AUG 2025

The Springs Valley SCOOP

Defend Yourself Against AI Voice Scams

Source: FTC.gov

Phishing scams are nothing new, but technology is constantly evolving, and so are the tactics scammers use. One of the newest and most alarming threats is AI voice scams, which leverage sophisticated artificial intelligence to impersonate the voices of loved ones or trusted figures.

Imagine receiving a frantic call from your child or grandchild, claiming they've been arrested or injured while traveling in a foreign country and desperately need money for bail or medical care.

Understandably panicked at such terrifying news, you rush to send the requested funds through a wire transfer or gift card, only to discover later that your child is safe and sound, and your money is gone.

This scenario, unfortunately, is becoming increasingly common. Scammers can target anyone, but family scams are particularly effective because they prey on our emotions and concern for loved ones.

Let's explore AI voice cloning technology, how it's used in scams, and most importantly, how you can protect yourself and your loved ones from falling victim.

WHAT IS AI VOICE CLONING?

Artificial Intelligence (AI) has revolutionized many aspects of our lives, but it also comes with its own set of risks. AI voice cloning technology is a prime example. This technology can mimic a person's voice with remarkable accuracy, using just a few seconds of recorded audio. Scammers obtain these recordings from social media videos, voicemail messages, or any other publicly available sources.

HOW DOES AI VOICE CLONING WORK?

Imagine a world where a machine can learn to mimic your voice perfectly, down to the subtle inflections and nuances that make it uniquely yours. That's the power behind AI voice cloning.

Scammers can use short audio clips – culled from social media posts, voicemails, or even robocalls – and feed them into an AI program. The program then analyzes the audio, learning the speaker's voice patterns and mannerisms. This allows the AI to synthesize speech that sounds eerily similar to the original speaker.

(continued on page 2)

(continued from page 1)

HOW SCAMMERS OBTAIN VOICE RECORDINGS

Scammers are resourceful when it comes to gathering voice samples. They might use social engineering tactics to trick individuals into recording their voice or simply scrape voice samples from online platforms. They may also use recordings from robocalls you've answered, so it's wise not to engage with spammy phone calls.

Once they have enough data, they feed it into an AI model that can replicate the voice and generate new audio clips that say anything the scammer wants.

HOW AI VOICE SCAMS WORK

Scammers use AI voice cloning to create convincing audio messages. They can impersonate friends, family members, or even official representatives from institutions like banks. The cloned voice can then be used in various scenarios to deceive victims into taking actions that benefit the scammer.

EXAMPLE OF AN AI VOICE SCAM

Imagine receiving a call that sounds like your sibling's voice, claiming they are in urgent need of money due to an emergency. The voice sounds familiar, and under pressure, you comply with their request. Later, you realize it was a scam, and the funds you transferred are gone. This is a typical example of how AI voice scams can unfold.

TYPES OF AI VOICE SCAMS AFFECTING CONSUMERS

AI voice scams are a rapidly emerging threat that targets a diverse range of victims. These scams leverage sophisticated AI technology to clone voices and create compelling, fraudulent communications that are difficult to distinguish from genuine ones. Understanding the various forms these scams can take and the techniques they employ is crucial for safeguarding oneself against potential losses.

EMERGENCY FAMILY SCAMS

The emergency family scams are aimed specifically at disabling their target with attacks at their most vulnerable side: their emotions. There's nothing more personal to people than their families, so a lot of family-related events are reacted to more quickly, with fewer questions, as long as there's the right threat to scam them with.

- **Exploiting Emotional Vulnerabilities:** Scammers will target emotions like love, concern, and panic to cloud your judgment. They might claim a loved one is in trouble, injured, or arrested, and needs immediate financial assistance to avoid a dire situation.
- **Highly Personalized Touch:** AI can use snippets of information gleaned from social media or online sources to personalize the scam. They might use real names, locations, or even reference recent events to make the scenario seem more believable.
- **Pressure to Act Quickly:** Scammers will often create a sense of urgency, urging you to send money immediately without verifying the situation. They might claim there's no time to contact other family members or explain details over email.

POLITICALLY MOTIVATED SCAMS

This particular type of scam is not necessarily an attempt to trick you out of money but is meant to either promote a political cause or discredit someone else's. Scammers take recordings of well-known political figures and use AI to manipulate their voices to say whatever they want to promote their personal agenda. Here are a few examples:

- **Campaign support:** Scammers may call during an election season to deliver messages, solicit support, or provide information. For example, the supposed caller may appear to endorse a particular candidate or cause.
- **Attack ads:** An AI clone of a recognizable voice, like the president or other well-known political figure, may target opponents with negative or misleading information disguised as a trusted source.
- **Manipulating public opinion:** Scammers may try to spread disinformation or propaganda using a familiar voice.

RED FLAGS: HOW TO SPOT AN AI VOICE SCAM

The key to staying safe from AI voice scams is awareness and just a dash of skepticism. Here are some red flags that should make you pause and say, "Wait a minute":

- **Urgency:** Scammers will often try to create a sense of urgency to cloud your judgment. Be cautious if you're asked to act immediately without time to think. Don't be pressured into making a quick decision, especially involving money.
- **Untraceable Payment Methods:** Requests for wire transfers, gift cards, or cryptocurrency should raise alarm bells. These methods are preferred by scammers due to their untraceable nature. Legitimate

(continued on page 3)

(continued from page 2)

businesses will not request payment via wire transfer, gift cards, or cryptocurrency. These methods are virtually untraceable, and once the money is sent, it's nearly impossible to retrieve.

- **Unknown Numbers:** Be wary of calls from unknown numbers. Scammers can use technology to "spoof" phone numbers, hiding their source. These numbers can be cloned or masked, providing scammers with anonymity.
- **Staying Calm is Key:** In the heat of the moment, it's easy to panic. However, staying calm and composed is crucial. Pause to assess the situation logically before taking any action.

  If you receive a suspicious call, take a deep breath and try to stay calm. Don't give out any personal information, and politely tell the caller you'll get back to them.

TIPS FOR PROTECTING YOURSELF FROM AI VOICE SCAMS

While AI voice scams can sound sophisticated and intimidating, the good news is there are concrete steps you can take to protect yourself. Here are some essential tips to keep you safe:

- **Don't Answer Calls from Unknown Numbers:** One of the simplest ways to protect yourself is to avoid answering calls from unknown numbers. Allow these calls to go to voicemail, and then decide if they require a response.
- **Verify Information:** If you receive a suspicious call, verify any information they give you. Call the person back at a known number or contact a mutual acquaintance to confirm the story.

  If it's a political call, do your homework to be certain the information they give you is true and accurate. If they're asking for a donation to a cause, you'll want to ensure that any entity you deal with is reputable and has a verifiable presence. Make any donations online through a trusted website rather than over the phone.
- **Don't Overshare on Social Media:** One of the ways scammers collect voice samples for AI cloning is through social media. Even a short video of you or a family member could be enough to create a compelling copy of their voice. Limit what you share online, and make sure that your posts are only visible to friends and family.
- **Keep Personal Information Private:** Avoid sharing personal information unless you are absolutely certain about the identity of the caller.
- **Simple but Effective: The Power of a Family Codeword:** Here's a low-tech yet surprisingly effective way to protect yourself and your family: create a secret codeword.

  This could be a random phrase or inside joke that only your family would know. If someone claiming to be a loved one calls and asks for money, simply ask for the codeword. AI can mimic a voice, but it can't guess a secret password.

REPORTING SCAMS AND LEARNING MORE

If you encounter a scam, report it to relevant authorities immediately. Various resources are available to help you learn more about consumer protection and how to avoid falling victim to scams.

- The Consumer Finance Protection Bureau offers a number of great resources for learning about scams and how to stay safe.
- Visit the Federal Trade Commission to report fraud or scams and find out next steps.

(continued on page 4

(continued from page 3)

THE FIGHT AGAINST SCAMS: AI FOR GOOD

While AI can be used for malicious purposes, the good news is that the same technology can also be harnessed to fight scams. Just as scammers use AI to deceive, many sectors are beginning to leverage AI to combat fraud. Security and protection agencies are developing AI-powered systems that can detect suspicious activity and flag potential scams before they occur. Advanced algorithms can detect suspicious patterns and alert authorities to promptly. These technologies are continually improving, making it harder for scammers to succeed.

FRAUD DETECTION SYSTEMS: YOUR AI GUARDIAN AGAINST SHADY TRANSACTIONS

Imagine having a 24/7 financial watchdog that monitors your accounts for suspicious activity. That's essentially what AI-powered fraud detection systems can do for financial institutions. Many financial institutions use AI-driven systems to detect fraudulent transactions in real-time. These systems analyze vast amounts of transaction data, looking for patterns and anomalies that might indicate fraudulent activity.

- **Here's how it works:** The system considers various factors, including the location of the transaction, the amount being spent, and your typical spending habits. If the system detects something unusual, such as a large purchase from a foreign country you've never visited, it can flag the transaction for review. This allows the financial institution to contact you and verify the legitimacy of the transaction before any funds are lost.

AI USE IN OTHER SECTORS

As AI technology continues to evolve, we can expect even more sophisticated tools and techniques to emerge in the fight against crime. Here are some other ways AI is already being used:

- Detecting phishing sites and emails.
- Identifying and blocking scam calls.
- Combating social media scams.

STAY VIGILANT, STAY SAFE

AI voice scams represent a new frontier in the world of fraud. By staying vigilant and informed, you can protect yourself from these sophisticated schemes. Be aware of the tactics scammers use and take steps to protect yourself to significantly reduce your risk of falling victim to a scam.

Remember the key points – avoid unknown numbers, verify information, and use a family codeword. Share this information with friends and family to help them stay safe. Awareness and preparedness are your best defenses against AI voice scams.

For additional resources and information on reporting scams, visit the website of the Federal Trade Commission (FTC) at

https://www.ftc.gov/

Welcome!

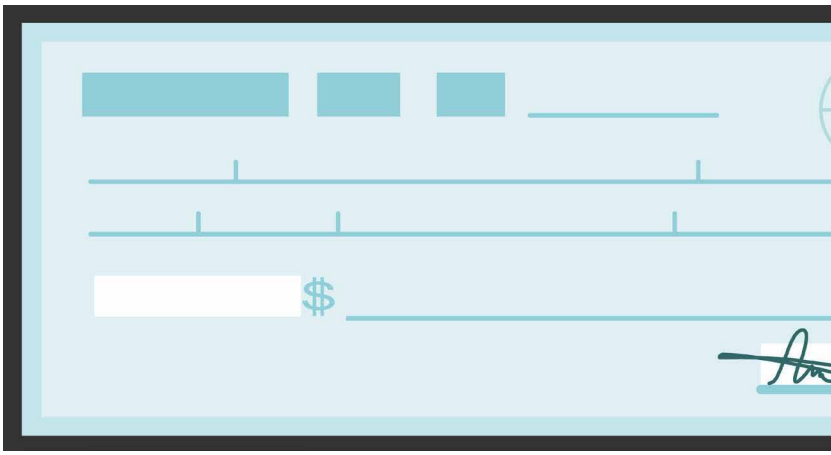
#TeamSVBT at the 2025 Jasper Strassenfest!

UNITED STATES POSTAL INSPECTION SERVICE

www.uspis.gov

HOW TO PREVENT
CHECK FRAUD

The United States Postal Inspection Service is the federal law enforcement branch of the United States Postal Service®. Postal inspectors are federal agents charged with enforcing over 200 federal statutes that protect the Postal Service, its employees, and the U.S. Mail™ from illegal or dangerous use.



18 U.S. CODE § 1344 BANK FRAUD: Shall be fined not more than $1,000,000 or imprisoned not more than 30 years.

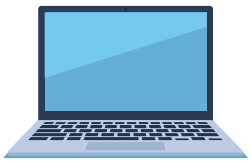
PROTECT YOUR MAIL
FROM MAIL THEFT AND CHECK FRAUD:

Get your mail promptly after delivery. Don't leave it in your mailbox overnight.

Contact the sender if you don't receive mail that you're expecting.

If you're heading out of town, ask the post office to hold your mail until you return.

Consider buying security envelopes to conceal the contents of your mail.



Sign up for informed delivery at USPS.com. It sends you daily email notifications of incoming mail and packages.

Use the letter slots inside your Post Office to send mail.

ICBA

UNITED STATES POSTAL INSPECTION SERVICE

www.uspis.gov

HOW TO PROTECT YOUR CHECKS

Use pens with indelible black ink so it is more difficult for a criminal to wash your checks.

Don't leave blank spaces in the payee or amount lines.

Don't write personal details, such as your Social Security number, credit card information, driver's license number or phone number on checks.

Use mobile or online banking to access copies of your checks and ensure they are not altered. While logged in, review your bank activity and statements for errors.

If your bank provides an image of a paid check, review the back of the check to ensure the endorsement information is correct and matches the intended payee, since criminals will sometimes deposit your check unaltered.

Consider using e-check, ACH automatic payments and other electronic and/or mobile payments.

Follow up with payees to make sure that they received your check.

WHAT TO DO IF YOU'RE A VICTIM?

- Contact your local community bank and request copies of all fraudulent checks. Your community bank is your ally in helping you avoid or recover from check fraud.

- If mailed, provide details (How, When, Where). These details matter to help ***us*** determine the point of compromise in the mail stream.

- Provide law enforcement with copies of checks and details about Bank of First Deposit (BOFD) for all stolen/altered and counterfeit checks.

www.uspis.gov | 1-877-876-2455

ICBA

Scan this QR code to Open an Account Online Today![3]

***Or**, open your account online at **svbt.bank**!*

ADVENTURE AWAITS

LET SPRINGS VALLEY GUIDE THE WAY

LEKI CROSS TRAIL 3 CARBON TREKKING POLES - PAIR

VALUED AT $139.73

Open any Springs Valley **eZChecking**[2] account by Saturday,

September 27, 2025,

and be entered into a drawing for a pair of

LEKI Cross Trail 3 Carbon Trekking Poles![1]

Isaac Briggeman
IT Intern

Jordan Briggeman
Vice President & Business Banker

Loyal to you, your family, and your future.

springsvalley
BANK & TRUST COMPANY

svbt.bank | **800.843.4947** | *Since 1902*

Member FDIC | EQUAL HOUSING LENDER

[1]No purchase necessary to win (need not be present to win). Entrants of drawings must be 18 years of age or older. Limit one entry per person per drawing. Entries accepted starting Monday, June 30, 2025, at 8:30 a.m. (EST) and will end on Saturday, September 27, 2025 ("Giveaway Period"), at 1:00 p.m. (EST). The Sponsor's clock will be the official timekeeper for the Giveaway. Drawing will be held on Wednesday, October 1, 2025. One (1) set of LEKI Cross Trail 3 Carbon Trekking Poles will be awarded at each Banking Center. The verifiable retail value of the prize is $139.73. No substitution or transfer of prize permitted. Official Terms & Conditions available upon request or by visiting svbt.bank/checking. Ask us for details. Bank rules and regulations may apply. To request a mail-in entry form, eMail marketing@svbt.bank or call 800.843.4947. LEKI is not a sponsor of, nor affiliated with this Giveaway. [2]Minimum opening deposit of $50.00 required. Some fees and conditions may apply. [3]Third party fees for internet, messaging, or data plans may apply.