Farmers
State Bank
& Trust Co.

CORPORATE CUSTOMER
ACCOUNT TAKEOVER & INFORMATION
Security Awareness

EQUAL HOUSING LENDER

FDIC

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.

EQUAL HOUSING LENDER

FDIC

“You’ve Won” Scams

Here's how they work:

You get a call, a card or an email telling you that your won a trip or a prize, a lottery or a sweepstakes.

But here's what happens next:

They tell you there's a fee, some taxes, or customs duties to pay. Then they ask for your credit card number or bank account information or they ask you to wire money. Either way, you lose money instead of winning it.

Here's what you can do:

1. Keep your money and your information to yourself. Never share your financial information and/or wire money to someone who contacts you and claims you've won something.

2. Pass this information on to a friend.

“IRS Imposter” Scams

Here's how they work:

You get a call from someone who says they from the IRS. They say that you owe back taxes. They threaten to sue you, arrest or deport you, or revoke your license if you don't pay right away. They tell you to put money on a prepaid debit card and give them the card numbers.

The caller may know some of your Social Security Number and the caller ID might show a Washington, DC area code.

The IRS won't ask you to pay with prepaid debit cards or wire transfers or a credit card over the phone. When the IRS first contacts you about unpaid taxes, they do it by mail, not by phone.

Here's what you can do:

1. Stop. Don't wire money or pay with a prepaid debit card. Once you send it, the money is gone.

If you have tax questions, go to irs.gov or call the IRS at 1-800-829-1040.

2. Pass this information on to a friend.

Please Report Scams to the Federal Trade Commission.

Call 1-877-382-4357

Go Online: ftc.gov/complaint

Fraud Scams: Quick Reference Guide

SCAM	DEFINITION	VICTIMS	INDICATORS
Business Email Compromise (BEC)	Targets a business or commercial client in the attempt to initiate a large funds transfer to an account under the fraudster's control.	CEOs, CFOs, Accountants, Bookkeepers, Accounts Payable	• Large wire or funds transfer to a new recipient. • Transfers initiated near end-of-day or cut-off windows; and/or before weekends or holidays. • Receiving account does not have a history of receiving large funds transfers. • Receiving account is a personal account and the company typically only sends wires to other businesses.
Employment Scam	A fraud targeting individuals with the promise of a job that typically involves processing financial transactions for the employer.	Job seekers, college students, underemployed, stay-at-home parents, retirees.	• The client is new or financially vulnerable, has little access to credit, no or inconsistent payroll, and/or has a low-dollar balance in their account. • Mobile deposits or ACH credits that are new or not typical for the client. • Immediate withdrawal or transfer of funds from the account. • Large purchases at locations that process funds transfers, such as big box stores, and international wire processers.
Lottery Scam	A type of fraud promising large lottery winnings in return for an initial processing fee from the victim.	General public but typically, those who may be financially vulnerable.	• Large funds transfer that is not typical for the client. • Funds transfers to international locations. • Large ATM withdrawals. • Large purchases at locations that process funds transfers, such as big box stores and international wire processers. • Client using lines of credit or pulling from investments, which is out of character for them.
Online & Payday Loan Scam	Fraud targeting individuals with the promise of a loan in exchange for a fee.	College students, underemployed, individuals facing some form of addiction.	• Mobile deposits or ACH credits that are new or not typical for the client. • Immediate withdrawal or transfer of funds from the account. • Large purchases at locations that process funds transfers, such as big box stores and international wire processers.
Romance	A fraud that targets victims who may be emotionally vulnerable, with the goal of having the victim send funds to the fraudsters.	Widows, widowers, retirees, divorcees, singles	• Large funds transfer that is not typical for the client. • Funds transfers to international locations. • Large ATM withdrawals. • Client using lines of credit or pulling from investments, which is out of character for them. • Large purchases at locations that process funds transfers, such as big box stores and international wire processers.

EQUAL HOUSING LENDER

FDIC

Four Signs That It's A Scam

1. Scammers PRETEND to be from an organization you know.

Scammers often pretend to be contacting you on behalf of the government. They might use a real name, like the Social Security Administration, the IRS, or Medicare, or make up a name that sounds official. Some pretend to be from a business you know, like a utility company, a tech company, or even a charity asking for donations.

They use technology to change the phone number that appears on your caller ID. So the name and number you see might not be real.

2. Scammers Say there's a PROBLEM or a PRIZE.

They might say you’re in trouble with the government. Or you owe money. Or someone in your family had an emergency. Or that there’s a virus on your computer.

Some scammers say there’s a problem with one of your accounts and that you need to verify some information.

Others will lie and say you won money in a lottery or sweepstakes but have to pay a fee to get it.

3. Scammers PRESSURE you to act immediately.

Scammers want you to act before you have time to think. If you’re on the phone, they might tell you not to hang up so you can’t check out their story.

They might threaten to arrest you, sue you, take away your driver’s or business license, or deport you. They might say your computer is about to be corrupted.

4. Scammers tell you to PAY in a specific way.

They often insist that you pay by sending money through a money transfer company or by putting money on a gift card and then giving them the number on the back. Some will send you a check (that will later turn out to be fake), tell you to deposit it, and then send them money.

What You Can Do to Avoid a Scam

- Block unwanted calls and text messages.

  Take steps to block unwanted calls and to filter unwanted text messages.

- Don’t give your personal or financial information in response to a request that you didn’t expect.

  Legitimate organizations won’t call, email, or text to ask for your information.

EQUAL HOUSING LENDER

FDIC