TRUST NO ONE:
Fraudsters Are Everywhere and Target Everyone

Fraudsters will utilize methods known as **social engineering** to trick or manipulate you into divulging personal and confidential information needed to access your accounts or to send them money directly.

ALWAYS BE SKEPTICAL of unsolicited phone, email, text, or social media interactions especially when someone is asking you to divulge personal or confidential information such as Social Security numbers, birth dates, phone numbers, emails, account numbers, usernames, passwords, credit card numbers, or bank account numbers.

VISHING

The act of making deceptive phone calls to trick individuals into revealing personal, confidential, and/or financial account information.

PHISHING

The act of sending deceptive email messages to trick you into revealing personal, confidential and/or financial account information.

SMISHING

The act of sending deceptive text messages to trick recipients into revealing personal, confidential and/or financial account information.

Never release personal, confidential, or financial account information to anyone you don't know — especially if they initiate contact and claim to be associated with a company or organization you are familiar with or have accounts with.

HOW TO AVOID BEING SCAMMED

- Don't overshare on social media. Fraudsters often use social networking sites to extract information to answer security questions or piece together any personal information they need to commit fraud.
- Be cautious about sharing any type of personal information unless necessary. Even the most basic data (birth dates, phone numbers, addresses, and email addresses) can be used to steal your identity.
- Verify the authenticity of any requests for information or transactions before providing any personal or financial details.
- Be wary of unsolicited offers you see in ads, pop-up windows, and email — especially from people or organizations you don't recognize or interactions that you didn't initiate.

1013-2024

LIMRA LOMA
Navigate With Confidence

HOW TO HANDLE Suspicious Phone Calls

1. **Don't provide any information** and instead ask them for their name and contact information and tell them you will contact the company directly.
2. **Hang up**. If they are legitimate, they won't get upset with you or try to convince you to not call the company or organization directly.
3. **Obtain the** company or organization's phone number through a reputable source such as the company website, online directory, recent bill, or financial statement.
4. **Contact the company directly** to confirm the request was legitimate and if not, inform the company that someone was impersonating one of their representatives. If it's a company that you have accounts with, ask them what additional security features they can put in place to protect your account.

HOW TO HANDLE Suspicious Emails or Text Messages

1. **Don't click on links or open attachments** in unexpected emails or texts, especially from individuals or organizations you don't normally interact with.
2. **Don't reply to unexpected emails or texts**, especially from individuals or organizations you don't normally interact with.
3. **Delete all unexpected emails or texts**, especially from individuals or organizations you don't normally interact with.
4. **Contact the company or organization directly** if you believe there is a possibility that the email or text was legitimate. Obtain the company or organization's phone number or email through a reputable source such as the company website, online directory, recent bill, or financial statement.

Never use the contact information provided in a suspicious phone call, email, or text to contact the company or organization unless you confirm it's legitimate through another reliable source such as company website, online directory, recent bill, or financial statement.

CONFIDENCE SCHEMES are prevalent and can often easily convince individuals to send money under false pretenses. Anyone of any age can fall victim to a confidence scheme — even savvy and cautious individuals can be deceived.

ROMANCE SCHEMES often begin with an unsolicited email or social media post or friend request from someone unknown. The fraudster will interact with their victim repeatedly to establish an ongoing friendship or romantic relationship. The fraudster will engage in normal interactions and conversations and even phone and/or video call for many weeks and even months before they ask for money. At some point they will tell the victim about a situation that requires them to pay for something they cannot afford, such as a family member's medical condition or arrest, they've lost their job, or they need money to visit. Sometimes they won't ask for money right away and hope they'll be offered a loan or cash gift by the victim. At some point they will ask for money and often start with small amounts. They may even pay the victim back for small initial loans to build trust. As the relationship continues, the amounts requested increase and repayments stop. Once the fraudsters have received all they believe they can get out of the victim, they will delete their account or stop responding.

INVESTMENT SCHEMES also often begin with an unsolicited email, text, or social media post or friend request from someone unknown. The fraudster will interact with their victim repeatedly to establish an ongoing friendship or even a romantic relationship. The fraudster will often tell stories and post pictures depicting a lavish or wealthy lifestyle to convince the victim that they are a successful investor and/or businessperson. They may carry on the relationship for weeks or months without asking the victim to invest in the hopes the victim will ask them to allow them to invest. If the victim doesn't ask, the fraudster will eventually ask the victim to invest and usually indicates or promises the returns will be substantial. Often the initial investment amount requested is small with subsequent requests increasing over time. Victims often receive statements showing investment gains and occasionally may even receive dividends or investment proceeds. Once the fraudsters have received all they believe they can get out of the victim, they will delete their account or stop responding and their victims' money is gone for good.

HOW TO HANDLE Romance or Investment Schemes

1. Don't give money or loans to anyone you meet online or via unsolicited phone calls, texts, or emails.
2. Always ask a trusted friend, relative, caregiver, financial professional, or local police for their advice before giving any money to anyone you meet online.

KIDNAPPING, ARREST, AND ACCIDENT SCHEMES are usually initiated with a phone call stating a loved one (often a grandchild) has been kidnapped, arrested, or involved in an accident. There is always the demand for money to be paid and paid quickly. The fraudsters will often have sounds of someone in the background crying or pleading for help and may have someone that sounds like the loved one talk to the victims briefly telling them to pay what's demanded and not call the police or their parents. The fraudsters will often ask for payment to be made via crypto currency, gift cards, and/or cash apps.

HOW TO HANDLE Kidnapping, Arrest, and Accident Schemes

1. Hang up and attempt to contact the loved one allegedly kidnapped, arrested, or in an accident. If you can't reach them, call their parents, other relatives, or friends. You will most likely learn that they were not kidnapped, arrested, or in an accident.
2. If unable to confirm the loved one is safe, call their local police department.

THE TYPES OF SCHEMES ARE ENDLESS Fraudsters continually devise new schemes to trick victims into parting with their money. Some popular scheme types include:

IRS — This is when you are notified that you owe the IRS money and if you don't pay, they will issue a warrant for your arrest or come to your house to collect. They often ask for payment to be made using gift cards or bitcoin. If someone contacts you claiming to be with the IRS, don't pay them. Instead, visit the IRS Recognizing Tax Scams and Fraud website to help validate the legitimacy of the request.

It Support/Help Desk — You may receive a call or an email allegedly from Microsoft, other tech company, or even your employer's help desk informing you there is an issue with your computer, and they need access to it. Once they access your computer, they may steal your personal information or lock it so you can't access it until you pay them to unlock it. Never allow anyone to access or "remote in" to your computer unless you initiate the request.

Charity and Disaster Fraud — Fraudsters create fake charities to collect funds for themselves. They will often strike after high-profile disasters such as hurricanes or floods when they know many people are looking to help. Only donate to established charities you know and trust. The Federal Trade Commission (FTC.gov) has a Donating Safely and Avoiding Scams website that will help you confirm a charity is legitimate.

DON'T BE FOOLED BY DEEPFAKES

Given recent advancements in technology, including generative AI, fraudsters can easily create highly realistic fake videos, audio, or images. These can be used by fraudsters to successfully impersonate anyone they choose. Fraudsters can easily convince you that you're interacting with someone you're not. They can even create audio and video images that appear to come from or be one of your friends or relatives. Deepfakes can be extremely hard to detect. Always independently verify interactions before sending money or anything of value to anyone you don't have a preexisting and confirmed legitimate relationship with.

DON'T BE A MONEY MULE AND ALLOW OTHERS TO USE YOUR BANK ACCOUNT

When a fraudster has successfully convinced a victim to send them funds, they need a legitimate and established bank account to receive them. To obtain access to a legitimate account, fraudsters often convince another individual to allow them to use their bank account. In exchange for access, the fraudster will usually allow the victim to keep a portion of the funds if they transfer the balance to a bank account controlled by the fraudster. This activity is illegal and can make you an accessory to a crime. **Never allow anyone to use your bank account or any financial account to facilitate the transfer of funds.**