COMMUNITY CYBER SAFE · TAKE-HOME GUIDE

Spot the Scam

How to recognize and shut down scams by phone, text, email, and social media

The one rule: Stop. If a message creates urgency, fear, or excitement, slow down — and verify by contacting the company or person yourself, using a number or website you look up, never one they gave you.

Every scam pulls one of these levers

- **Urgency —** "Act now or lose access." Real organizations give you time.
- **Fear —** "Your account is locked / you owe money / you'll be arrested."
- **Authority —** "This is the IRS / your bank / Microsoft."
- **Reward —** "You've won" or "a refund is waiting."

Red flags — almost certainly a scam

- A request for payment by gift card, wire transfer, cryptocurrency, or payment app
- A pop-up saying your computer is infected with a number to call (always fake — never call)
- Anyone asking for a password, a one-time code, or remote access to your device
- Pressure to keep it secret or to act immediately
- A caller ID or email address that's slightly "off" (spelling, extra characters)

New: AI voice-cloning of family members

Scammers can now copy a loved one's voice from just a few seconds of audio and call pretending to be in trouble and needing money fast.

- **Defend with a family code word —** a private word only your family knows. If a "relative" calls in a panic, ask for it.
- **Always hang up and call back** on a number you already have for them.

What to do

- ☐ Don't click links or call numbers from unexpected messages
- ☐ Verify independently — look up the real number yourself
- ☐ Talk it over with someone you trust before sending money or information
- ☐ Report scams at ReportFraud.ftc.gov

Report a scam: ReportFraud.ftc.gov · More tips: consumer.ftc.gov