Stay Safe on Your Phone & Computer

A simple, plain-English guide to protecting yourself from online scams and fraud

⚠ Common Tricks Scammers Use

Fake Phone Calls

Someone calls pretending to be from Medicare, Social Security, or the IRS. They say you owe money, or your benefits are at risk — and demand you pay immediately.

> *Example: "This is the IRS. You owe $1,200. Pay now with gift cards or we will arrest you."*

Fake Tech Support

A pop-up message appears saying your computer has a virus. They tell you to call a number. The 'technician' then asks to take control of your computer and steal your information.

> *Example: "WARNING: Your computer is infected! Call Microsoft Support immediately."*

Romance Scams

Someone contacts you online and builds a warm friendship or romance over weeks. Then they ask for money — usually because of an emergency they invented.

> *Example: "I'm a widowed doctor working overseas. I need $500 to get home to meet you."*

Prize & Lottery Scams

You receive a message saying you've won a prize or lottery. But first, you must pay a small 'fee' to collect your winnings. There are no winnings — the fee goes straight to the scammer.

> *Example: "Congratulations! You've won $50,000! Just send us $200 to process your prize."*

Grandparent Scams

Someone calls claiming to be your grandchild in trouble, or a lawyer calling on their behalf. They beg you for money and tell you to keep it secret.

> *Example: "Grandma, it's me — I was in an accident. Please wire $2,000 and don't tell Mom."*

Fake Links & Emails

An email or text arrives looking like it's from your bank or Amazon. It asks you to click a link and enter your password. The link leads to a fake website that steals your information.

> *Example: "Your Amazon account is on hold. Click here to verify your information immediately."*

Tips to Protect Yourself Online

1

Hang up — then call back yourself.

If someone calls claiming to be from your bank, Medicare, or a government agency, hang up. Then find the official number yourself (from their website or your statement) and call them directly.

2

Never pay with gift cards or wire transfers

The government and legitimate businesses will never ask you to pay a fine using an iTunes gift card, Google Play card, Zelle, Venmo, or Western Union. This is always a scam.

3

Don't click links in emails or texts.

If you get a message with a link, even if it looks real — don't click on it. Instead, open your browser and go directly to the website by typing the address yourself.

4

Call a trusted family member or friend first.

Before sending any money or sharing any information, call someone you trust. Scammers hate this. Tell them what's happening and ask for their opinion. A second pair of eyes can catch what panic makes you miss.

5

Keep your phone and computer updated.

Updates often fix security problems that scammers can exploit. When your phone or computer asks you to update, it's usually a good idea to say yes.

6

Use strong passwords — or ask for help.

Use a different password for each account and make them long (12+ characters). If that's hard to remember, ask a trusted family member to help you set up a password manager app.

7

Protect your devices from malware.

Protect your phone, tablet, and computer with malware protection. Secure your devices with TargetProof.

☑ Quick Safety Checklist

Before you click, share, or send money — ask yourself:

- ☑ Did I contact them first, or did they reach out to me out of the blue?
- ☑ Does the URL look secure? Is there a locked icon in front of the URL?
- ☑ Am I being told to act fast or keep this a secret?
- ☑ Are they asking me to pay with gift cards, wire transfer, or crypto?
- ☑ Does the email address or phone number look slightly "off"?
- ☑ Have I called a trusted family member or friend to check?
- ☑ Does something about this feel wrong or is it too good to be true?

SOS Need Help? You Can Report It.

If you think you've been scammed — or someone is trying to scam you — report it. You won't get in trouble. Your report helps protect others too.

Elder Fraud Hotline (DOJ): 1-833-FRAUD-11

AARP Fraud Helpline: 1-877-908-3360

FTC Report a Scam: ReportFraud.ftc.gov

Contact TargetProof: 1-770-312-6613

Notes: