

Online Fraud Prevention

Essential Tips for Older Adults

Programs @ The Blue Marble

Online fraud targets people of all ages, but older adults often face higher risks. Scammers use tricks that can seem very convincing, making it easy to fall victim. Protecting yourself online is possible with the right knowledge and habits. This post shares practical tips to help older adults stay safe from online fraud.



Keeping your devices secure helps prevent online fraud

Understand Common Types of Online Fraud

Knowing how scammers operate is the first step to staying safe. Some common scams aimed at older adults include:

- **Phishing emails** that look like they come from banks or trusted companies, asking for personal information.
- **Fake tech support calls or messages** claiming your computer has a virus and asking for remote access.
- **Online shopping scams** where fake websites sell products that never arrive.
- **Romance scams** where fraudsters build fake relationships to ask for money.

- **Investment scams** promising high returns with little risk.

Recognizing these scams helps you avoid falling into their traps.

Use Strong Passwords and Two-Factor Authentication

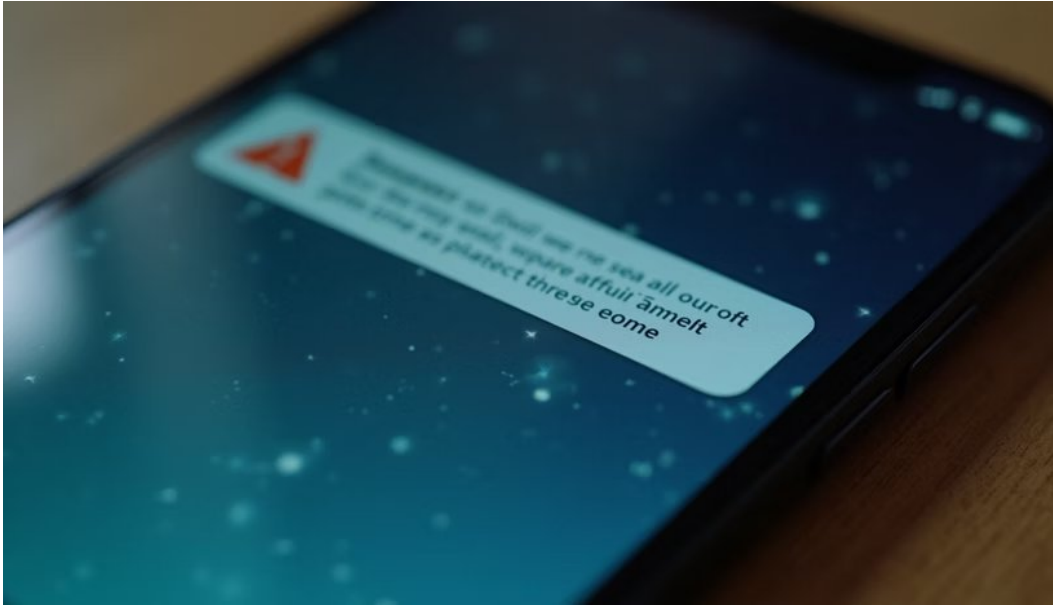
Passwords protect your online accounts, but weak or reused passwords make it easy for fraudsters to break in. Follow these tips:

- Create passwords with a mix of letters, numbers, and symbols.
- Avoid using obvious information like birthdays or pet names.
- Use different passwords for each account.
- Consider a password manager to keep track of your passwords safely.
- Turn on two-factor authentication (2FA) when available. This adds a second step, like a code sent to your phone, making it harder for scammers to access your accounts.

Be Careful with Emails and Links

Scammers often use emails or messages to trick you into clicking harmful links or sharing personal details. To stay safe:

- Don't open emails from unknown senders.
- Avoid clicking on links or downloading attachments unless you are sure they are safe.
- Check the sender's email address carefully; scammers often use addresses that look similar to real ones.
- If an email asks for personal or financial information, contact the company directly using a phone number or website you trust.
- Look for spelling mistakes or unusual language in emails, which can be a sign of fraud.



Warning signs of phishing emails on a smartphone screen

Protect Your Personal Information Online

Sharing too much information can make you a target. Keep these points in mind:

- Avoid posting sensitive details like your full address, phone number, or financial information on social media.
- Be cautious when sharing information in online forms or surveys.
- Use privacy settings on social media to control who sees your posts.
- Never share passwords or PINs with anyone, even if they claim to be from a trusted company.
- Shred documents with personal information before throwing them away.

Keep Your Devices and Software Updated

Fraudsters exploit weaknesses in outdated software to access your information. Protect your devices by:

- Installing updates for your computer, smartphone, and apps as soon as they are available.
- Using antivirus software and keeping it updated.
- Avoiding public Wi-Fi for sensitive activities like banking or shopping online.
- Logging out of accounts when finished, especially on shared devices.

Verify Before You Trust

Scammers often create a sense of urgency to pressure you into quick decisions. Take time to verify:

- If someone calls or emails asking for money or information, hang up and call the company or person back using a trusted number.
- Check online reviews or reports about unfamiliar companies or websites.
- Ask a family member or friend for advice if you feel unsure about an offer or request.
- Remember, legitimate organizations will not rush you or threaten you.



Taking time to verify information helps prevent online fraud

What to Do If You Suspect Fraud

If you think you have been targeted or scammed:

- Stop all communication with the suspected scammer.
- Change your passwords immediately.
- Contact your bank or credit card company to report suspicious activity.
- Report the fraud to local authorities or consumer protection agencies.
- Inform family members or trusted friends for support.

Taking quick action can reduce damage and help prevent further fraud.

Programs @ The Blue Marble