Fraud Education

Protect Yourself From Fraud

Have a Question?

safe & secure

Arm yourself against fraud
with these important tips.

Financial fraud is pervasive and can happen to anyone. At Rollstone, we believe that your best defense is to educate yourself and be vigilant. The information and links on this page will help you arm yourself with the knowledge needed to avoid fraud and loss. Always remember – if something seems suspicious, it probably is.

As a reminder, Rollstone Bank & Trust will NEVER call, email, or text you and ask for confidential financial information. If you are ever unsure of something with our name on it, please contact us for verification. If you think you are a victim of fraud or identity theft, report it to us immediately by calling 800.640.1166, and also report it to the Federal Trade Commission (FTC).

Listed below are some of the more common scams, along with tips on how to identify and avoid them.

Tech Support Scams *Expand*

Legitimate tech companies will not contact you by phone, email, or text message to tell you there's a problem with your computer. Along the same lines, security pop-up warnings from

legitimate tech companies will not ask you to call a phone number or click on a link. If you suspect there is a problem with your computer, call or visit a reputable business in your area.

Scams Against Seniors *Expand*

While anyone can become a victim, fraudsters often target senior citizens, as they typically have more money than young people. Talk to your elderly family members about scammers and help educate them about various scams, such as grandparent scams, romance scams, and more.

Social Engineering *Expand*

Social engineering attacks occur when a scammer uses information to build trust with potential victims. The attacks can take many forms and often start with a fake email designed to trick people into giving up personal information. They may also come in by way of phone calls or text messages. To protect yourself from falling prey:

- Uncover email addresses by right-clicking on the sender's name to see the message properties.
- Verify information through a separate channel, such as a Google search.
- Do not click on links or open attachments unless you are 100% sure that they're legitimate.
- Trust your intuition. Take a pause and ask yourself, "Does this make sense?"

If you are victimized, notify your bank and report the scam to the Federal Trade Commission.

Phishing *Expand* Phishing is when a scammer sends email or text messages, supposedly from a legitimate company like your bank or credit card company, to trick you into giving out personal information, like account numbers, passwords, or your Social Security number. They use your information to access your

accounts, which can lead to identity theft and financial loss. Common features include:

- Too good to be true – it's very unlikely that you won the lottery or a free iPhone. Do not open suspicious emails making lavish claims.
- Sense of urgency – if you're being pressured to act quickly, the email is probably a scam. Pause and ask yourself, "Does this make sense?"
- Hyperlinks & attachments – clicking on a link or opening an attachment that's sent with a phishing email could lead to viruses or malware being installed on your computer.
- Unusual sender – if you get an email that is unexpected or out of the ordinary, don't open it, whether you know the sender or not. If you're unsure if it's genuine, reach out to the sender through another means and ask if they sent it to you.

Imposters *Expand*

Imposter scams begin with a call, text message, or email, and the scammer pretends to be an authority, like law enforcement or the IRS, or someone you know, like a friend or family member. They may even pretend to be a charity. Then they try to convince you to send them money or share personal information.

Learn how to recognize imposter scams and what to do if you suspect you've been victimized.

Romance *Expand*

Scammers take advantage of people looking for love, often through social media apps. They pretend to be romantically interested in the target and play on their emotions to get them to provide money, gifts, or personal details. Some

warning signs of a romance scam:

- They send you a picture that looks more like a model than a normal photograph
- They want to leave the social media or dating site and communicate through email or text message instead.
- They lavish you with attention.
- You never meet them in person. They make plans to meet, but always have an excuse to cancel.
- They need money fast to deal with some sort of emergency.

Veterans *Expand*

Military veterans, active-duty service members, and their families are frequent targets of con artists. In fact, they are targeted more often and lose more money to fraud than civilians. Scams include fraudulent calls from companies that pretend to be affiliated with the Veterans Administration or a veterans charity, like the DAV.

Victims in the military community lost $414 million to fraud in 2022. Learn how to recognize scams and protect yourself.