CORPORATE CUSTOMER
ACCOUNT TAKEOVER & INFORMATION
Security Awareness

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).

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.

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 is software designed to infiltrate a computer system without the owner's informed consent.
- Viruses are computer programs that can copy themselves and infect a computer.
- 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.
- Ransomware is a type of malicious software that infects a computer and restricts users access to it until a sum of money is paid to unlock it.
- Rogue Software/Scareware is a form of malware that deceives or misleads users into paying for the fake or simulated removal of malware. Users are misled into installing from a Browser plug-in, Image, Screensaver, Zip file attached to an email, etc.
- 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. This commonly accomplished using Social web site, Auction site, Online payment processors, etc.).
- E-Mail Usage is the fastest, most effective method of spreading malicious code (Electronic Greeting Cards, Chain Letters, Jokes, Graphics, etc.).
- Hoaxes attempt to trick or defraud users (Browser Plugin, Email attachment, free software, etc.).

WHAT CAN BUSINESS DO TO PROTECT!

- Education is Key – Train employees
- Install & Maintain Real Time Anti-virus/Anti-spyware/Firewall software and keep it up to date. Use these tools regularly to scan your computer.
- 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 & firewalls to prevent unauthorized access to your computer or network. Change the default passwords.
- Install security updates to operating systems and all applications as they become available.
- Block Pop-Ups.
- Do not open suspicious attachments from e-mail.
- Do not use public Internet access points.
- Reconcile Accounts Daily.
- Note any changes in the performance of your computer – loss of speed, computer locks up, unexpected rebooting, unusual popups, etc.

ATM & Debit Card Safety Tips

- Protect your card and pin as if it were cash. Report lost or stolen cards immediately. Don't write your PIN on your card or give the number out to anyone. Avoid using numbers that are easily identified (birth date, phone number, etc.).
- Conduct your transactions privately, quickly and efficiently. Shield the ATM keypad during the transaction.
- Be watchful for "Skimmers", which is used to copy identifying information from the magnetic strip on your card. If the machine looks like it has been tampered with or has loose parts don't use it.
- Take the receipt with you. Discarded ATM receipts can lead to identity theft and account hijacking.
- Check your debit card account frequently. If you find unauthorized charges contact your bank immediately.
- Lock your car doors and roll up passenger windows when using the ATM.
- Observe lighting and landscape. If lights are out or landscape blocks the view, select another ATM and notify the bank.
- If you use the ATM at night, consider taking a friend along.
- It's best to count your money later. Be aware of your surroundings.

Account Hijacking & Identity Theft

- Account hijacking occurs when a criminal obtains your personal banking information and uses it to take over your bank accounts. It can take weeks or months to discover.
- Hijacking by Phishing deceives customers into providing their user names, passwords and account numbers via deceptive emails, fake (spoofed) web sites or both.
- Hijacking with Spyware works by inserting malicious software on a person's personal computer. Spyware can be loaded when a user opens an email attachment or clicks on a pop-up advertisement.
- Here are some basic safety tips you can implement immediately.
    - Password Protection – Experts advise a combination of letters and numbers. Avoiding pet names, your home address and similar easy to crack codes.
    - Virus Vaccines – Your computer's anti-virus software is like a vaccine. It works at first, but you need to keep it up to date to protect against new strains.
    - Update the Firewall – This protective wall between the outside world and your computer can help prevent unauthorized access. Updates are called patches and you should always have the latest.
    - Anti-spyware – Every computer connected to the internet should have the software installed and updated regularly.
    - No Phishing Allowed – If you receive an unexpected email or one that you consider suspicious, delete it. Your bank will never email you and ask you to go to another site to verify information.
    - Dumpster Diving – Shred unwanted documents containing personal information and all unsolicited credit cards or loan offers.

Online & Mobile Banking Threats

- If you use online or mobile banking understand the risks and know how fraudsters might trick you, is a critical step in protecting yourself.
    - Smishing/Phishing – This is the criminal attempting to steal your personal information through fraudulent emails or smart phone texts.
    - Card Skimming – This is a criminal's attempt to gain a victim's personal information by tampering with ATM machines.
- Before you create an online account, shop or enter any personal information on a website, check for signs that the organization and the site are secure and trustworthy.
    - Look for security indicators. The "https" at the beginning of the Web address, a symbol such as a padlock and/or a color change.
    - Do some research, investigate the business at the Better Business Bureau's site (bbb.org) or through an online search. Confirm the business or seller's physical address and phone number. Read through returns, refunds or shipping policies, terms of use and reviews.
    - Read the privacy policy. Understand what personal information the site collects, how it's used and if it's shared.
- Remote access to financial accounts is connected through internet devices such as smartphones, laptops, tablets or desktop computers. These devices are connected to the internet using a modem/router, which is either wired or Wi-Fi. Here are some essential steps to secure your internet devices.
    - Passcodes and Passwords – Never allow your passwords to be remembered by your browser software. Reset the default password. Use a combination of upper- and lower-case letters, numbers and symbols and should be at least 10 characters.
    - Security Software – Each device requires specific security software protection. Install a software that detects, prevents and removes all viruses, malware or spyware found on your internet devices.
    - Software Updates – Software updates provide the best defense against online threats. Some of these software updates provide a needed fix for security weaknesses.
    - Wireless Networks – The router serves as the pathway to the internet for all your devices. The router ID renamed by you, a strong password and enabling the preinstalled firewall are essential protection.
- Device Use and Best Practices
    - Wi-Fi hotspots that are public and shared by many users are not secure.
    - Always log off.
    - Back up your data regularly.
    - All your internet devices should auto lock with a short time period.
    - When not in use shutdown or turn off your devices.
    - Enable each device to have your data erased or wiped remotely.

Your Protections under REG E

- Banks follow specific rules for electronic transactions issued by the Federal Reserve Board. The rules cover all kinds of situations revolving around transfers made electronically. Under the consumer protections provided under Reg E, you can recover internet banking losses according to how soon you detect and report them.
- If you report the losses within two days of receiving your statement, you can be liable for the first $50. After two days, the amount increases to $500. After 60 days, you could be legally liable for the full amount. These protections can be modified by state law or by policies at your bank, so be sure to ask your banker how these protections apply to your particular situation.