Cybersecurity Essentials for Older Adults: Keeping Safe Online

Older adults are spending more time online for banking, shopping, and connecting with loved ones. Unfortunately, scammers know this and often target seniors. In **2022**, **over 88,000 Americans over age 60** fell victim to cyber-fraud, losing a combined **$3.1 billion** – a dramatic **84% increase** in losses compared to the previous year. These crimes can be devastating, but the good news is that there are **simple steps** you can take to greatly **improve your online security**. This guide covers **seven key topics** and practical tips to help you stay safe. Each section includes a quick summary and a one-page checklist of actions you can take. Let's empower ourselves with knowledge – **you're never too old to learn how to outsmart the scammers!** 💪

Cyber Scam Trends Impacting Older Adults (2023-2024)

Cybercriminals are increasingly targeting older Americans with scams that exploit trust, fear, and new technologies. **Americans over 60 reported losing $3.4 billion to scams in 2023** – an all-time high, and an **11% increase over 2022**. Fraud complaints from seniors also jumped by 14% year-over-year to more than 101,000 reports. These numbers reflect only reported cases; in reality, many incidents go unreported due to shame or lack of awareness. The FTC estimates actual losses may be **far higher – up to $61.5 billion in 2023** – when factoring in unreported fraud.

Fraud losses have surged dramatically in recent years. The $3.4B reported lost by seniors in 2023 is more than **triple** the losses reported just a few years earlier in 2020. In fact, **2022 saw an 84% spike** in total losses from the prior year – jumping from about $1.7B in 2021 to $3.1B in 2022. While the growth moderated to +11% in 2023, the dollar amounts are at record highs. *Average loss per senior victim* is also very high: about **$33,900 in 2023**, compared to a few hundred dollars for younger adults on average. And it's not just small

scams – thousands of older individuals suffer **devastating six-figure losses** that wipe out retirement savings. The FTC reports the number of seniors losing **$100,000+** has **more than tripled since 2020**. Tragically, some victims have even lost their entire life savings, leading to *catastrophic* personal crises.

Top Scams Targeting Seniors

Certain types of scams disproportionately affect older adults. According to official data from the FBI and FTC, the *most common fraud schemes* targeting seniors include **tech support scams, impostor scams, investment/cryptocurrency scams, romance scams, and lottery or sweepstakes scams**. Below is a brief overview of these leading scam types and their impact:

Tech Support Scams

Most frequent scam reported by seniors. In 2023, older Americans filed **17,800+ complaints** about tech/customer support fraud, with ~$590 million in losses. Scammers *pose as tech support* (e.g. "Microsoft" or "Amazon" technicians) and claim the victim's computer or account has a problem. They convince victims to grant remote access to their device or bank accounts, then steal funds under the guise of "fixing" nonexistent issues. Seniors are particularly vulnerable – the FTC found adults 60+ were **over 5 times more likely** than younger people to report losing money to a tech support scam.

Impostor Scams

Criminals impersonate trusted figures or organizations. These include **government impersonation** scams (fraudsters pretend to be IRS, Social Security, Medicare, etc.), **"grandparent" scams** (a caller impersonates a grandchild in urgent trouble), and business imposters (fake bank or Amazon representatives). **Impostor scams are the #1 fraud category** in FTC reports. In 2024, government impersonation scams in particular **surged** – reported losses jumped from $171M in 2023 to $789M in 2024. Older adults are **53% more likely** than younger to lose money to a *family/friend impersonation* scam (e.g. the "Grandma, I'm in jail" call) and 41% more likely to lose money to a *government impostor*. These scams often invoke urgency and fear: the caller demands secrecy ("don't tell anyone") and immediate payment (frequently via untraceable methods like gift cards or wire transfers) to resolve a fake crisis.

Investment & Crypto Scams

Highest-dollar losses for seniors. Fraudulent investment opportunities – including bogus stock schemes and now many **cryptocurrency scams** – cost older Americans **over $1.2 billion in 2023**, the largest loss of any scam type. Such scams often promise low-risk, "guaranteed" returns and may involve complex ruses (Ponzi schemes, fake investment websites, or "investment coaches"). A prevalent version is the *"crypto romance" scam* (also known as *pig butchering*): scammers cultivate a relationship (often via a dating site or social media), then lure the victim into a fake crypto investment platform and steal the funds. The FBI warns that *cryptocurrency-based frauds* are exploding – in 2023 about **$1.3 billion (nearly 40% of all money lost by seniors)** was converted into cryptocurrency by scammers. Many victims are instructed to withdraw cash and deposit it into a **Bitcoin ATM** machine, making the transaction irreversible. Investment scams are particularly devastating to older adults because they often involve life savings; the FTC noted a 34% jump in seniors' losses to investment fraud from 2022 to 2023.

Romance & Confidence Scams

Emotional scams that prey on trust. In a typical **romance scam**, a con artist pretends to develop a romantic interest in the victim (often online), then eventually requests money (for an emergency, travel, medical bills, or an "investment opportunity"). Older singles looking for companionship are prime targets. In 2023, seniors reported **$356 million lost** to confidence/romance schemes. These scams often go hand-in-hand with other frauds: for example, many romance scammers eventually steer victims into crypto investments (combining romance and investment fraud). The emotional toll of these betrayals can be severe; victims may not only lose money but also experience heartbreak and embarrassment. **Never send money or gifts to someone you haven't met in person**, no matter how friendly or genuine they seem online – that's a key safety message from law enforcement.

Lottery & Sweepstakes Scams

"You've won!" – but it's fake. Many older adults receive calls or letters claiming they've won a lottery, prize, or sweepstakes – but they must pay a fee or taxes upfront to collect it. **No legitimate contest demands payment for a prize** – this is a telltale sign of fraud. While these scams are less costly on average than investments, they are common: seniors are nearly **3 times more likely** than younger people to report losses to a prize/lottery scam. In 2023, Americans over 60 reported ~$67 million lost to lottery/sweepstakes scams, and likely far more went unreported. Usually the scammer pressures the victim to wire money or send prepaid gift cards to cover "fees." Remember: if you have to pay, it's **not a real prize**.

(Note: "BEC" (Business Email Compromise) scams also account for significant losses affecting some seniors – about $382 million in 2023. BEC scams typically involve a hacker impersonating a company or executive via email to trick victims (often employees) into sending money. These primarily impact businesses, but retirees involved in real estate transactions or small business owners can be victims as well.)

Evolving Scam Tactics & Trends (2023–2024)

Overseas call centers and phone-based fraud: Many scams against seniors are perpetrated via *phone*. The FBI's 2023 data shows that **"call center" schemes (phone scams) overwhelmingly hit older adults** – victims over 60 made up 40% of all call-center scam complaints and **58% of the losses** in that category (about $770 million). Criminal groups, often based overseas (e.g. in India or elsewhere), run boiler-room call centers that

specialize in tech support scams, government impersonation calls, and lottery cons targeting the elderly. They use VoIP technology to spoof caller ID, making it look like the call is from a legitimate 1-800 number or a local area code. These callers are highly trained in **pressuring tactics** – they create a sense of **urgency or panic**, and often instruct the senior *not to tell anyone* (to isolate the victim). For example, a fake "IRS agent" might threaten arrest if a supposed tax debt isn't paid immediately, or a fake grandson might beg the grandparent not to inform Mom and Dad. *If you receive an unsolicited urgent call demanding money or personal info, it's almost certainly a scam.* Hang up and verify the story through an independent source.

Artificial intelligence (AI) in scams: A worrying new trend is scammers using **AI voice cloning** to make impersonations even more convincing. In 2024-2025, authorities began warning of *"deepfake" voice scams* where criminals create a voice imitation from a sample (for instance, lifting a grandchild's voice from a TikTok/Instagram video). The scammer then calls the victim using that cloned voice to convincingly portray the relative in distress. The FCC issued a consumer alert in 2025 about this tactic, urging: **"Don't trust the voice. Call the person back on a known number to verify the story".** If a supposed loved one ever contacts you with an emergency request for money, always pause and verify – even if the voice sounds familiar. Ask questions only the real person would know, use a family 'safe word', or call them directly. As the FCC warned, **never send money based solely on a call like this**. The use of AI to enhance scams is on the rise, so a healthy skepticism is more important than ever.

Increased use of cryptocurrency and digital payments: Scammers are steering victims away from traditional checks and into **harder-to-trace payment methods**. Bank wire transfers, app payments (like Zelle or Venmo), and especially cryptocurrency are now commonly demanded. The FBI's Elder Fraud Report notes that older adults lost **more money via bank transfers and cryptocurrency than any other payment method** in 2023. Many scams that used to ask for wire transfers now ask victims to go to a Bitcoin ATM or crypto kiosk (found in some grocery or convenience stores) to send money. Once crypto is sent, it's nearly impossible to recover. **Gift cards** also remain popular with fraudsters – the scammer will instruct the target to buy gift cards (Amazon, Google Play, iTunes, etc.) and read off the codes. In fact, gift cards were the *most frequently reported form of payment* in tech support and family impersonation scams reported to the FTC. Remember: **no legitimate business or government agency will ever demand payment in gift cards, cryptocurrency, or by sending cash in the mail**. Those are immediate red flags of a scam.

Scams via email and social media: While phone calls hit the oldest demographics hardest, scammers also reach seniors through email and social media. The FTC's 2024

data showed **email was the top initial contact method** for fraud across all ages, followed by phone and text messages. Phishing emails targeting older users may pretend to be from a bank ("Your account is locked, click here to verify"), a familiar company, or even a friend's hacked account sending a suspicious link. Social media is often the hunting ground for *romance scammers* and bogus investment opportunities. Seniors on Facebook have been targeted by messages from false identities (for instance, someone posing as a widower in the military, striking up a friendship that leads to requests for money). **Be cautious online:** Don't click unexpected links or attachments. Be wary of friend requests or messages from strangers (or even from friends, if it's out of character). Strengthen your privacy settings so that scammers can't easily harvest personal info from your profiles. The more they know (your grandkids' names, your recent posts, etc.), the more convincingly they can manipulate you.

Key Insights from Officials and Advocates

> **"This report underscores the fact that seniors are a particularly vulnerable victim group and are often specifically targeted for fraud by bad actors."** – FBI Assistant Director Mehtab Syed, urging families and communities to stay vigilant. Law enforcement has made elder fraud a priority, but **education and prevention** are critical.
>
> **"The seismic growth of reported fraud continues unabated… The impact on older adults is often catastrophic."** – Kathy Stokes, AARP Director of Fraud Prevention, commenting on the record $12.5 billion in overall U.S. scam losses in 2024. Older victims not only lose money, but can suffer *emotional and health harms*, family strain, and loss of financial independence.
>
> **"Combatting the financial exploitation of those over 60 years of age continues to be a priority of the FBI… Do not be afraid or embarrassed to report."** – FBI Assistant Director Michael Nordwall, encouraging victims to come forward and report scams. Reporting helps authorities track and dismantle fraud rings, and can connect victims with support. **No one should suffer in silence** – these crimes are underreported, and breaking that silence is key to stopping the scammers.

Sources: This summary draws on the latest data and warnings from the FBI's Internet Crime Complaint Center (IC3) 2023 **Elder Fraud Report**, the Federal Trade Commission's 2024 **Protecting Older Consumers** report, and analyses by AARP and consumer protection experts. All statistics are from these reputable sources.

Remember: Knowledge is power. By understanding the tactics and scale of these scams, older adults and their families can better protect themselves. Share this information with

friends and neighbors. If something seems off – a strange phone call, a deal too good to be true, a sudden online romance – **trust your instincts** and check it out. Staying informed is the best defense against fraud.