RICHTER GUARDIAN

RGSA 01-19-24-01
Date: January 19, 2024

Unveiling the Dark Side of Voice-Cloning Artificial Intelligence

INTRODUCTION

Voice-cloning AI, which is the technology that enables the replication of a person's voice, can assist researchers with collecting and analyzing data from different languages, dialects, and accents. Voice-cloning AI is versatile and finds applications in various creative domains.

However, the revolutionary technology also poses significant risks, as cybercriminals can take advantage of families and small businesses with voice-cloning AI. Deep learning models can now replicate the nuances, inflections, and specific characteristics of a person's voice with just a few minutes of sample media.

IMPLICATIONS FOR FAMILIES AND SMALL BUSINESSES

While there are positive and creative uses for voice-cloning AI, it is important to be aware of the potential risks and misuse. Here are some ways in which voice-cloning AI could lead to cybercriminal activity:

1. **Impersonation and Social Engineering:** Cybercriminals could use voice-cloning AI to mimic the voices of individuals in positions of authority, such as company executives. In doing so, cybercriminals could instruct employees into making unauthorized transactions.
2. **Phishing Attacks:** Voice-cloning could be used to voice-phish; individuals can be deceived into sharing sensitive information over a call.
3. **Extortion and Blackmail:** Cybercriminals may leverage voice-cloning to create audio deepfakes of the targeted individual for the purpose of extortion or blackmail.

RECOMMENDATIONS

Given the sophistication of these threats, Richter recommends individuals and businesses to safeguard themselves by employing the following:

- **Multi-factor authentication (MFA)** – If you currently use voice verification as a type of authentication, ensure to include another form of verification to help safeguard against voice-cloning AI.
- **Establish protocol within your small-business** – Set clear protocols for financial transactions and sensitive data sharing. Keep these protocols confidential.
- **Remain skeptical** – Individuals should exercise caution when receiving unexpected calls, especially if the caller requests sensitive information.

CONTACT US

Have a quick question? Send us an email.
Email: support@richterguardian.com

Phone number: +1 844.908.3950
Monday to Friday 9 a.m. to 5 p.m. (Eastern Time)

Need assistance upgrading your device?
Schedule a session with us by clicking here or by using this link:
https://calendly.com/richter-guardian/upgrade-assistance