PERCEPTION
POINT™

Perception Point Security Awareness Training

Strengthening Your Last Line of Defense

In today's digital landscape, cybersecurity awareness training isn't just a necessity; it's a strategic imperative. Most cybersecurity awareness programs are designed to educate employees on how to recognize and avoid phishing, BEC, and other social engineering tactics. Yet despite organizations' best efforts, employees continue to fall victim to these attacks. This is due to the intentional design of social engineering, which aims to elicit emotional responses, urging targets to act impulsively and "click."

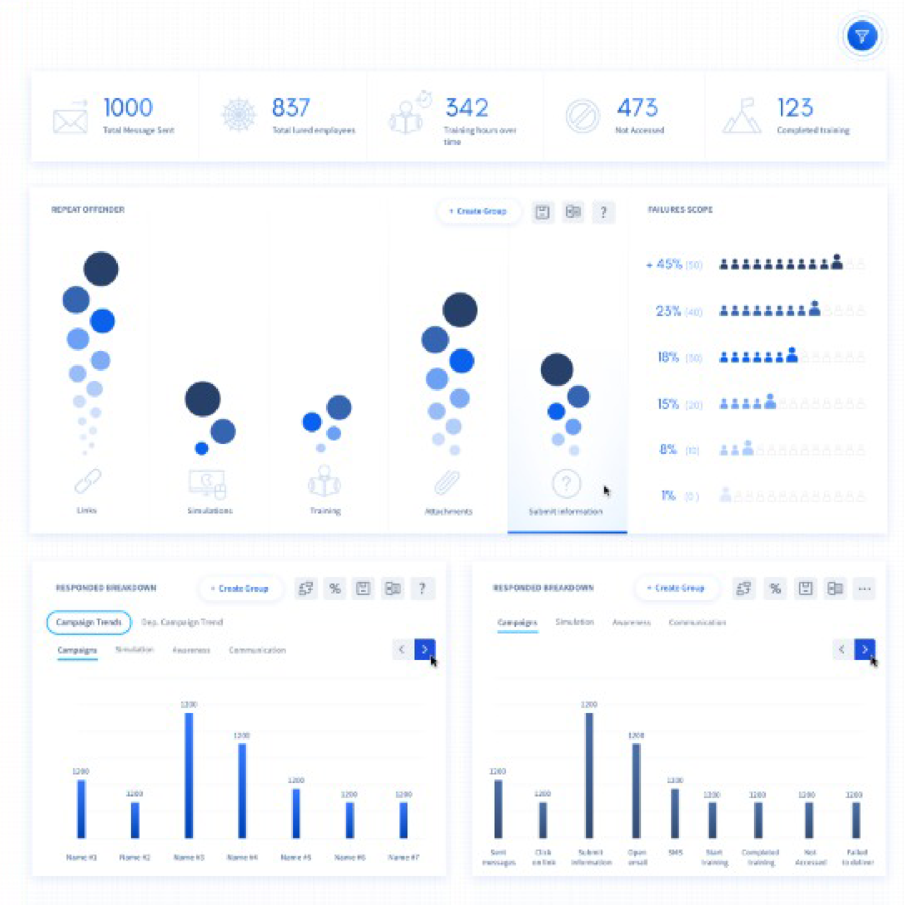
Our security training program, integrated with our Advanced Email Security solution, aims to counter these attacks by focusing on employee behavior, specifically their emotional responses, rather than just relying on enhancing their knowledge through rational thinking.

In an era where the human element remains a critical factor in cybersecurity, investing in security training is an essential tool to fortify an organization's resilience against an ever-evolving array of cyber threats.

PERSONALIZE YOUR EMPLOYEES' TRANING

As cyber threats continue to evolve in sophistication and frequency, it becomes increasingly difficult for employees to distinguish between the malicious and the legitimate. By offering a uniquely personalized approach to cybersecurity training, we empower employees and reduce the risk of human error for your organization.

Our program leverages machine learning algorithms to seamlessly integrate best practices from behavioral psychology and marketing methods. The result is a cybersecurity training program tailored to the specific needs of each of your employees that reduces the likelihood of successful cyberattacks, data breaches, and other malicious activities.



Better Training; Better Cyber Behavior

Our program ensures that every employee receives automated, individualized cybersecurity training. This system pulls from the actual threats targeting your organization, creating phishing simulations based on real-time interactions or past performance risk scores. These simulations evaluate your employees' cybersecurity skills, provide exercises to practice the correct behavior, and automatically enroll them in additional training as necessary.

The program crafts targeted phishing attack simulations for various departments, roles, or groups within the organization. We track simulation progress for both individuals and groups, ensuring continuous momentum towards cybersecurity awareness and compliance objectives.

SIMULATION

Simulations focus on a range of social engineering attacks, with templates updated automatically and regularly to keep you armed against the latest cyber threats.

- ☑ Ransomware
- ☑ Deceptive Phishing
- ☑ Quishing
- ☑ CEO Fraud/Whaling
- ☑ Spear-Phishing
- ☑ SMS
- ☑ Business Email Compromise (BEC)
- ☑ Credential Theft
- ☑ Malware & Malicious Attachments

AUTOMATION & ANALYTICS

- Real-world, social engineering attacks crafted from the latest intelligence, designed to imitate highly sophisticated attacks.
- Employee segmentation, automated by cognitive computing and machine learning algorithms.
- In-depth analysis of every keystroke during employee training sessions.
- Comprehensive insights into each employee’s journey towards behavioral change.
- Simulated attacks automatically rolled out to individual employees and groups, with instant result analysis and follow-up recommendations.
- Automatic employee enrollment in extra training, as needed.
- Seamless integration with active directory and address book updates.

LANGUAGES

Security training is available in 28+ languages, including:

العربية 汉语 Čeština Nederlands English Français Deutsch עברית Italiano

日本語 한국어 Português Русский Slovenčina Español ไทย Tiếng Việt

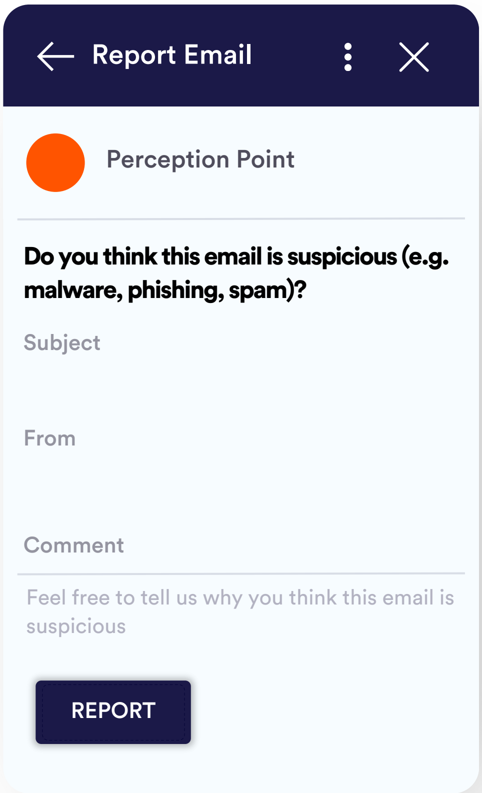
End User Reporting

End user reporting is included with security awareness training.

Integrated with Advanced Email Security, a simple button allows your employees to report any suspicious emails directly to our platform. With this new capability, your trained employees become part of your security stack, helping you to prevent the next attack.

Once an end user reports a suspicious email, our Incident Response team is alerted with all the relevant data to investigate the potential incident. In the case the email was deemed malicious, you will receive a detailed report and the system will automatically retrieve all similar emails from all relevant email boxes.

Transforming Your Employees from the Last Line to an Active Line of Defense!



Do you think this email is suspicious (e.g. malware, phishing, spam)?

Subject

From

Comment

Feel free to tell us why you think this email is suspicious

About Perception Point

Perception Point is a Prevention-as-a-Service company for the fastest and most accurate next-generation detection, investigation, and remediation of all threats across an organization's main attack vectors - email, web browsers, and cloud collaboration apps. The solution's natively integrated and fully managed incident response service acts as a force multiplier to the SOC team, reducing management overhead, improving user experience and delivering continuous insights; providing proven best protection for all organizations.

Deployed in minutes, with no change to the enterprise's infrastructure, the patented, cloud-native and easy-to-use service replaces cumbersome legacy systems to prevent phishing, BEC, spam, malware, zero-days, ATO, and other advanced attacks well before they reach end-users. Fortune 500 enterprises and organizations across the globe are preventing attacks across their email, web browsers and cloud collaboration channels with Perception Point.

To learn more about Perception Point, visit our website, or follow us on LinkedIn, Facebook, and Twitter.