MACON-BIBB
EMPLOYEES CREDIT UNION
"Where People Are Worth More Than Money"

Learn to Avoid Fraud

Crooks use clever schemes to defraud people every day. They often use deception and tricks to get you to send money or give them your personal information. Study the methods and tricks used to steal from you. If you are 60 or older, fraudsters assume you are not experienced with today's technology and take advantage of you. Even much younger people fall prey to the sophisticated ways these criminals steal money and sensitive personal information. Invest time studying this and other articles about how to protect yourself.

Scammers often pretend to be someone you trust, like an employer, a government official, a family member, a charity, or a company you do business with. Don't send money or give out personal information in response to an unexpected request whether it comes as a text, a phone call, or an email. Follow these practical tips to help avoid losing your money or even your identity to heartless thieves.

1. **Text Messages.** We all look at text messages quickly because in the past they have almost always been from someone we know. But today your mobile phone number is likely on many lists. A recent common technique is to send you a text saying there's a problem with your Amazon, Apple, Google, utility, bank or phone account which must be corrected immediately. If you tap the link, it takes you to a web page which requests your personal information such as email address, account number and password. Sometimes tapping the link installs malicious software on your phone which sends back as much of your personal information as it can find.

   Don't believe text messages from unverifiable senders. When in doubt, just delete the message. The credit union will never send you a text message you didn't expect.

2. **Phone Calls.** Don't answer phone calls if you don't recognize the caller ID. If it's important they will leave a message. Also, you can't trust caller ID. Scammers use technology to display fake caller ID information, so the name you see is not always real. If someone you're assuming is legitimate calls asking for money or personal information, hang up. If you think the caller might be telling the truth, hang up and call the organization to verify the caller is an employee. A good number to call is the one printed on a credit/debit card, a bill, or a statement.

   Today you can't afford to be polite by answering every phone call. The credit union will never call you to ask for account information.

3. **Email.** If you receive an email from a name and email address you recognize, don't assume it's legitimate. Scammers use technology to display what appears to be a trusted identity, but you can verify it with a simple method. If you are using a smartphone, tap the sender's name. Their actual email address will appear under their name. If you are using a computer, hover your cursor over the sender's name to display their actual email address, and hover over any links to see if it goes to a legitimate website. Look for mis-spelled words and poor grammar – these are red flags.

   The credit union will never send you an email asking you to reply with sensitive personal information.

4. **Other Tips.**
   - Never pay upfront for a promised prize, gift or service.
   - Pay online or by phone only with your credit card, not a debit card, Western Union or MoneyGram. Credit cards are the only way to have significant fraud protection.
   - Be skeptical about free trial offers that require giving them your credit/debit card information.
   - Before you give up money or personal information, talk to someone you trust. Do not give in to high-pressure sales tactics.