Corporate Account Takeover

FIRSTAMERICANBANK
Your Community Bank Since 1903.

Your online security is our top priority

At First American Bank, online security and the protection of your account information is our priority. We have provided some basic information about potential fraudulent account takeover and steps you can take to protect yourself. We have also offer two security software programs to assist you with online protection.

Trusteer Pinpoint software can be downloaded during your log on session to eBusiness Online Banking.

Trusteer Pinpoint detects viruses and malware that can be on your computer. We are notified of any threats and contact you in order to have any threats removed from your computer.

Guardian Analytics FraudMAP® Online (FMAP). This software notifies First American of any anomalies in your online banking session, taking a proactive approach to notify you of any potential threats. FMAP instantly and automatically protects commercial accounts from a wide array of fraud schemes such as: account takeover, suspicious online activity, and fraudulent ACH, wire, bill-pay and other transactions, enabling you to intervene before your money is gone.

Corporate Account Takeover (CATO) is a form of corporate identity theft where a business' online credentials are stolen by malware. Criminal entities can then initiate fraudulent banking activity.

Account Takeover (ATO) is when a fraudster obtains and uses a victim's personal information to take control of existing bank or credit card accounts and carries out unauthorized transactions against them.

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.

Types of Threats:

- 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, crime ware, most rootkits, and other malicious and unwanted software.
- A computer program that can copy itself and infect a computer.
- The term "virus" is also common, 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.
- 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

Examples of corporate emails that could result in a threat.

- Electronic Greeting Cards
- Chain Letters
- Jokes and graphics
- Spam and junk e-mail

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:

Layered Security

Detection is closely associated with protection because some measures that protect also help identify fraud. A single layer of protection is easy for hackers to penetrate. If one layer develops a security weakness then hopefully the other layers will provide sufficient protection.

- Monitoring of IP Addresses
- New User Controls
- Calendar File – Frequencies and Limits
- Dual Control
- Fax or Out of Band Confirmation
- Secure Brower or Secure Browser Key
- Pattern Recognition Software
- Train employees on Fraud warning signs
- Dedicate a computer for online banking only
- Download Trusteer Pinpoint for online banking protection.

Contact the Bank immediately:

- If you suspect a fraudulent transaction.
- If you are trying to process an Online Wire or ACH Batch and receive maintenance page or you are asked for password verification.
- If you receive an email claiming to be from the Bank requesting personal/company information.

FIRSTAMERICANBANK

Your Community Bank Since 1903.