UGEFCU
UTICA GAS & ELECTRIC FEDERAL CREDIT UNION

215 Old Campion Road
New Hartford, NY 13413
(315) 733-1596
www.ugefcu.com

For more identity theft prevention tips, call or stop by our office UGEFCU today. And if you ever become a victim of identity theft, remember that we're here to help. Call (315) 733-1596 or toll-free 800-990-7499 or visit www.ugefcu.com

NEWSLETTER ARTICLES:

NCUA Adv. #121 - August 2023

Chatbots and Voice-Cloning Fuel Rise in AI-Powered Scams

Cybercrime experts warn that new tech offers scammers frighteningly effective tools

AARP Bulletin: Alex Hamerstone, a cyber analyst at TrustedSec

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. 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. They have the potential to level up criminals' ability to impersonate anyone — your grandchild, a policeman.

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."

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. 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.

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. 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."

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 voice-mail, 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."

Smart tech

When we asked ChatGPT, "Can ChatGPT be used for scams?" it responded, "As an AI language model, I don't have any malicious intent and I am not capable of initiating any scams or fraudulent activities on my own. However, just like any other technology, there is always a risk that malicious individuals or groups could use me in ways that are not intended, such as using my responses to deceive people for their own gain."

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

continued inside page 2

continued from page 1 "Chatbots and Voice-Cloning"

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 'back-door,' 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 report-fraud.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.

Before You Wire Money

article from FTC (Federal Trade Commission)

Scammers pressure you to wire money to them because it's easy to take your money and disappear. Wiring money is like sending cash — once it's gone, you probably can't get it back. Never wire money to a stranger — no matter the reason they give.

Why Scammers Want You To Wire Money

If you need to send money to someone you know and trust, wiring money through companies like Western Union and MoneyGram can be a useful way to get money there quickly. But scammers also find wire transfers useful. Scammers know that:

- once you wire money to them, there's usually no way to get your money back
- they can pick up your money at any of the wire transfer company's locations
- it's nearly impossible to identify who picked up the money, or track them down

Never wire money to anyone:

- you haven't met in person
- who says they work at a government agency like the IRS, SSA, or a well-known company
- who pressures you into paying immediately
- who says a wire transfer is the only way you can pay

Also don't wire money to someone who tries to sell you something over the phone. Not only will you not have the same protections you would paying with a credit card, but it's illegal for a telemarketer to ask you to pay with a wire transfer, like those with MoneyGram and Western Union. Report them if they ask you to pay this way.

Spot the Scam

Here are some common ways scammers try to convince people to wire money:

Fake Check Scams

Someone sends you a check and tells you to deposit it. They tell you to wire some or all of the money back to them — or to another person. The money appears in your bank account, so you do it. But the check is fake. It can take weeks for the bank to figure it out, but when it does, the bank will want you to repay the money you withdrew.

Scammers make up lots of stories to try to convince you to deposit a check and wire money:

- Scammers say you've won a prize and need to wire money back to cover taxes and fees.
- Scammers say it's part of a mystery shopping assignment to evaluate a wire transfer service.
- Scammers overpay you for something you're selling online, then ask you to wire back the extra money.
- Scammers say you got a job you applied for, send you a check to buy supplies, but tell you to wire back part of the money.

continued "Before You Wire Money"

Romance Scams

Romance scammers create fake profiles on dating sites and apps. They strike up a relationship with you and work to build your trust, sometimes talking or chatting several times a day. Then, they make up a story — like saying they have an emergency — and ask for money. A romance scammer might also contact you through social media sites like Instagram, Facebook, or Google Hangouts.

Family Emergency Scams

You get an unexpected call from someone who pretends to be a friend or relative. They say they need cash for an emergency and beg you to wire money right away. They might say they need your help to get out of jail, pay a hospital bill, or leave a foreign country. They often ask you not to tell anyone in your family. Their goal is to trick you into sending money before you realize it's a scam.

Apartment Rental Scams

You respond to an ad for an apartment with surprisingly low rent. Before you've even seen the apartment, you apply and are told to wire money — maybe for an application fee, security deposit, or the first month's rent. After you wire the money, you find out that there is no apartment for rent, or that the scammer put their contact information on someone else's photo or rental ad. Scammers run a similar scam with vacation rentals.

What To Do If You Wired Money to a Scammer

• If you sent money using a wire transfer company like MoneyGram or Western Union, contact that company right away. Tell them it was a fraudulent transfer. Ask them to reverse the wire transfer and give you your money back.

MoneyGram at 1-800-926-9400
Western Union at 1-800-448-1492
Ria (non-Walmart transfers) at 1-877-443-1399
Ria (Walmart2Walmart and Walmart2World transfers) at 1-855-355-2144

• If you sent the wire transfer through your bank, contact them and report the fraudulent transfer. Ask if they can reverse the wire transfer and give you your money back.

Report Fraud

If a scammer asked you to wire money, report it to the FTC at ReportFraud.ftc.gov.

FRAUD!ORG
a project of the National Consumers League

Report scams to the National Fraud Information Center/ Internet Fraud Watch at fraud.org.
Sign up for email scam alerts and read more scam articles.

Is that really your friend messaging you online?

by Fraud.org staff

Social media has made it easier than ever to connect with people you know. This also means that scammers are only a few clicks away from causing serious harm. Consumers have submitted numerous reports to Fraud.org about scammers who have solicited money and personal information while impersonating someone else on a social media platform.

This impersonation typically happens in one of two ways. **1.** In an account takeover, the fraudster gains unauthorized access to someone's account. **2.** The other way is by setting up an imposter account where the fraudster creates a new account pretending to be someone else, often by using pictures that their target had publicly uploaded before.

In both cases, the scammer will use the hacked or impersonated account to distribute a web link or ask for personal information from accounts in their target's following/friends list. These messages often come with a plausible sounding ask. *For example*, imposter accounts may claim that they are trying to regain access to their original account and to help them do so, you must answer their questions or click on a link. It is also common for compromised accounts to share fraudulent money-making opportunities for things like fake cryptocurrencies or government programs.

If you think an imposter is contacting you, remember the following tips:

1. Do not open any links or comply with requests for information. Even if they provide reasonable justification for their requests, you could be putting your own account at risk by cooperating. It is best not to interact or respond to a suspicious account.

2. Do not send them money. It is unusual for people to ask for money over social media. If you are close enough with someone that they are asking for help, they should be able to get in touch with you by other methods.

3. Contact the person another way. If you think someone might be impersonating your friend on social media, send your friend a text message and see if it is really them. If you suspect that their phone may be stolen (or that they are a victim of SIM-swapping), ask a mutual friend if they have noticed unusual behavior as well.

4. Report the account. Most social media platforms allow users to report accounts for suspected impersonation, fraud, or both. The sooner the platform becomes aware of the problem, the quicker they can take action.

5. Pay attention to warnings from the platform. Major digital platforms that allow messaging between users will automatically filter out suspicious communications. Think twice before opening messages flagged as spam.

If you or someone you know has been a fraud victim, help yourself and other by reporting it! By using Fraud.org's secure online complaint form, your complaint will be shared with our network of consumer protection and law enforcement agency partners.