VOICE CLONING AND VISHING

Katherine Rackliffe



DEFCON 2025

VOICE CLONING

VOICE CLONING (EXAMPLE)



Schwab voice ID Service

Access your account with your voice.

Schwab's voice ID service allows you to access your account just by speaking one simple phrase, "At Schwab, my voice is my password."

* Schwab's voice ID service is not available on all contact numbers.

Schwab voice ID Service

Access your account with your voice.

Schwab's voice ID service allows you to access your account just by speaking one simple phrase, "At Schwab, my voice is my password."

* Schwab's voice ID service is not available on all contact numbers.

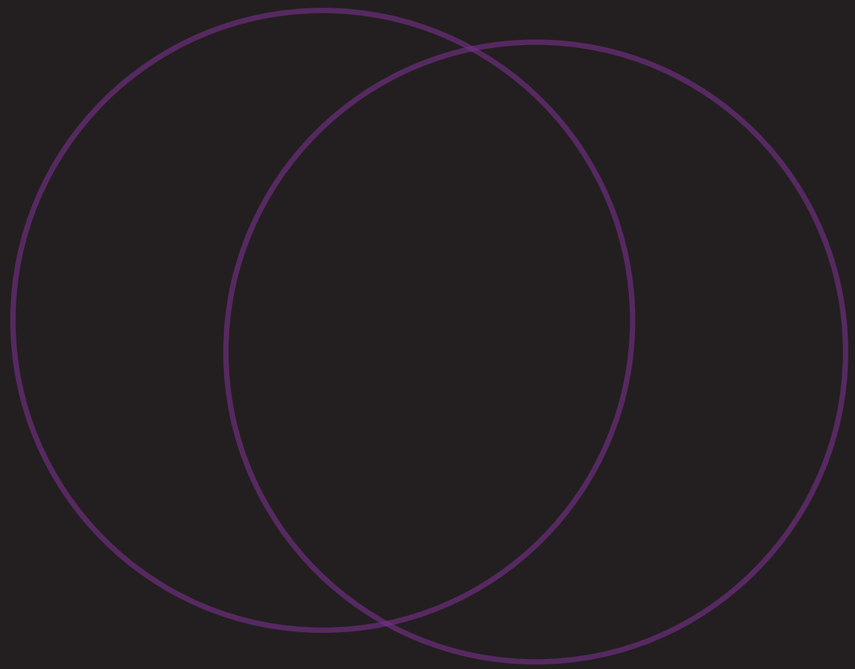
Phishing: A social engineering attack where an attacker manipulates others for financial gain or to install malware

Vhishing: Phone call phishing attacks that use the human voice, often for financial gain

Cloned vishing: Phone call phishing attacks that use an AI cloned voice

COMMON CYBER ATTACKS WITH VOICE CLONING

- Family members calling for help
- Authority figures
- Fooling voice recognition verification, for banks



REAL-WORLD EXAMPLES

Bank fraud

- https://www.forbes.com/sites/thomasbrewster/2021/10/14/huge-bank-fraud-uses-deep-fake-voice-tech-to-steal-millions/



forbes.com

Fraudsters Cloned Company Director's Voice In $35 Million Heist, Police Find

Thomas Brewster

5–6 minutes

Scams

- https://www.cnn.com/2023/04/29/us/ai-scam-calls-kidnapping-cec/index.html



'Mom, these bad men have me': She believes scammers cloned her daughter's voice in a fake kidnapping

By Faith Karimi, CNN

8 minute read · Updated 9:26 AM EDT, Sat April 29, 2023

WHY STUDY THIS?



- How effective are these voice clones in a scam?
- Are people prepared to spot these types of scams?
- How do we convince others that this is a real risk?

HOW DO WE STUDY THIS?



- Cybersecurity is hard to study
- Set up an fake vishing study! Then see how many people fall for it.
- ...The ethics paperwork for this was a nightmare

- Step one: Lit review

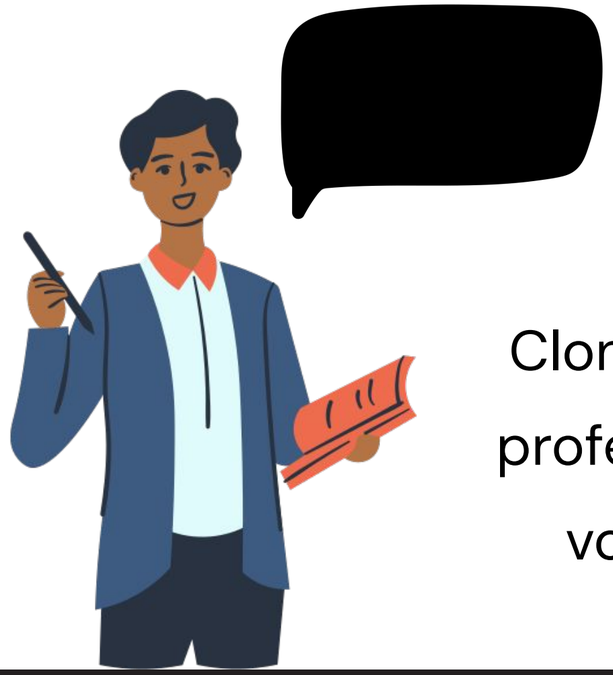
- Step two: Ethics paperwork

- Step three: Recruitment

- Step four: Run the study

- Step five: Data analysis

- Step six: Write thesis



Clone the professors voice



Create a malicious message

The message:

Hello,

This is Professor [Professor's Name] in [class name]. I hope you're doing well. I'm currently updating the class registration records and I need your student ID number to fix an error with your registration. Could you please text me your BYU student ID number? You can find your 9-digit student ID number on your BYU ID card.

Thanks!

Professor [Professor's



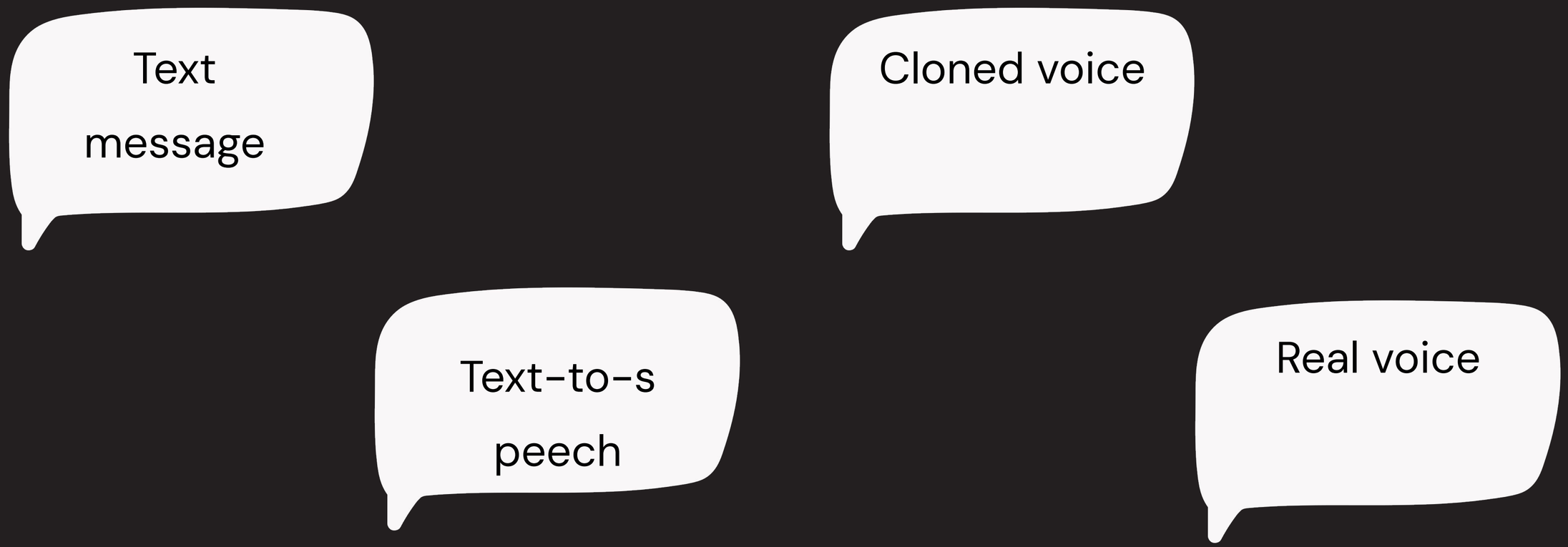
Send the message to students





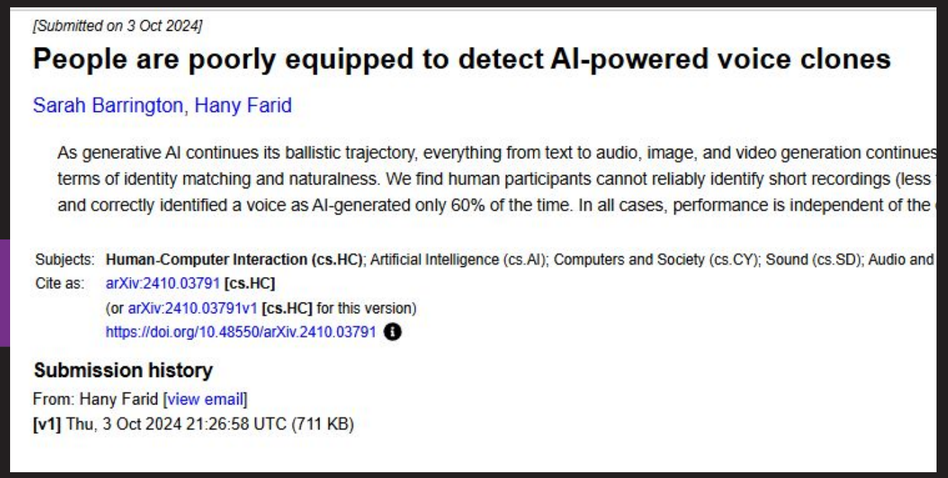
Analyze results

Four types of phishing message



PRELIMINARY FINDINGS

- People are not equipped to tell the difference between a cloned or real voice: http://arxiv.org/abs/2410.03791



[Submitted on 3 Oct 2024]

People are poorly equipped to detect AI-powered voice clones

Sarah Barrington, Hany Farid

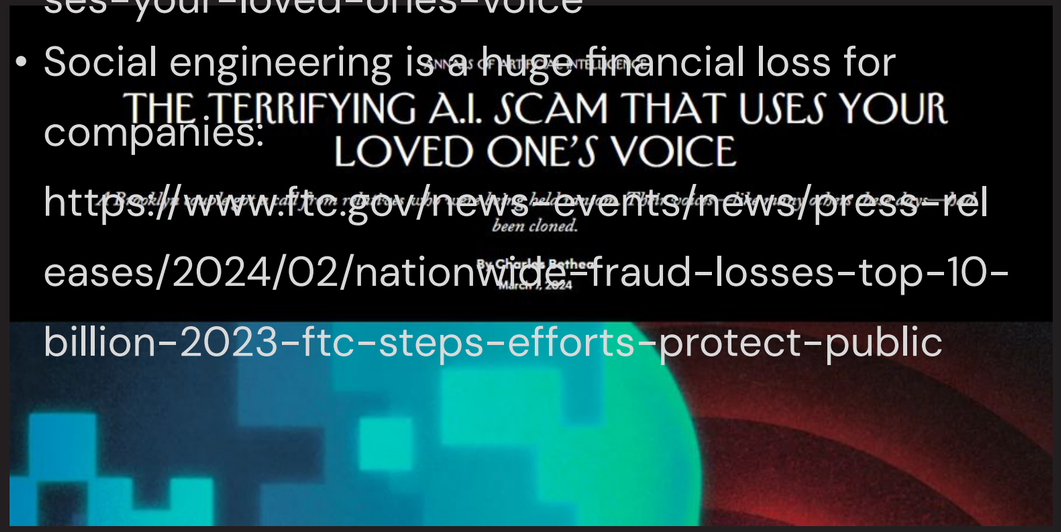
As generative AI continues its ballistic trajectory, everything from text to audio, image, and video generation continues terms of identity matching and naturalness. We find human participants cannot reliably identify short recordings (less and correctly identified a voice as AI-generated only 60% of the time. In all cases, performance is independent of the

Subjects: **Human-Computer Interaction (cs.HC)**; Artificial Intelligence (cs.AI); Computers and Society (cs.CY); Sound (cs.SD); Audio and
Cite as: arXiv:2410.03791 **[cs.HC]**
(or arXiv:2410.03791v1 **[cs.HC]** for this version)
https://doi.org/10.48550/arXiv.2410.03791

Submission history

From: Hany Farid [view email]
[v1] Thu, 3 Oct 2024 21:26:58 UTC (711 KB)

- There's not that much research on this type of attack, but a lot of news articles: https://www.newyorker.com/science/annals-of-artificial-intelligence/the-terrifying-ai-scam-that-uses-your-loved-ones-voice
- Social engineering is a huge financial loss for companies: https://www.ftc.gov/news-events/news/press-releases/2024/02/nationwide-fraud-losses-top-10-billion-2023-ftc-steps-efforts-protect-public



ANNALS OF ARTIFICIAL INTELLIGENCE

THE TERRIFYING A.I. SCAM THAT USES YOUR LOVED ONE'S VOICE

been cloned.

By Charles Bethea
March 7, 2024

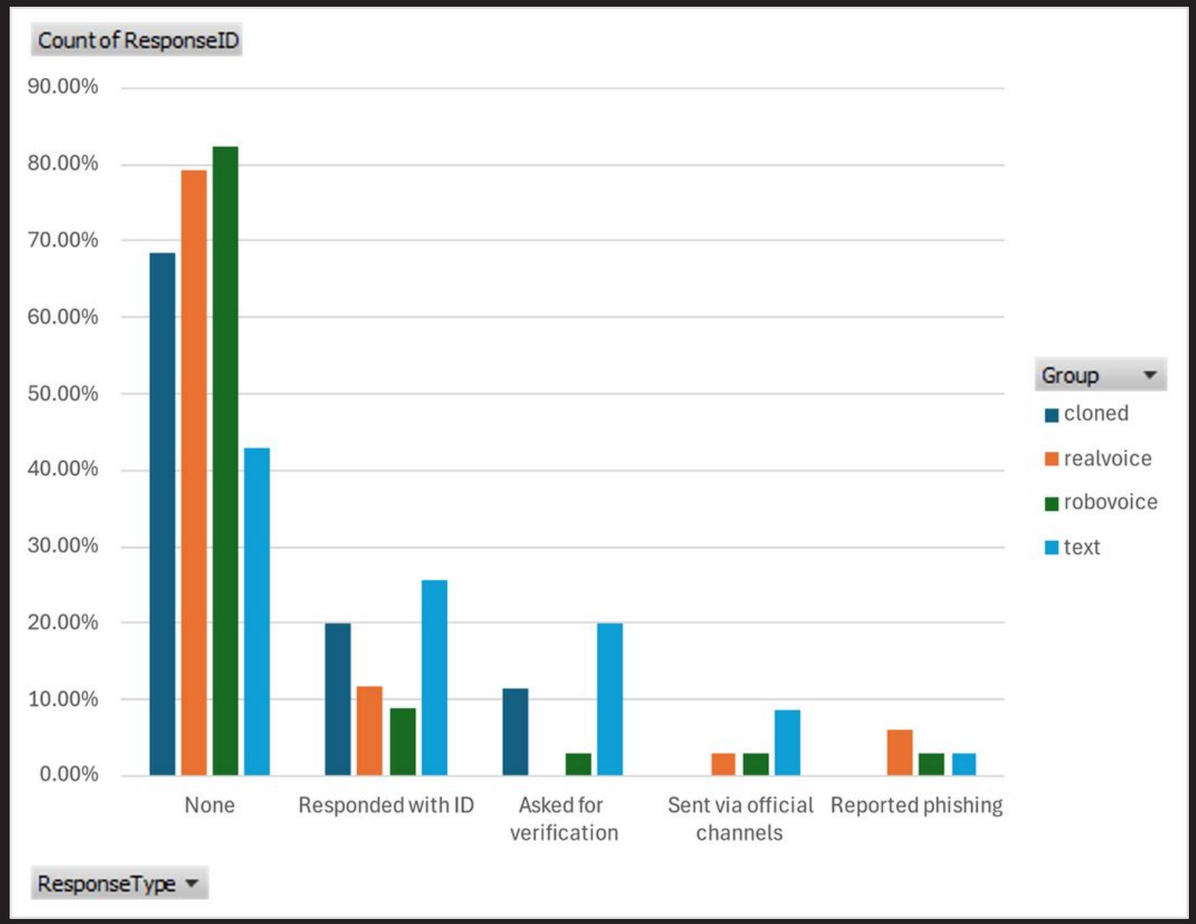


For Release

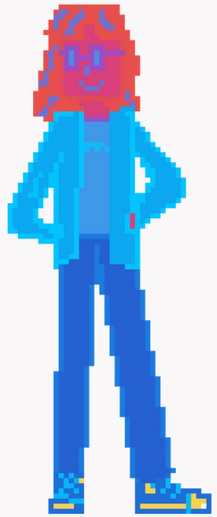
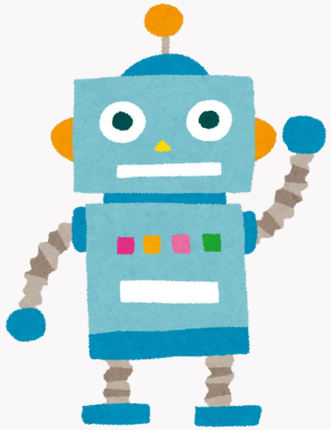
As Nationwide Fraud Losses Top $10 Billion in 2023, FTC Steps Up Efforts to Protect the Public

TYPES OF RESPONSES

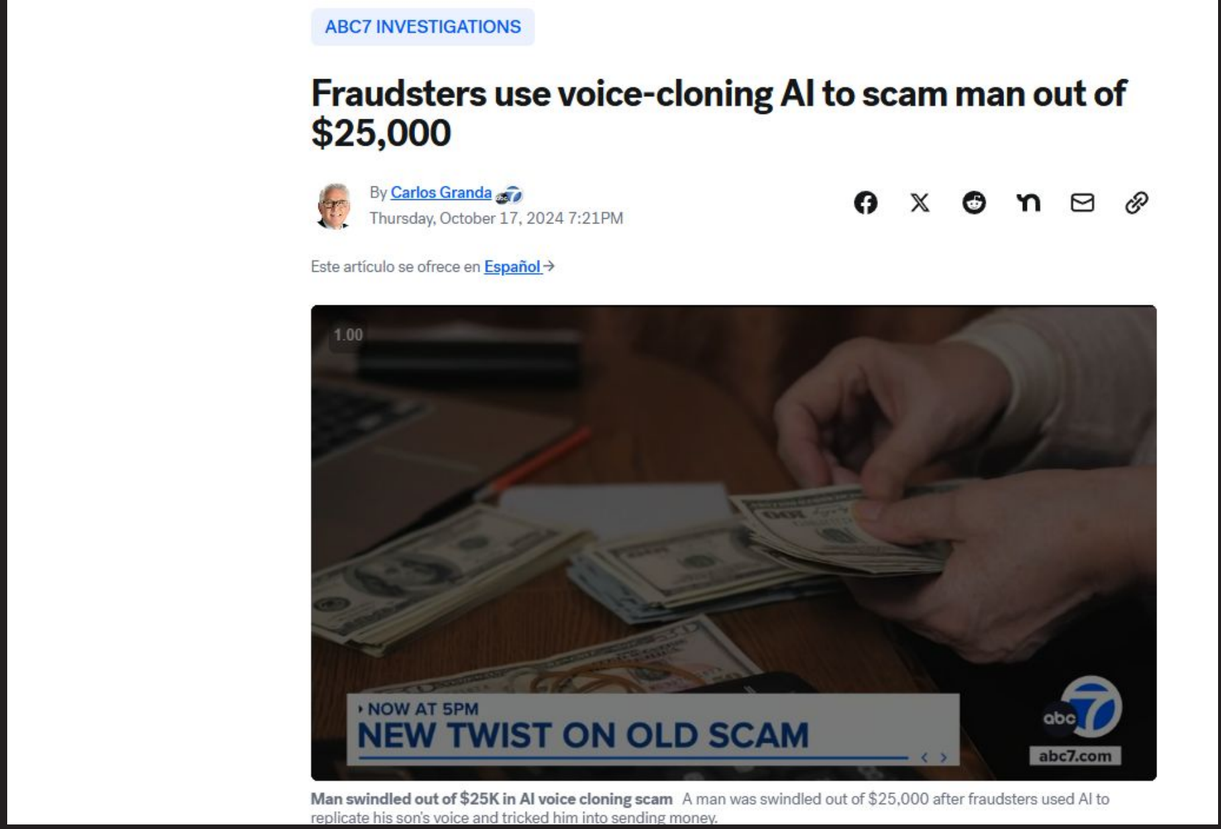
- No response (typical with phishing)
- Responded with student ID
- Asked for verification
- Sent through other means (such as email)
- Report phish/scam



WHO WINS?

Real voice recording	Voice clone	Text to speech	Text message
			
• Same response rate when compared to voice clone	• Identical results to real voice • People can't tell the difference, particularly over the phone	• Low response rate • Still some responses!	• Higher response rate • Higher reporting rate

WHAT CAN WE DO NOW?



The usual cyber answers...

- Two-factor authentication
- Identity verification
- Awareness

My Website:
https://katherineracklIffe.org/

THANK YOU

Linkdn:linkedin.com/in/katherineracklIffe/

Summary:

- What voice cloning is
- How it is used in cybersecurity vishing attacks
- The structure for a study to determine how effective it is
- References, resources, and other academic articles studying voice cloning

