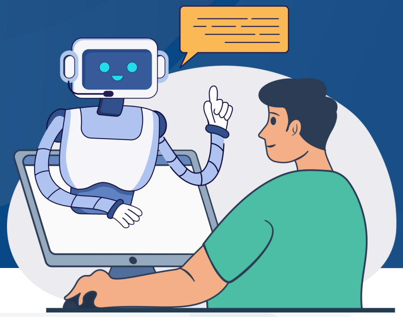
Using Voice Phishing

To Train Your Employees



What Is Simulated Voice Phishing

Simulated voice phishing is a training technique that uses AI to engage employees in realistic phone calls that mimic real-world social engineering attacks. These calls are designed to test and improve employee response to voice-based phishing in a controlled, safe environment.

Why It Matters

Phone-based phishing attacks are on the rise and often target employees directly on their mobile devices. Unlike emails, voice phishing can create pressure in real time, making it harder to spot deception. Simulated training helps staff build confidence and awareness before a real attack occurs.

Key Benefits Of Voice Phishing

Realistic threat exposure

Employees experience the tactics used in real voice phishing attacks. These simulations recreate pressure and urgency, helping staff build instinctive responses before facing an actual scam. It’s a direct investment in reducing human risk where it matters most.

Broader training coverage

Voice phishing fills a gap that email simulations don’t cover. It trains staff to handle threats over the phone, reflecting how real attacks now span multiple channels. This helps strengthen your defence across the full spectrum of social engineering techniques.

Automatic follow-up training

When someone falls for a simulated call, targeted training can be automatically assigned. This ensures the right people get the right support at the right time, without extra admin effort. It’s efficient, responsive, and focused on actual risk.

Actionable insights

Outcomes from each call feed into your CanIPhish dashboard. You’ll see who picked up, who engaged, and what happened next. These insights help you track risk, measure progress, and make data-driven decisions about where to focus.

Personalized scenarios

Every call is generated in real time by AI, creating a unique experience for each user. This makes training more engaging and forces employees to think critically. There are no patterns to memorize, just real decisions in real situations.

No call recordings

Nothing from the call is recorded or transcribed. Only the outcome and essential metadata are logged. This protects employee privacy while still giving you visibility into what occurred, helping maintain trust and compliance.

Executive Considerations

- **Organizational sign-off:** Activation requires a signed agreement authorizing CanIPhish to conduct simulations on your behalf.
- **Transparency and control:** Employees are informed, can opt out at any time, and are never recorded.

caniphish