play a video clip
- Software shared on peer-to-peer networks
- A free online malware scanning service

TYPES OF SECURITY THREATS & COUNTERMEASURES

- **PHISHING**
  - Phishing is the 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

TYPES OF SECURITY THREATS & COUNTERMEASURES

- **E-MAIL USAGE**
  - Some experts feel e-mail is the biggest security threat of all. Email is the fastest, most-effective method of spreading malicious code to the largest number of users. Email is 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 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

TYPES OF SECURITY THREATS & COUNTERMEASURES

- **HOAXES**
  - Hoaxes attempt to trick or defraud users. A hoax could be malicious, instructing users to delete a file necessary to the operating system by claiming it is a virus. It could also be a scam that convinces users to send money or personal information. Phishing attacks fall into this category.
    - Browser plug-in (typically toolbar)
    - Image, screensaver or ZIP file attached to an e-mail
    - Multimedia codes required to play a video clip
    - Software shared on peer-to-peer networks
    - A free online malware scanning service

WHERE DOES IT COME FROM?

- Malicious websites (including Social Networking sites)
- Email
- P2P Downloads (e.g. File Sharing Sites)
- Ads from popular web sites

WHAT CAN BUSINESS DO TO PROTECT!

- Education is Key – Train employees
- Install and Maintain Real Time Anti-virus/Anti-spyware/Firewall software and keep it up to date. Use these tools regularly to scan your computer. Allow for automatic up dates and scheduled scans.
- Secure 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 routers and firewalls to prevent unauthorized access to your computer or net work. 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
- Recommend dual control from separate devices
- Note any changes in the performance of your computer – Dramatic loss of speed, computer locks up, unexpected rebooting, unusual popups, etc.
- Perform a risk assessment regarding online payment services
- Review Insurance coverage needs related to electronic thefts

COMMUNICATION

- Make sure that your employees know how and to whom to report suspicious activity at your Company & First American Bank and Trust.
- CONTACT THE BANK IF YOU:
  - Suspect a Fraudulent Transaction
  - If you receive an email claiming to be from the Bank and it is requesting personal/company information.

1-800-738-2265

Tips for Mobile Banking Security **NEW**

- **Stay protected with mobile banking: safety suggestions for accessing your checking account**

  Mobile banking from First American Bank and Trust is safe and convenient with a mobile banking app; Protected by mobile banking security measures including state-of-the-art encryption, firewalls and secure logins. However, there are always general precautions you can take when accessing any of your online accounts, from email to banking.

  With your Smartphone there are several different ways to use mobile banking and each one has a unique set of tips to follow. Follow these general guidelines for the highest level of mobile banking safety.

  - **Avoid making your personal information readily accessible.** Don't share your PIN, password or security question with anyone or save it on your phone.
  - **Password-protect your phone** so others cannot access your information if it is lost or stolen.
  - **Monitor your records** and accounts on a regular basis.
  - **Report a stolen smartphone with your wireless provider** so all the major wireless service providers will allow for remote "bricking" of the phone, which deactivates your phone on any wireless network without your permission.

Tips for Mobile Banking Security **NEW**

- **Mobile banking safety when using a mobile web browser**

  With Smartphones becoming more popular, many people are using mobile web browsers to handle their banking. These web browsers do have some built in features, like standard site encryption, to protect your mobile banking security. For added mobile banking security follow the tips below:

  - **Log out and close your browser** when you are not using the internet on your phone
  - **Set up daily alerts to track account activity**. This is a great way to detect fraudulent activity on your account.
  - **Use secure, encrypted websites** for transactions on your mobile phone
  - **Don't click through to websites from emails**, even if they look like they are from your bank. Always visit your bank's website by typing in the domain, or bookmark it.
  - **Never give your password or account number** on a site you are unsure about
  - **Avoid public Wi-Fi**, if possible

Tips for Mobile Banking Security **NEW**

- **Enjoy mobile banking security with a mobile banking app**

  Using a mobile banking app may be the safest way to access your checking account from a mobile phone. These applications link directly to your bank's computers, often making them faster, and the interface is easier to use. And since the bank designed the mobile banking app, they will have taken extra precautions to ensure proper security measures are implemented.

  Most mobile banking apps are resilient to phishing (a way for a third party to obtain your sensitive information by posing as your bank) since there is no browser, but there are additional mobile banking safety measures you can take to further protect yourself.

  - **Log out of the application** when you're not using it
  - **Add mobile security** software to your device, if possible