SCAM TACTICS

RECOGNIZING SCAM TACTICS

Scams come in many forms, but they all have one goal: to deceive and/or manipulate people to achieve financial gain. Whether it's through a phone call, online or face-to-face interaction, criminals use manipulation, fear and false promises to trick victims. Their goal is to convince people to send money, share personal information or provide access to their accounts. Understanding key scam tactics is crucial to protecting yourself and others.

SCAM COMMUNICATION METHODS

Criminals use a variety of communication methods to perpetrate scams. They often intentionally select a method based on the type of scheme and the potential victims targeted. For example, social media or messaging apps may be the most effective methods to reach younger individuals for a cryptocurrency investment scam. Criminals choose the schemes and communication types that will generate the most money.

Social Media / Message Apps
Common path for criminals to initiate contact – such as offering a fake product or new "friendship" to impersonate someone else.

Phone Calls / Text Messages
Widely used method for contacting potential victims, often resulting from numerous data breaches that have exposed this information.

Emails
Prevalent outreach method based on the ease of creating and sending messages to a large number of people.

COMMON SCAM TACTICS

Each tactic can be a red flag to identify typical scam requests.

Urgency and Pressure

Creating a false sense of urgency can motivate quick action without thinking about potential risks.

- **Example:** "Your account will be locked in 10 minutes unless you act now."
- **Tactic:** Panic often bypasses rational thinking, making victims more likely to comply quickly.

SCAM TACTICS

Impersonate Legitimate People, Businesses or Government Agencies for Credibility

Criminals pretend to be trustworthy – such as an employee of a well-known business, organization or government agency.

- **Example:** A criminal claims to be from a tech support company and requests access to your computer to remove malware.
- **Tactic:** They often spoof (impersonate) phone numbers or email addresses to look legitimate.

Too-Good-to-Be-True Offers

Victims can be lured with unsolicited offers of large rewards, lottery wins or high-paying work that requires little effort.

- **Example:** "You've won $25,000 – you can claim it for a small fee."
- **Tactic:** Excitement can cloud judgment.

Fear and Threats

Fear-based scams make you believe something bad will happen if you don't take immediate action.

- **Example:** "Your grandchild has been kidnapped – send money now."
- **Tactic:** Emotions are exploited to override logical thinking.

Requests for Untraceable Payments

Criminals often ask for payment through gift cards, wire transfers, prepaid cards or cryptocurrency.

- **Example:** "Buy gift cards and send me the codes on the back of the card."
- **Tactic:** These methods are challenging to trace or recover funds.

Build Trust

Some criminals develop relationships over time to earn your trust before asking for money.

- **Example:** A person you've met online says he loves you but needs help with a financial emergency.
- **Tactic:** Emotional manipulation happens over weeks or months.

SCAM TACTICS

Fake Websites and Links

Criminals create fake websites that look real to steal your login credentials or personal information.

- **Example:** A fake merchant website asks you to "log in to verify your account."
- **Tactic:** Website addresses and internet links differ slightly from legitimate sites or use strange domain names.

Confidentiality

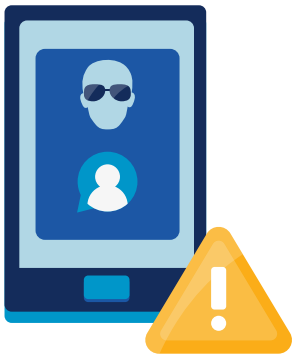
Criminals convince victims to avoid sharing details of requests or transactions with their family or friends, which may otherwise expose the scams.

- **Example:** "You are the subject of a criminal investigation. Do not discuss this case with anyone or risk severe penalties."
- **Tactic:** Criminals posing as law enforcement or government officials may use that alleged authority to prevent disclosure of details that could expose the scam.

SIGNS YOU'RE BEING SCAMMED

Be vigilant for these scam indicators:

- Urgent request to send money
- Promised something valuable for little or no effort
- Out-of-the-blue contact by someone claiming to be in authority
- Pressure for you to act fast or risk penalties



CONCLUSION

Criminals adapt quickly, but their core tactics remain the same: pressure, deception and manipulation. Your best defense is staying informed and alert. When in doubt, pause, verify – and never give out personal or financial information.

The scams mitigation toolkit was developed by the Federal Reserve to help educate the industry about scams and outline potential ways to help detect and mitigate this fraud type. Insights for this toolkit were provided through interviews with industry experts, publicly available research, and team member expertise. This toolkit is not intended to result in any regulatory or reporting requirements, imply any liabilities for fraud loss, or confer any legal status, legal definitions, or legal rights or responsibilities. While use of this toolkit throughout the industry is encouraged, utilization of the toolkit is voluntary at the discretion of each individual entity. Absent written consent, this toolkit may not be used in a manner that suggests the Federal Reserve endorses a third-party product or service.