Proofpoint Security Awareness Training Enterprise

PRODUCTS

- Security Awareness Training Enterprise
- Targeted Attack Protection
- Threat Response Auto-Pull

KEY BENEFITS

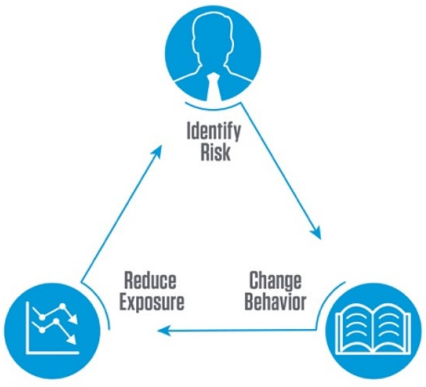
- Reduce successful phishing attacks and malware infections by up to 90%
- Reduce risk from phishing and other cyber attacks by changing users' behavior
- Maximize effectiveness of efforts by providing targeted and tailored education to users
- Reduce exposure and IT overhead with informed users and automated incident response
- Measure user behavior change with CISO Dashboard and real-time reporting

With more than 85% of breaches involving human error,[1] teaching your employees how to thwart cyber attacks is critical for the security of your organization. After all, technologies that detect and block threats before they reach users simply can't stop everything. Your people must recognize and be empowered to act when faced with phishing, ransomware and business email compromise (BEC) attempts.

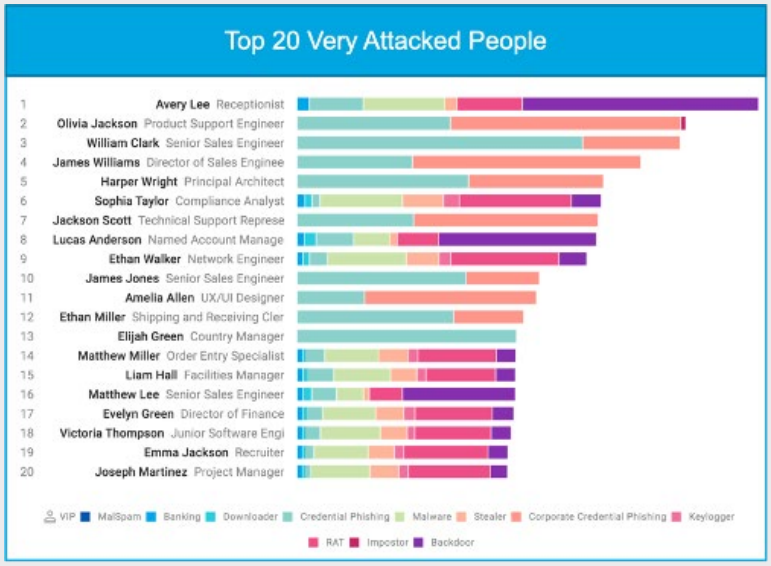
Proofpoint Security Awareness Training Enterprise helps you deliver the right training to the right people for the right response to today's dangerous attacks. It turns your users into a strong line of defense that proactively protects your organization.

We help you:

- Identify user risk
- Change employee behavior
- Reduce your organization's exposure



1 Verizon. "2021 Data Breach Investigations Report." May 2021.



A sample Very Attacked People (VAP) report. Customers can use simulated phish with the latest attack trends on these high-risk users then auto-enroll users who fall for a simulation into training.

Identify Risk

Determine who is being attacked and evaluate their ability to protect themselves

Not all employees are attacked with the same frequency or force. Many factors paint different employees as more attractive targets to cyber attackers than others. Integration with Target Attack Protection (TAP) lets your administrators identify the areas and people of highest risk. Armed with this information, they can prepare and implement preventative measures more efficiently. They'll be able to develop and run more prescriptive, impactful security awareness programs that are based on real risk.

This powerful integration identifies your organization's Very Attacked People™ (VAPs) and Top Clickers. It provides you with insight into the types of threats they receive and engage with. With this data, you can enroll users in simulations and Knowledge Assessments to determine risk. You can also assign training to drive change in behavior.

Our Phishing Simulations help you scope your organization's susceptibility to phishing attacks. With thousands of different phishing templates across 13 categories, you can evaluate users on multiple threat types. These threat types include:

- Attachment-based (DOC, HTML, PDF, DOCX, XLSX)
- Link-based
- Data entry/Credential-based

We add new templates every week. Constant updating ensures that the latest attack trends are always represented. We draw our Dynamic Threat Simulation phishing templates from Proofpoint threat intelligence. The templates are designed to address customer requests and seasonal topics.

Proofpoint's real-time sharing of threat intelligence is from the No. 1 deployed solution across the Fortune 100, Fortune 1000 and Global 2000. That means templates are relevant to what users may see in real attacks.

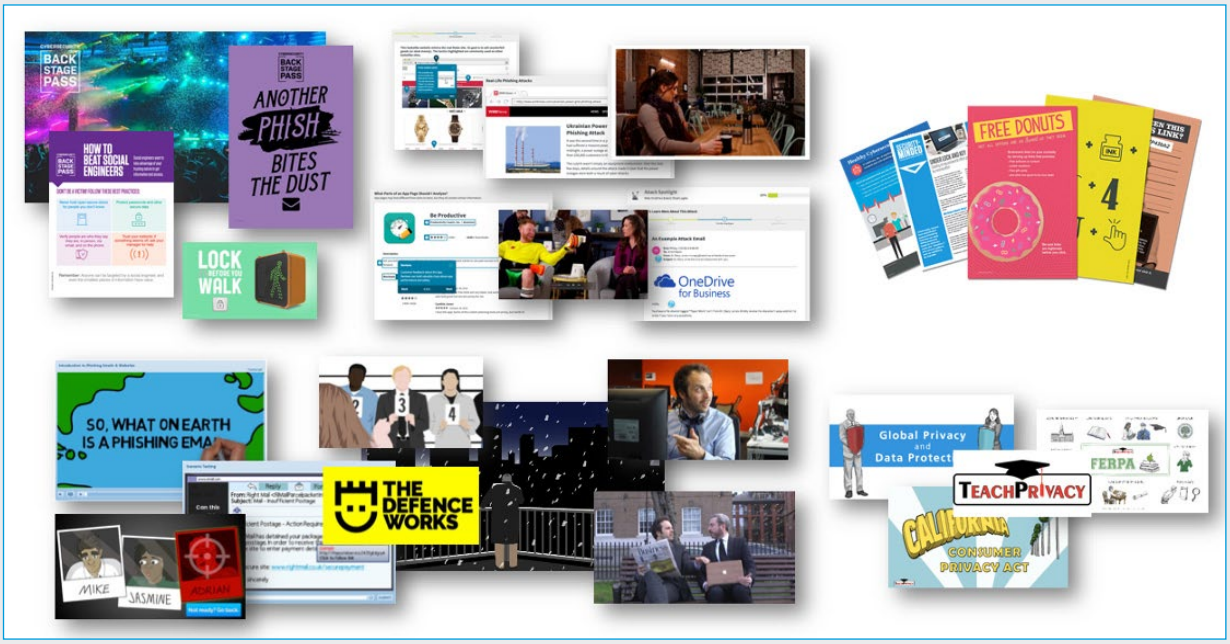
When a user falls for a simulated attack, they receive "just in time" teaching. These lessons teach:

- The purpose of the exercise
- The dangers of real-world attacks
- How to avoid future traps

You can assign more training automatically to anyone who falls for a phishing simulation.

You can also see how much your employees understand about infected removable memory devices. USB Simulations teach them about the dangers of infected USB devices. This feature also includes just-in-time educational content for users who fall for a simulation. You can access USB Simulations at any time, for unlimited campaigns.

But simulations can only convey specific risk in specific threat vectors. Our Knowledge Assessments help you understand what your users know across a broad range of domains. Example



topics include cloud applications, insider threats, mobile devices, passwords and more.

You can also:

- Use comprehensive assessments covering all control domains
- Select predefined assessments from a library of hundreds of questions in more than 40 languages
- Auto-enroll users in relevant training if they score below a certain level

You can create custom questions as well. Use this feature to gauge knowledge of your organization's policies and procedures. Once you establish a baseline for your users, you can follow recommendations to address knowledge gaps and reduce risk.

Change Behavior

Deliver training based on real-world threats, user behavior and knowledge gaps

The ultimate goal is behavior change. We tailor our education for impactful experiences to users. Focusing on areas of high risk, we can deliver our programs to the VAPs or Top Clickers that Proofpoint TAP identifies. We can also focus on users who fail simulations or score below a certain threshold in a Knowledge Assessment.

We have helped millions of users go from risky to ready. And they now form strong lines of defense for their organizations.

We ensure our content drives behavior change as follows:

Methodology and Consumability

- Proven best practices for adult behavior change
- Accessible and searchable content through our Content Library
- Hundreds of diverse and assorted training modules and program materials
- CISO-guided core curriculums to build necessary skills based on the type of user (privileged, role-based, etc.)

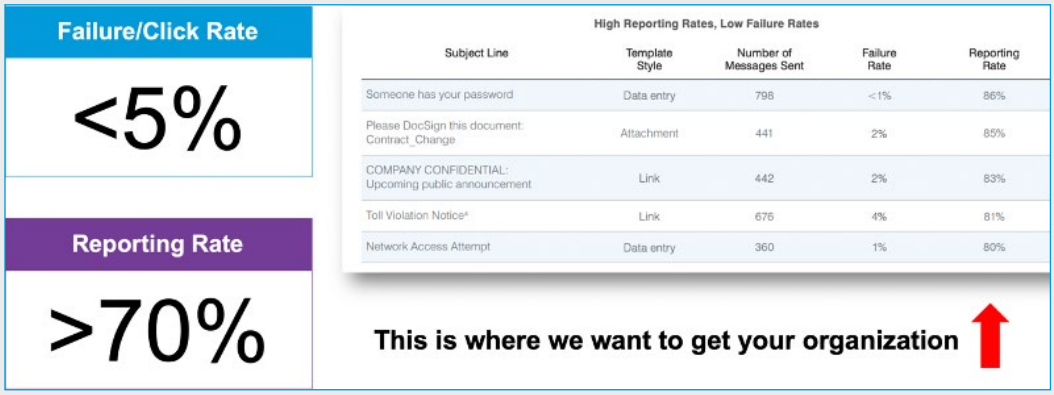
Global and Multicultural Support

- More than 40 languages and regional references (domains, names, etc.) for the entire Core Curriculum
- Inclusive and diverse text and images

New Threat Readiness

- The market's best threat intelligence to stay ahead of attackers
- Billions of daily threat samples from email, cloud and social media
- Threat-led content like our Threat Alerts, Attack Spotlight modules and simulation templates

Our best practices, campaigns and curriculums help you put together engaging, multichannel educational experiences. Varied content is critical. Proofpoint's fast-growing library contains



Real customer results of top performing organizations from Proofpoint's 2020 State of the Phish Report.

more than 300 training modules. It includes hundreds of PDFs, infographics, videos, memes and more. We have different styles and types of material to match any organization's culture and user preference. And our partnership with TeachPrivacy ensures even more compliance coverage.

[To view available content, download the Proofpoint Content Solution Brief]

Content Delivery

Improve content relevance with your users in mind. With our self-service Customization Center, you can:

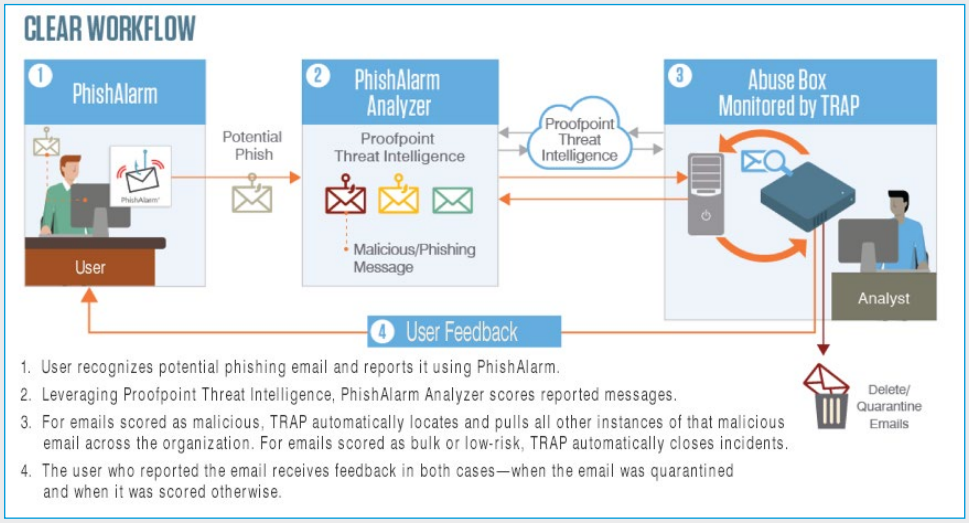
- Tailor training using verbiage, images and questions that are relevant to your users.
- Clone and modify modules, lessons and pages to make changes in real-time.
- Toggle training modules (with questions) to awareness modules with one switch.
- Maintain efficacy with our Learning Science Evaluator. This provides feedback if the length, amount of on-screen content or number of questions in a challenge gets off track

If you have your own Learning Management Systems (LMS) that uses SCORM-based files, your administrators can easily customize and export training modules to the LMS. They can combine multiple modules, and even prioritize the order users can take them.

Reduce Exposure

Knowledgeable users report potential threats, which reduces attack surface

Empower your people to report suspicious messages with a single click. Use our PhishAlarm® email client add-in. And after reporting an email, users get instant positive reinforcement in the form of a "thank you" pop-up message. With this add-in, you won't need



to get headers and attachments from users who would otherwise forward emails to an abuse mailbox. In typical organizations, the rate of users who report simulated attacks varies between 10% and 20%. With educated users, successful clients have consistently seen rates of more than 70%.

But simulated attacks are not as risky as real threats. Our threat intelligence provides industry-leading aggregation and correlation of threat data across email, users, cloud, domains, networks and social media. We have world-class threat intelligence, sandboxing and detection engines to identify malicious messages. These can deliver dispositions automatically using Threat Report to security teams about user-reported messages. Threat Report also specifies exactly what about the messages makes them malicious. This saves time for your incident response teams. It also provides insight into how your security awareness program is decreasing email-based risk.

With our automated Closed-Loop Email Analysis and Response (CLEAR) solution, reported messages are sent to Threat Response Auto-Pull (TRAP). These messages can then be automatically quarantined or closed. Or they can be sent to your incident response team for further analysis. Administrators can set up customized response messages to users based on the message type. These messages are sent back to users to reinforce behavior and help build a security-aware culture.

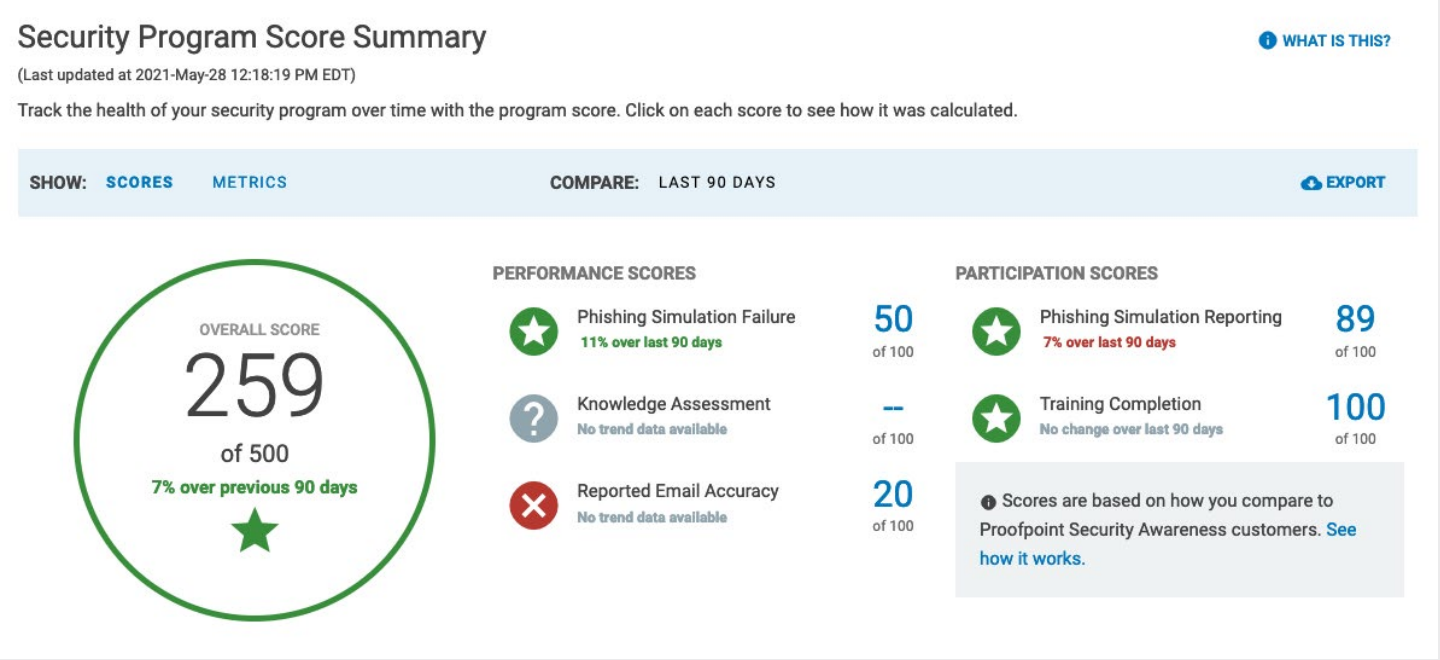
Measure and Adapt

Measure how user behavior change is impacting key outcomes

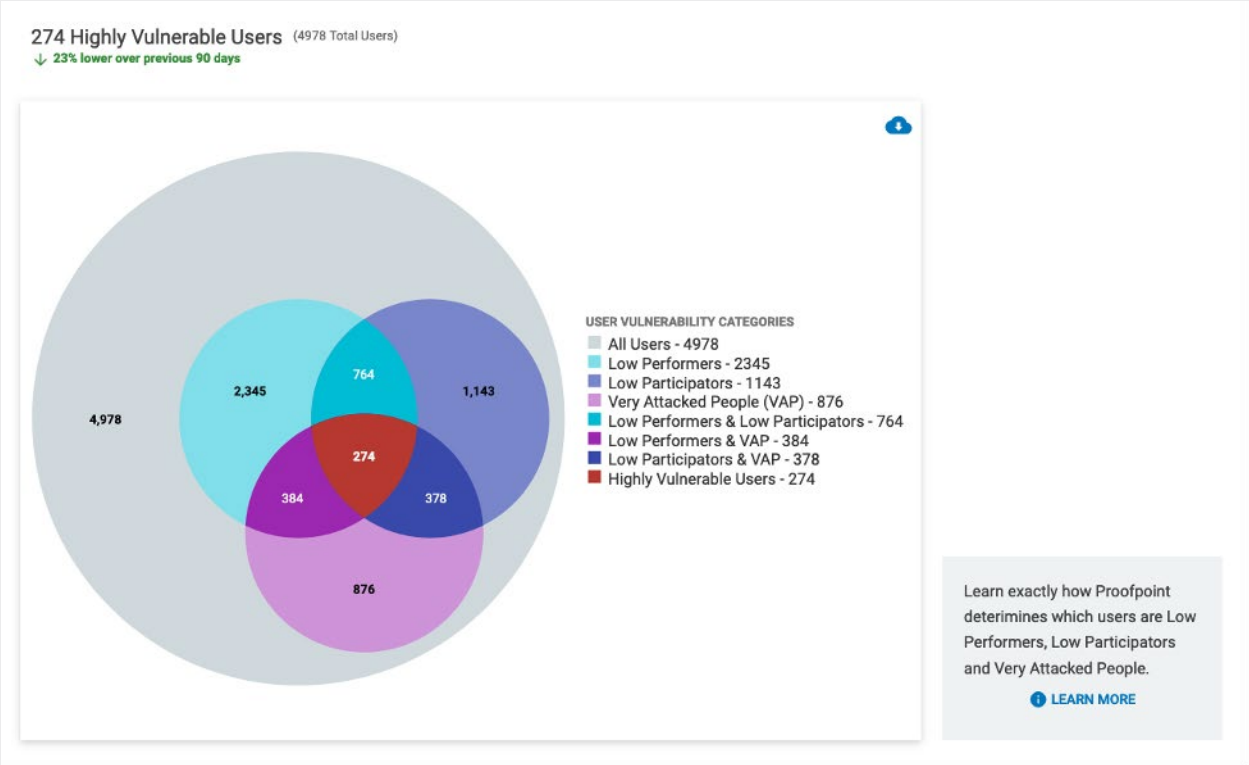
Our CISO Dashboard provides powerful insights for your C-level executives. If you want to share security awareness results with your CISO/CIO or other key stakeholders, look no further.

In the CISO Dashboard you'll find:

- Your overall program score.
- Performance of the different components of your program.
- Benchmarking compared to others in your industry.
- Areas of focus needed in your program.
- Trending performance data.
- User vulnerability data. This includes low participators, low performers and Very Attacked People (VAPs) if you have Proofpoint TAP.



The score summary of the CISO Dashboard provides powerful, fast insights about your program's current status, with scores benchmarked against other Proofpoint customers



The User Vulnerability section of the CISO Dashboard helps you run a more focused, impactful program by setting up activities for vulnerable users.

With real-time reports, your administrators don't need to wait for results to show assignment status. They get fast feedback to adjust the program. Our real-time reports cover everything from phishing simulations to training assignments.

Use them to:

- Get a fast, high-level view of progress of a specific assessment or training assignment
- Demonstrate completion for compliance or audit purposes
- Quickly export a report for a last-minute meeting or request from a stakeholder
- Take action on users who are overdue in an assignment

Our Results API is also included. It provides you with access to reports and analysis including training, phishing, knowledge assessment, users and email. You can then integrate this information into common business intelligence tools or a learning management system.

LEARN MORE

For more information, visit **proofpoint.com**.

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ: PFPT) is a leading cybersecurity and compliance company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web. More information is available at **www.proofpoint.com**.