The psychology of scamming: How fraudsters hijack your brain

If you think you can't be duped by internet and phone scammers, you're the victim they're looking for. Here's how fraudsters get inside your head and swindle people who think they can't be "had."

Robin Chenoweth: The news reports get more bizarre by the day.

WDTN2 Dayton: A 74-year-old woman is behind bars after admitting that she robbed a bank at gunpoint in Fairfield Township near Cincinnati. … Investigators say she might have done it to get money to send to a scammer she met online.

Robin Chenoweth: A worldwide network of scammers seems willing to go to any length to cash in.

KTLA 5: She says a man claiming to be tech support then told her seven hackers were buying child porn from her Wells Fargo account and that she needed to move the money immediately. … He was very convincing. He was even able to give her information she hadn't provided. Her bank account numbers. Her recent banking activity. Even that she had recently used her checking account to buy flowers. He knew it all.

Robin Chenoweth: Internet and phone fraud have become exceedingly profitable. The Federal Trade Commission says that consumers reported losing more than $10 billion in the United States alone last year. But the consequences can be even more dire than lost life savings.

CBS Mornings: Eighty-one-year-old William Brock received threatening calls last month saying his family was in danger and demanding money. Then the scammers also called an Uber driver to pick up a package from Brock's home. Brock then confronted her with a gun believing that she was connected the threats he had been receiving and now he's charged with murder.

Robin Chenoweth: If you think you are too young, too educated or too savvy to fall for crimes like these, you are putting yourself at risk, experts say.

Yaniv Hanoch: In my mind, the number one reason why people fall prey to fraud is because they don't think that they are the person that will become a victim of fraud. So when they receive the call, or the email, they think, “Okay, I can engage in this conversation. But nothing is going happen to me.” So, my most important advice to the individual is think “vulnerable.” Always think that they can scam anybody.

Robin Chenoweth: In this episode of the Ohio State University Inspire Podcast, we tackle common myths about who gets scammed and why. We talk to a behavioral scientist about how scammers use psychological tactics to get inside people’s heads, exploiting vulnerabilities that people might not realize they have. And we learn from an Ohio State professor of consumer science about the best ways to protect yourself from what experts call a “pandemic” of fraud that is growing ever more sophisticated. I’m Robin Chenoweth. Carol Delgrosso is our audio engineer. Inspire is a production of the College of Education and Human Ecology. If you spend time online or have a smart phone or an email account — let’s face it, we’re talking about almost everyone — you have been targeted by scammers. You click on the wrong link and your computer seizes up.

Fake security message: Important security message: Your computer has been locked up. Your IP address was used without your knowledge or consent.

Robin Chenoweth: You get a call saying you qualify for student loan forgiveness. A bogus email tells you your PayPal or bank account has been compromised. These and other scams have been going on for years, so you might think you’re wise to their tricks. But as technology gets smarter and communication becomes more seamless, it’s getting much more difficult to spot the rogue players. And even the tech savvy and financially literate are getting defrauded.

News 5 Cleveland: New research shows that young people are being duped more often and they’re losing millions of dollars.

WAFB5: A new study from Better Business Bureau shows that young adults between the ages 18 to 24 are the ones losing more money to scam than older adults. … Scammers are using Instagram and X to target many high school and college students.

Robin Chenoweth: Yaniv Hanoch is professor of Decision Science at the Center for Business in Society at Coventry University in the United Kingdom. He spoke with me and Ohio State’s Cäzilia Loibl, a professor of consumer science in the College of Education and Human Ecology. They both members of the International Association for Economic Psychology.

Yaniv Hanoch: If you just look at the numbers, the estimates, is that about $5 trillion a year have been defrauded either from individuals or from organizations, etc. To put it in context, this is roughly the budget of the U.S. per year. … If you asked me a year ago, as an expert on fraud,

“Yaniv, can you be duped?” I would have been confident, cocky. And I would say, “Never, never.” Have I been victim of fraud, you bet it. … I presented my research to one of the ministry departments in the UK. And they're all counter fraud experts. So that's their daily work, to detect fraud against the government. So, these are individuals you can think that eat, drink, read, you know, sleep fraud. There were about 200 people in the audience and I ask, naively, you know, that anybody here is a victim of fraud, assuming that nobody would raise their hand. But 50 people raised their hand. And these are the people that were willing to raise their hand.

Cäzilia Loibl: People try to hide it because it's so unpleasant and touches a nerve to be scammed and taken advantage of. So, I believe that adds to the psychological burden of fraud.

Robin Chenoweth with Hanoch and Loibl: It's not just elderly people anymore, right?

Yaniv Hanoch: No, oh, the data shows...if you look at the actual data of who has been scammed, elderly are not the most common population by far. It’s middle age. If you look at trend, young adults, Tik-Tok, we talking about adolescents, rising number of-— I do not know precisely what they take from them — but they are rising number among them.

Robin Chenoweth: Data by the Federal Trade Commission, in fact, dispels a lot of misconceptions. People in their 30s reported more fraud than any other age group last year; 20- to 29-year-olds reported more fraud than those in their 70s. And people 70 and older lost less money by far than middle-aged victims of fraud.

Yaniv Hanoch: If you think about, if you are a scammer, who would you like to scam?

Robin Chenoweth with Hanoch and Loibl: I think you'd be scamming the person with the most money, right?

Yaniv Hanoch: Precisely. If I can scam not that I'm going to, you know, Elon Musk or Bill Gates, all I need is one time. If I can take, you know, a good chunk of their holding. you know, I can retire happily ever after.

Robin Chenoweth: Right.

Yaniv Hanoch: First it's people with money, then they might have individuals with slightly less money. … Middle class and above, and especially people that might have money in their bank. And these are the individuals that think probably that, most of themselves as, “It's not going to happen to me.”

Robin Chenoweth: News reports and conversations with those who are swindled bear this out. Here’s James, a retired police officer who appeared on The Daily after being frauded out of $900,000 in a timeshare scam.

The Daily: I didn’t want to believe that I had fallen for this. I didn’t feel that I was that foolish and stupid when it came to this. You know? I guess I didn’t want to believe that I could be fooled.

Robin Chenoweth: This man, in the UK, fell for a business-related scam that cost him $10,000.

YouTube: In hindsight, I can’t believe I was so f&%#ing stupid. The part of me that feels extremely violated is the part who me that thinks I would never, ever fall for something like this. Like, I have so many years’ experience in this. I have like a computer science degree. I am so familiar with the world of scams that someone like me should never, ever be falling for this. However, they were so ridiculously convincing, with all the right names, all the right profile pictures, saying all the right things, that at the time they actually had me thinking they were all the right people.

Robin Chenoweth: Fraudsters have dreamed up every kind of scam, touching every aspect of life and every kind of person. Grandparent scams, in which imposters use AI to generate voices of family members in distress. Romance scams. IRS scams. Social security and debt scam.

Cäzilia Loibl: Precious metal, cryptocurrencies or real estate investment.

Robin Chenoweth: Student loan forgiveness scams.

Cäzilia Loibl: The FTC, the Federal Trade Commission received 495,000 fraud reports in the first quarter of 2023 on student loan forgiveness fraud.

Robin Chenoweth: The fake job scam, where you interview, get hired and give the phony employer your bank account number so they can deposit a hiring bonus.

Cäzilia Loibl: It's everywhere. You almost can't escape it.

Yaniv Hanoch: You cannot. … You can think of it as a pandemic. The extent of it, and the scope of it and the type of fraud that is being perpetrated on all of us constantly. … They know the name of your boss. They know the name of your friends. They harvest information from social networks in order to identify information and capitalize on that. … They're really at the front of technology, unfortunately, and able to use it without any scruples. Nothing is stopping them from using AI now for really pushing the boundaries. So, if fraud was bad so far, I, I don't want to be a prophet, but my prediction would be that things are probably going to get worse in their capacity to fool us, to imitate… In the U.K., at least, in many cases, you get phone calls from the bank. So, they will be able to imitate banks or other such institution, credit card brands, Social Security, tax, etc., far, far better than our ability to distinguish between them, between what is real and what is scam will be much harder to detect in the future.

Robin Chenoweth: So, how do you stop it? You might do what Loibl does: Never answer your phone unless someone from your contact list calls. Many scammers don’t leave voice messages.

However, the worldwide fraud network is very reactive, Hanoch says. Fraudsters impersonating businesses or government officials have shifted tactics since 2020, the FTC says. They are calling less and emailing and texting more. You should apply filters to emails and not take risks by answering unknown texts. But… if you find yourself innocently stepping into a situation where someone asks for bank information or to send money or gift cards or withdraw cash from your account, it pays to familiarize yourself with the psychology behind the scammers' game. Hanoch uses the cautionary tale of Charlotte Cowles, a finance journalist in New York.

Yaniv Hanoch: She writes how she never, ever dreamed of her, or never seen herself as a person who can fall prey to scam. And she writes how she handed $50,000 in a shoebox to somebody in a car that she doesn't know.

Robin Chenoweth: Here are excerpts from an audio recording of Cowles story in The Cut, used with her permission.

The Cut: A polite woman with a vague accent told me she was calling from Amazon customer service to check some unusual activity on my account. … Had I recently spent $8,000 on MacBooks and iPads? I had not. The woman, who said her name was Krista, told me the purchases had been made under my business account. "I don't have a business account," I said. … Krista transferred the call to a man who identified himself as Calvin Mitchell. He said he was an investigator with the FTC, gave me his badge number, and had me write down his direct phone line in case I needed to contact him again. … "I'm glad we're speaking," said Calvin. "Your personal information is linked to a case that we've been working on for a while now, and it's quite serious." He told me that 22 bank accounts, nine vehicles and four properties were registered to my name. The bank accounts had wired more than $3 million overseas, mostly to Jamaica and Iraq. Did I know anything about this? "No," I said. Did I know someone named Stella Suk-Yee Kwong? "I don't think so," I said. He texted me a photo of her ID, which he claimed had been found in a car rented under my name that was abandoned on the southern border of Texas with blood and drugs in the trunk.

Robin Chenoweth: I asked Hanoch to break down how the scammers were operating.

Yaniv Hanoch: They create an element of trust. First, they are all they were CIA, the Federal Trade Commission. They were Amazon Fraud Unit, or whatever it was. So, they try to establish a trustworthy relationship as much as they can in the first initial stages. And that is by giving names that we all trust, like the CIA, like the Federal Trade Commission, or the bank, or the police, things that we usually trust. So, once you trust those individuals, you have less reason to suspect that they're cheating you, or committing fraud.

Robin Chenoweth with Hanoch: So this whole authority figure thing though… I don't know if it's the same in Britain, as it is here in the United States. We're really taught to revere authority figures, and does that play a part in the scammers being able to dupe us?

Yaniv Hanoch: Big time. Yeah, big time. If you look at what we know from research about communication and persuasion, authority is one of the chief factors where people are obeying or following or adhering or accepting. Although there's been a lot of erosion over authority of for example, government. … Or maybe it's partially the story. … There's been a lot of material out there in social network, etc., fake news, not fake news. Actually, knowing what is true and what is not is become a much harder task for the average person, and also for the sophisticated person.

The Cut: Then he read me the last four digits of my Social Security number, my home address, and my date of birth to confirm that they were correct.

Robin Chenoweth: The phony FTC agent transferred her to a “colleague at the CIA” who told Cowles the same details about the illegal activity but knew still more about her.

The Cut: Then he asked more questions about my family members, including my parents, my brother, and my sister-in-law. He knew their names and where they lived.

Yaniv Hanoch: They are able to create further trust and reliability by providing you with some information, not a lot of information, but some information that is sufficient for you to drop your guard even further. So, they might know your name. They knew that she had a child, a son. They knew the last four digits of Social Security.

Robin Chenoweth: All this information was likely found in the internet and social media searches and on the dark web. But all the while as scammers are building this false trust, they are engaging in the ultimate psychological deception. Call by call, text by text, they are inducing panic.

The Cut: A home in New Mexico affiliated with the car rental had subsequently been raided, he added, and authorities found more drugs, cash and bank statements registered to my name and Social Security number. He texted me a drug-bust photo of bags of pills and money stacked on a table. He told me that there were warrants out for my arrest in Maryland and Texas and that I was being charged with cybercrimes, money laundering and drug trafficking.

Yaniv Hanoch: They create a state of as much panic or fear as possible. … But, the next person she spoke to, she was already on the FBI most-wanted for channeling money to Jamaica and to Russia and dealing drugs and being involved in a wide range of criminal activities. … So, you're not thinking straight.

Robin Chenoweth: Your reality is distorted. Intense fear and panic causes reptilian, fight-or-flight modes to kick in in the brain. The high-level thinking — what Hanoch and Loibl call System 2 thinking — takes a back seat. The scammer has hijacked your mind. So, when he tells you to tell no one — not even your spouse — what is happening, you might just comply.

Yaniv Hanoch: This kind of chaotic scenario that is being presented, they present to you eventually some order and, you know, resolution.

Robin Chenoweth with Hanoch: I see.

Yaniv Hanoch: They create the chaos on a certain matter. And they are, as the authorities, they are able to solve this chaos or this predicament that you are in.

The Cut: He explained that the CIA would need to freeze all the assets in my name, including my actual bank accounts. In the eyes of the law there was no difference between the real and the fraudulent ones, he said. … "I am going to help you keep your money safe."

Robin Chenoweth: What could have stopped Charlotte Cowles — or anybody who is scammed — from putting $50,000 cash into a shoebox and putting it into a stranger's car? You must break the psychological grip that the scammers have on you, even for just a moment. Cäzilia Loibl.

Cäzilia Loibl: I believe is one step is to slow down before you take action. To think it over, to wait a day, or wait just an hour before taking any action. Is it a request that comes suddenly and unexpectedly? Just to step away for an hour, and then review it again. That's good advice anyways, when doing difficult or high-impact things.

Yaniv Hanoch: If possible, talk to somebody else. … Even have conversation with your pet, in the sense of the moment you verbalize it, you might be able to realize that this is out of the ordinary. That this is not something that would typically occur. So if I spoke to my wife, if I had brought my wife in and I said, "Look, what do you think about this? What is going on?" She would have said, "Yaniv, it's a scam. Can't you see?" … Think about, would you recommend that to your friend? To your parents? To somebody else? Would you tell them, you know, just put the $50,000 in the box and give it to a stranger? No. The moment you verbalize it, what it does, it brings in what your, we call System 2.

Cäzilia Loibl: Yes.

Robin Chenoweth with Hanoch and Loibl: System 2?

Yaniv Hanoch: System 2. More your intellectual level. What many scammers do is they build on your emotion; they kidnap your intellect. They put it aside and they stress you to think something really bad is going to happen to her. … To think…if she would have thought about it rationally, if she had a moment to reflect about it, if he had a conversation with her partner, they would have said, "You're insane. Of course it's a scam." But she was in this world that the scammers are able to create for us.

Robin Chenoweth: The IRS, banks, courts will never call or text you asking you for money. Any police officer or federal official asking for money for any reason would be charged with

extortion. It is your constitutional right to talk to a lawyer about any matter, at any time. Scammers can manipulate caller IDs to be any name or number they choose. In a crisis, a bank's app or website are the best places to find contact information. It's a lot to keep track of. But there are people out there to help guide you.

Robin Chenoweth with Hanoch and Loibl: Dr. LoibI I wanted to ask you, you're teaching students who will later become financial planners for people … My financial planner went through our college program. … And if there were ever something to come up, I probably would be talking to him. Is that something you suggest to people, call your financial planner and ask them, does this sound right?

Cäzilia Loibl: Definitely, families, individual should work with a financial planners, before they make a decision. And if something doesn't look right, I recommend it. And financial planners often perceive themselves as educators, to provide individuals and families with a good solid financial education on many aspects of the financial marketplace. So I would think that scams and fraud issues are part of the conversation.

Robin Chenoweth: Having trusted relationships with a banker, a financial adviser, a lawyer, an accountant can be invaluable when you are in a pinch. But to really fight financial fraud, it's going to take more, Hanoch says.

Yaniv Hanoch: Just telling people, "Be careful, be on guard" is not going to be enough. We need the government on various levels … all of them been involved in setting limits, for example, working with social networks. … Tik Tok, as I mentioned, is another avenue. And many others are really a breeding ground for scams. So, there's really a need to be an orchestrated effort for various organizations such as government, such as social network, high tech company. … Think of the bank. … If you go to the bank now and you never send money to Jamaica or took large amounts of cash, there should be a mechanism in the bank that says look, if Robin takes her 50 grand that which is almost everything that she has- suddenly in cash or wants to transfer it to some unknown country for unknown business, we put a stop to it and go through a procedure. The procedure can be, we want to see, we want to wait, we want to verify... There can be some protocol to mitigate it and to help us. We are humans, that's what they count on. That we are humans and that we panic, and that we obey rules. When the police come and ask us for information we provide them. So this is where we really need the companies to assist us, whether it is Amazon, Facebook, whoever to help put stricter safeguards. And banks, because a lot of money is being channeled from banks to these nefarious activities with very little oversight.

The Daily: Yeah, it's been a swell experience. All of it brought on by my, evidently, my stubbornness to not believe that I could be a victim.

Yaniv Hanoch: I really want to stress that we cannot be careful enough, or on guard enough.

Robin Chenoweth: To read about more ways to safeguard yourself and those you care about against fraud, see the link in our episode notes.

https://ehe.osu.edu/news/listing/cant-happen-me-surefire-way-be-scammed