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 site, 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 Bank of Little Rock will never ask for sensitive information from you via e-mail (ex. Social security number, access ID, passcode 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. Bank of Little Rock 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 <FI Web address>, 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.

- **Choose a good passcode** - Your online passcode, along with your access ID, authenticate your identity when accessing online accounts. You should carefully select a passcode that is difficult to guess and not use personal information or a word that can be found in the dictionary.
- **Keep your passcode safe** - Even the best passcode is worthless if it’s written on a note attached to your computer or kept in your checkbook. Memorize your passcode and never tell it to anyone.
- **Change your passcode regularly** - It’s important to change your passcode regularly. Every time you choose a new passcode, 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 Internet 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 (501)376-0800.