Tactics of a Scammer

HOW TO IDENTIFY A SCAM

STAR

Make no mistake, scams are big business and fraudsters are good at what they do. They have no shame and will say anything — make up outrageous stories, promise you the world, gain your trust and even attempt to put you in great fear — whatever it takes to get to your money and personal information.

Although a scammer will use any means necessary, there are some common tactics to look for:

1. **Impersonation:** Scam artists use distance, the internet and technology to stay anonymous and hidden. They love to impersonate government officials, retail business employees and even bank employees. A scammer loves to impersonate individuals from organizations you trust and do business with.
2. **Urgency:** "You must act now," "final request," "immediately"...by creating a sense of urgency and applying pressure, a scammer is hoping you are distracted and that you make mistakes. Creating a false sense of urgency is a tactic utilized to get you to provide information you would not normally divulge. Maybe it's a great deal or the threat of danger, always take caution when you feel pressured to make quick decisions.
3. **Social Media:** Historically scammers have utilized email, text messages and phone calls to perpetrate their activities. While scammers still use these methods, social media has become a hot spot for all kinds of fraud schemes. According to the FTC, in 2022 consumers reported losing more than $1.2 billion to fraud that started on social media. Beware of marketplace purchases, employment offers, investment deals and online relationships that lead to requests for money. Linked ads to fake stores can also intercept your personal information or funds.
4. **Isolation:** Scammers often deploy isolation techniques. They will instruct you and often demand that others are not to be trusted. Their frauds are more effective when they keep you from talking to trusted sources.

If you find yourself in a call or in an interaction where your information is being requested, take the following steps:

1. Be suspicious of any unexpected contact.
2. Slow it down. Pause, hang up the phone or ignore the message. This will give you time to research the offers and claims being made.
3. Find help, talk to someone. Make a call to a family member or friend, possibly even a call to 911. Reach out to anyone you trust. You may also come to your local STAR branch or contact customer solutions at 1-800-395-STAR (7827).
4. Practice online safety and security. Use different passwords for your online services, change them often and consider a reputable password manager. Utilize multi-factor authentication whenever possible.
5. Do not provide personal identifying information or financial identifiers to strangers or unexpected contacts. Never provide usernames, passwords, or access codes.

STAR is committed to your financial security and privacy. For more tips and information, visit STAR'S security page. STAR also has a dedicated Fraud team ready to assist in any fraud-related matter.

https://www.starfinancial.com/security