

Fraud Prevention Tips

Protect Yourself From Internet Scams

There are many scams that take place online. Here are just a few to be aware of:

- **Phishing** – You receive an email that appears to come from a bank. The email will warn you of a serious problem. The email will encourage you to click on a link that directs you to a fake website. Then you will be asked for account or personal information.
- **Keystroke Logging (Keylogging)** - Keylogging is a method by which fraudsters record your actual keystrokes and mouse clicks. Keyloggers are “Trojan” software programs that target your computer’s operating system (Windows, Mac OS, etc.) and are “installed” via a virus. They can be particularly dangerous because the fraudster will capture your user ID and password, account number, Social Security Number, and anything else you type. If you are like most users and have the same ID and PIN/Password for many different online accounts, you will essentially grant the fraudster access to any company with whom you conduct business. After all, they’ve got your login credentials so they appear to be a valid user. Here are some ways you can prevent yourself from being a victim of keystroke logging:
 1. 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.
 2. Keep your Operating System up-to-date with the latest security patches.
- **Lottery/Sweepstakes** – You are the lucky winner even though you never entered any lottery or sweepstakes. To claim your prize you are told to send in money first to pay taxes or something similar. After you send in your money, you never receive any winnings.
- **Work At Home Employment Opportunities** – In a work at home scam you are sent money via check, wire or ACH and are instructed to return a portion back to your employer. Unfortunately, the check wire or ACH was sent fraudulently.
- **Advance Fee Fraud (419 Scams)** – You receive notification that some long lost unknown relative has left you money, or, you have just been given the opportunity of a life time as someone looking for a business partner is willing to let you have millions of dollars. Unfortunately, you have to send them money not just one time, but again and again without receiving any of the promised millions.
- **Romance** – Your perfect match asks you for assistance with a financial matter. They just want your bank and account information so you can help them deposit funds. They tell you to keep a small amount for your troubles and return the remainder to them. Then your bank calls to tell you the check he or she sent to you was returned. Now you owe your bank the money and your new found match no longer responds to your calls.
- **Hard To Find Purchases** – Be wary of non-local sellers of hard to find items that require payment by MoneyGram or Western Union. Always use a credit card online for purchases. Otherwise, once you send that money it’s gone, and your hard to find item may never arrive.
- If you believe you are the victim of an online fraud scam:
 - Contact Bank Mutual Customer Service for assistance if you believe your accounts are at risk at 1-800-261-6888.
 - File a police report.
 - For more information or to file a complaint, see the Internet Crime Complaint Center website at <http://www.ic3.gov>



Bank Mutual

Trust. The feeling is Mutual.

bankmutual.com

Member
FDIC