

# Train your team to fight AI cyberattacks and deepfakes before they impact your organization

*"AI allows for scalable, customized attacks that bypass traditional security tools, as the focus is on human weaknesses rather than the technology stack."*

Google Cloud Security 2026, cybersecurity forecast

## AI voice phishing simulations

Train your team with AI voice attacks. Create perfect voice clones. Choose from hundreds of real-life scenarios and launch simulations that sound real.

## OSINT spear-phishing and other text-based attacks

Test your multichannel attack risks with AI-powered, personalized simulations in email, SMS and chats, using OSINT-found company data.

## Interactive, chat-based security awareness training

Bring security awareness to everyone in the team with interactive chat-bot courses, where employees understand security, not just memorize.

## AI voice phishing simulations – train your team with latest capabilities in security awareness space:

### 1 Create the perfect voice clone

Create a cloned voice in seconds, seamlessly adjust settings for perfect tonality and pace.

### 2 Design the attack path

Define the attack goal that AI will aim to achieve. Adjust dialogue tactics and add additional information for further realism

### 3 Review attack analysis and fix human vulnerabilities:

AI automatically analyzes call simulations providing necessary insights for smart decisions

+ Add new voice

🔍 Search voices by name or category

### Select one or more tactics that will guide the conversation strategy

Psychological, tactics that manipulate emotions and decision-making

✓ Authority impersonation

Urgency creation

Fear/Threat

### ⊗ Target Failed Simulation

#### Attack Goal

You're Sarah, CEO of Acme. You're calling John, a cybersecurity consultant at Acme. You just came back from the New York office and forgot the Wi-Fi password for the Washington office. Your goal is to make John give you the correct Wi-Fi password. You absolutely must hear the password from John before you hang up.

## OSINT spear-phishing and other text-based simulations cut the probability of successful attacks by up to 10 times

1. Deploy personalized, context-driven messaging automated by AI based on unique organization profile (simulations are relatable, mimicking real hackers)
2. 1-time set-up, continuous testing with smart scheduler, taking care of company events (weekends, holidays, events, etc.)
3. In accordance with latest cybersecurity standards (NIST, ISO 27001, SOC2)

Hello **Name - Alex Peterson**

Given your position of **Position - QA engineer** at

**Job - Alibaba Group**

I wanted to invite you to the conference in

**Location - New York** on **Interest - Testing**

Please register with the following link:

[Registration link](#)

Best regards,  
John Conrad



Hey! Ready to become slightly more unhackable today?

Do I get a cool badge for this?

Haha, I like your spirit.

Do I get a cool badge for this?



A digital badge, a virtual high five, and the eternal respect of all your future devices

## Engaging, hyper-personalized, chat-based security awareness

1. Relatable, interactive, 5-minute long — a recipe for an ideal security awareness training (exactly our approach that everyone loves)
2. Practical examples turned into minigames, letting you experience security, not just read about it (each course has gamified tasks for the user, bringing value to their personal protection)
3. Adaptive course difficulty with optional deep dives for more savvy users (not everyone wants to see over and over that "password123" is bad. We got them covered as well!)

## Teams of various sizes already tried and liked Brightside AI

AI voice phishing simulations

From €1/seat/month

Awareness training & phishing simulations

From €0.5/seat/month

Get in touch for FREE 2-week trial

<https://brside.com>