Smartphone Safety Guide for Seniors

Welcome!

This guide is designed to help you stay safe while using your smartphone. Scammers are everywhere, but with a few simple tips, you can protect yourself easily.

Tips to Avoid Scams

- Never share personal information (like Social Security or bank details) in texts or emails.
- If a message sounds urgent or scary, it's probably a scam. Take a moment and don't panic.
- Don't click on links from unknown senders.
- Hang up on callers who ask for money, especially gift cards or wire transfers.
- Only install apps from your phone's official app store (Apple App Store or Google Play Store).
- Enable automatic updates to keep your phone secure.
- Ask a trusted family member before responding to anything suspicious.

What Scams Look Like

- You get a message saying: 'Your bank account has been locked. Click here to unlock it.'
- A call claims: 'You owe money to the IRS. Pay now or go to jail.'
- An email says: 'Congratulations! You won a prize. Just send us your credit card info.'

What You Can Do

- Use strong passwords or biometrics (fingerprint, face unlock).
- Install antivirus or scam blocker apps from trusted sources.
- Turn on two-factor authentication for important accounts.
- Call a family member or trusted friend if you're unsure.
- Report scams to your mobile carrier or the FTC.

Smartphone Safety Guide for Seniors

Real-World Scam Examples (Explained)

1. WhatsApp Investment Scam

Scammers create fake investment groups on WhatsApp pretending to be successful stock traders. They share fake screenshots of profits to build trust. Victims are urged to deposit money into fake 'investment platforms'. Once money is sent, scammers vanish. One case in the UK led to £2.7 million in losses.

2. Pig Butchering Scam

This scam builds emotional or romantic trust over weeks or months, often via dating apps or social media. Once trust is established, the scammer introduces a fake investment opportunity (often crypto). The victim deposits money and sees fake returns, prompting larger investments - then everything disappears.

3. AI Romance Scam

An elderly woman was targeted by a scammer using an AI-generated image and voice of a U.S. Army colonel. He promised her love and a cash delivery of over £600,000. She was tricked into paying fees to 'release' the money, losing over £20,000.

4. Tech Support Scam

A popup or call claims your phone or computer is infected. The scammer says you must pay for tech support to fix it. Victims give remote access or credit card info to 'fix' a fake problem. They often get charged hundreds for nothing.

5. SSA Impersonation Scam

Scammers pretend to be from the Social Security Administration. They say your number is suspended due to fraud, and you must pay to fix it. Some use robocalls, others send fake documents. Scared victims have sent money via gift cards or bank transfers.

Smartphone Safety Guide for Seniors

Top Online Scams of 2024 (Explained)

Investment Scams

What it is: Scammers pose as financial advisors or platforms. They promise high returns and show fake gains. Victims invest large sums - which disappear when the scammers vanish. These scams often use crypto or trading apps.

Example: Fake crypto platform asks for $1,000 to start. Shows $3,000 in 'profits'. Then asks for $5,000 more to withdraw - and vanishes.

Business Email Compromise

What it is: Hackers gain access to a business email and impersonate the CEO or finance officer. They send fake invoices or wire requests to staff. The company unknowingly sends money to criminals.

Example: Employee receives an email from the 'CFO' asking for a $25,000 urgent wire. It's a hacker.

Tech Support Scams

What it is: A popup or fake call claims your device is infected. You're told to pay for urgent support. In reality, nothing is wrong - the scammer is charging for fake services.

Example: A popup on your phone says 'Your device is infected - call now'. You call, and they ask for $300 to 'fix' it.

Romance Scams

What it is: Scammers pretend to fall in love online. Once trust is gained, they invent an emergency and ask for money. They often target lonely or elderly people and can keep the scam going for months.

Example: A fake soldier claims he's stuck overseas and needs $2,000 for a plane ticket to visit you.

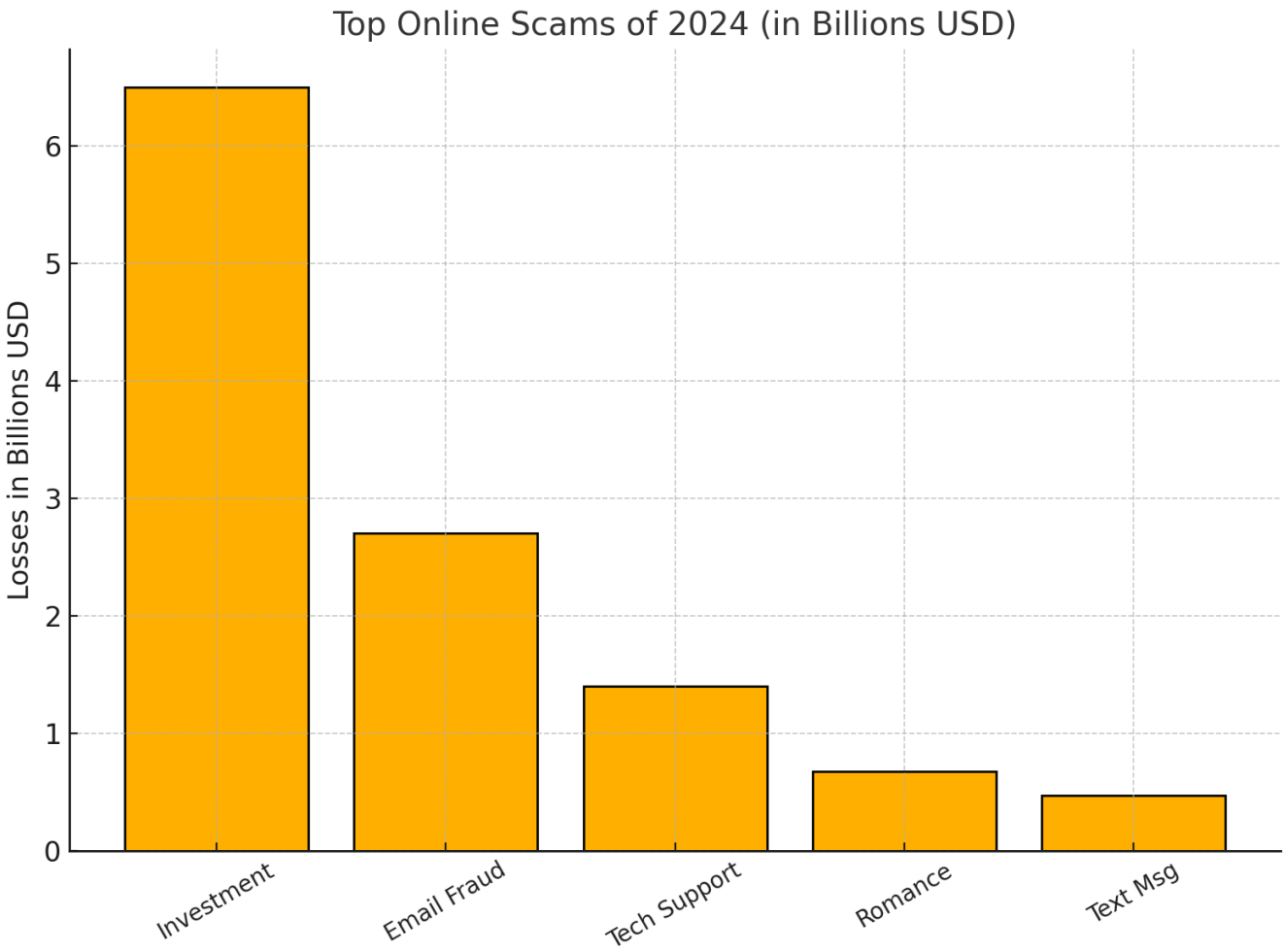
Text Message Scams

What it is: You get a text saying there's an issue with a package, bank account, or payment. A link leads to a fake login page that steals your credentials.

Example: Text: 'Your Amazon package is delayed. Click here to reschedule.' It leads to a fake Amazon login page.

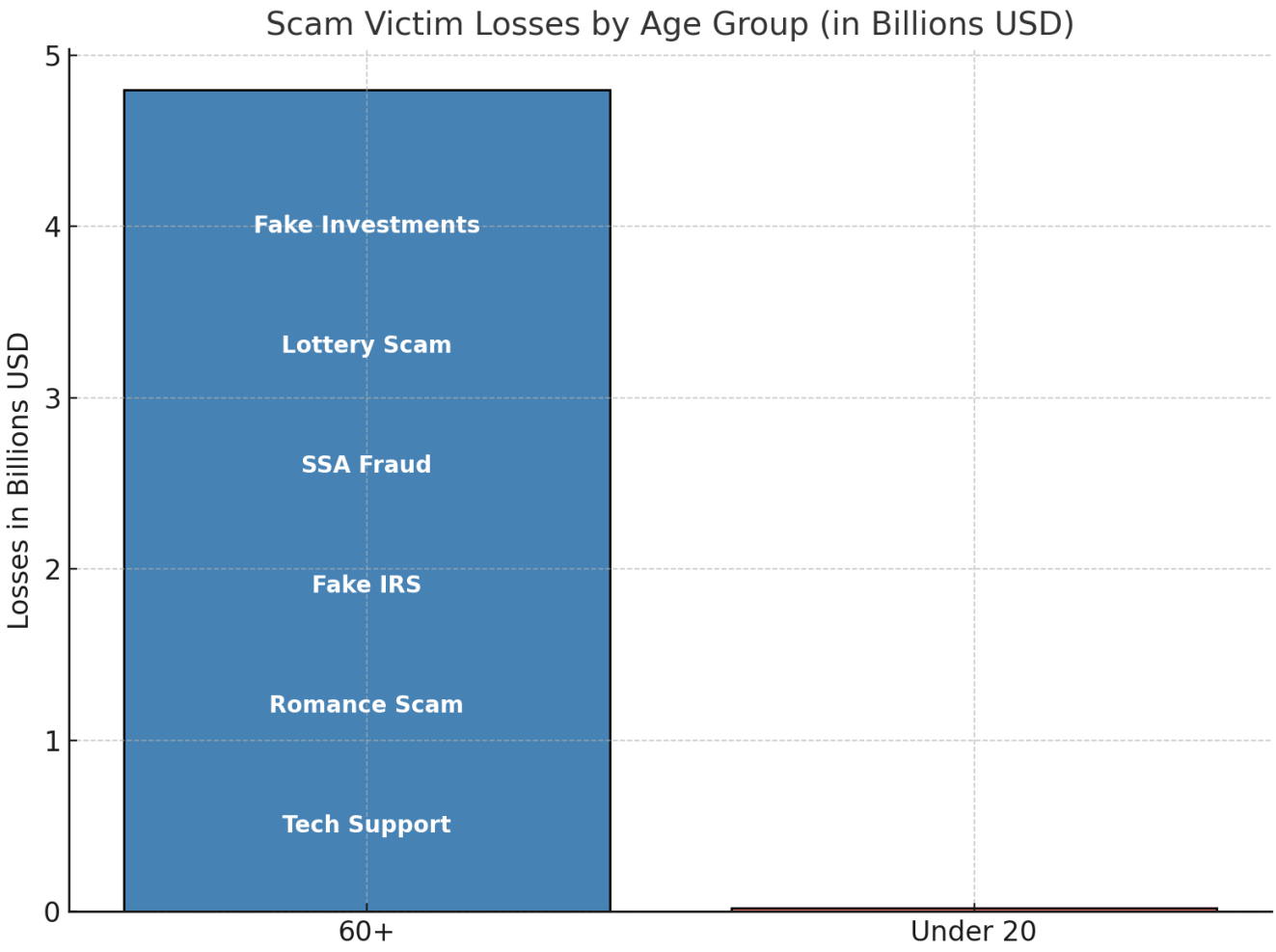
Smartphone Safety Guide for Seniors

Top Online Scams of 2024 - Chart



Smartphone Safety Guide for Seniors

Scam Victim Demographics by Age Group



Smartphone Safety Guide for Seniors

Common Scams Targeting People Over 60

Tech Support Scams

Many seniors are tricked by fake warnings about computer or phone viruses. They're pressured into paying hundreds for 'fixes'.

Romance Scams

Seniors often fall for long-term fake relationships. Scammers request money for emergencies or travel.

Government Impersonation

Scammers pretend to be from the IRS, Social Security, or Medicare, threatening arrest or lost benefits unless payment is made.

Prize/Lottery Scams

Victims are told they've won money or a prize but must pay taxes or fees to claim it. The prize never arrives.

Investment Scams

Scammers lure seniors with fake retirement investment opportunities. Losses are often large and unrecoverable.