How to Avoid Scams and Fraud

How to Avoid Scams and Fraud

Online scams are becoming increasingly sophisticated, targeting people of all ages. But with some knowledge, you can protect yourself and your loved ones.

Scammers stay scamming

Preventing a scam is easier than getting money back after a scam. Here's a quick guide to some of the most common scams out there today:

Pig Butchering

In this long-term scam, cybercriminals build a relationship of trust over weeks or months through social media or dating apps. They often start with a seemingly mistake text. The scammers work to convince the victim to invest in a fake cryptocurrency or other get-rich-quick opportunities. Once they've "fattened up" the victim with the illusion of success, they disappear with the money.

Grandparent Scams

This scam targets the elderly by impersonating a grandchild or relative in distress, often claiming to be in legal trouble or an emergency. Scammers ask for money urgently, usually through untraceable methods like wire transfers or gift cards.

Romance Scams

Targeting people on dating platforms, scammers create fake profiles, build emotional connections, and ask for financial help, claiming emergencies, the need for airline tickets, or investment opportunities.

Accidental Deposit Scams

Scammers pretend to mistakenly send you money via payment apps (like Venmo, Zelle, or PayPal) and then contact you to request it back. However, the original payment was made with a stolen or fake account, and returning it means you lose real money

Tech Support Scams

You get a call or pop-up alert claiming your computer is infected. The scammer, pretending to be from tech support, requests remote access to your device to “fix” the issue, stealing personal info or demanding payment for non-existent services.

UPS or Delivery Text Scams

Scammers send a fake text message pretending to be from a delivery company like UPS, FedEx, or DHL, or the United States Postal Service. The message usually claims there’s an issue with your package and includes a link to “resolve” it. Clicking the link leads to a phishing site that tries to steal personal information or payment details.

How to Avoid Scams

These scams follow different playbooks, but if you watch out for red flags, you can avoid these scams and new ones that pop up!

- **Never text back if the message was unexpected.** Don’t even tell them they have the wrong number.
- **Hang up and call back.** If you receive an unexpected phone call from a loved one, law enforcement, or someone else claiming authority, hang up and call back through a number from your contacts list or verified through a web search.
- **Have a safe word.** Talk to your family and agree to a safe word or phrase that could be used if someone is distressed during a phone call. If you get an unsettling phone call from a loved one, ask for the safe word. Never post this information online or send it through text or email.
- **Refuse to pay the suspicious way.** Scammers generally request payment in forms like gift cards, crypto, or wire transfers, so any request to pay these ways is a red flag.
- **Be wary on social media and dating apps.** Know that scammers pose as genuine users on these platforms to connect with potential victims.

Getting Out

If you suspect that you or someone you know is the victim of a scam, stop sending money immediately and end contact. The scammer might become threatening, angry, or attempt to make you feel guilty, but this is a persuasion technique, and you have the power.

Don’t delete messages – take screenshots for evidence.

Report that you’re a victim of a scam to:

- Your bank or other financial institution
- ic3.gov
- Your local police department
