GUMC HEALTH AWARENESS INITIATIVE - APRIL 2024
Top Scams to Watch Out for in 2024 - Addendum

Criminals are getting more sophisticated and supercharging old scams with new technology. One reason that scammers are so difficult to stop, security experts say, is that they keep raising their game. They're continually perfecting their scams, taking advantage of tech innovations and honing their methods to better manipulate their targets. "We keep coming up with different tools to combat scams and fraud, but it's just like playing whack-a-mole," says Better Business Bureau spokesman Josh Planos.

Scammers have become much more adept at impersonating legitimate institutions, including creating websites and messages that are "carbon copies" of legitimate health care providers, businesses and banks, with fewer grammatical mistakes and other red flags for scams, according to Planos.

And criminals are not only taking advantage of technological innovations such as artificial intelligence (AI), they're also growing ever more adept at psychological manipulations — their "game of persuasion," says Aaron Foss, former chief executive and founder of Nomorobo, a firm whose technology aims to thwart robocalls. Foss explains that today's scammers in overseas call centers, for example, are often trained to minimize their accents and coached on ways to connect emotionally with their targets.

Here are six of the scams that experts say you should be watching out for this year:

1. **Check cooking scam** - Last year, the big thing was check washing, where thieves stole paper checks from postal boxes, mailboxes or even carriers and then washed the checks with chemicals, keeping the signature but erasing
2. the amount and the payee so they could fill in a new name and amount. But now, they've discovered a less messy way to steal. In check cooking, thieves take a digital picture of a stolen check and then use commercially available software to alter it. "It looks very real, even with the watermarks and all," explains Michael Bruemmer, vice president of data breach resolution and consumer protection at Experian, a global credit verification and financial services firm. Criminals can print a new phony check or else just deposit the altered image using a bank's mobile app, he notes.

How to stay safe: Consider using a safer payment method, such as a credit card. But if you choose to write paper checks, scammers still need to steal a physical copy. Make it harder for them. Instead of putting the check in a mailbox, drop it off directly at the nearest post office. And continually monitor your checking account and watch for any suspicious transactions.

2. Voiceprint Scams - Thanks to technological advances, it's possible for thieves to capture a recording of your voice and then use a software program to generate an imitation "deepfake" version that can be used to impersonate you. "That voiceprint can be used to access your insurance or your financial institution or apply for a driver's license," Bruemmer says. The New

York Times reported on a recent case in which a representative at a major bank received a call from a deepfake copy of a Florida investor's voice, requesting that the bank move the man's money elsewhere. Fortunately, the fraud attempt was spotted by the bank before the real investor lost his savings.

How to stay safe: To prevent your voice from being duplicated, "don't answer the phone," Bruemmer advises. "If someone needs to get hold of you, they can text you." Bruemmer even is cautious about answering calls that appear to be from people on his contact list, since the call could be coming from a phone that's been stolen or had its SIM card cloned, he says.

3. **Delayed-action sweepstakes scam -** Sweepstakes scammers, who call or write to say that
4. new variation on the old formula, according to Bruemmer. Instead of trying to get you to pay taxes or other fees in advance to collect the nonexistent prize, the scammers will ask for personal information so that they can validate you and set up the payout. "They'll say, just give us your banking information and your Social Security number, and we'll file with the IRS and we'll take care of everything," he explains. "But, boom, it's just another form of identity theft." Instead of quickly looting your bank account — what Bruemmer calls a "smash and grab" — the scammers may play a long game. They'll write small checks on your account to see whether you notice the fraudulent activity. If you don't, they'll continue to use the account to obtain credit cards and lines of credit in your name that they can siphon off, giving them a potentially bigger payday down the road.

How to stay safe: As with previous variations of the sweepstakes scam, remember that if it seems too good to be true, it probably is. If you get a call from someone claiming that you've won a huge prize, the safest bet is to just hang up. And never, ever provide any personal information.

4. Virtual celebrity scam - Celebrities have had online presences for years, but the trend really gained momentum during the pandemic, when stars who couldn't make public appearances tried to stay connected with their fans by doing online concerts and other events on social media. Fans have become accustomed to that constant virtual intimacy, which leaves them vulnerable to celebrity scammers. "You're on Instagram or Facebook, and someone pretending to be Celine Dion or her manager reaches out to you," explains Amy Nofziger, director of victim support for AARP's Fraud Watch Network. If it's a fake manager, "They might say, 'Celine loves your comments. She'd love to talk to you. Here's her private account.' " But after you connect to an impostor pretending to be the superstar singer, the talk gradually turns to how her fortune is tied up in a lawsuit, and she could use a $50,000 loan from you, or a similar story involving a need for your money.

How to stay safe: If you get a direct message from someone claiming to be a famous performer or superstar athlete or representing them, be skeptical. It's almost certain to be a scam.

5. Multistage grandparent scam - This is a new, more sophisticated version of the old grandparent scam, in which crooks call and pretend to be a grandchild who's been arrested and needs bail money to get out of a nonexistent legal jam. In the past, grandparent scammers were often small-timers who would plead for a few hundred dollars. But these days, Foss says, they often set up call centers staffed with young people who are paid a few bucks for every grandparent that they can connect with. After posing as grandchildren who've been jailed after a car accident, they'll provide a case number and instruct the target to call their defense attorney or the local prosecutor. "When Grandpa calls up, they say, 'Oh, do you have the case number?'" Foss explains. It's actually a subtle psychological trick to see whether the grandparent is compliant and will follow their instructions to send thousands or even tens of thousands of dollars.

Some scammers have a third conspirator pose as a courier and go to a grandparent's home to pick up the money in person, according to Steve Baker, a former Federal Trade Commission official who now publishes the Baker Fraud Report newsletter.
How to stay safe: If you get a call from an unfamiliar number from a family member claiming to be in trouble, don't panic. Instead, after you've finished talking — and certainly before sending money — the Federal Communications Commission recommends that you call or text the person at his or her usual number and check to see whether the family member is actually in trouble. If they don't answer, contact other family members or friends if you have any concern that the emergency could be real. Scammers plead with you to keep the situation a secret precisely so you won't try to confirm it.

6. Paris Olympics scams - Criminals try to find ways to exploit big events that are in the news. With the Paris games coming up this summer, Nofziger suspects that we may start seeing a revival of the fake emergency scam, which bears similarities to the grandparent scam but is slightly different. It could work something like this: A scammer hacks someone's email account, and shortly after, all of that person's contacts will receive the same message — something to the effect of, "Hey guys, I'm over in Paris and my wallet got stolen! Can anyone please help me out by sending gift cards or a Venmo deposit?" To the recipients, it's a potentially convincing ruse. "You're thinking very quickly, well, Amy was in Paris two years ago, and she loves the Olympics, so it all makes sense," Nofziger explains. "Yeah, I'll send you money." And Olympics officials are warning ticket seekers to avoid bogus ticketing sites and scam emails purporting to be from Paris 2024 (the official website for the games) or the Olympic committee.

How to stay safe: Resist the urge to react immediately if you hear from a friend in Paris needing cash. Instead, follow the Federal Trade Commission's advice and try another way to contact the person who supposedly is in need, such as calling them on the phone. Alternatively, reach out to a trusted source who knows the person and would be aware of whether or not they went on a trip to Paris. If you're intending to go to Paris and receive emails regarding tickets to the games, the official website for Paris 2024 notes, "You will never be asked for the login details for your ticketing account (ID and password)" or "banking details." Check the sender's email address; scammers will often change one letter or number, or use .com rather than .org, hoping recipients will mistake the fake address for the legitimate one.

Helpline - Call the AARP Fraud Watch Network Helpline toll-free at 877-908-3360 Monday-Friday, 8 a.m. - 8 p.m. ET, if you suspect fraud or have fallen victim to a scam.