types of <u>scams</u>

Lottery and Sweepstakes Scams

Emails or letters stating you won a sum of money and instruct you to keep the notices secret and send money for fees. Criminals make money by convincing victims to pay for processing taxes, or delivery, or provide bank account information to verify their identity.

Romance or Sweetheart Scams

A new love interest, usually met online, asks for money for many reasons and can never meet in person. Do not give out your online banking credentials to someone you meet online, but have never met in person.

Technology Expert Scams

Scammers call and claim to be computer techs employed by well-known companies such as Microsoft or Apple. The caller will state they have detected a virus or malware on your computer. They will diagnose a nonexistent problem and ask you to pay for unnecessary or harmful services.

IRS Scams

Scammers will call claiming your taxes need to be paid or you will get arrested. The IRS will not call you and demand immediate payment. They will send you a bill and will never request payment in gift cards.

Grandparent Scams

Scammer poses as your grandchild stating they need money to post bail or pay for another emergency event.

Phishing

Phishing scams are when you receive an email from a familiar entity such as your credit union, credit card company, or government agency asking you to confirm your account credentials. A legitimate company would never send emails asking for account information because they already have it. Delete the email and do not hit reply.

Card Skimmers

Card skimmers are devices that can be attached to a gas pump or ATM in order to steal card information. Look for a security seal at the gas pump or ATM - these are used as a way to prevent tampering. If you notice unauthorized charges on your card, report it to your financial institution.



888.213.2848 american1cu.org

Boldly Generous. Convenient. Uncomplicated.