

HOW FACEBOOK AND GOOGLE SCAMMERS GET YOU

The man Judith Boivin came to know as her FBI handler called twice a day for three months. He'd ask about her life and tell her about his family.

He knew about her 78-year-old husband's struggles with Parkinson's disease and when they had to see the doctor. She told him about her kids and grandkids and when she was leaving town. Sometimes he'd let her in on his plans, like that trip to Italy to attend a friend's wedding. While he was gone, he told her, another agent would take over their daily 9 a.m. and 6 p.m. check-ins.

An alliance developed, she said. "I was respectful of him, and he seemed to be respectful of me."


This is how people are drawn into what scam experts call "the ether."

These seemingly innocuous conversations are actually well-rehearsed orchestrations of a relationship, the flood of attention designed to work them into such a heightened state of emotion that they suspend reason. But these interactions rely on secrecy, because the criminal can't risk raising questions from outsiders, or anyone who might seed doubt and break their hold.

You know, what I do is I ask them questions until I find their emotional Achilles' heel. According to a con man interviewed by Doug Shadel, a fraud prevention expert

There's a common misconception that financial fraud victims are uneducated, lonely, isolated, or lacking common sense — none of which applies to countless victims. There's also an assumption that seniors are more vulnerable to fraud because of deteriorating cognitive skills. In fact, according to the Federal Trade Commission, people in their 20s are scammed at higher rates than older Americans. This is partly because they spend more time online, where there is simply more exposure to fake shopping sites, bogus job offers and investment scams.

I well, I guess I told him about my husband



Anyone can be conned, said Doug Shadel, a fraud prevention expert who has spent much of his career studying scammers and co-authored “Weapons of Fraud: A Source Book for Fraud Fighters” with Anthony Pratkanis, professor emeritus of psychology at the University of California at Santa Cruz. The two have listened to hours of scam calls and know how a master “con criminal” or “con grifter,” as they call them, wheedles past defenses.

As one con man told Shadel: “I ask them questions until I find their emotional Achilles’ heel.”

The simple truth is older Americans like Judith, now 80, are targeted because many have amassed great wealth through workplace retirement plans, traditional IRAs, home equity and other investments. In fact, Fidelity Investments reported a record number of 401(k) and IRA millionaires in the second quarter.

Meanwhile, the number of adults 60 and older scammed out of \$100,000 or more has tripled since 2020, according to the Federal Trade Commission’s annual report on elder fraud.

Americans were scammed out of more than \$10 billion in 2023, FTC data show, with seniors representing nearly a fifth of that tally. But because most scams are not reported, the FTC estimates these numbers represent only a fraction of the losses.

Shadel and Pratkanis said the levers used to swindle Judith out of nearly \$600,000 followed a template of sorts; a three-part strategy that swindlers customize to each potential victim.

The first step is to gain their trust.

“To get you to trust me, you have to like me,” Shadel said. “And to trust me, you’ve got to be like me. If you’re a Democrat, I’m going to be a Democrat. If you’re a Republican, I’m going to be a Republican. I’m just trying to match whatever interests you have with my interests so that you will trust me.”

To build this level of intimacy, scammers spend hours on the phone with their victims or bombard them with email or texts. The exchanges are intended to extract personal details to build rapport ahead of any request for money.

So if you're lonely, the grifter will play into your desire for intimacy. If you're a caregiver, it might be identifying with your exhaustion. If you're a Beyoncé or Taylor Swift fan, they bond with you over their music.

The second step of the fraud playbook is to get victims "under the ether," the frenzied state in which they suspend reason.

Everyone has something that, when surfaced into awareness, "destabilizes them or causes them to go into some emotional state," he said. "And it doesn't seem to matter if it's a positive emotion or a negative emotion."

You get folks talking, and a road map to overcoming their doubts will present itself.

"We tell people, 'don't give out your bank account information or Social Security number,' and that's all true," Shadel said. "But you also shouldn't be telling a complete stranger about your grandchildren or what your concerns are in life."

He knew when you were going out of town.



The scammers quickly assess the situation, peppering the victim with questions to feel them out and extract information that could be used against them. They sample for psychological triggers — such as the potential for financial losses after being told their personal information or Social Security number had been stolen, or the desire to develop an intimate connection, which is what romance scammers exploit.

They also capitalize on their fears and worries, such as an ailing spouse. "I was carrying the responsibilities of having my husband with Parkinson's, and a lot of my life had changed after his diagnosis," Judith said, reflecting on her state of mind.

In fact, on the day of that first phone call with the scammer in September 2023, she had been driving her husband of 33 years to a doctor's appointment and was distracted.

We're looking at it from the outside, and we may not see all the little details and trappings that create that powerful situation for the targeted victim. Anthony Pratkanis, professor emeritus of psychology at the University of California at Santa Cruz

Lastly, the impostors try to create a sense of urgency. For example, they might tell a victim that if they don't move their money out of their accounts, the people who stole their Social Security number will take it all, or the funds will be frozen as part of a criminal prosecution.

"It's baked into our brains to respond to threats," Shadel said. "You've got to create a reason for them to do something now."

Criminals construct a wonderland of the mind, a reality that appears authentic to the scam target. This is why the oft-used maxim, "If it's too good to be true, it probably is," isn't the most effective way to fight fraud.

Shadel and Pratkanis like to use Walt Disney's Pirates of the Caribbean ride to illustrate how scammers conjure up these fantasy worlds. Both get participants to suspend reality.

At the amusement park, customers willingly participate in an illusion. Of course the treasure and cannon blasts are fake. Yet a minute into the ride, "you're totally swept up in it," Pratkanis said.

"You're rocking back in the boat. You're looking all around to see the pirates and everything that's happening. At that moment, you're not thinking, 'Gee, did I leave my lights on in the car?' That world is totally gone for you. It's behind you now."

U as he coaching you?

How real and intense can it get for victims?

L
o
a
d
e
d
:
2
8
:
5
1
%

“It’s scary how good some of them are,” Pratkanis said of the scammers he has engaged with. “Even me, role-playing on the calls and knowing that there is zero chance of me going in for the fraud, it’s hard.

“I know exactly what’s going on, and I’m like, ‘Man, I can really see how somebody ... could easily get wrapped up in this.’”

Resources for financial fraud victims

If you or a loved one has been scammed, call the AARP Fraud Watch Network helpline at 877-908-3360 or go online at aarp.org/fraudhelpline.

AARP Fraud Victim Support Group provides an online forum for scam victims. Group sessions are confidential and led by trained facilitators. They also are open to friends and family; go to aarp.org/fraudsupport.

Though coming forward can be difficult if you’ve been victimized, it’s important to notify law enforcement. File a complaint with the Federal Trade Commission at ReportFraud.ftc.gov and the FBI’s Internet Crime Complaint Center at ic3.gov.

About this series

This is part two of **Scammed**, a seven-part series that deconstructs how one woman lost her life’s savings in a government impersonation scam.

Illustrations by Koen De Gussem with animation by Charlotte Dua and Karolien Raeymaekers. Art direction and print design by Kathleen Rudell-Brooks. Digital design and development by Audrey Valbuena. Video production and editing by Josh Carroll, Amber Ferguson and Tom LeGro. Audio production by Charla Freeland. Photo editing by Haley Hamblin. Design editing by Junne Alcantara.

Editing by Robbie Olivas DiMasio. Project editing by KC Schaper and Rivan Stinson.
Copy editing by Sophie Yarborough. Additional support from Maite Fernández
Simon, Megan Bridgeman and Kathleen Floyd.