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

Chatbots and Voice-Cloning Fuel Rise in AI-Powered Scams. A Houston-area couple received a call last month from their adult son — or at least they thought it was him: The voice sounded exactly like him. He said he'd been in a car accident where he hit a woman who was six-months pregnant, had just been released from the hospital, and now was in the county jail about to be charged with DWI, according to a KHOU 11 News report. He needed $5,000 to get himself out of this mess. Absolutely convinced that the caller was their child, they handed over the cash to an intermediary who came to their home pick it up.

How'd the scammers pull it off? Most likely by using artificial intelligence (AI) to clone the son's voice, says Alex Hamerstone, a cyber analyst at TrustedSec, an information security consulting company. He points to the case in Houston as one vivid example of how the latest generative AI technology, including voice-mimicking software, deepfake videos, and chatbots like ChatGPT can be used by bad actors. They have the potential to level up criminals' ability to impersonate anyone — your grandchild, a police officer, even your spouse — Hamerstone notes.

"There are a lot of scams out there that are pretty worrisome, and I always try to kind of temper that a little bit," he says, "but this one really does scare me." Other experts are also concerned about AI's potential for harm. Last month, a group of tech leaders, including Elon Musk and Apple cofounder Steve Wozniak, posted an open letter online warning that "AI systems with human-competitive intelligence can pose profound risks to society and humanity," and calling for a six month pause in the training of AI systems, so experts can take time to develop and implement "a set of shared safety protocols."

A game-changer for impostor scams - The scheme described above — a version of the "grandparent scam," where grandparents are targeted by criminals pretending to be grandchildren in crisis — is common, "but before [the use of this software] the voice could have been a giveaway," says Steve Weisman, a professor of white-collar crime at Bentley University in Waltham, Massachusetts, and an expert in scams, identity theft and cybersecurity. With voice-cloning tech, he adds, scammers need to capture only a few seconds of the child's audio, "which they can get from a TikTok video or an Instagram video or anything like that," to offer a convincing impersonation.

In another widely reported incident this month, an Arizona woman named Jennifer DeStefano said she received a call from what sounded like her 15-year-old daughter, Briana, who was on a ski trip, crying and claiming that she was being held by kidnappers demanding ransom money. DeStefano confirmed that her daughter was safe, but was shaken that the voice sounded exactly like Briana's. She attributed the uncanny likeness to AI.

And anyone can use this technology: "It's just like downloading any other app," Hamerstone says. "If you were recording this conversation, you could feed it into the software and type out whatever you want me to say, and it would play my voice saying that." If the person listening asks questions, AI has the potential to create responses in Hamerstone's voice that would make sense to the listener. "It's unbelievable to see it," he adds. "You cannot tell. It sounds just like the person… It's just much more difficult to tell what's real and what's fake."

Adding to the difficulty? There's easily available tech that allows users to spoof any number — your grandchild's, your bank's, you name it. The same concerns apply to written messages, through emails, texts, or social media messaging, experts say. Scams are often perpetrated by international crime organizations from places like North Korea, Nigeria and Russia, Weisman notes, and because English is not always their first language, "the syntax and the grammar were pretty much laughable. But now, using AI, the scammers can tailor these phishing emails to English and make them so much more convincing." "Bad actors and cybercriminals now have basically access to very powerful tools," says Eyal Benishti, founder and CEO of Ironscales, a

company that helps organizations protect against social engineering and email phishing scams. “It’s opening a new era of potential threats.”

Worries for the future - Benishti is particularly concerned that eventually criminals will be able to use a “multi-pronged” strategy to perpetrate their scams, including voice-cloning, AI generated emails, and deepfake videos. He offers a scenario: Your boss emails you with a request, “then leaves you a voicemail, saying, ‘Hey, did you get my email? It's very urgent. I really need you to do that.’ And…at some point, you will even get a Zoom call where you will see a video, and you will totally believe that you're speaking with her, [seeing] her face, her facial expressions…. This kind of multi-media approach is what I’m scared of the most.”

With advanced AI, a criminal will also be able to give the software tasks, he says, such as “your task is to convince Christina to wire money or give a credit-card number… Now go and figure out, based on her reply, how to do it.” Benishti adds that in time, “these things will be not just easier and more automated, but the volume will increase significantly — so much so that at some point, “you [won’t be able to] trust anything that is being communicated to you if it is not face-to-face.”

Fake ads, fake AI - It’s worth playing around with a chatbot to get a sense of the technology’s potential (and it’s kind of fun). But note that cybercriminals are advertising AI tools on social media and search engines with links that will download malware onto your computer if you click on them, according to a new warning from the Federal Trade Commission (FTC), which recently launched a new Office of Technology in February “to strengthen the FTC’s ability to keep pace with technological challenges in the digital marketplace.”

Some are fake sites, the FTC says, but “some ads actually take you to the real software and download the malware through a ‘backdoor,’ which makes it hard to know you got hacked. Then, the criminals could steal your information and sell it to other hackers on the dark web, or get access to your online accounts and scam others.”

How to protect yourself as AI fuels more sophisticated scams:

Don’t trust your caller ID. If you get a call from a business, hang up and find their number (for a bank, it will be on your statement, for example), then call them directly. No matter what the pitch, anyone asking you to pay them with a gift card is a scammer, according to the FTC.

Pause before you click. Never click on a link in an email or text message without confirming that it’s from a legitimate source. Criminals can now craft extremely sophisticated looking messages, as well as fake websites that convincingly mimic real ones.

Consider choosing a safe word for your family. Share it only with family members or others in your inner circle. If someone calls claiming to be a grandchild, for example, you can ask for the safe word or words — rubber ducky, Fred Flintstone, whatever — and if the caller doesn’t know it, it’s clearly a scam, Weisman says.

Call back your “grandchild” in crisis. If you don’t have a safe word and your supposed grandchild or child calls saying they’ve had a medical emergency or some other crisis (sometimes they say they’ve been kidnapped), they may add that their phone is broken so you can’t call them. Pause, take a breath (criminals try to rattle you to disrupt your rational thinking), and tell them you want to try to call them back anyway. Chances are your real grandchild will pick up, unharmed and bewildered by your concern.

Don't click on ads to download software. The FTC says that if you see an ad for software that piques your interest, rather than clicking on it, go to the website by typing in the address. If you search for it, the agency’s recent warning adds, “remember that scammers also place ads on search engines. They’ll appear at the top of your search results page and might have a label that says ‘Ad’ or ‘Sponsored.’ Scroll past those to get to your search results.”

Guard your personal information. To avoid identity theft, be careful with disclosing your full name, your home address, your Social Security number, credit card and banking information, and other personal details. Definitely don’t share them with someone you only know from email or texting.

Spread the word. Educate your loved ones on the latest scams and the advice noted above.

Report scams. If you spot or have been victim of a scam, report it to the police, as well as the Federal Trade Commission (FTC) at reportfraud.ftc.gov. The more information authorities have, the better they can identify patterns, link cases and ultimately catch the criminals.

You can also report scams to the AARP Fraud Watch Network Helpline, 877-908-3360. It's a free resource, with trained fraud specialists who can provide support and guidance on what to do next and how to avoid scams in the future.