Security Information

How to Protect Yourself from Online Fraud

The increased sophistication and rapid growth of online fraud continues to be a challenge. These scams appear in many forms, especially fraudulent emails and Web sites, spyware and viruses, and pop-up advertisements.

Fraudulent Emails and Websites

This particular type of fraud occurs when someone poses as a legitimate company to obtain personal data, such as account numbers, and then makes transactions with this information illegally. A common form of this scam is called “phishing”. Phishing refers to cyber-criminals who attempt to gather sensitive personal information from consumers through emails and/or through imitations of legitimate Web sites. To combat phishing, please remember that First National Bank will never ask for sensitive information from you via e-mail (ex. Social security number, access ID, password or account number, or ATM/debit card number and PIN).

Spyware and Viruses

Spyware and viruses are destructive programs loaded on your computer without your permission or knowledge. Spyware appears as a legitimate application on your computer but actually monitors your activity and collects sensitive information. Viruses are harmful programs spread through the Internet that can compromise the security of your computer. Maintaining up-to-date anti-spyware and virus protection software and firewalls help avoid these risks.

Pop-Up Advertisements

Pop-ups appear in a separate browser window and, when clicked, can download harmful spyware or adware to your computer. While some make legitimate offers, many pop-ups are attempts to obtain your sensitive information. First National Bank will never ask you to verify personal financial information in pop-up advertisement.

Helpful Tips to Protect You

While online banking is safe, as a general rule you should always be careful about giving out your personal financial information over the Internet. Review the following tips to protect your personal information while using the Internet.

- Regularly log into your online accounts to verify that your bank, credit, and debit card statements and transactions are legitimate.
- Be suspicious of any e-mail with urgent requests for personal financial information.
- If you receive an unsolicited e-mail from any source asking you to click on a link to visit a site and input personal data, be very wary of it.
- Be cautious about opening any attachments or downloading any files from e-mails, regardless of who sent them.
- Instead of clicking on links in emails, type in the URL that you're familiar with, such as www.fnbfst.com, or select the Web address saved in your browser’s "Favorites".
- If an offer sounds too good to be true, it probably is and should be avoided.
- If you have any doubts about the validity of an email, contact the sender using a telephone number you know to be genuine.

- Before you initiate an online transaction, make sure your personal information is protected by looking for indicators that the site is secure. URLs for secure sites typically begin with https instead of http and display a lock in the lower right corner of your browser.
- Use anti-virus software and keep it up-to-date.
- Make sure you have applied the latest security patches for your computer. Most software providers, like Microsoft, offer free security patches.
- If you have broad-band Internet access, such as cable modem or DSL, make sure that you have a firewall.

We take numerous steps to keep your account information secure. However, you must take precautions as well. It is critical that you use a highly secure password for all of your financial accounts. Avoid using your pet's name, child name or any other publicly know information that could easily be guessed. The most secure passwords are a combination of letters and numbers, not simply an address, phone number or birth date. For added security, remember to change your password on a regular basis and avoid using the same password for multiple accounts.

Choose a good password - Your online password, along with your access ID, authenticate your identity when accessing online accounts. You should carefully select a password that is difficult to guess and not use personal information or a word that can be found in the dictionary.

Keep your password safe - Even the best password is worthless if it’s written on a note attached to your computer or kept in your checkbook. Memorize your password and never tell it to anyone.

Change your password regularly - It’s important to change your password regularly. Every time you choose a new password, our online banking system runs a quick program to test its safety. If we can guess it, we will immediately ask you to choose another one.

Remember to log off properly - You may not always be at your own computer when banking online. Therefore, it’s important to log off using the “log off” link at the top of each Online Banking page. If you forget to do so, the system automatically signs you off after 10 minutes of inactivity.

If you need any assistance, you can also contact us at 432.336.8541.

How We Protect Your Online Security

The security of your financial information is one of First National Bank’s most important responsibilities. We maintain our Online Banking platform using stringent information security guidelines and use many lines of defense to protect your account information. From authentication, SSL, encryption software, high-end firewalls, and automatic log off, your information is always safe and secure.

- **Authentication** ensures that you, the legitimate user is communicating with us and not a fraudster who does not have authority to access your online accounts.
- **SSL** stands for "Secure Socket Layer." This technology allows users to establish sessions with secure Internet sites, meaning they have minimal risk of external violation. Once inside the Online Banking site, our use of SSL technology keeps you and your account information secure.
- **Encryption** turns words and phrases into coded language. All of your online activities during an Online Banking session become a string of unrecognizable numbers before entering the Internet. We employ the strongest forms of cryptography that are commercially available for use over the Internet, so your account information will read as gibberish to everyone but you and our financial institution.
- **High-end firewalls** protect our computer systems interacting with the Internet against unauthorized access by outside individuals or networks.

- **Automatic log off** is done automatically after 10 minutes of inactivity during an Online Banking session. So, if you forget to log off after your online session, we will do this for you to prevent anyone else from accessing your account.

From the moment account information leaves your computer to the time it enters our Online Banking system; we take numerous steps to ensure your information is secure in cyberspace. We make sure only authorized people with secure browsers can access our system.

- You must enter your password, and we must verify it before you are allowed to access your accounts.
- Only browsers supporting the SSL security protocol with 128-bit encryption can be used to log on to our system.
- Once online, we make sure only you can view any information about your accounts.
- SSL uses a digital signature to make sure that no one can send you false information; your browser will only accept information from the Online Banking system.
- SSL also uses the highest level of encryption supported by your browser to encrypt all information before it is sent. This ensures that only the browser that logged on can read any information the system supplies.

Identity Theft

Identity Theft is a growing concern and suspected or confirmed Identity Theft should be dealt with right away. For more information on the steps you should take, please visit the following Federal Trade Commission website: ***http://www.ftc.gov/bcp/microsites/idtheftedu/microsites/idtheft***