HOW SCAMS OCCUR

Scams are no longer simply awkward emails from distant princes asking for your bank details. They are now highly sophisticated operations run by individuals and organized groups who leverage technology, psychology and timing to exploit their victims. To protect yourself and others, it's crucial to understand how scams occur – how they start, how they manipulate and how they succeed.

THE SETUP: TARGETING THE VICTIM

Criminals often begin by identifying potential targets. This can happen in various ways:

- **Random targeting:** Mass emails, robocalls and text messages are sent out in bulk, hoping someone will bite.
- **Selective targeting:** Criminals use data breaches, social media or public records to zero in on specific individuals who are the most likely to respond, such as the elderly, job seekers or those looking to invest.
- **Phishing and social engineering:** Criminals may gather information from public profiles to personalize the scam, increasing its credibility.

During this phase, criminals' goals are to establish contact and build a foundation for manipulation.

BUILDING TRUST

Once the initial contact is made, criminals use psychological techniques to weaken their potential victim's defenses.

- **Emotional pleas:** Romance scams generate a sense of affection and companionship. Charity scams tug on your heartstrings. Investment scams excite you with visions of wealth.
- **Fear and urgency:** Threatening calls from "government officials," fake tech support people claiming your computer is infected, or bogus messages from your bank demanding immediate action are designed to quickly induce fear and panic.
- **Authority impersonation:** To gain credibility, many criminals pose as trusted individuals, such as public figures, employers, friends or relatives.

The goal is always to exploit basic human emotional responses: trust, fear, greed and love.

HOW SCAMS OCCUR

THE HOOK: ASKING FOR SOMETHING

Once criminals have built enough trust or fear, they make a request. This is the critical point where the scam turns into theft.

- **Money:** Traditional money transfers, cryptocurrency, gift cards or donations.
- **Information:** Personal details, passwords, bank account numbers or Social Security numbers.
- **Access:** Granting remote access to your computer, installing malicious apps or clicking on infected links.

The initial "ask" is often small, just enough to test the waters before scaling up to larger requests.

THE EXIT: VANISHING ACT

Once criminals get what they want, they disappear:

- Phone numbers go dead.
- Email addresses bounce back.
- Websites vanish or become inactive.
- Social media profiles are deleted or blocked.

Often, victims don't even realize they've been scammed until much later – when a package never arrives, money is gone or identity theft surfaces.

REPETITION OR RETARGETING

Some criminals don't stop after one incident. They may:

- Re-target the same victim, pretending to be someone else (e.g., offering "recovery" services for the initial scam).
- Sell victims' information on the dark web, leading to more scams down the line.
- Use successful scams as templates, refining their tactics and updating them for different platforms or regions.

HOW SCAMS OCCUR

COMMON CHANNELS USED BY CRIMINALS

- Phone calls (vishing)
- Text messages (smishing)
- Emails (phishing)
- Social media messages
- Fake websites or pop-ups
- Online marketplaces or dating apps

No matter the medium, the method remains the same: contact, build trust or fear, extract value and disappear.

Scams happen because they work. They exploit our human vulnerabilities. Knowledge continues to be your best defense. By understanding the methods criminals use, you can identify the red flags, better resist manipulation and help stop the cycle of scams.

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.