

Technology has made Americans, and their money, more available to scammers.

BY ALAN GREENBLATT

oward, a retired professor who's written several books, considers himself pretty smart. Nonetheless, he got duped. He received a "very official-sounding call" one morning from someone purporting to be from Amazon's fraud division. There was a problem with Howard's account that needed to be cleared up – but to do so, he had to go out and buy an expensive gift card to make the transition work.

The caller had gotten Howard worked into a panicky state, so

he went along. He only wised up when the caller said the first gift card didn't clear up the problem and he needed to buy another one. "I don't know whether it was worth \$400, but it was a good lesson to learn," said Howard (who asked that his real name not be used so as not to become more of a target). "I haven't gone for one since then."

There's nothing new about scams, but they have proliferated in recent years, costing consumers billions of dollars. In 2023, the Federal Trade



26 THE AMERICAN LEGION MAGAZINE DECEMBER 2024

1 of 5

Commission reported losses of \$2.7 billion from more than 5 million cases of fraud – including 1 million instances of identity theft and more than 850,000 of imposter fraud, in which someone claimed to be from a company, a relative in distress, a potential love interest or some other guise.

Veterans lost \$350 million last year, losing on average 20% more to scams than members of the general public. "Anytime you are online, just know wherever you are there is a criminal there as well waiting to target you, and the same with a phone call or a text message," said Amy Nofziger, director of fraud victim support for AARP, which runs a helpline that receives between 300 and 450 calls per day.

The number of scams has grown for one simple reason: technology. It's now easy for scammers to send out thousands of emails or texts at next to no cost, or have machines do the dialing to thousands of numbers. (That's why there's that telltale pause when you answer the phone, and it takes a beat before another person comes on the line.)

Meanwhile, we're all more accessible to criminals. It wasn't that long ago that they had to try to find us at home, or maybe at work. Now we carry mini-computers around all the time, ready to receive emails or texts from people claiming to be Nigerian princes.

"Now scammers can reach people anywhere," said Cinthya Lavin, a vice president at the Better Business

**\$10 billion** Amount U.S. consumers reported losing

a),e()}function p(){return y}function q(a

to scams and fraud in 2023, up from \$3.5 billion in 2020 Source: FTC

vOf(a):return=11++h88this

## **Target: Young servicemembers**

Deanna Nelson runs the state attorney general's office in Watertown, N.Y. Because the Army's Fort Drum is nearby, she's become an expert in scams. Active servicemembers are prime targets for scams



perpetrated by landlords and companies selling loans or consumer goods such as faulty cars and computers. There have always been a few sketchy businesses around bases, but now scammers run sophisticated campaigns targeting members of the military on a nationwide basis.

According to the Federal Trade Commission, scammers stole \$477 million from veterans, military personnel or their spouses in 2023, a 13% increase from the previous year. "Companies in the area and nationally have made it their business to separate the military from their income streams," Nelson said.

People in the service are a major target for grifters for several reasons. Often, they're young and living away from home and managing their finances for the first time. Not only do they collect steady pay, but they are concerned with keeping their credit records clean as a condition of employment. That means they pay their bills no matter how blatantly they've been ripped off.

"The companies realize that servicemembers are going to pay," Nelson said. "It's not worth it to sacrifice their security clearance or military service not to."

During a permanent change of station, servicemembers need to secure housing and often find a new car and child care, all within a short period of time. Having to make payments and deposits leaves them particularly susceptible to fraud involving payment apps. The number of complaints submitted by servicemembers about scams involving payment apps has jumped dramatically in recent years – nearly doubling between 2020 and 2022 alone, according to the Consumer Financial Protection Bureau.

Servicemembers, in fact, are more likely to report such scams than the population as a whole. Instead of being respected, too many are getting ripped off.

"We have military men and women who should be focused on their missions," says Bob Cooper, a former Tennessee attorney general, "but who are being distracted by these fraudulent sales that create unnecessary anxiety for them."

28 THE AMERICAN LEGION MAGAZINE DECEMBER 2024

## \$4.57 billion

Financial losses due to fake investment scams

Source: Government Accountability Office

## 5.4 million

this[a]&&this[a]!==c&&d.push(this[a][a]):return f.length?e.apply(d.f):d)).b.find[]d("find".fu

e()}function=p(){return y}function=q(a,c){return=y.html(z),c&&b(äheader

Reports of fraud, identity theft and other scams received by the FTC in 2023

## \$1.86 billion

Amount lost in 2023 via bank transfers

Source: FTC

Bureau. "Five years ago, you really wouldn't see people receiving fake text messages about jobs or packages, and now they do."

Technology has made not only individuals but their money more readily available. Most of the relevant regulations were crafted at a time when the big fear was bad guys coercing people to collect and cough up the daily maximum amounts they could withdraw from an ATM. Now, much more of their money can be transferred instantly and irrevocably using gift cards, payment apps and crypto ATMs.

Everyone can and will be targeted for scams, but certain groups are heavily preyed upon – seniors in particular. They're part of a generation that grew up when answering the phone felt imperative. They may feel lonely and welcome calls. Some may have cognitive impairment; even if they don't, they may not be as tech savvy as younger digital natives.

"I'm aware that my bank is never going to call me for my password or two-factor identification," said Christopher Brooks, a computer science professor at the University of San Francisco. "My mother-in-law, she doesn't get that. Scammers can get the victim to circumvent the security system for them."

The other reason seniors present a major target is that they have accumulated wealth. Not all, certainly, but older people are more likely to have built up assets than someone in their 20s. But scammers are happy to go after anyone with money. Young people are often victims because they're new to managing money and their own accounts, said Colleen Tressler, a senior project manager with the Federal Trade Commission's division of consumer and business education.

"Young people are much more on social than any generation before and they're maybe not as savvy about not sharing information – and realizing that the person on the other end may not be legitimate and has nefarious plans for the use of that information," she said.

Each year, Americans lose more than \$1 billion to romance scams, falling for online declarations of love and, ultimately, requests for money. "They're good talkers and they often work from a script, so they're ready for anything you might raise," said Adam Rust, director of financial services at the Consumer Federation of America. "They are very good at luring you in, and very clever people fall for them."

Some scams are quite detailed and elaborate, involving personally tailored information and deepfake videos. But scamming is mostly a volume business. There's a reason you probably get a half-dozen calls every day. Not everyone has to fall for a scam for it to work. Tricking a handful out of a thousand can be profitable.

"The problem is, a lot of people don't believe it's ever going to happen to them, so they don't watch out for the red flags," Nofziger said.

Don't trust, always verify In the early 20th century, the Eiffel Tower was for sale. At least, according to Victor Lustig, who went around to the scrap metal merchants of Paris telling them the authorities were so worried about the tower's structural integrity that they were going to tear it down, putting a whole lot of scrap iron on the market. He even convinced a merchant named André Poisson that his bid – the equivalent of \$1 million today – would be the winner at auction, going so far as to accept a bribe to make the transaction seem more plausible.

Lustig concocted not only a story but a convincing background, staying at one of the fanciest hotels in Paris and calling himself the "deputy director of the Ministry of Posts and Telegraphs" while also claiming to be a count.

THE AMERICAN LEGION MAGAZINE DECEMBER 2024

3 of 5 12/3/2024, 10:54 AM

"A lot of scammers will give themselves titles," said Rodney Hobson, author of "The Book of Scams." "They may be quite meaningless titles and completely fictitious, but it sounds very impressive. People will always believe someone who's got a title."

That's why scammers will claim to be from your bank or cable company or represent the post office, or will send emails supposedly from your boss or your boss' boss. Whether they're preying on your greed or your desire to help out, they borrow trust by claiming either to be a person in a position of authority or someone personally connected to you.

So how you do you know it's not really your bank or Amazon that's calling? If someone claims they're with your bank, simply say you need to call them back. And don't call back the number they give you (as Howard did). Look up the right number.

It may be unfortunate, but you have to be suspicious. If something sounds too good to be true, it almost certainly is. Ask yourself why some unknown "stockbroker" is calling you, of all people, to get you in on a can't-miss deal.

"It's amazing how many people think they can win the lottery when they haven't even bought a ticket," Hobson said.

It's not important that you keep up with all the latest scams to recognize them right off. Scams are always evolving. What is important is that your spidey sense starts to tingle as soon as you're asked for one of two things: money or information. If they're trying to get you to send money, slow the transaction down, stay calm and take steps to make sure you know for sure whom it is you're dealing with.

Lots of your personal information is already out there, sold and resold by entities you've willingly given it to, such as credit card companies (or taken out of their control by data breaches). Your bank already knows your birthday and Social Security number; no one legitimate is going to call and ask. Scammers will often know just enough about you to sound authoritative, but if you give them anything more, that helps them complete a puzzle that will allow them to set up credit cards in your name or put you on the hook in some other way.

One way to prevent that is by freezing your credit reports. There are three main credit bureaus: Equifax, Experian and TransUnion. It costs you nothing to freeze your accounts, which will prevent scammers from being able to use your information to open credit cards or take out loans. You can always open them back up temporarily if you need to.

"It just locks everything down," Tressler said.
"You may have an identity theft try, but they won't
be able to get any of the information they would
need to open up a new credit card or get a
mortgage or a car loan."

Everyone should check their credit reports periodically for fraud and mistakes, she continued. And if you have been a victim of fraud, it's important to report it. The money you sent through a payment app is likely gone for good, but reporting scams to the local police or your state's attorney general or the FTC provides information about the current scams being run, while giving shape to the scope of the problem. This information also gets checked routinely by law enforcement agencies so they can detect patterns regarding the type of people or regions being heavily targeted at any given time.

Nowadays, it's a good idea to update the wisdom of Ronald Reagan: don't trust, always verify.

"The ones that play on people's desire to be helpful are a clever way to get people to divulge their personal information," Brooks said. "It makes us less helpful as a society, just because there are scams out there."

Alan Greenblatt is the editor of Governing.

**\$1,450** Median loss reported by people in their 80s or older, compared with \$480 among people in their 20s Source: FTC

phochfilled vetrict" function d(adc) f0hicet

**\$110 million** Amount lost to scams involving Bitcoin ATMs, a

10-fold increase since 2020 Source: FTC

32 THE AMERICAN LEGION MAGAZINE DECEMBER 2024

4 of 5

5 of 5