livingsecurity

LIVING SECURITY PHISHING SOLUTIONS

Today's attackers use many channels to spread malware. Living Security's phishing, smishing, and vishing solutions help raise users' awareness of these threats by helping you create highly-relevant, personalized simulations. What's more, our Email Threat Simulator and Incident Responder add layers of security and fast malware removal. When you pair these solutions with Unify, you can quickly identify risky users, then alert, train, or otherwise mitigate them.

Phishing Simulator

Living Security Phishing Simulator allows you to gauge your security culture with 4000+ AI-powered, ready-to-test phishing scenarios in 30+ languages and trains your employees to identify and respond to these attacks.

- Multiple Scenarios: Realistic MFA-themed, data submit, attachment, and click-only scenarios to test and train employees' ability to identify and respond to actual phishing attacks.
- No whitelisting required for O365: Our phishing simulator creates a simulation email directly in the inbox.
- False click mitigation allows you to visualize and eliminate automated security tool clicks on simulated phishing campaigns.
- Customizable templates to simulate a variety of phishing attacks.
- Multiple phishing scenarios randomly delivered to your employees to improve individual security culture.
- SSL-enabled phishing domains in your phishing scenarios that make your campaign realistic and secure while you're improving your security culture.
- Fully API-driven platform, including the ability to deploy training directly from Living Security Training to risky employees when identified by Living Security Unify. End-to-end testing to training all within Living Security's platform.

Vishing Simulator

If you have a customer support phone number, you need vishing simulation. Living Security Vishing Simulator delivers 200+ AI-powered ready-to-test vishing simulations in 100+ languages/dialects to train your employees to recognize and respond to these attacks.

- Scenario Customization: Simulate various vishing scenarios, including AI-powered text-to-speech and voice upload.
- Realistic Scenarios based on real-world attacks relevant to your organization.
- Automated Reporting
- Continuous Updates: Ensures your training remains updated with the latest vishing techniques.
- Fully API-driven platform to automate your tasks and integrate with any LMS.

Smishing Simulator

In smishing, attackers use SMS messages to trick recipients into providing sensitive information. Using over 300+ ready-to-use templates in 30+ languages or customizing your own, you can quickly identify the weakness within your organization and fix the problem.

- Scenario Customization: Customize existing or create personalized scenarios.
- Comprehensive Library: Access a constantly updated collection of over 300+ smishing scenarios to simulate real-world SMS attacks.
- Continuous Updates: New scenarios are added regularly, ensuring your training remains updated with the latest smishing techniques.
- Real-time, automated reporting.
- Varied Difficulty Levels: Tailor the experience based on your employees' proficiency levels.

Incident Responder

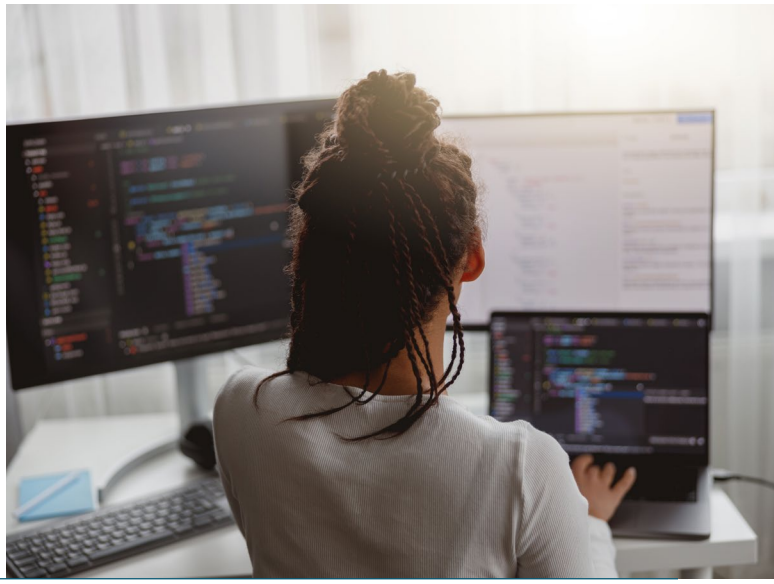
Living Security's automated phishing incident response tool helps you identify and respond to email attacks in minutes, then it proactively removes the threat from all other email addresses immediately to limit the attack's impact.

- Find and remove suspicious emails from your inboxes in minutes. For example, a scan and removal from 7500 inboxes took just five minutes.
- Works with your existing email security tools, analysis engines, SOAR, and other platforms, including Living Security Unify.
- Phishing Reporter lets employees easily and immediately report phishing emails directly from their inbox to Incident Responder.
- Create customizable rules for efficient classification of reported emails.
- Easily investigate through your email server, including Office 365, Google Workspace, Exchange Online, or On-Prem Exchange EWS.
- AI capabilities detect and prevent zero-day attacks

Email Threat Simulator

Living Security's Email Threat Simulator (ETS) continuously tests your secure email gateway solutions, including Office 365 and Google Workspace, by sending real-world attacks to a dedicated test inbox. Even if you believe you have tight email security, you'll identify attacks that bypass your SEGs and other vulnerabilities. ETS improves your defenses and helps in the remediation process, optimizing your technological investments.

- Include real-world malicious email attachments to test the robustness of your security solutions like antivirus, anti-spam, or sandbox.
- Test your email security by sending complex, multi-stage threats often used by advanced persistent threats (APTs).
- Test your vulnerabilities associated with various file formats like PDF, MP4, DOC, M3U, XPL, EXE, and more.
- Test your email gateway, data loss prevention (DLP), Sandbox, and all similar security products in your network against a specific malicious attack vector.
- Seamless Email Testing with Outlook Web Access: Integrate with Outlook Web Access or O365 for email security testing if you have restricted services like POP3/IMAP.
- Automatically scan your email gateway tools with continuously-updated attack vectors to maintain your security at all times.



About Living Security

Living Security, the global leader in human risk management, transforms human risk into proactive defense by quantifying human risk to engage the human with relevant content and communications to truly change human behavior. Living Security solves the challenges of human risk through risk identification, awareness and training, and risk reduction all through an integrated platform. Living Security is trusted by security-minded organizations like MasterCard, Verizon, Biogen, AmerisourceBergen, Hewlett Packard, and more.
Learn more at www.LivingSecurity.com.