SCAM DETECTION FOR INDIVIDUALS

Scams rely on sophisticated and ever-evolving tactics. However, we can all play a role in detecting them. Ask yourself the following three questions when encountering a potential scam.

1. **Is it phishing?** Determine whether an email, phone call, or text message is likely to be phishing, a form of social engineering where criminals attempt to deceive individuals to share sensitive information or make a payment.
   Potential red flags:
   - No relationship with the sender
   - Mismatch between the sender's name and email domain
   - Typos, misspellings or poor formatting

2. **Does the message contain markers of common scam tactics?** Criminals often repeat tactics to deceive individuals for financial gain.
   Potential red flags:
   - Sense of urgency or attempts to elicit fear
   - Too-good-to-be-true offers
   - Common scam schemes: investment, romance, job/employment

3. **Can you verify the legitimacy of the organization or the offer/request?**
   Potential red flags:
   - Cannot easily verify that the organization is real — not merely plausible — in ways other than responding to the inquirer
   - Unsolicited requests for money, personal information or account access

SCAM DETECTION FOR INDIVIDUALS

Don't Take the Bait: Spot Phishing

- Unsolicited contact
- No previous relationship with business or entity
- Email domain different than that of the sending organization
- Logos or branding in message appear incorrect, blurred or are not included
- Phone calls flagged as "Spam Likely" or "Potential Spam" by the carrier
- Links that contain random characters or references to some other entity or domain

If you can spot any of these phishing indicators, you may have detected a scam.

Recognize the Signs: Stay Informed and Aware

- Sense of urgency or attempts to elicit fear
- Requests for personal information or up-front payments
- "Risk-free" investment offers or "guaranteed" returns
- Unusual requests for money from a "friend" or "family member"
- Merchandise offered at incredibly low prices

If you can spot any of these common scam tactics / schemes, you may have detected a scam.

Confirm Your Instincts: Verify and Investigate

- Confirm job postings on actual business website or on a trusted job board
- Read independent online reviews of the business or merchant
- Search the web for investment fund name, company, cryptocurrency name/symbol
- Refer to reputable websites and registries, such as Better Business Bureau and Charity Navigator, to verify legitimacy of organization details

If you cannot verify the legitimacy of an organization or offer/request, you may have detected a scam.

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.