OUCH! September 2024

Phantom Voices: Defend Against Voice Cloning Attacks

The Unexpected Call: A Story of Deception

Margaret, a retired teacher, enjoyed her peaceful mornings in her small suburban home. One day as she was enjoying her morning coffee, she received a frantic call from her grandson, Jacob, who was away at college. His voice was filled with panic as he explained that he had been in a car accident and needed money urgently to pay for the damages and avoid legal trouble. If he did not get the money right away, he could end up in jail. The voice on the other end was unmistakably Jacob's - Margaret's heart raced with worry. Without questioning, she rushed to her bank and wired money to the account Jacob provided. It wasn't until Margaret called Jacob's mother later that day to learn how Jacob was doing that Margaret learned she had been scammed. The call had been a cruel trick, a cyber-criminal had used Artificial Intelligence (AI) voice cloning technology to mimic Jacob's voice, exploiting Margaret's love and concern for her grandson.

What is Voice Cloning?

Voice cloning is when someone uses AI to recreate a person's voice to include their voice patterns, intonations, and speech rhythms, creating a near-perfect replica.

A voice cloning attack begins with a cyber-criminal collecting audio samples of the target's voice. These samples can be harvested from various sources such as videos on YouTube or personal posts on TikTok. After training on the recorded audio, AI generates new audio that sounds like the target. This generated voice can be used in various ways, from phone calls to voice messages, making it a potent tool for deception.

When creating voice cloning attacks, cyber-attackers often do their research first. Most of the information they need is publicly available on social media sites. They study their intended victims, to include both the person's voice who they are going to replicate but also the victim they are going to call. Cyber criminals not only learn who their victims know and trust, but which emotional triggers are the most effective. When making these phone calls, cyber-attackers often modify their Caller ID, so when the victims look at their phones, the phone call appears to come from a number the victim trusts. Caller ID can be easily spoofed and is not a good way to validate or authenticate people who call you.

Protect Yourself

The first step to protecting yourself is just being aware that voice cloning is now possible and becoming easier for cyber-attackers to do. Some steps you can take to protect yourself include:

- **Privacy**: Be aware of and limit the information you share with others, and restrict who can access recordings of you on social media.
- **Clues**: Be on the lookout for common indicators that something is wrong. Whenever someone calls you with a tremendous sense of urgency or is pressuring you to act right away, it is most likely a scam. The greater the sense of urgency, such as demanding money right away, the more likely someone is trying to rush you into making a mistake. Other common indicators include something that is too good to be true (no you did not win the lottery) or when you get an unexpected call that seems just odd.
- **Verify**: If you are not sure if a phone call is legitimate, hang up and call the individual back on a trusted phone number. For example, if you get a phone call from a senior executive or co-worker in your company, call them back on a trusted phone number that you know is truly theirs. If you get an odd phone call from a family member, try calling them back (perhaps even use video call) or call another family member that knows them well.
- **Passcode**: Create a secret passphrase or passcode that only you and your family know. That way if you get an odd phone call that seems to be from a family member, you can validate if it's them by seeing if they know your secret passcode.

Guest Editor

Maria Singh is a Cyber Content Manager at EnterpriseKC and a passionate WiCyS member with over 14 years of technology and cybersecurity experience. She holds a SANS GIAC GSEC certification and is a Master of Science in Cybersecurity candidate at Purdue University. As past President of Women in Security Kansas City and OCA Corporate Achievement award recipient, Maria inspires women in STEM and cybersecurity. Her speaking engagements and leadership pave the way for future generations to thrive in these fields.

Resources

Top Three Ways Cyber Attackers Target You: https://www.sans.org/newsletters/ouch/top-ways-attackers-target-you/
Stop Phone Calls Scams: https://www.sans.org/newsletters/ouch/stop-phone-call-scams/
Emotional Triggers – How Cyber Attacks Trick You: https://www.sans.org/newsletters/ouch/emotional-triggers-how-cyber-attackers-trick-you/