Microsoft Security

Attack Simulation Training

Empower your employees to defend against phishing attacks with intelligent simulations.

Attack Simulation Training is a behavior-based solution to mitigate expensive phishing risk across your organization. Using real phish simulations and hyper-targeted training to train employees, Attack Simulation Training measures behavior change and automates design and deployment of an integrated security awareness training program.

Your people are your perimeter. Empower them.

Who is Attack Simulation Training for?

Chief Information Security Officers

Understand phishing risk across the organization at a glance. Investigate high value targets, and potential impact of compromise. Measure real ROI on your training programs through quantified behavior change metrics.

Security Administrators

Automate simulation creation, management, and cleanup. Intelligently tailor email templates to target users for the most effective simulations. Automate rich reporting and analytics.

Information Workers

Interactive training aligned to your personal context, learning style, and knowledge level. Integrate into your schedule and productivity tools.

Customer benefits

Assess risk

Measure your users for a baseline awareness of phishing attacks.

- **Accurately detect risk by phishing** employees using real phish emails attackers use against your organization.
- **Automate simulation creation,** payload attachment, user targeting, and scheduling. Use Azure Active Directory groups to automate user importing.
- Tailor simulations to your employee's contexts—region, industry, function—with **granular conditionality** on harvesting.

Improve user-behavior

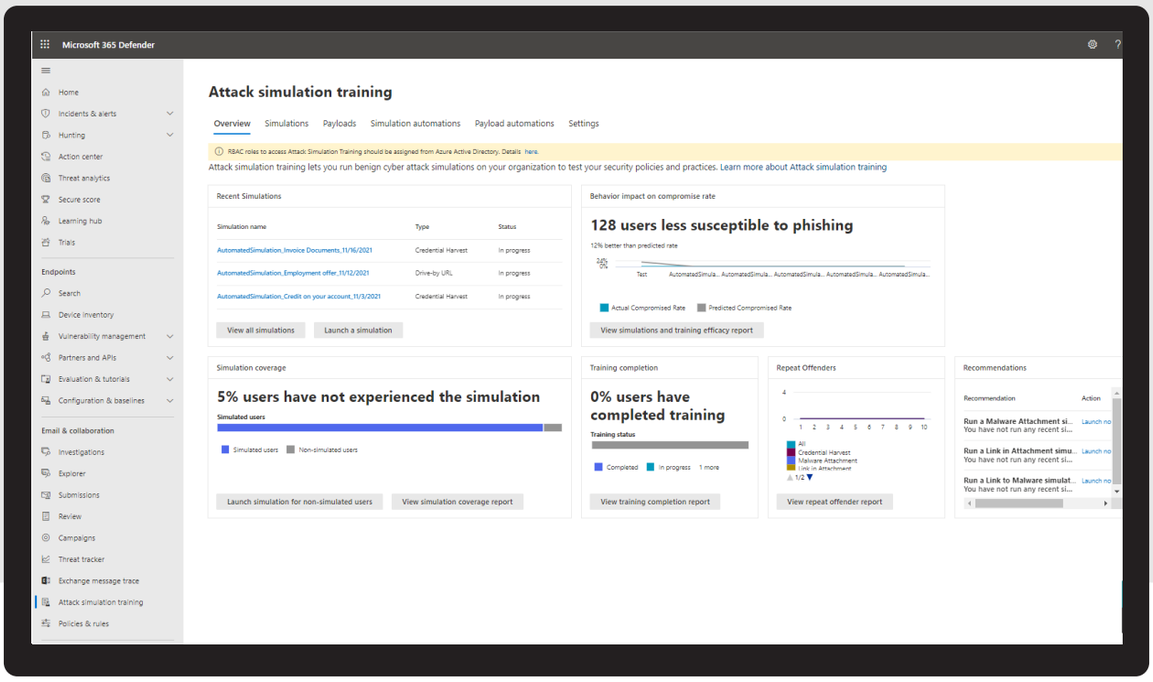
Remediate risk with hyper-targeted training designed to change behavior.

- A huge library of phish training content **enables personalized and highly specific training targeting based on simulation performance.**
- **Nanolearnings, microlearnings, and interactivity** cater to diverse learning styles and reinforce phishing risk awareness.
- **Customize your training landing page** with editable tags, adding your own link to trainings, and company logo.

Evaluate progress

Assess phishing risk mitigation across your social engineering vectors.

- **Gain visibility over your organization's training and simulation status** through completion and coverage metrics.
- **Track your organization's progress** against a baseline predicted compromise rate.
- **Use the user susceptibility score** to trigger automated repeat offender simulations and add context to simulation results.



Solution benefits

Accessible, diverse content

- Targeted, risk-based training framework that improves click rates
- Mobile responsive content that facilitates on-the-go training
- Inclusive learning modules available in a variety of formats

Straightforward implementation

- Seamlessly create, launch, and monitor security awareness and phishing campaigns

Easy-to-use interface

- Quickly modify your training environment with simple, intuitive controls

Multilingual support

- Craft a dynamic training program or phishing simulation in your preferred language(s)
- Dedicated customer support and Managed Services in English and French

Customizable

- A variety of courses and phishing simulation customization options
- Add logos, links, and edit colors to personalize your learning experience
- Create custom reports through our Graph API endpoints.

Hybrid security awareness options

- Leverage additional Terranova Security training for proactive security awareness training

25+ Training topics include (but are not limited to):

TERRANOVA SECURITY

Information Security Awareness topics

- Email
- Social Engineering
- Phishing
- Business email compromise

Microlearning library

- Vishing
- Web Phishing
- Mass Market Phishing - Amazon Gift Card
- Spear Phishing
- Whaling
- C-Level Email Impersonation
- Business email compromised (BEC)

Nanolearning library

- Phishing - Ransomware
- Phishing - Vishing
- Phishing - Six Clues That Should Raise Your Suspicions
- Phishing - Spear Phishing - CEO Fraud
- Phishing - Phishing website
- Phishing - Smishing
- Phishing - Anatomy of a Spear Phishing Attack

Start today

Attack Simulation Training is available to all Microsoft 365 E5 customers, Microsoft Security E5 customers and Microsoft Defender for Office 365 P2 customers.

Get access now

→ aka.ms/AttackSim