FIRST STATE BANK
of BEDIAS

★ Since 1907 ★

MEMBER FDIC

Cyber Security
Survival Guide

Table of Contents

First State Bank of Bedias

As a First State Bank of Bedias customer you can always expect us to proactively take steps to keep you safe and secure. In response to the recent data breach that occurred over the 2013 holiday season at Target stores and Neiman Marcus we immediately determined if your account was compromised. We then personally contacted those of you that were affected and provided you with a new secure debit card.

Additionally, in our continued efforts to protect your information we want to make you aware that phishing e-mails are now being sent out that appear to be from Target. These e-mails play on the fears of the public – specifically, those who are concerned that their card has been compromised. We ask that you please proceed with caution if you receive an e-mail appearing to be from Target. DO NOT OPEN any links that may be included in these e-mails as that could potentially allow access to your personal information.

We will continue to remain vigilant with this matter and in all matters pertaining to your personal information. If you have any further questions, please contact your Banking Officer, come into one of our branches, or call us at (936) 395-2141.

What is Corporate Account Takeover?

Corporate account takeover is a type of fraud where thieves gain access to a business' finances to make unauthorized transactions, including transferring funds from the company, creating and adding new fake employees to payroll, and stealing sensitive customer information that may not be recoverable.

Cybercriminals are targeting small businesses with increasingly sophisticated attacks. It is common for thieves to send emails posing as a bank, Delivery Company, court or the Better Business Bureau. Criminals use spoofed emails, malicious software and online social networks to obtain login credentials to businesses' accounts, transfer funds from the accounts and steal private information, a fraud referred to as "corporate account takeover."

Corporate Account Takeover Awareness and Prevention

Fraud Tactics

Different fraud tactics all share the same goal: to obtain your personal, confidential and financial informations for fraudulent use.
From obtaining your information "the old-fashioned way" via discarded mail, to emails that ask you to verify personal information under the guise of a trusted source – like your financial institution – fraudulent activity comes in many different forms:

Dumpster Diving: Thieves rummage through trash looking for bills or other paper that includes your personal information.

Malware: Also known as 'malicious software', malware is designed to harm, attack or take unauthorized control over a computer system. Malware includes viruses, worms and Trojans. It's important to know that Malware can include a combination of all three of the types noted.

Phishing: A scam that involves the use of replicas of existing Web pages to try to deceive you into entering personal, financial or password data. Often suspects use urgency or scare tactics, such as threats to close accounts.

Vishing: of phishing attack where the attacker uses a local phone number in the fake email as a means of obtaining your sensitive information. The goal is to fool you into believing the email is legitimate by instructing you that responding to the request by phone is safer than responding by email and shows authenticity. The unsuspecting caller is then tricked through an automated phone system to relinquish their sensitive information.

Pharming: Pharming takes place when you type in a valid Web address and you are illegally redirected to a Web site that is not legitimate. These 'fake' Web sites ask for personal information such as credit card numbers, bank account information, Social Security numbers and other sensitive information.

Trojan: A Trojan is malicious code that is disguised or hidden within another program that appears to be safe (as in the myth of the Trojan horse). When the program is executed, the Trojan allows attackers to gain unauthorized access to the computer in order to steal information and cause harm. Trojans commonly spread through email attachments and Internet downloads. A common Trojan component is a **"keystroke logger"** which captures a user's keystrokes in an attempt to capture the user's credentials. It will then send those credentials to the attacker.

Spoofing: Spoofing is when an attacker masquerades as someone else by providing false data. Phishing has become the most common form of Web page spoofing. Another form of spoofing is URL spoofing. This happens when an attacker exploits bugs in your Web browser in order to display incorrect URLs in your browser location bar. Another form of spoofing is called "man-in-the-middle". This occurs when an attacker compromises the communication between you and another party on the Internet. Many managed firewalls and unified threat management systems can be updated or configured to significantly prevent this type of attack.

Spyware: Loaded on to your computer unbeknownst to you, spyware is a type of program that watches what users do and forwards information to someone else. It is most often installed when you download free software on the Internet. Unfortunately hackers discovered this to be an effective means of sending sensitive information over the Internet. Moreover, they discovered that many free applications that use spyware for marketing purposes could be found on your machine, and attackers often use this existing spyware for their malicious means.

Pop-Ups: A form of Web advertising that appears as a "pop-up" on a computer screen, pop-ups are intended to increase Web traffic or capture email addresses. However, sometimes pop-up ads are designed with malicious intent like when they appear as a request for personal information from a financial institution, for example

Virus: A computer virus is a malicious program that attaches itself to and infects other software applications and files without the user's knowledge, disrupting computer operations. Viruses can carry what is known as a "payload," executable scripts designed to damage, delete or steal information from a computer.

A virus is a self-replicating program, meaning it copies itself. Typically, a virus only infects a computer and begins replicating when the user executes the program or opens an "infected" file.

Viruses spread from computer to computer only when users unknowingly share "infected" files. For example, viruses are commonly spread when users send emails with infected documents attached.

Retro-Virus: This virus specifically targets your computer defenses. It will look for vulnerabilities within your computer operating system or any third party security software. Most security vendors have some form of tamper-proof measure in place, so it is important to keep your patches up-to-date. Retro Viruses are usually combined with another form of attack.

Worm: A worm is similar to a virus but with an added, dangerous element. Like a virus, a worm can make copies of itself; however, a worm does not need to attach itself to other programs and it does not require a person to send it along to other computers.

Worms are powerful malware programs because they cannot only copy themselves, they can also execute and spread themselves rapidly across a network without any help.

Security Center

Report Fraud

If you know, or even think, you've been a victim of identity fraud, take immediate action and follow these five steps.
More specifics can be found on the FTC's Privacy & Identity Site.

Report the fraudulent activity. If the activity is related to First State Bank of Bedias, please http://www.bediasbank.comcontact us directly.

If it is related to another financial institution, your credit card company, or any other organization contact them directly.

Contact one of the three consumer reporting companies and have a fraud alert placed on your credit report. This will help stop fraudsters from opening any additional accounts in your name. Contact only one of the following (the others are required to contact the other two):

Equifax: 1-800-525-6285; www.equifax.com; P.O. Box 740241, Atlanta, GA 30374-0241
Experian: 1-888-EXPERIAN (397-3742); www.experian.com; P.O. Box 9532, Allen, TX 75013
TransUnion: 1-800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

Close any accounts that you know - or even think - might have been tampered with or opened fraudulently. Report the transgression to a security spokesperson at the relevant company. Ask them about any additional steps - they'll probably ask you to send relevant copies of the fraudulent activity.

You can also use the FTC Theft Affadavit ID Theft Affidavit (PDF, 56KB) as formal certification of your dispute.

File your complaint with the FTC. Use the online complaint form; or call the FTC's Identity Theft Hotline, toll-free: 1-877-ID-THEFT (438-4338); TTY: 1-866-653-4261; or write Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Sharing your identity theft complaint with the FTC will help law enforcement officials track down identity thieves and stop them.

Call or visit the local police or police in the community where the identity theft took place and file a report. Have a copy of your FTC ID Theft complaint form available to give them. Obtain a copy of the police report and the police report number.

Fraud Prevention

It's not always easy to identify online fraud. Understanding how fraudulent activity takes place helps with prevention, and keeps you safe.

Safeguard your email

Email is often a vehicle used to transmit malware and commit fraud. It is important to evaluate your email behaviors and develop good habits to help protect your computer and your identity.
In addition to viruses and worms that can be transmitted via email, phishing also threatens email users. A type of email fraud, phishing occurs when a perpetrator, posing as a legitimate, trustworthy business, attempts to acquire sensitive information like passwords or financial information.

To safeguard your email

Never open or respond to SPAM (unsolicited bulk email messages).

Delete all spam without opening it. Responding to spam only confirms your email address to the spammer, which can actually intensify the problem.

Never click on links within an email.

It's safer to retype the Web address than to click on it from within the body of the email.

Don't open attachments from strangers.

If you do not know the sender or are not expecting the attachment, delete it.

Don't open attachments with odd filename extensions.

Most computer files use filename extensions such as ".doc" for documents or ".jpg" for images. If a file has a double extension, like "heythere.doc.pif," it is highly likely that this is a dangerous file and should never be opened. In addition, do not open email attachments that have file endings of .exe, .pif, or .vbs. These are filename extensions for executable files and could be dangerous if opened.

Never give out your email address or other sensitive or personal information to unknown web sites.

If you don't know the reputation of a Web site, don't assume you can trust it. Many Web sites sell email addresses or may be careless with your personal information. Be wary of providing any information that can be used by others for fraudulent purposes.

Never provide sensitive information in email.

Forged email purporting to be from your financial institution or favorite online store is a popular trick used by criminals to extract personal information for fraud.

Don't believe the hype.

Many fraudulent emails send out urgent messages that claim your account will be closed if sensitive information isn't immediately provided, or that important security needs to be updated online. Your financial institution will never use this method to alert you of an account problem.

Be aware of poor design, and/or bad grammar and spelling.

A tell-tale sign of a fraudulent email or Web site includes typos and grammar errors as well as unprofessional design layout and quality. Delete them immediately.

Backup your sensitive data records.

Consider backing up all sensitive files. This will not only help you restore damaged or corrupted data, but it will help protect against fraud attacks and help recover lost files if needed.

Safeguard your identity online

In addition to protecting your email, there are a number of guidelines to follow that will help safeguard your identity online. Check out FSBB Education Center if you would like more information.

Do not allow a Web site to keep sensitive information or credentials for future convenience.

It is a common practice when registering for access to a Web site or making a purchase from a Web site to be asked if you want to keep your access credentials, credit card number or other sensitive information on file as a matter of convenience. This common request is referred to as "remembering" for the future use.

Be selective about where you surf.

Not all Web sites are benign. Sites that are engaged in illegal or questionable activities often host damaging software and make users susceptible to aggressive computer attacks.

Don't choose "Remember My Password."

You should never use the "remember password" feature for online banking or transactional Web sites.

Don't use public computers for sensitive operations.

Since you cannot validate the computer's integrity, there's a higher risk of fraud when you log in from a public computer.

Work on a computer you trust.

Firewalls, antivirus, anti-spyware and other protection devices help keep a computer properly monitored and provide peace of mind. These tools are important in order to protect your computer and data. A good firewall is critical if you commonly access the Internet via a wireless connection. It is also important to keep your computer up-to-date with patches to security tools as well as to the operating system and other programs on your computer. Make sure to configure your computer to update all security fixes.

Select a strong password.

The best password is an undetectable one. Never use birth dates, first names, pet names, addresses, phone numbers, or Social Security numbers. Use a combination of letters, numbers and symbols. Be sure to change your passwords regularly.

Use a secure browser.

Only use secure Web pages when you're conducting transactions online (a Web page is secure if there is a locked padlock in the upper right-hand corner of your browser).

Sign off, shut down, disconnect.

Always sign off or logout from your online banking session or any other Web site that you've logged into using a user ID and password. When a computer is not in use, it should be shut down or disconnected from the Internet.

Lock your computer when it is not in use.

This helps protect you from unauthorized user access.

Beware of shoulder surfing.

This is a common tactic that happens in public places such as coffee shops, airports, libraries etc. where an attacker will look over your shoulder when you're logged in to obtain your sensitive information. Be vigilant and aware of prying eyes.

Set up a timeout.

The Timeout feature is an additional safety check. It can prevent others from continuing your online banking session if you left your PC unattended without logging out. You can set the Timeout period in the User Options screen.

Enhance Security Login

Online Security: Everyday, Everywhere

Your online security has always been a top priority.

That's why Enhanced Login Security is so important. This security service is free, easy, and most importantly, gives you extra protection from fraud and identity theft.

Enhanced Login Security significantly increases your level of protection online. Not only will your password and user id be recognized, but your computer will be recognized as well. If we don't recognize your computer - you've logged in from a public computer or one you haven't used before - you will be prompted to provide information that only you will know. This step acts as an additional line of defense against unauthorized access to your accounts.

Security Alerts

Text Message/Emails

First State Bank of Bedias has identified activities in which individuals are sent fraudulent text messages and e-mails that request certain personal data such as account numbers, social security numbers, Online Banking user names and passwords. These e-mails usually state that there is a need to update information or that there is a problem with your account. It will then direct you to a link to update your personal information. If you receive such a message, **DO NOT PROVIDE ANY OF YOUR INFORMATION**. As a reminder to our customers, First State Bank of Bedias wants to protect your identity and confidential information. We will never ask you for personal information online or by a text message. If you ever receive a message where this information is requested, **DO NOT GIVE OUT THIS INFORMATION**.

First State Bank of Bedias Security Response Team
If you think that your account information has been compromised, please contact us immediately at (936) 395-2141. Our Security Response team will review the message, verify that it was not sent by First State Bank of Bedias, and help you to determine if your information has been compromised. In the case of phishing attempts, First State Bank of Bedias will begin the process of shutting down any associated websites.

Phone Requests for Personal Information

As a reminder to all First State Bank of Bedias customers, First State Bank of Bedias or any of its affiliate companies would never call to request a customer's account number or ATM/Debit MasterCard PIN number. If you ever receive a call requesting your personal account information, please do not disclose the information and immediately contact First State Bank of Bedias's Customer Contact Center at (936) 395-2141 to notify us of the situation. As always, we thank you for your loyalty and business.

The Small Business Guide to Corporate Account Takeover

The vast majority of cyber thefts begin with the thieves compromising the computer(s) of the business account holders. Perpetrators often monitor the customer’s email messages and other activities for days or weeks prior to committing the crime. The corporate customer is most vulnerable just before a holiday when key employees are on vacation. Another risk period is on a day the business office is relocating or installing new computer equipment. Employees may be distracted and think a problem conducting online banking is due to a new network or equipment.

Combating account takeover is a shared responsibility between businesses and financial institutions. Bankers can explain the safeguards small businesses need and the numerous programs available that help ensure fund transfers, payroll requests and withdrawals are legitimate and accurate. First State Bank of Bedias put together this brief guide to help our small business customers educate themselves and prevent being a victim of corporate account takeover. After reviewing this guide, if you would like to help ensure your business is protected against cybercriminals or have any questions, please contact First State Bank of Bedias today.

How do I protect myself and my small business?

A shared responsibility between First State Bank of Bedias and the business is the most effective way to prevent corporate account takeover. We work with business customers to help them understand security measures needed within the businesses and to establish safeguards on the accounts that can help the bank identify and prevent unauthorized access to funds.

Consider these tips to ensure your business is well prepared:

- Protect your online environment**.** It is important to protect your cyber environment just as you would your physical location. Do not use unprotected internet connections. Encrypt sensitive data and keep updated anti-virus and anti-spyware protection on your computers. Change passwords from the default to something complex, including at point-of-sale terminals. Update anti-virus and anti-malware programs frequently. Update, on a regular basis, all computer software to protect against new security vulnerabilities (patch management practices). Adhere to dual control procedures. Use separate devices to originate and transmit wire/ACH instructions. Transmit wire transfer and ACH instructions via a dedicated and isolated device. Adopt advanced security measures by working with consultants or dedicated IT staff.
- Partner with your bank for payment authentication**.** Talk to your banker about services that offer call backs, device authentication, multi-person approval processes, batch limits and other tools that help protect you from unauthorized transactions.
- Pay attention to suspicious activity and react quickly. Put your employees on alert. Look out for strange network activity, do not open suspicious emails and never share account information. If you suspect a problem, disconnect the compromised computer from your network and contact your banker. Keep records of what happened. Practice ongoing account monitoring and reconciliation, especially near the end of the day.
- Understand your responsibilities and liabilities. The account agreement with your financial institution will detail what commercially reasonable security measures are required in your business. It is critical that you understand and implement the security safeguards in the agreement. If you don’t, you could be liable for losses resulting from a takeover. Talk to your banker if you have any questions about your responsibilities. Utilize resources provided by trade organizations and agencies that specialize in helping small businesses.

- Educate your employees. You and your employees are the first line of defense against corporate account takeover. A strong security program paired with employee education about the warning signs, safe practices, and responses to a suspected takeover are essential to protecting your company and customers. Provide continuous communication and education to employees using online banking systems. Provide enhanced security awareness training will help ensure employees understand the security risks related to their duties. Communicate to employees that passwords should be strong and should not be stored on the device used to access online banking.

For additional information, contact First State Bank of Bedias today. You can also visit the following websites to learn more about how to protect your small business:

- **U.S. Chamber of Commerce: Internet Security Essentials for Business**
- **Federal Communications Commission: Small Biz Cyber Planner**
- **Federal Communications Commission: 10 Cybersecurity Strategies for Small Business**
- **Better Business Bureau: Data Security Made Simpler**
- **NACHA – The Electronic Payments Association Sound Business Practices for Businesses to Mitigate Corporate Account Takeover**