tips to protect yourself

- Do not send money to someone you don't know or have not met personally.
- Do not respond to online solicitations for "easy money."
- Give only to well-known and credible charities.
- Do not agree to deposit a check and wire money for anyone.
- Do not reply to messages or emails asking for personal or financial information.
- Use caution answering the phone from an unfamiliar number.
- Phone numbers can be faked. Even if your caller ID shows that a caller is using a number in your area, they could actually be from another state.
- Do not open emails from senders that you do not recognize or click on unknown links in them.
- Use strong passwords with at least eight characters, including letters, numbers, and symbols.
- Do not trust "free" credit report information.
- Never allow strangers to come into your home and take information about you or your assets.
- Never sign contracts that have blank lines in them. Someone can add clauses later that harm you.
- No legitimate company will ask to be paid in Apple or Google Play cards.
- You should never have to send money back to someone that sent you a check for lottery winnings, a new job, or the sale of an item. Sending cash back always equals fraud.
- Do not file a false claim with your credit union. By filing a false claim you are a co-conspirator to fraud.
- Treat your mail carefully. Place outgoing mail in a secure collection box and remove mail from your mailbox promptly.
- Only carry what you need in your wallet. Do not carry your social security card keep it at home in a secure location.
- Only give your social security number to trusted entities such as your financial institution, your employer, government agencies, law enforcement, and insurance companies.
- Protect your PIN number.
 - Do not give your PIN to anyone over the phone or internet.
 - Never let someone enter your PIN for you.
 - Do not write it on your card.
 - Memorize your PIN.



888.213.2848 american1cu.org

Boldly Generous. Convenient. Uncomplicated.