AI Vishing

Phone phishing by voice, or “vishing,” takes on a new dimension when scammers use artificial intelligence to create familiar voices.

Unlike conventional vishing scams where humans make the calls, AI vishing employs advanced technology to deceive victims.

With just a sample of a person’s voice from a social post scammers can artificially replicate the speech patterns, tone, and inflections of people you trust.

Equipped with tech that allows them to carry on human-like conversations, these AI imposters can be highly effective scam artists.

Avoid becoming a victim

First, pay attention to the tone and inflection. Despite their general accuracy, AI-generated voices can still lack the natural variations in pitch and emotion.

Listen for unnatural pauses and language that sounds scripted. If the conversation feels off, the voice may not be genuine.

If you suspect AI vishing, verify the caller’s identity. Ask questions only the legitimate caller can answer.

AI vishing scams often use pressure tactics to make you act quickly without thinking. Be wary of calls that are urgent in nature.

Assess before responding, even if the caller sounds convincing. If something feels off, trust your instincts.

Never share personal or sensitive information over the phone unless you’re certain of the caller’s identity.

Using caller ID and call blocking technologies can also help, as these tools provide extra layers of protection against AI-generated calls.

Report suspicious calls to your IT or security team to help protect others.

Barracuda