TECHGUARD S·H·I·E·L·D

SECURE · HOLISTIC · INTEGRATED · EMPLOYEE · LEARNING · DEFENSES

AIG CYBER LOSS PREVENTION PROGRAM

Phishing Simulations & Security Awareness Training Platform

Run realistic simulations with **3,000+ phishing templates** across diverse attack types.

Explore **500+ security awareness modules** focused on real-world threats and everyday risks employees face.

Content is **offered in 34 languages**, with availability varying by individual module or template.

Build Cybersecurity into Your Culture

Simulate Phishing Attacks

Prepare your organization for the most challenging threats they face by simulating the same domain spoofing, typosquatting and attack techniques scammers find most effective.

Customize Phishing Templates

Every aspect of the phishing simulator and training is customizable, giving you the ability to tailor employees' phishing training to your organization's greatest threats.

Report Phishing Emails

Turn your employees into active members of your cybersecurity defense with the PhishNotify email reporting plugin.

Automate Your Security Awareness Training

- Stream TechGuard training modules from your learning management system (LMS) with SCORM packages.
- Provision learners using one of our automated solutions and dynamically assign learners to groups for personalized education.
- Leverage pre-built program plans to efficiently structure and scale your training curriculum.
- Integrate PhishNotify with Outlook or Gmail to empower users to report suspicious emails instantly, streamlining threat escalation to administrators.
- Build your own custom integrations using our open API.
- Connect with your identity provider to authenticate employees via SSO or deliver a universal training link.

Get started today by submitting the webform to TechGuard, and we will follow up with your onboarding steps - techguard.com/aig

Please be sure to whitelist TechGuard's domain to ensure you receive all onboarding communications.

TECHGUARD S·H·I·E·L·D®

SECURE · HOLISTIC · INTEGRATED · EMPLOYEE · LEARNING · DEFENSES

Following the introductory phase, your team can expect a series of coordinated setup tasks and information exchanges. The checklist below details the items we'll work through together to ensure all prerequisites are in place for a smooth implementation.

Your Onboarding Journey Includes:

01 **Engage Stakeholders & Administrators**

Align district leadership and key decision-makers on goals, timelines, and expectations.

02 **Company Branding**

Customize your platform with your district's logo and messaging to create a familiar learning environment.

03 **Allowlisting**

Ensure successful email delivery by allowlisting S.H.I.E.L.D. IPs, domains, and headers.

04 **Upload Learners**

Add employees to the platform using secure upload methods.

05 **Install & Configure PhishNotify**

Deploy the PhishNotify add-in to empower users to report suspicious emails directly from their inbox.

06 **Content Selection**

Choose training modules and phishing templates that align with your organization needs and compliance requirements.

07 **Configure Account Settings**

Set up user roles, permissions, and notification preferences.

08 **Run Baseline Phishing Campaign**

Launch an initial simulation to assess your organization's current awareness level.

09 **Communicate Awareness Plan**

Share your cybersecurity awareness goals and expectations with employees to foster engagement and transparency.

10 **Launch AwareEd Program Plan**

Begin your formal training program with curated content and ongoing support.