Fraud Prevention Tips

Don't become a victim.

The old adage that "if it's too good to be true it probably is" applies today more than ever. There has been an increase in scams to defraud people of their money and identity. Criminals use the mail service, phones, and increasingly email and the Internet, to perpetrate a wide variety of fraudulent activities.

To help you become more informed and better prepared we're providing you with some helpful tips.

What is fraud?

Fraud is an intentional misrepresentation or concealment of information in order to deceive or mislead. The ultimate goal of the perpetrator is to get your money through deception. Unfortunately there are many types of fraud and new methods are being devised every day.

Two common fraud methods are:

Identity theft: Identity theft occurs when your personal information (anything from bank account numbers to your name and address) is stolen and the thief is able to use your information without your permission, such as purchasing items with money from your account, potentially, damaging your credit record and good name in the process.

Phishing: This type of online scam exploits both email and the Internet. By using a combination of spam emails and fake representations of legitimate corporate websites (e.g., bank, a credit card company, internet provider, etc.), the "phisher" is able to gain access to your most critical financial information (account numbers, Personal Identification Numbers (PIN), etc.).

Phony emails are often urgent in nature that ask you to update or validate your information. Some even pretend to protect you against fraud or invoke national security as a way to deceive you.

How does it happen?

Some of the most common methods of fraud involve the following:

- You receive an email pretending to be a representative of your bank which asks for your account numbers, security codes, passwords, PIN or other financial information to "authenticate the account." Tri Counties Bank will never ask for this information via email.
- Someone offers to pay you extra for your time and trouble.
- Someone pays you for a sold item for more than the asking price, then asks that you send or wire extra funds elsewhere.
- Someone gives you a cashiers' check and you do not know the person.
- A "relative or friend" emails or calls, claiming their wallet was stolen while on vacation, or they've been put in jail, and requests that you immediately send funds to help get them back home or resolve their situation.
- You are asked to send money before you can collect a prize or lottery winnings.

How can I avoid it?

- DO NOT share your personal information with anyone that emails or calls you.
- Make sure you know "who" and "why" before giving out your personal information.
- Shred receipts, bank statements and unused credit card offers.
- Watch for missing mail (credit card bills, utility bills, bank statements, etc.).
- DO NOT mail bills from your own mailbox if it cannot be locked or if the postal box is full and items could be removed.
- Review statements and bills frequently for unauthorized items.
- DO NOT buy from an unfamiliar company. Legitimate businesses understand that you want more information about their company and are happy to comply.
- DO NOT pay in advance for services. Pay for services only after they are delivered.
- DO NOT pay for a "free prize." If a caller tells you the payment is for taxes, he or she is violating federal law.
- Never send money or give out personal information such as credit card numbers and expiration dates, bank account numbers, dates of birth, or social security numbers to unfamiliar companies or unknown persons.
- If you have been victimized once, be wary of persons who call offering to help you recover your losses for a fee paid in advance.
- Always protect your PINs and passwords, change them frequently.
- When selecting passwords or passphrases remember that longer is stronger.

If you think you may have provided information to someone you suspect of fraud, change your password immediately and contact the company where your information may have been compromised.

Above all, protect your personal and account information at all times.

tri counties bank

Service With Solutions®

1-800-922-8742 | TriCountiesBank.com

Member FDIC
ADV-0079 (05/20)