HARTFORDFUNDS

Our benchmark is the investor.®

Scammers Are Smarter Than Ever:

How to protect your identity—and your wealth

By Liz Loewy, Co-Founder and Chief Operating Officer at EverSafe

Several years ago, my friend's father—who was still sharp and independent, even in his 90s—received a call from his grandson. He said he'd been arrested and needed help immediately. "Please, don't tell Mom," he pleaded. "I'm in trouble." Male voices were in the background and thought to be police. My friend's father ended the call and immediately phoned his best friend, who persuaded him not to send any "bail money."

The fact that he chose not to call his daughter until hours later was noteworthy. But as I learned from countless cases such as this—both during my years as a prosecutor and now at EverSafe—scammers understand that a grandparent's greatest wish is to nurture a close, trusting relationship with their grandchild, even if it means keeping a few secrets from mom and dad. Knowing this, scammers often exploit that emotional bond. Thankfully, my friend's father didn't fall for this common scam, but not everyone is so fortunate.[1]

There have always been scams, but the digital age has certainly created more opportunities for fraudsters

Most adults in the US have been targeted by an online scam attempt or attack.[1] Older individuals are seen as more susceptible to these crimes. Why? A few reasons. As notorious bank robber Willie Sutton famously said about why he robbed banks, "That's where the money is."

To his point, Americans aged 55 and older own most of the nation's wealth.[1] And given that about 1 in 9 seniors has been diagnosed with Alzheimer's disease, the place "where the money is" has never been more vulnerable to scammers.[2]

What We'll Cover:

- Why it's so easy to get scammed
- Recognizing red flags
- How technology can help you get ahead of the scammers

First, Why It's So Easy to Get Scammed

Unfortunately, scammers are getting more sophisticated and opportunistic. With so much of our daily life now happening online, our personal information is more exposed than ever. And with that exposure comes more opportunities for scammers to commit fraud and identity theft.

Modern scams are also more convincing than ever, thanks to advances in artificial intelligence, social media, and deepfake technology. Scammers now create messages, websites, and even audio or video clips that look and sound incredibly real—often mimicking trusted companies, government agencies, or even loved ones.

These scams are designed to trigger emotional reactions such as fear, urgency, or sympathy. Here are some ways they use emotions against their victims:

Digital Payment Scams

Maria receives a text that appears to be from PayPal, claiming she was charged for concert tickets she never purchased. Worried, she calls the number in the message. To "fix" the issue, the fake agent asks for her full name, email, and bank details—then uses the information to transfer money from her account.

Government Imposter Scams

Tom receives a call from someone claiming to be a Medicare representative. They say his benefits will be cut unless he confirms his Social Security number. He shares it and becomes a victim of identity theft.

Fake URL or QR Code Scams

Linda scans a QR code on a flyer advertising a free brain-health webinar. The website looks legitimate but steals her personal information and installs malware on her phone. Days later, she notices suspicious activity in her email and bank account.

Anyone Can Fall for a Scam

Scammers don't rely on what you know—they rely on how you feel in the moment. Their tactics are designed to catch people off guard emotionally, clouding their judgment and leading to impulsive decisions. This is why even tech-savvy individuals can be fooled when a scam appears to come from a trusted source or mimics a loved one in distress. The truth is, anyone can be vulnerable when the right emotional buttons are pushed. That's why awareness and caution are critical.

> Many scammers aren't just tech-savvy—they're master manipulators. They know how to use psychological tactics to engender trust, fear, and even affection to get what they want.
>
> —Liz Loewy

Second, Recognizing Red Flags

Even though scams are designed to look and sound legitimate, there are warning signs you can watch for—especially if you know where to look.

1. **Scare tactics disguised as tech or security alerts**

   Scammers often try to scare you into acting quickly. You might get a pop-up saying your computer is infected, or a call claiming your Social Security number has been suspended. Real tech support will never ask you to call a number from a pop-up. The Social Security Administration (SSA) generally initiates contact through official letters before making any phone calls and will never suspend your Social Security number.

   What to do: Hang up or close the message. If you're concerned that it wasn't a scam, contact the organization directly using a phone number or website you trust—not the one in the message—to confirm. Never click links in the communication or open attachments.

2. **Strange email addresses or sender names**

   Scam emails often look like they're from a bank, a government entity such as Medicare, or even a friend. But if you hover your mouse over the sender's name, the email address may look suspicious or unfamiliar (e.g., support@secure-paypal-alerts.ru instead of support@paypal.com).

   What to do: Always check the full email address. If it looks odd or doesn't match the organization's official domain, don't click on any links or attachments. Close it and block the sender.

3. **Spelling errors, strange fonts, or awkward language**

   Many scam messages, whether in email or text form, contain typos, unusual formatting, or phrases that don't sound quite right, such as "Greetings from Amazon," "Dear customer" instead of your name, or "Your account is being terminated unless you verify now."

   What to do: Trust your instincts. If a communication looks sloppy or feels irregular, it could likely be a scam. The safest course of action is to close it and block the sender.

4. **Unexpected requests for personal or financial information**

   A scammer might send an email or text pretending to be from a trusted company saying, "We've detected suspicious activity on your account. Please confirm your identity to prevent suspension."

   No legitimate company will request sensitive data such as your Social Security number, bank account, or password via email, text, or an unsolicited call.

   What to do: First, always avoid logging into financial accounts, shopping online, or entering personal information while on public Wi-Fi. These activities can expose your data to hackers unless you're using a secure connection like a VPN.

   If you're unsure about the legitimacy of a request, go directly to the company's official website and contact customer service using a verified phone number. Only share personal information if you initiated the contact with the actual company and are certain of whom you're speaking with.

5. **Urgent messages or threats from "law enforcement"**

   Scammers may impersonate police officers, federal agents, or court officials in an attempt to scare their targets into acting quickly. You might receive a call or email claiming you have unpaid speeding tickets, toll charges, or that you missed jury duty and now owe a fine. They may demand payment through gift cards, wire transfers, or digital wallets, and threaten arrest if you don't comply.

   What to do: Hang up or delete the message. Genuine law enforcement professionals do not demand payment over the phone or threaten arrest without due process. If you're unsure, contact the agency directly using an official, verified phone number.

6. **Suspicious friend requests or messages on social media**

   Scammers often create fake profiles to impersonate someone you know—or someone you'd want to know. They might send a friend request posing as a grandchild, an old classmate, or even a romantic interest. Once connected, they eventually ask for money, personal information, or try to lure you into clicking malicious links.

   What to do: Don't accept friend requests from people you don't recognize or haven't spoken to in years. If something feels off, trust your gut. Verify the person's identity through another channel before engaging and never share sensitive information over social media.

7. **Suspicious phone calls from unknown numbers**

   Scammers often use phone calls to impersonate loved ones, law enforcement, or financial institutions. They may have the ability to spoof caller IDs to look legitimate, create urgency, or use silence and pauses to record your voice. Even saying "yes" can be risky—it may be used to authorize fraudulent charges or train AI voice clones.

   What to do: Avoid answering calls from unknown or anonymous numbers. If you do answer and there's a long pause before someone speaks, don't say anything and hang up immediately. Speaking, even briefly, can confirm your number is active or provide audio that scammers can misuse. Never say "yes" or share personal information unless you're absolutely certain who is on the other line. If you're unsure, hang up and call the organization's official number. Finally, refrain from recording a voice mail message with your name. The best approach is to use the standard voicemail greeting from your telecom provider.

While scammers are increasingly using technology to defraud victims, the good news is that you can fight fire with fire and use technology to protect yourself—and loved ones.

Third, How Technology Can Help You Get Ahead of the Scammers

Scams are constantly evolving—and many no longer come with warning signs like suspicious calls or emails. That's why relying on awareness alone is no longer enough. Technology-based protection has become essential for staying ahead of increasingly sophisticated threats and to your digital and financial safety.

Key features to look for:

- Monitoring across your full financial picture—including bank, investment, retirement, and credit card accounts
- Alerts that can be shared with designated family members, caregivers, or financial professionals—without giving them the ability to move funds
- Coverage of credit activity from all three bureaus, Dark Web surveillance, and real estate holdings
- Email monitoring for suspicious communications suggestive of scams
- Support with recovery and remediation if fraud occurs

EverSafe offers all of these features and more. While it's one of the more comprehensive options available—especially for seniors and families—it's important to research and choose the service that best fits your needs.

You May Be Thinking, "I Think I'm Pretty Savvy. Is Paying for this Service Really Worth It?"

Many people feel confident in their ability to spot a scam, especially if they've never fallen for one before. But that confidence can make us more vulnerable. Scammers count on people thinking, "That would never happen to me—or my parents."

Fraud-protection technology isn't about replacing your instincts—it's about backing them up. These tools can spot suspicious activity early, alert you quickly, and help you act before real damage is done.

Sooner or Later, We'll Likely All Get Scammed

Scammers are getting smarter, faster, and more convincing. With AI tools that mimic voices, scrape social media, and generate realistic messages, it's no longer a question of if—but when. In fact, 73% of US adults have already experienced some kind of online scam or attack.[3]

That's why awareness is no longer optional—it's essential. Knowing what to look for, being careful about what you share online, and using fraud-protection technology can make all the difference. Think of it as digital self-defense: spotting red flags early, limiting your exposure, and having tools that help you respond quickly.

In today's hyper-connected world, caution isn't overreacting—it's smart protection.

Next Steps

1. Be mindful of red flags
2. Share this information with loved ones
3. Explore fraud-protection tools

Liz Loewy, Co-Founder and Chief Operating Officer at EverSafe

A nationally recognized elder justice advocate, Liz Loewy spent over 30 years as a prosecutor in the Manhattan District Attorney's Office, where she led the Domestic Violence Unit and then founded the Office's first Elder Abuse Prosecution Unit. A frequent speaker at conferences in the U.S. and abroad, she serves on the Financial Exploitation Advisory Board of the National Adult Protective Services Association. Liz is co-author of *Financial Exploitation of the Elderly* and has been featured in major media outlets including NPR, ABC News, and the Wall Street Journal.

[1] Wealth Distribution in the U.S. By Generation, smartasset.com, 7/24

[2] 2025 Alzheimer's Disease Facts and Figures, alz.org, 9/25

[3] Online Scams and Attacks in America Today, pewresearch.org, 7/25