

Scammers

(continued from page 22)

the line that long?” Hall said. “But then I look at this girl I know, and they managed to get her to go all the way.”

The Business of Scamming

The Federal Trade Commission reported the overall loss Americans experienced via financial scams in the 2023-24 fiscal year to be between \$23.7 billion and \$158.3 billion. The figures differ so much because so many losses go under- or unreported, the FTC said in the report.

Matthew Radolec, D.C.-based vice president of Incident Response and Cloud Operations at data security firm Varonis, said he sees these phishing attempts in two parts; the scam is the technique being used to get access to money, and the actual crime itself is the loss of the money.

Because these crimes are digital, it's hard to know who to report them to, or how to follow up. Many scammers also ask for cryptocurrency payments, or transfer them to crypto accounts shortly after the transaction.

“There's no insurance for accidentally wiring someone \$10,000,” Radolec said. “If you fall for a ruse, you fall for a ruse. It's like a carnival trick, a sleight of hand. It's a digital form of that.”

Kimberly Sutherland, a Georgia-based vice president of fraud and identity at LexisNexis Risk Solutions, said they've seen a 20% year-over-year increase in digital fraud since 2021, affecting as much as 1.5% of all transactions, though many of those attempts are caught before they can go through.

A few decades ago, scammers were focused on getting enough information from a company or individual to pull off a fake transaction. But as data breaches have become more common, the personal data unearthed makes it easier to pose as someone a victim knows, or give them details to become trustworthy.

Sutherland said the concept of synthetic identities - carefully crafted digital profiles of someone who doesn't actually exist - have also deepened criminal's abilities to get access inside a variety of institutions like banks, colleges and corporations.

“You don't have to steal an identity. Why not create a brand new one?” Sutherland said. “It started with jokes like, ‘I can get a credit card in the name of my dog,’ and it became sophisticated fraud rings who could actually create identities and nurture them to be used by others.”

Individuals and companies are not the only ones at risk of financial scams. Government institutions have reported an increase in financial crimes in recent years. In California, community colleges have reported at least \$5 million in losses to AI-simulated students who applied for financial aid.

One of the most current, wide-spread scams are texts and alerts from toll payment agency E-ZPass, asking a user to pay an outstanding bill at the included

There's no insurance for accidentally wiring someone \$10,000. If you fall for a ruse, you fall for a ruse. It's like a carnival trick, a sleight of hand. It's a digital form of that.

Matthew Radolec, vice president of Incident Response and Cloud Operations at Varonis

link. Last year, E-ZPass said the FBI's Internet Crime Complaint Center had received more than 2,000 complaints about the texts.

Those who had filled out the included form should contact their banks, the company said.

It's similar to a longstanding scam posing as UPS trying to deliver a package. It plays on our human nature of trust and curiosity, O'Leary said.

AI is Playing a Role

AI has lowered the barrier for setting up a scam, O'Leary said. Many programs that can be used to fake a persona, to send out mass text messages or phishing links are as easy as downloading an app.

“It's almost a step by step for someone who wants to make a quick buck,” O'Leary said.

Large language models and AI chatbots can easily be prompted to sound like someone else, and give non-English speakers a much easier ability to communicate, O'Leary said.

Radolec has seen an uptick in AI bots being used to gain credentials to company databases or pay systems. Bots can hold legitimate conversations with a target to build rapport, and plant phishing scams to gain passwords in standard documents.

“The next thing you know, you can log in as me,” Radolec said.

From there, scammers can divert paychecks to offshore accounts, sell data on the dark web or plant further phishing attempts in internal systems.

Because of the rapid advancements in AI technologies, phishing attempts and scam strategies are constantly changing. Now, AI tools can help alter legitimate images, and create deepfakes, or likenesses of someone's image or voice, in just a few minutes.

It's the strategy behind an increasingly common scam on grandparents. They get a call from someone that sounds exactly like their grandchild, saying they need a wire transfer or cash for bail.

Many digital scams target older people, both because they're expected to have less technical knowledge to spot a ruse, and because they tend to have larger sums of money accessible. In its report, the FTC estimated between \$7.1 billion and \$61.5 billion in losses for older adults.

AARP, Amazon, Google and Walmart have partnered on a new initiative that will be based out of Pittsburgh, called the National Elder Fraud Coordination Center, an attempt to tap in private companies who have resources in data privacy to assist in national law enforcement investigations.

Its founder and CEO, former FBI agent Brady Finta, said that the technical side of these crimes are often partnered with an emotional side, like pretending to be a

family member in trouble.

“They're talking you through the crime,” Finta said. “They're adding this anxiety and thought process to you and to overcome your normal decision making processes.”

Legislation, Enforcement

There are hundreds of thousands of victims of financial scams each year, and they're reporting them to different places - local police, state organizations, federal agencies, and the tech platforms where the crimes occurred, Finta said.

Part of the reason some financial scams go unreported is that there's not one clear route, government agency or law enforcement agency that has ownership over them.

There are 13 federal agencies, including the FBI, CFPB and the FTC, that work to counter scams, but they do not share one overarching strategy.

Finta is hoping to begin connecting fraud cases across the country and make these investigations more comprehensive.

And the U.S. may be facing less protections than it currently has. Susan Weinstock, CEO of the Consumer Federation of America, said she's worried that Congress just voted on a resolution under the Congressional Review Act that removed the rule that required digital payment apps like Venmo and Apple Pay to be regulated for fraud.

“Years ago, nobody had heard of Venmo or CashApp, and now these things are ubiquitous,” Weinstock said. “So it puts consumers in a really tough, scary position to be subject to fraud and not have the ability to deal with it.”

Because the strategies behind these financial scams change often and because there are few ways to track these crimes after they happen, a lot of responsibility falls on individuals and institutions to be able to spot them. Radolec's first piece of advice is to slow down.

“Is it really your grandson calling from jail? Is it the end of the world if he spends a night in jail? he asks.

Adding another person into the loop of communication is another strategy that will usually knock off an impersonator. If it appears to be a higher-up at work making a strange request for access to your finances, there's no harm in looping in another person to review.

Lastly, cybersecurity experts all said it's always safer to get in contact with the original source. If someone on the phone says they're with your bank, hang up and call the bank directly to verify information.

“A lot of times they're trying to create a sense of urgency that's from a false place, so how can we ground ourselves?” Radolec said.

Public Notice

(Published in The Scott County Record Thurs., April 24, 2025)1t

SCOTT COUNTY COMMISSIONER'S PROCEEDINGS MARCH 2025

GENERAL FUND

SALARIES	\$ 78,664.74
COMMODITIES	1,411.84
CONTRACTUAL SERVICES	57,064.52
CAPITAL OUTLAY.....	3,532.82
OTHER.....	175,910.43

SHERIFF FUND

SALARIES	52,531.19
COMMODITIES	9,676.98
CONTRACTUAL SERVICES	13,421.68
CAPITAL OUTLAY	0.00
OTHER.....	0.00

COUNTY HEALTH FUND

SALARIES	18,453.68
COMMODITIES	6,921.14
CONTRACTUAL SERVICES	1,138.59
CAPITAL OUTLAY	1,246.88
OTHER.....	0.00

NOXIOUS WEED FUND

SALARIES.....	5,425.80
COMMODITIES	7,344.30
CONTRACTUAL SERVICES.....	953.18
CAPITAL OUTLAY	0.00

ROAD AND BRIDGE FUND

SALARIES.....	47,703.93
COMMODITIES	-5,457.96
CONTRACTUAL SERVICES.....	8,678.93
CAPITAL OUTLAY	93,000.00

FIRE DISTRICT FUND

SALARIES	1,250.00
COMMODITIES	1,377.08
CONTRACTUAL SERVICES.....	7,281.68
CAPITAL OUTLAY	0.00

TREASURER'S SPECIAL FUND

SALARIES	4,510.02
COMMODITIES	0.00
CONTRACTUAL SERVICES	103.77
CAPITAL OUTLAY.....	0.00
OTHER	420.84

PERRY NOWAK
Chairman

MARIE ALLEN
Scott County Clerk

Tree Trimming • Stump Grinding
Lawn Aeration/Thatching • Yard Clean-up
Snow Removal and more

VALLEJO & SONS, LLC
EST 2021

TJ Vallejo Free Estimate

YOU DON'T KNOW WHAT YOU DON'T KNOW.

WITHOUT PUBLIC NOTICE YOU ARE LEFT GUESSING.

Public notices in our newspaper help you stay informed about government, corporate and private activities that touch your world. An informed citizenry is the core of our democracy.

Since knowing is so important, we joined the other newspapers in Kansas and also publish our public notices online.

KANSASPUBLICNOTICES.COM