HARTFORDFUNDS
Our benchmark is the investor.®

Old Scams, New Twists

Protect yourself from financial fraud in the digital age.

A mother's cell phone rings unexpectedly. She answers the call and hears the voice of her teen daughter frantically screaming for help. Seconds later, a deep-voiced male comes on the line demanding a $50,000 ransom payment.

Terrified, mom races home and finds her daughter safe in her bedroom. Soon enough, mom learns she's been the victim of a so-called AI deepfake—a cloned voice sample used by scam artists employing artificial intelligence techniques to scare us into parting with our cash or private information.

This true story[1] would be any parent's worst nightmare. But it's only one alarming example of the increasing sophistication of scam artists and the growing ease with which potential victims are targeted.

An estimated $2.6 billion was taken from Americans in the first half of 2023, and 67% of reported fraud losses originated on social media, according to the Federal Trade Commission. Social-media scams stole nearly $658 million, while website or app fraud took another $432 million. Scams that originated with phone calls accounted for another $426 million while email scams—the most prevalent of scam tools—accounted for $198 million in losses.[2]

Victims aren't always the stereotype painted for us—a naïve centenarian struggling with cognitive decline. It could just as easily be any of us. The sad truth is many of those victims are unknowingly willing participants who simply don't have the training to spot when they're being deceived by a scammer.

Bad Guys Are Real

Attackers. Bad actors. Malicious users. No matter what you call those trying to scam you, they're certainly not good guys. Worst of all, these callous criminals are becoming more sophisticated. With additional data about you from multiple sources—including social media—floating around the web, it's not out of the ordinary to get an unsolicited phishing email that passes for a legit communication. They know more info about you than you may suspect.

Key Points

- Financial scams—conducted over the phone and online—can rob unsuspecting Americans of millions of dollars each year.
- Many victims of financial fraud are unknowingly willing participants who aren't trained to spot when they're being deceived.
- Stop and question the validity of any stranger requesting you take an action that may involve your identity or finances.

[1] "The Chilling Rise of AI Scams," The Guardian, 9/4/23.
[2] "Consumer Sentinel Network," Federal Trade Commission, 6/30/23.

More often than not, they're trying to get you to do something. Click, call, or reply. Is some unknown person coming into your life asking for something? Be skeptical. Even a quick survey can turn into a thorny trap.

Be Alert When You Receive an Alert

Here's a three-step action plan to think through for the next time you get an unsolicited email, friend request, or phone call:

1. **Stop –** Don't just jump in and accept any Facebook friend request or answer any phone call or email. Take a timeout.
2. **Think** – Does it make sense? Are you expecting an email communication or call? Is the friend request coming from a total stranger?
3. **Protect** – Verify the sender. Once you open an email, evaluate a friend request, or pick up the phone, investigate whether the person is asking you to do something. If you're still confused, call back the individual or organization with a number you have from a business card, the back of a credit card, or from an official website.

> "Is some unknown person coming into your life asking for something? Be skeptical.

Here's a specific example:

You receive an email from your bank. It informs you of fraudulent activity on your account. You need to log in immediately to verify your information. They're trying to help you stop someone from further hurting you financially. The communication looks like it's from your bank. It has the same look and feel of your monthly statement.

Since it's from your bank, do you do what it's asking?

Turns out, the email's not from the bank at all. It's from the bad guys. They've put the login page on a phishing site that's been designed to steal your information. You log in, and now they have your info. The same trick can happen over the phone. Numbers on caller ID can be spoofed, too. In fact, scammers are now calling from numbers that look like they're local. They know you're more likely to answer if you recognize the area code.

The bottom line: Don't trust anyone—even someone claiming to be from a place as reputable as a bank. Don't willingly share personal information over the phone. Verify the identity of anyone asking you for anything. Then take the time to process it. You probably don't have all of the facts. Do a quick Google search to determine as much as you can while speaking with them. Why are they reaching out to you in the first place?

(See **"Common Scams To Be Aware of Today" on page 3** for more information on possible scenarios.)

Victims Come in All Shapes and Sizes

People think fraud can't happen to them. Often, it takes somebody close to us to fall victim for us to accept that this is a very real possibility.

Seniors aren't the only victims. However, older folks are prime targets, as they tend to be less comfortable working with new technology. There's an opportunity for someone to take advantage of that lack of comfort.

Unfortunately, the public receives virtually no training on how to deal with these situations. So, there's little awareness of what to do. And this threat will never ever end. Defend yourself from being a victim.

Learn how to take shelter from financial fraud—in whatever form it may come. It could be the voice of a loved one—or a fake voice looking for an easy mark.

Common Scams To Be Aware of Today

Here's a compilation of some of the biggest schemes perpetrated on vulnerable consumers. Learn the various methods used and how you can best prevent falling victim.

1. **Medicare scams**
   Perpetrators may pose as a Medicare representative to obtain personal information.
2. **Counterfeit prescription medicines**
   Cheap prescription drugs online, where seniors increasingly go to find better prices, are often bogus counterfeit medications.
3. **Funeral home and cemetery scams**
   Money is extorted from relatives of the deceased to settle fake debts. Disreputable funeral homes could capitalize on unfamiliarity, or a customer's grief, by adding unnecessary charges to the bill.
4. **Charity fraud schemes**
   After high-profile disasters, fake charity creators use social media, emails, or phone calls seeking donations that end up in the pockets of fraudsters.
5. **Peer-to-peer payment scams**
   Scammers can turn popular payment apps like Zelle into a theft tool by texting or calling you to warn that a thief is trying to steal your money through the app. They pretend to help "fix" the issue by having you send money to yourself—but the money goes to the scammer's account.
6. **SIM swapping**
   Thieves can steal your phone number and assign it to a new SIM card in a phone they control, making it easy for them to log in to your accounts or reset your passwords. Ask your mobile phone carrier if it offers extra security to help prevent SIM swapping.
7. **Cryptocurrency investment schemes**
   Fake investment professionals contact you through social media promising to grow your money if you open an account with cryptocurrency. Click an unexpected link they send, or send crypto to a QR code, and your money is gone.

8. **Homeowner/reverse-mortgage scams**
   Homeowners are pressured to take out equity in their home to use as payment for reported necessary repairs.
9. **Sweepstakes and lottery scams**
   Scam targets are contacted to inform them that they've won a financial prize, but are required to advance payment of a fee to collect the winnings.
10. **The grandparents scam**
    Scammers pose as grandchildren and ask for money to solve some unexpected financial problem. Or, someone calls on behalf of a grandchild who is either (fictionally) in jail, a hospital, or another country.
11. **Tech support**
    A fake technical-support representative calls to fix a nonexistent computer issue with the goal of gaining remote access to a victim's computer.
12. **IRS impersonation**
    Victims are told they're due a tax refund or that they have unpaid taxes. The IRS will never initiate contact via phone calls, email, or social media.

Artificial Intelligence (AI) Scams
Cybercriminals need as little as three seconds of someone's voice to successfully clone it and make it usable in a scam call with help from generative AI tools. In a recent survey by McAfee, 70% of respondents doubted they could tell the difference between a cloned voice and the real thing. Cloned voices have been used in calls faking police requests for emergency funds to get a family member out of trouble. Other scammers have used the cloned voices of children or relatives while typing out fake "distress" sentences in real time over the phone.[3]

[3] "Artificial Impostors–Cybercriminals Turn to AI Voice Cloning for a New Breed of Scam", McAfee.com, 5/15/23.
Sources: ABC, IRS, FTC, Axios, FBI.gov, Experian, National Council on Aging.
Hartford Funds Distributors, LLC, Member FINRA