INTERNET BANKING AUTHENTICATION

Keeping Your Banking Information Safe in a Digital World

Security Update

IMPORTANT INFORMATION REGARDING PHISHING SCAMS:

Please be aware that other banks are experiencing fraudulent text scams (SMS Phishing) in our area.

A fraudulent text message is sent alerting recipients that their debit card has been blocked or suspended. The fraudulent text message instructs recipients to follow a link in order to "solve the problem" or "login." DO NOT CLICK ON THIS LINK.

If the link in the text is clicked, the recipient is redirected to a fraudulent website that appears to be the Bank's branded website, but it is not. On this fraudulent website, the user is asked to provide their debit card number, debit card expiration date and debit card CVV code. Providing this information could result in fraudulent charges occurring on your debit card. Also, it is possible that potentially harmful malware could be downloaded to the device which received the text simply by opening the website page.

Understanding the Risks

According to the Federal Financial Institutions Examination Council (FFIEC), there have been significant changes in the threat landscape recently. Fraudsters have continued to develop and deploy more sophisticated, effective, and malicious methods to compromise authentication mechanisms and gain unauthorized access to customers' online accounts. Rapidly growing organized criminal groups have become more specialized in financial fraud and have been successful in compromising an increasing array of controls. Various complicated types of attack tools have been developed and automated into downloadable kits, increasing availability and permitting their use by less experienced fraudsters. Malware surreptitiously installed on a personal computer (PC) can monitor a customer's activities and facilitate the theft and misuse of their login credentials. Such malware can compromise some of the most robust online authentication techniques, including some forms of multi-factor authentication. As a result, cyber-crime complaints have risen substantially each year since 2005, particularly with respect to commercial accounts. Fraudsters are responsible for losses of hundreds of millions of dollars resulting from online account takeovers and unauthorized funds transfers.

Protecting Your Account Authentication

There are a variety of technologies and methodologies financial institutions can use to authenticate customers. These methods include the use of customer passwords, personal identification numbers (PINs), digital certificates using a public key infrastructure (PKI), physical devices such as smart cards, one-time passwords (OTPs), USB plug-ins or other types of "tokens", transaction profile scripts, biometric identification, and others.

Authentication methods that depend on more than one factor are more difficult to compromise than single-factor methods. For example, the use of a logon ID/password is single-factor authentication (i.e., something the user knows); whereas, an ATM transaction requires multifactor authentication: something the user possesses (i.e., the card) combined with something the user knows (i.e., PIN).

Mutual authentication is a process whereby customer identity is authenticated and the target Web site is authenticated to the customer. One reason phishing attacks are successful is that unsuspecting customers cannot determine they are being directed to spoofed Web sites during the collection stage of an attack. The spoofed sites are so well constructed that casual users cannot tell they are not legitimate.

First Freedom Bank uses additional layers of security in the event you log in from a device that has not been used in the past. Instead of simple challenge questions you used in the past, you will be asked to validate your identity thru a one-time security code via a phone call or SMS message. These enhanced security features help safeguard your information.

Protecting Your Account
Layered Security

Layered security is characterized by the use of different controls at different points in a transaction process so that a weakness in one control is generally compensated for by the strength of a different control. Effective controls that may be included in a layered security program include, but are not limited to:

- fraud detection and monitoring systems that include consideration of customer history and behavior and enable a timely and effective institution response;
- the use of dual customer authorization through different access devices;
- the use of "positive pay," debit blocks, and other techniques to appropriately limit the transactional use of the account;
- enhanced controls over account activities; such as transaction value thresholds, payment recipients, number of transactions allowed per day, and allowable payment windows (e.g., days and times);

First Freedom Bank utilizes several of the above security measures to protect its customers. Our fraud monitoring service constantly monitors activity on all accounts and will flag patterns of activity which are outside of the usual pattern for that customer. If unusual activity is detected, we may contact you to determine whether the activity is legitimate. Please note that First Freedom Bank will never independently contact you to ask for your online banking username and password. If we contact you, we will positively identify ourselves as First Freedom Bank employees. If you are concerned about the possibility of fraud, you may wish to call us back and ask to speak to the individual who contacted you.

Additionally, the Bank has set transaction volume and dollar limits on electronic and point-of-sale activity which should limit exposure to potential fraud.

For our business customers, another layer of security is required to send money out of your account via ACH. Most customers will be required to separately verify that the requested activity is legitimate prior to the Bank making these types of payments.

How Not to Get Hooked by a "Phishing" Scam

Internet scammers casting about for people's financial information have a new way to lure unsuspecting victims: They go "phishing."

Phishing is a high-tech scam that uses spam or pop-up messages to deceive you into disclosing your credit card numbers, bank account information, Social Security number, passwords, or other sensitive information.

According to the Federal Trade Commission (FTC), phishers send an email or pop-up message that claims to be from a business or organization that you deal with - for example, your Internet service provider (ISP), bank, online payment service, or even a government agency. The message usually says that you need to "update" or "validate" your account information. It might threaten some dire consequence if you don't respond. The message directs you to a Web site that looks just like a legitimate organization's site, but it isn't. The purpose of the bogus site? To trick you into divulging your personal information so the operators can steal your identity and run up bills or commit crimes in your name.

Red Flags of Identity Theft

- mistakes on your bank, credit card, or other account statements
- mistakes on the explanation of medical benefits from your health plan
- your regular bills and account statements don't arrive on time
- bills or collection notices for products or services you never received
- you are turned down unexpectedly for a loan or job
- calls from debt collectors about debts that don't belong to you
- a notice from the IRS that someone used your Social Security number
- mail, email, or calls about accounts or jobs in your minor child's name
- unwarranted collection notices on your credit report
- businesses turn down your checks

Customer Awareness
Steps to Protect Yourself

Understanding the risks and the various channels that fraudsters use to steal your information is an important first step. You should also make your computer as safe as possible by regularly installing and updating the following:

- Anti-virus software
- Anti-malware programs
- Firewalls
- Operating system patches and updates

You can also visit the following websites to learn more about online safety and security:

www.staysafeonline.com

www.ftc.gov

www.usa.gov

www.idtheft.gov

Business customers should also perform periodic internal assessments to ensure the highest level of possible security for their accounts. Those assessments should take into consideration the business' internal controls such as policies, procedures, system administrator access, and transactional risk levels, among other things.

Your Protections Under Regulation E

First Freedom Bank follows regulatory guidelines for disputed electronic transactions. These guidelines are found in Regulation E, issued by the Consumer Financial Protection Bureau (CFPB). Under those guidelines, consumers may recover losses associated with electronic transactions based on how quickly they are reported to the Bank. It is important that you notify us as soon as possible if you identify activity on your account which you suspect is fraudulent.

If You Have Questions or Concerns

If you notice suspicious activity in your account or experience security-related events, you should immediately contact First Freedom Bank at (615) 444-1280.