Online and Mobile Banking Security Awareness

Protecting Yourself from Online and Mobile Banking Fraud

The online banking industry has seen an increase in fraudulent activity. With key loggers, virus attacks and phishing scams becoming more prevalent, are you doing all you can to protect yourself from becoming a victim of fraud?

For the past several years, there has been a lot of focus on identity theft. While very serious and very damaging, there are many other ways that the "bad guys" can wreak havoc on your life and your finances. Services like the ones available from the three major credit reporting agencies and companies who provide protection against other people establishing credit or identities using your Social Security Number are very valuable and worthwhile, but true identity theft is not the only threat out there in these digital times.

Account Takeover: Many cyber criminals, also referred to as fraudsters, don't just want to steal your identity in the traditional sense or get a credit card, mortgage or checking account in your name and live their life off of your good credit history, they simply want to take your money and move on to the next victim. While most companies that do business on the Internet including Financial Institutions are very diligent in providing online protection for their customers, the first line of defense is knowledge about what you, the end-user, can do to protect yourself - an electronic way of "Looking Out for Number One." The two most prevalent types of fraud, "Keylogging" and "Phishing", occur from viruses on your computer. In both cases, the end result is the fraudster capturing your login credentials, and taking over your account.

Keystroke Logging or Keylogging: Keylogging is a method by which fraudsters record your actual keystrokes and mouse clicks. Key loggers are "Trojan" software programs that target your computer's operating system (Windows, Mac OS, etc.) and are "installed" via a virus. These can be particularly dangerous because the fraudster has captured your user ID and password, account number, Social Security Number - and anything else you have typed. If you are like most other users and have the same ID and PIN/Password for many different online accounts, you've essentially granted the fraudster access to any company with whom you conduct business. After all, they've got your login credentials so the fraudster appears to be a valid user.

Here are some ways you can prevent yourself from being a victim of keystroke logging or keylogging:

- Use Anti-Virus Software. This is the single most important thing you can do to protect your computer from viruses. There are many on the market today – some cost money while others are free. If you opt to use a free version, make sure it is being offered by a reputable company and do research on the company and its product before installing.
- Keep your Operating System up-to-date with the latest security patches.

Phishing: Phishing is a scam where Internet fraudsters request personal information from users online. These requests are most commonly in the form of an email from an organization with which you may or may not do business. In many cases, the email has been made to look exactly like a legitimate organization's email would appear complete with company logos and other convincing information. The email usually states that the company needs you to update your personal information or that your account is about to become inactive, all in an effort to get you to click the link to a site that only looks like the real thing. If you click on the link to go to the phony website and enter all of your information, you've just been the victim of a phishing attack. The fraudsters have just captured all the necessary information to access your accounts online.

No reputable business will ever email you requesting that you update your personal information, including account numbers, system passwords or Social Security Numbers via a link to their site.

Follow these guidelines to protect yourself from phishing scams:

- Never click on a link from a business requesting that you provide them with personal information.
- Pay close attention to the URL (Internet address) behind the link. Often in phishing attempts, if you hover the cursor over the link the fraudsters want you to click on, it has nothing to do with the actual company they claim to be.
- If your Financial Institution uses watermarks or personal images, do not log in unless you see the correct image on the screen.
- Report any phishing attempts to your Financial Institution.

If you are unsure that the request is valid, open a new Internet session and manually key in the business' web address. If the business genuinely needs information from you, they will have you log in to your online account to see the request. In most cases, you'll just be greeted with a message indicating that the business will never email you requesting personal information.

There is no security system available that will stop fraud if the perpetrator has all of this information, so it is imperative to take the necessary steps to prevent them from getting the information in the first place.

Online and Mobile Banking Security: Information you provide in connection with Online Services will be stored on secure servers and protected by advanced encryption techniques. The URL addresses are encrypted on all Internet banking transaction screens, and no sensitive information is displayed in the URL. Internet banking transactions screens have an HTML command that does not permit the screen details to be saved or viewed in cache. These commercially reasonable security measures are intended to keep your information secure and to prevent unauthorized access. **Effective security; however, is dependent on your responsible behavior in protecting your Log-in Credentials and controlling access to the devices that you use to access Online Banking Services.**

Protecting Your Log-In Credentials - Log in Credentials means your personal ID, password, and any other unique device (such as token or fingerprint) used to access Online and Mobile Banking Services.

- Change your passwords often. Even if your financial institution doesn't require it, it is a good practice to change your passwords at least every six months. An easy way to remember: change them when you change your clocks to adjust for Daylight Savings Time.
- Don't use the same ID and PIN/Password for every online account you have.
- Never disclose your login credentials to other people or companies.
- Do not store your ID and Password information where others could gain access to it. It is best not to write the information down at all.
- Do business with a financial institution that offers two-factor authentication for accessing your information online.
- If offered by your financial institution, take advantage of hard- or soft-tokens which provide a unique onetime-use password each time you access your account. This is especially important for business accounts with multiple users.
- If accessing information via a wireless network, ensure that the network is secure. Accessing sensitive information (or any website) over a non-secure network simply leaves the door open for criminals. Even if you aren't visiting a site where you enter an ID and password, you are still leaving your computer exposed to possible threats.

Mobile Banking Security Tips - With Mobile banking usage on the rise so are cyber security threats for mobile device users. Take measures to ensure you're do not become a victim of fraud.

- Consider a screen lock on your mobile device with a password or PIN feature. Many mobile devices offer this option, as well as other customizable security settings, which can help keep your device and information secure.

- Do not use your full or partial Social Security number as your Personal Identification Number (PIN), user ID or Password Do not store your PIN and personal data on your mobile device.

- Depending on your mobile device, you may have the option to use a biometric feature (such as a fingerprint scanner) to authenticate your identity and gain access to the Online Banking Service. If you choose to activate a biometric feature, it is your responsibility to control access to Online Banking Service just as you would with your personal ID and password. You acknowledge that any person who has a biometric feature stored in your device may be able to access your Online Banking Service.

- Always take advantage of any security features offered by your mobile device, mobile carrier, or bank. By not using security features, it leaves your personal and financial information open to anyone who may be looking for it.

- Always accept updates and patches to your device's software as soon as it's available. These updates patch vulnerabilities and fix software issues.

- Always download apps from approved sources like your mobile service provider or mobile device manufacturer's market place. Fraudulent mobile apps may capture your personal information and transmit it to their servers. Download your First State Bank Central Texas Mobile App at www.fsbcentex.com.

- Do not use free public Wi-Fi connections for your banking transactions. Use your phone carrier's internet connection for enhanced security.

- When using a mobile browser to access your account information, never click on a link of the Bank's URL, always type the URL into your browser address bar, www.fsbcentex.com to access your NetTeller Online Banking service.

- Always log out of your account when you are finished with your banking activity. No doing so leaves an opportunity where an account could be accessed prior to the inactivity auto log out feature takes effect.

- Disable Bluetooth when not in use. In public areas, others can detect your device and access it through Bluetooth. Disconnecting helps prevent others from obtaining information or sending malicious code to your device.

- Never respond to urgent email or text message claiming to be from First State Bank Central Texas or any company that request your account or personal information. This is could be "phishing" an attempt to obtain your personal information.

- Regularly delete text messages and old calendar entries, clear browser history, and delete files. Remove all information prior to disposing of, recycling or donating your device.

- Be aware of shoulder surfing while accessing mobile banking. Never leave your mobile device idle while your banking session is still active.

- Backup your personal data, such as contacts, documents, and photos so that may be restored if your device is lost or stolen. Learn how to remotely wipe your mobile device. If your device is ever lost or stolen, you should know how and be able to remotely wipe it – which means removing all of your personal data and restoring the device back to its factory state. There are apps that can also help you to locate and recover your device when lost.