



How to identify a scammer

Online scams

WATCH OUT FOR:

- ✓ **Too good to be true offers:** Urgency to “act now”
- ✓ **Typos:** Misspelled names or numbers in place of letters, e.g., Goog1e
- ✓ **Incorrect domain:** Ensure accurate URL endings, i.e., .gov, .com, .edu, .org

HOW TO HANDLE:

Visit business websites or apps directly. Verify info listed on official websites and reviews to confirm a business’s reputation is positive.

Email scams

WATCH OUT FOR:

- ✓ **Fake emergencies:** Requests to send money quickly to help a loved one
- ✓ **Tone:** Feel of email isn’t aligned with the sender, e.g., unprofessional or impersonal
- ✓ **Demands for personal information:** Asks you to share password, Social Security number or bank account info

HOW TO HANDLE:

Report as junk or spam and delete. Let impersonated organizations know a scammer is at work.



For more tips, scan the code.

Call and text scams

WATCH OUT FOR:

- ✓ **Bank impersonation:** A text or caller claims to be your bank, e.g., “Citizens Fraud Department”
- ✓ **Unprompted communications:** Contact by someone you have never interacted with
- ✓ **Requests unusual payment methods:** Insists you pay immediately through cashier's check, money order, Bitcoin, prepaid debit card, etc.

HOW TO HANDLE:

Contact the company directly using a number from a verified source to confirm legitimacy.

Social media scams

WATCH OUT FOR:

- ✓ **Account hackers:** Hacked account of someone you know or a fake account reaches out to you with ill intention
- ✓ **Dating:** Attempt to initiate a romantic relationship, with the ultimate goal of asking you for money
- ✓ **Investment opportunities:** Advertisement for “amazing” investment opportunities often involving cryptocurrency

HOW TO HANDLE:

Do not accept friend requests from people you don't know. Check existing friends' accounts for suspicious activity.

 Citizens®