Why Should I Partake
In Simulated Voice Phishing Training?

What Is Voice Phishing?

Voice phishing, or vishing, is a type of scam where someone calls and tries to trick you into sharing sensitive information. These calls often sound urgent, seem legitimate, and may appear to come from someone you trust.

How Training Helps

Simulated voice phishing gives you a safe way to experience these tactics firsthand. You'll receive a realistic call from an AI voice that uses common techniques seen in real attacks. The goal is to help you recognize warning signs and respond with confidence.

Your voice is never recorded. Nothing you say is stored or transcribed.

If you interact with the call in a way that suggests you might be at risk, you may be assigned a short follow-up training. This helps reinforce what to look out for in the future.

The Technology Behind It

Simulated voice phishing uses generative AI to create lifelike phone calls that sound natural and unscripted. The AI can hold a conversation, respond in real time, and use common social engineering tactics to apply pressure or build trust.

As this technology continues to advance, it's making voice phishing more convincing and much harder to spot. What used to sound robotic or obviously fake can now pass for a real person. Attackers can generate and launch these scams at scale, turning what was once a low-effort trick into a widespread and serious threat.

What You Need To Do To Take Part

Before you can receive any simulated calls, you'll need to give permission through a quick two-step process.

1. **First, you'll get an email asking you to provide consent**. Once you agree, you'll be taken to a verification page.
2. **Next, you'll receive a text message with a six-digit code.** Enter that code on the page to confirm your phone number.

Both steps must be completed before any simulations can begin.

How to Opt-Out

You can opt out at any time using one of the following methods:

- Reply to the SMS with STOP or UNSUBSCRIBE
- Say "stop calling me" during a simulation, then say "yes" to confirm
- Ask your IT or Security team to remove you

caniphish