



PLATFORM

2025/26

HUMAN RISK

TRACKING, TESTING & TRAINING

PLATFORM ECOSYSTEM

From evolving cyber threats to growing compliance demands, organizations face mounting pressure to strengthen their information security. At the core of that effort is **human risk management** — not just training employees, but actively measuring and improving their security behavior. By combining awareness training with real-world phishing simulations and AI-driven insights, organizations gain a clear view of their human risk posture and the tools to reduce it.



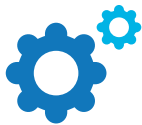
TRUSTED TRAINING PARTNERS

We work with leading training providers to deliver a wide range of content — from **general security awareness** to **role-based** and specialized **compliance training**. Topics include **HIPAA, GDPR, CCPA, PCI-DSS**, and more — ensuring your team stays informed, compliant, and prepared.

68% of breaches involve humans.

Verizon's 2024 Data Breach Investigations Report, 68% of breaches involved a non-malicious human element, such as falling victim to phishing attacks or making inadvertent mistakes.

OUR PLATFORM PHILOSOPHY



Managing Human Risk starts with visibility, action, and education. Our platform combines real-time employee risk tracking, phishing simulations with one-click reporting, and targeted training through our LMS and SecurityTips — giving you the tools to reduce risk, boost awareness, and build a stronger security culture.



TRACKING RISKS

- Dynamic risk scores based on real behavior
- Spotlight high-risk users for targeted action
- Trigger automated responses and workflows



TESTING & REPORTING

- Realistic phishing simulations
- One-click email reporting for users
- Clear, actionable testing analytics

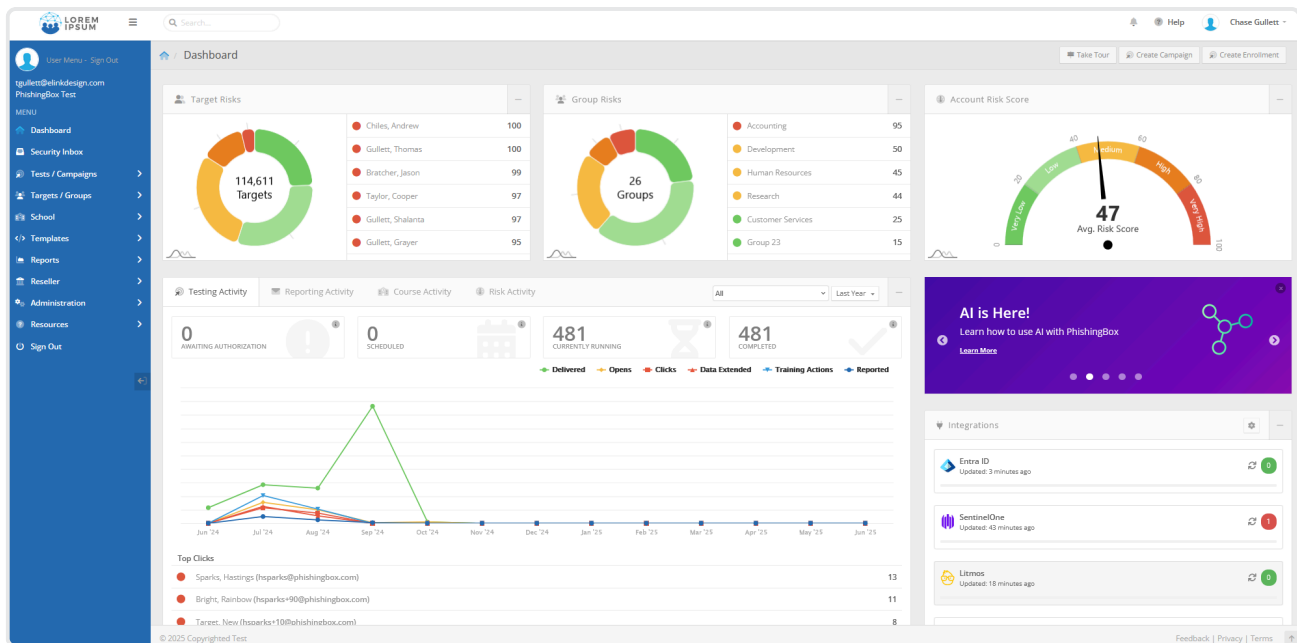


TRAINING

- Personalized, role-based learning
- Track progress and prove compliance
- Embedded microlearning with SecurityTips

TRACKING RISKS

Our platform gives you real-time visibility into **employee risk** through a **dynamic scoring system** tailored to your environment. We spotlight high-risk individuals, groups, and departments, so you know exactly where to focus your efforts. With flexible **human firewall rules** and deep integration across your security stack — from identity providers to XDR and antivirus — you can trigger timely interventions, automate training, and take action before small risks become big problems.



Microsoft
Entra ID



CROWDSTRIKE



okta

ninjaOne



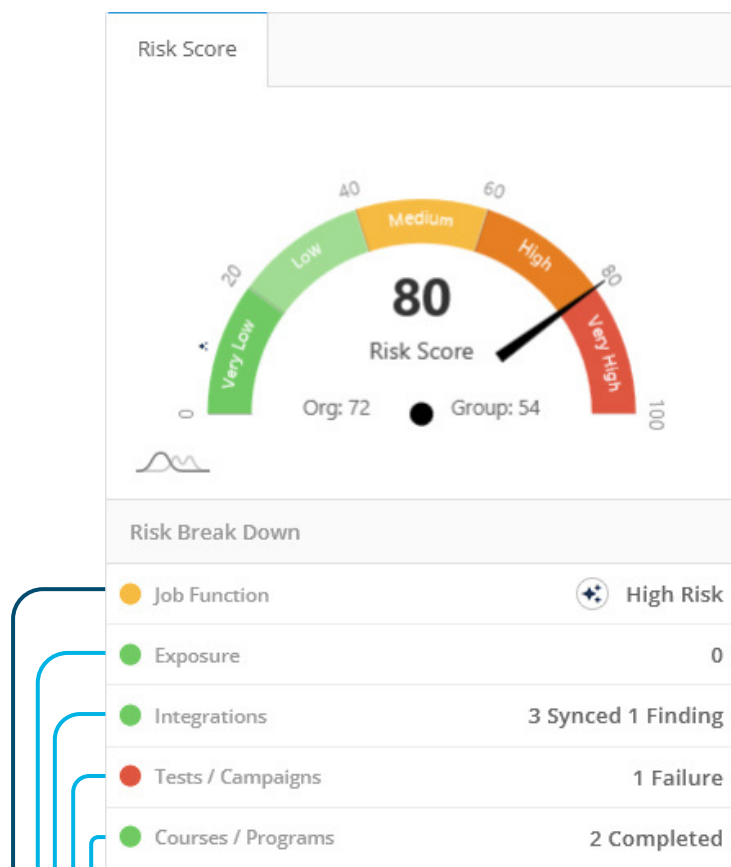
SentinelOne



bamboohr™

litmos

RISK SPOTLIGHTS



Job Function

Based on the target's job title, department, tenure, number of direct reports, group affiliations, and activity patterns, we determine the target's impact level within the organization. This reflects how critical the individual is to operations and the potential consequences if their account is compromised.

Exposure

Measures how visible a user is online. Public social media profiles, videos, and other content increase a user's attractiveness to attackers. It also considers third-party monitoring findings for exposed personal or company data. The more exposed a user, the higher their risk score.

Integrations / Security Tools

Assesses risk using signals from integrated security tools like endpoint protection, MDM, SIEM, and EDR platforms. Findings such as missing protection, outdated systems, or frequent login failures increase the score. Strong security tooling lowers exposure, while missing tools increase vulnerability.

Tests / Campaigns

Evaluates how users interact with simulated phishing emails, focusing on risky actions like clicking links or entering credentials, as well as positive behaviors like reporting phishing. Actions are scored by severity and recency. Positive behaviors lower the score and indicate growing security awareness.

Courses / Programs

Measures user engagement with security awareness education, a key factor in reducing human risk. Tracks formal training completion, JIT micro-learning triggered by risky actions, and SecurityTips usage for bite-sized ongoing lessons. These signals reflect how well users reinforce good security habits.

Impact x Probability = Risk Score

Human Resources
Information Systems

bamboohr™

SAP SuccessFactors
SAP

ADP
Workforce Now

Paycor

gusto

RIPLING

CUSTOMIZED RISK SCORE

Risk Scores come in all shapes and sizes, not all are alike—your organization shouldn't have to settle for a generic approach to human risk.

With PhishingBox, you can fully customize your Risk Score to match your security priorities and organizational structure. Adjust probability categories, fine-tune weighted averages, and apply impact modifiers to specific groups or job titles to reflect the real risk they pose within your environment.



Organization Risk Scores is an average of the Target/Users that make up the account.

Group Risk Scores is an average of the Target/Users that make up the group.

HUMAN FIREWALL RULES

Each integration in PhishingBox includes a set of “Human Firewall Rules” you can enable, disable, or adjust. These rules allow you to control how different user behaviors impact the overall risk score, ensuring your scoring reflects what truly matters in your security posture.

Human Risk Score Finding Rules

Use the table below to override any HRS scoring rules you would like.

⚠ Remember, the score follows golf-style rules, the lower the score the better (i.e., bad things add to the score, and good things subtract from the score).

Search...

Show 10 entries Showing 31 to 40 of 105 entries

All Sources Filter

	Rule name	HRS Factor	Description	Integrations	Score	Actions
<input type="checkbox"/>	Sign-in: Mass Access to Sensitive Files	Security Tooling	This detection looks at your environment and triggers alerts when users access mu...	▲	10	
<input type="checkbox"/>	Sign-in: Microsoft Entra threat intelligence	Security Tooling	This risk detection type indicates user activity that is unusual for the user or ...	▲	5	
<input type="checkbox"/>	Sign-in: New Country	Security Tooling	This detection considers past activity locations to determine new and infrequent ...	▲	5	
<input type="checkbox"/>	Sign-in: Password Spray	Security Tooling	A password spray attack is where multiple identities are attacked using common pa...	▲	5	
<input type="checkbox"/>	Sign-in: Suspicious browser	Security Tooling	Suspicious browser detection indicates anomalous behavior based on suspicious sig...	▲	5	
<input type="checkbox"/>	Sign-in: Suspicious inbox manipulation rules	Security Tooling	This detection looks at your environment and triggers alerts when suspicious rule...	▲	5	
<input type="checkbox"/>	Sign-in: Suspicious inbox forwarding	Security Tooling	This detection looks for suspicious email forwarding rules, for example, if a use...	▲	5	
<input type="checkbox"/>	Sign-in: Token issuer anomaly	Security Tooling	This risk detection indicates the SAML token issuer for the associated SAML token...	▲	5	
<input type="checkbox"/>	Sign-in: Unfamiliar properties	Security Tooling	This risk detection type considers past sign-in history to look for anomalous sig...	▲	5	
<input type="checkbox"/>	Sign-in: Verified threat actor IP Address	Security Tooling	This risk detection type indicates sign-in activity that is consistent with known...	▲	15	

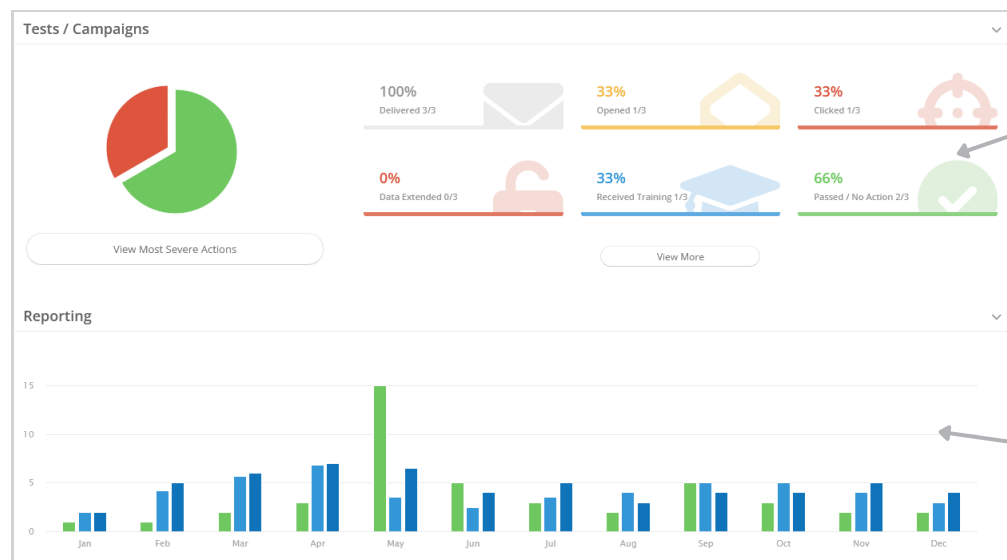
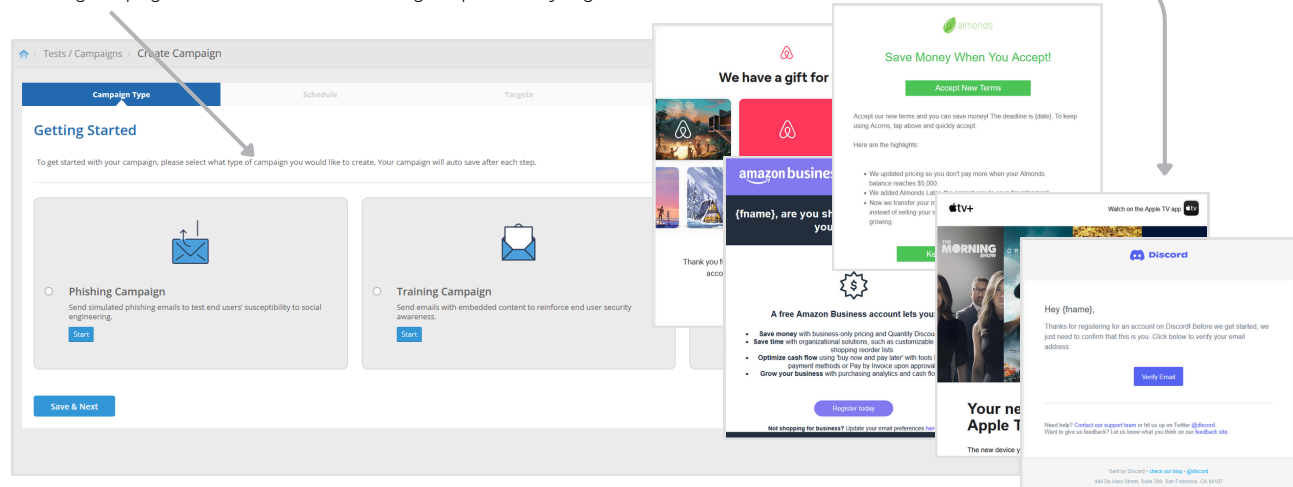
Show 10 entries Showing 31 to 40 of 105 entries

TESTING & REPORTING

PhishingBox Phishing Simulator offers a robust **Phishing Template Library** with pre-built scenarios with Just-in-Time training pages that align with each threat. **Automatically enroll users in targeted training** when they fail a phishing test, reinforcing learning when it's most effective. **Advanced Human Detection** and new **AI agentic integrations** help reduce false positives, ensuring accurate results while strengthening your organization's human firewall.

Phishing Campaign Wizard
Easily set up and configure recurring campaigns.

Template Library
Pre-built phishing, landing and training templates ready to go.



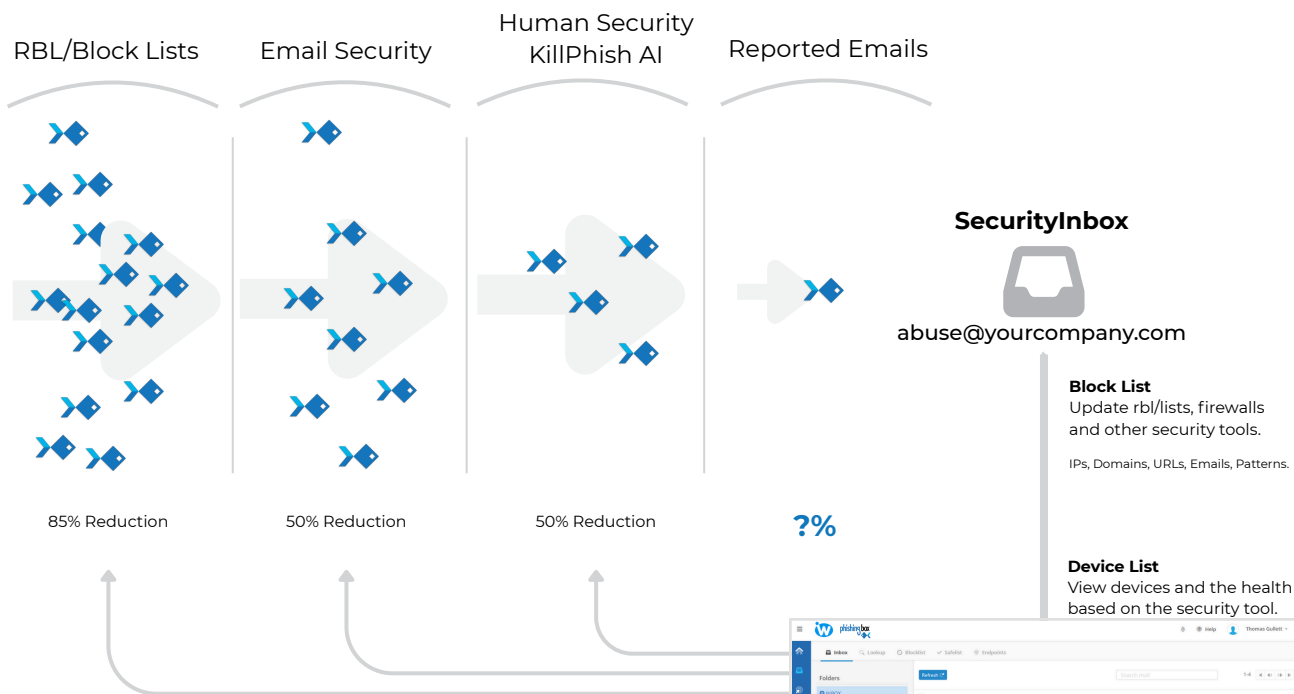
Testing Results
Easily see the status of phishing tests and training.

Reporting Results
Easily see the status of reporting activity compared to the account and industry.

SECURITY INBOX

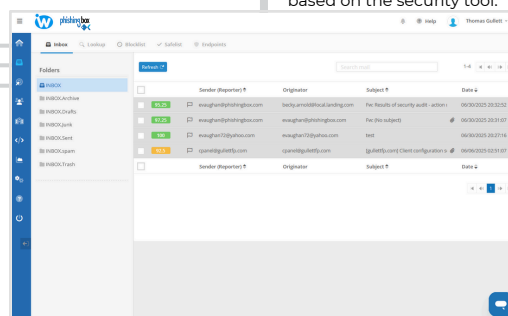
Security Inbox consolidates reported phishing emails and findings from integrated security tools into a single, streamlined workflow. It makes it easy to investigate and confirm real threats while filtering out noise, helping your team take fast, informed action. Security Inbox provides a unified view of emerging risks, enabling you to respond effectively and strengthen your organization's defenses.

PHISHING ATTACKS



AGENTIC ANALYSIS

- Parse headers for SPF/DKIM/DMARC and IP geolocation.
- Use NLP to detect urgency, threatening language, or sensitive requests.
- Extract and validate all URLs, checking for mismatches and domain age.
- Hash attachments and check against malware databases.
- Contextually check sender/recipient patterns for anomalies.



Take Down Notices

Include detailed attack information when submitting take down requests or cease and desist notices to ISPs, domain providers, and free email providers.

Clone Real Attacks

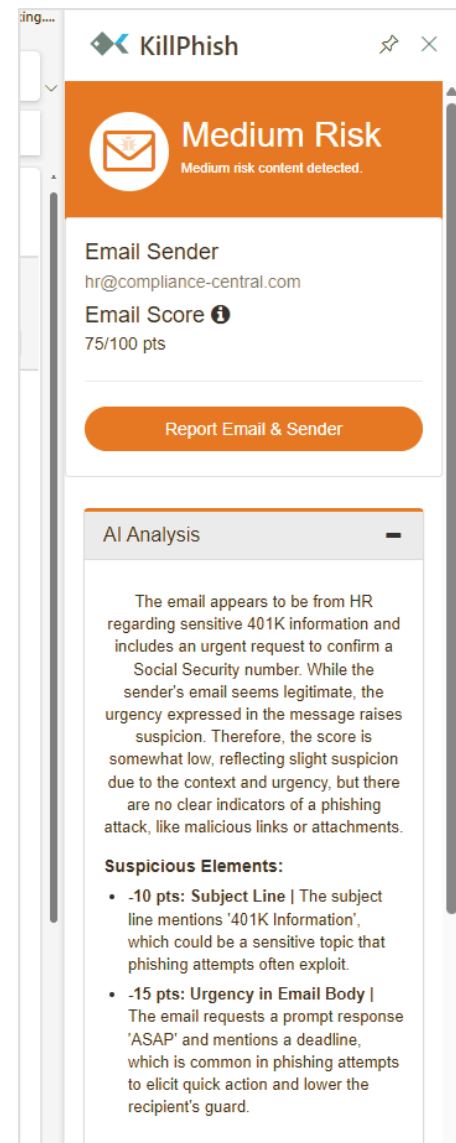
Use our cloning ability to download and clean real phishing threats and use them with our phishing simulator.

KILLPHISH AI

Go beyond blocking threats — **educate users at the moment of risk**. Our AI-enhanced email protection doesn't just detect phishing — it helps users understand why something is suspicious. With AI, email security becomes more than a filter — it becomes a **human-aware layer of defense** that transforms risky moments into teachable ones.

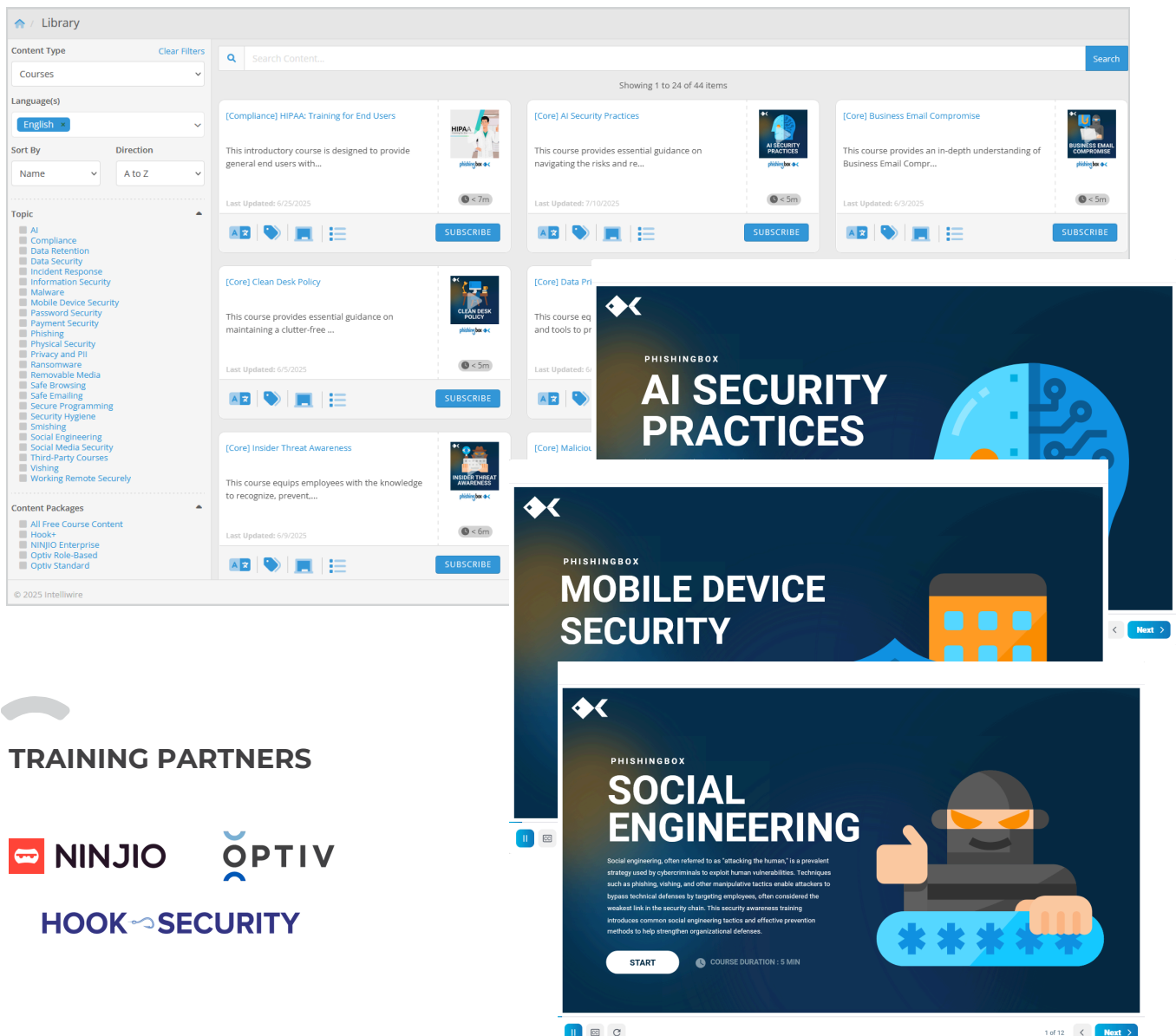
HIGHLIGHTS

- **Explain the “Why”** - AI highlights red flags like spoofed domains, unusual sender behavior, or mismatched URLs — making phishing tactics visible and understandable.
- **Build User Judgment** - Empower users to think critically about emails instead of blindly trusting filters.
- **React in Real Time** - Deliver contextual, on-the-spot warnings directly in the inbox — before the click happens.



TRAINING

Deliver training through our **Learning Management System (School)**, customized with your logo and domain to serve as your dedicated training center. Use it to deliver our SCORM courses and host content from other providers. Our **Training Library** lets you purchase training partner courses, and you can easily upload and manage your own SCORM files, centralizing all security, compliance, and employee training in one branded platform.



The screenshot displays the PhishingBox Training Library interface. On the left, there is a sidebar with filters for Content Type (Courses), Language(s) (English), Sort By (Name), Direction (A to Z), and a Topic list including AI, Compliance, Data Retention, Data Security, Incident Response, Information Security, Malware, Mobile Device Security, Password Security, Payment Security, Phishing, Physical Security, Privacy and PII, Ransomware, Removable Media, Safe Browsing, Safe Emailing, Secure Programming, Security Hygiene, Smishing, Social Engineering, Social Media Security, Third-Party Courses, Vishing, and Working Remote Securely. Below the sidebar, there are Content Packages: All Free Course Content, Hook+, NINJO Enterprise, Optiv Role-Based, and Optiv Standard. The main area shows a grid of course cards, each with a title, description, last updated date, and a 'SUBSCRIBE' button. The courses include:

- [Compliance] HIPAA: Training for End Users**: This introductory course is designed to provide general end users with... Last Updated: 6/25/2025. Duration: < 7m.
- [Core] AI Security Practices**: This course provides essential guidance on navigating the risks and re... Last Updated: 7/10/2025. Duration: < 5m.
- [Core] Business Email Compromise**: This course provides an in-depth understanding of Business Email Compr... Last Updated: 6/3/2025. Duration: < 5m.
- [Core] Clean Desk Policy**: This course provides essential guidance on maintaining a clutter-free ... Last Updated: 6/5/2025. Duration: < 5m.
- [Core] Data Privacy**: This course eq and tools to pr... Last Updated: 6/5/2025. Duration: < 5m.
- [Core] Insider Threat Awareness**: This course equips employees with the knowledge to recognize, prevent... Last Updated: 6/9/2025. Duration: < 5m.
- [Core] Malicious**: This course eq and tools to pr... Last Updated: 6/5/2025. Duration: < 5m.

Overlaid on the right side of the screenshot are three course preview cards:

- AI SECURITY PRACTICES**: A card with a blue background and a circuit-like graphic.
- MOBILE DEVICE SECURITY**: A card with a dark blue background and a graphic of a building.
- SOCIAL ENGINEERING**: A card with a dark blue background and a graphic of a person wearing a mask and holding a thumbs up.

At the bottom of the Social Engineering card, there is a 'START' button and a 'COURSE DURATION: 5 MIN' indicator. The bottom right corner of the screenshot shows a pagination indicator '1 of 12' and a 'Next' button.

TRAINING PARTNERS



NINJO



OPTIV

HOOK SECURITY

TRAINING TOPICS



AI Security



Compliance



Data Security



Email Inbox



Incident Response



Information Security



Malware



Mobile Device Security



Password Security



Payment Security



Phishing



Physical Security



Privacy and PII



Ransomware



Removable Media



Safe Browsing



Safe Emailing



Secure Programming



Security Hygiene



Smishing



Social Engineering



Social Media Security



Vishing



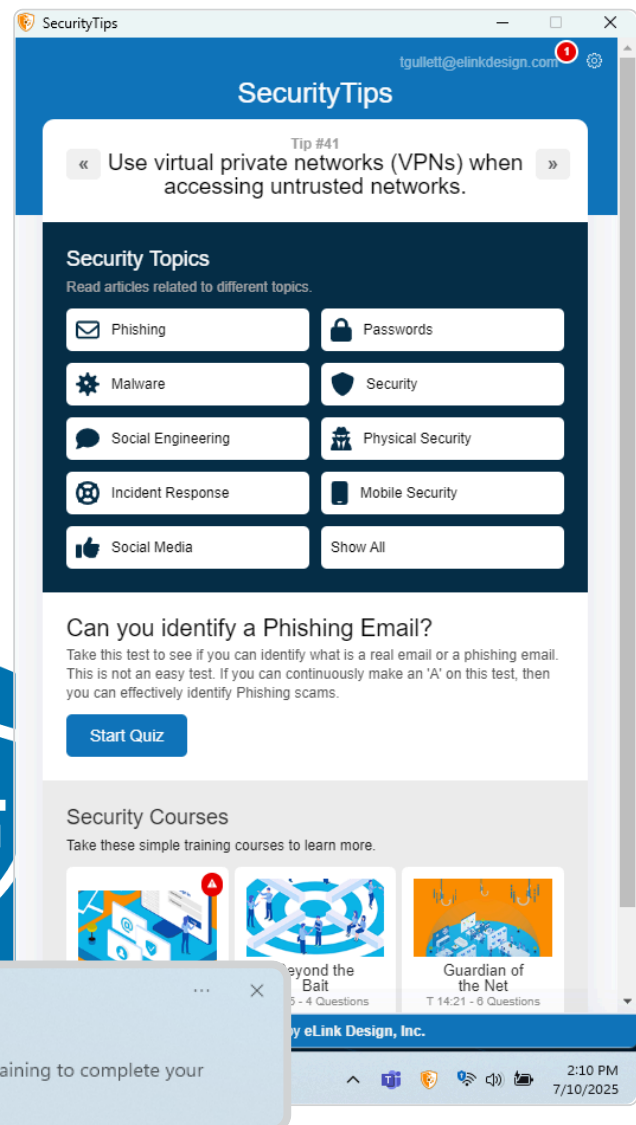
Working Remote Securely

SECURITYTIPS

SecurityTips.com strengthens your human firewall with bite-sized security lessons delivered to employee **Desktops, SharePoint, or any modern web application**. With real-time micro-training triggered by risky behaviors and a library of engaging modules, SecurityTips keeps security awareness top of mind without disrupting workflows. Empower your team to recognize and avoid threats while building a culture of security across your organization.

HIGHLIGHTS

- **Notifications** - Send training enrollment alerts via desktop, Slack, and Teams, ensuring users don't miss courses. One click logs them in to start training immediately.
- **Security Articles** - Offer a library of short, actionable security articles users can browse anytime for ongoing awareness.
- **Training Wall Enforcement** - Require critical training by a set date, blocking other tasks until courses are completed to ensure compliance.
- **Real-Time Security** - Deliver urgent security alerts directly to users, keeping them informed and ready to act.



ABOUT US



Ransomware was identified as a top threat across **92%** of industries.



VISION

To create a world where cybersecurity is strengthened at its foundation by empowering every person to recognize and stop social engineering threats.



Mission

To help organizations reduce human risk by providing innovative phishing simulation, security awareness training, and social engineering testing tools that are easy to deploy, scalable for any size, and designed to strengthen the human layer of cybersecurity.



PhishingBox originated in **2006** as a tool used by an audit firm to conduct social engineering testing while conducting IT security audits for their clients. **eLink Design, Inc** was the contracted firm to perform the development. In **2016**, eLink Ventures, along with other investors, purchased the software and created the stand-alone company, **PhishingBox LLC**.

HQ in Lexington, Kentucky
www.phishingbox.com



phishing box



400 E. Vine St., Suite 301
Lexington, KY 40507



+1 (877) 634-6847



info@phishingbox.com