proofpoint.

SOLUTION BRIEF

Proofpoint Security Awareness Training Enterprise

PRODUCTS

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

KEY BENEFITS

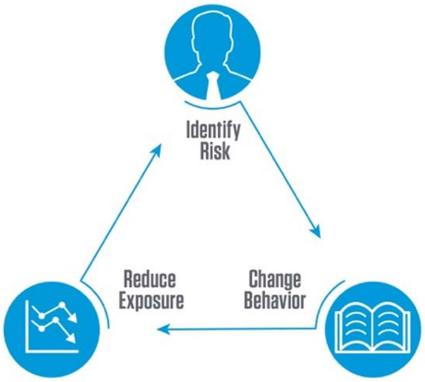
- Reduce successful phishing attacks and malware infections by up to 90%
- Reduce risk from phishing and other cyber attacks by changing users' behavior
- Maximize effectiveness of efforts by providing targeted and tailored education to users
- Reduce exposure and IT overhead with informed users and automated incident response
- Track progress with dynamic reporting and benchmarking

With more than 90% of cyber attacks targeting users,[1] educated employees are critical to protecting your organization. Technologies that detect and block threats before they reach users simply can't stop everything. Your people must realize and be empowered to act when phishing and business email compromise attempts reach them. The solution helps you teach your employees how to prevent cyber attacks from succeeding.

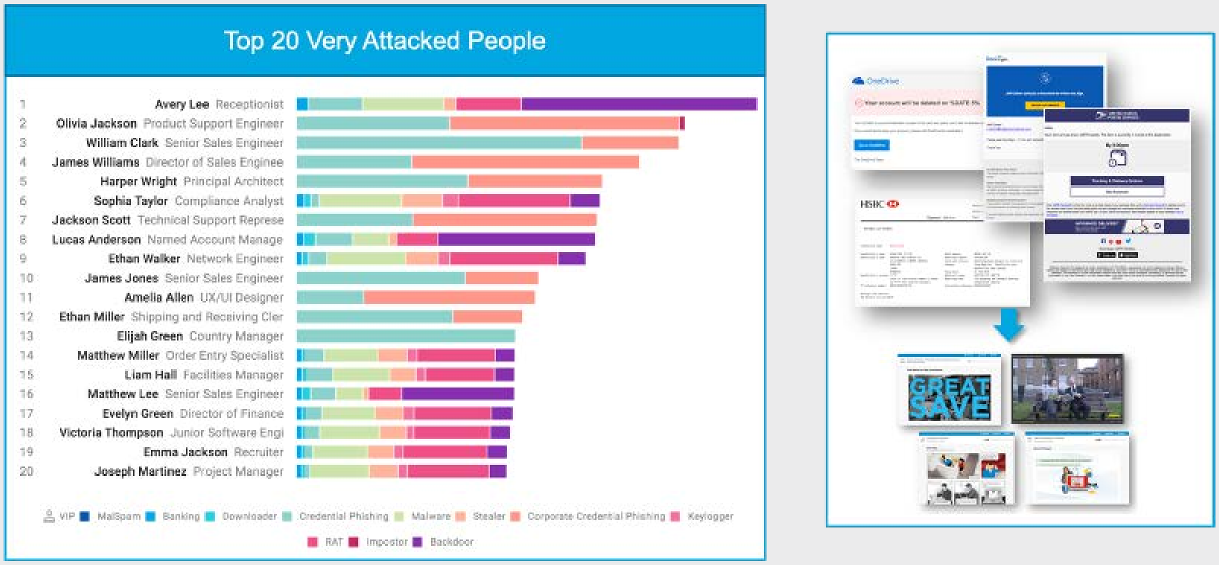
Proofpoint Security Awareness Training Enterprise helps you deliver the right training to the right people for the right response to today's dangerous attacks. It turns your users into a strong line of defense, proactively protecting your organization.

We help you:

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



[1] Verizon. "2019 Data Breach Investigations Report." July 2019.



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

Identify Risk

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

Not all employees are attacked with the same force. There are many factors that make an employee a desirable target for cyber attacks. With Proofpoint's integration with Target Attack Protection (TAP), your administrators can focus on areas of highest risk. And they can ensure maximum effectiveness. This is achieved by running a more prescriptive, impactful security awareness program. One that is based on real risk in their email environment.

This powerful integration provides details about your Very Attacked People(VAPs) and Top Clickers in your organization. And it gives insight into the types of threats they're receiving or engaging with. You can use this information to enroll users into simulations and knowledge assessments to assess risk. Or you can provide education assignments to drive behavior change.

ThreatSim® Phishing Simulations help you understand your organization's susceptibility to a variety of phishing attacks. With thousands of different phishing templates across 13 categories, you can evaluate users on multiple threat types, including:

- Malicious attachments
- Embedded links
- Requests for personal data

We add new templates every week to ensure that the latest attack trends are represented. Our Dynamic Threat Simulation phishing templates are drawn from Proofpoint threat intelligence. It is done along with customer requests and seasonal topics. Proofpoint's real-time sharing of threat intelligence is from the number one 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. They learn:

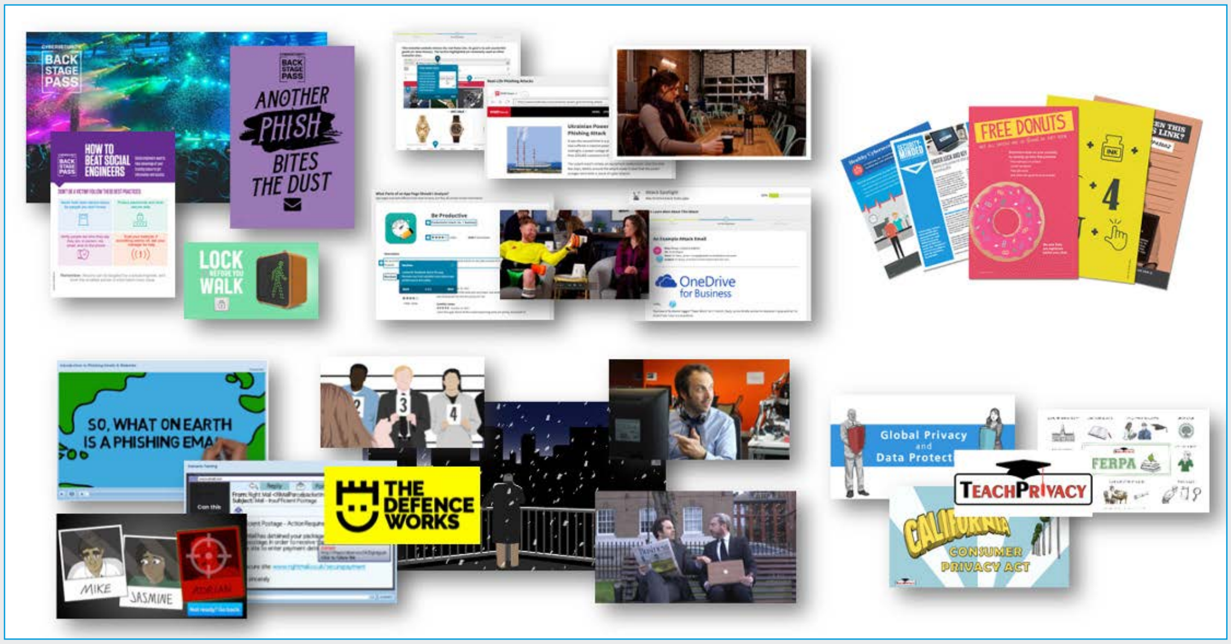
- The purpose of the exercise
- The dangers of real-world attacks
- How to avoid future traps

You can also assign additional education automatically to anyone who falls for a phishing simulation.

You may also want to understand how much your employees know about infected removable memory devices. ThreatSim USB Simulations teach your employees about the dangers of infected USB devices. You can access USB simulations at any time and in any quantity. This feature includes "just-in-time" educational content. It is for users who fall for a simulation.

Simulations however, can only convey specific risk in those threat vectors. CyberStrength® is a powerful knowledge assessment tool. It lets you:

- Assess user vulnerabilities beyond email and USB drives, covering a broad range of critical security issues such as use of mobile devices, social engineering scams, passwords and web browsing.
- Select predefined assessments from a library of hundreds of questions in more than 40 languages and auto-enroll users into appropriate training
- Create custom questions to gauge knowledge of your organization's policies and procedures
- Follow recommendations to reduce your users' risk in assessed topic areas once you establish a baseline


BACK STAGE PASS
ANOTHER PHISH BITES THE DUST
HOW TO BEAT SOCIAL ENGINEERS
LOCK BEFORE YOU WALK
Be Productive
OneDrive for Business
FREE DONUTS
SO, WHAT ON EARTH IS A PHISHING EMA
MIKE
JASMINE
ADRIAN
THE DEFENCE WORKS
Global Privacy and Data Protect
TEACHPRIVACY
FERPA
CALIFORNIA CONSUMER PRIVACY ACT

Change Behavior

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

With the ultimate goal of behavior change in mind, our education is designed to deliver tailored, impactful educational experiences to users. We ensure a program focused first on the areas of high risk. Education can be delivered to Very Attacked People (VAPs) or Top Clickers identified from Proofpoint Targeted Attack Protection (TAP). In addition, education can be focused on users who fail simulations or that score below a certain threshold in a knowledge assessment.

Proofpoint's content leadership has helped millions of users go from risky to ready as a strong line of defense for the organization. Here's how we ensure our content drives behavior change:

Methodology and Consumability

- Utilize proven best practices for adult behavior change
- Make content accessible and searchable through our Content Library
- Enjoy content diversity and assortment with hundreds of training modules and program materials
- Have CISO-guided core curriculums to build necessary skills based on the type of user (privileged, role-based and more)

Global and Multicultural Support

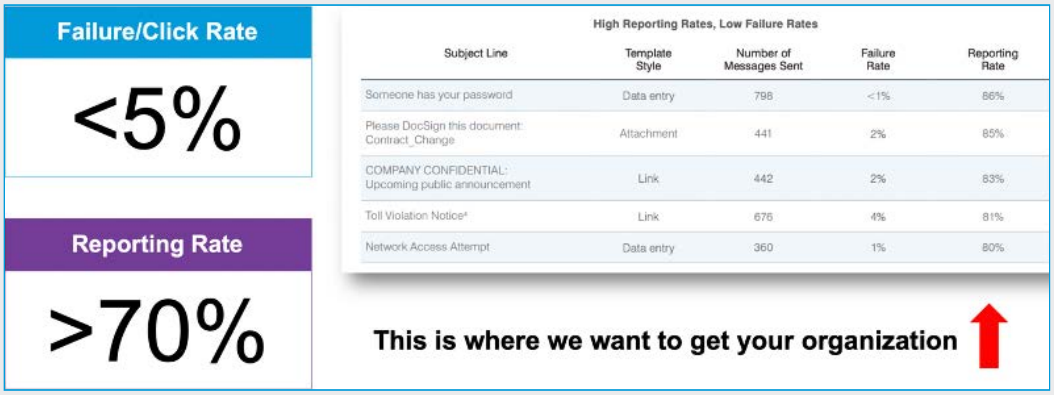
- More than 40 languages and regional references (domains, names, etc.) for all Core Curriculum
- Inclusiveness and diversity of text and images

New Threat Readiness

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

Variety and assortment of content is critical to having content that works for your users. Proofpoint's fast-growing library contains more than 200 training modules. Our hundreds of program materials include PDFs, infographics, videos, memes and more. Our acquisition in May 2020 of The Defence Works and partnership with TeachPrivacy ensure even more content coverage. These different styles can suit any organization's culture. Our best practices, campaigns and curriculums help you put together engaging, multi-channel educational experiences.

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



Failure/Click Rate

<5%

Reporting Rate

>70%

High Reporting Rates, Low Failure Rates

Subject Line	Template Style	Number of Messages Sent	Failure Rate	Reporting Rate
Someone has your password	Data entry	798	<1%	86%
Please DocSign this document: Contract_Change	Attachment	441	2%	85%
COMPANY CONFIDENTIAL: Upcoming public announcement	Link	442	2%	83%
Toll Violation Notice[4]	Link	676	4%	81%
Network Access Attempt	Data entry	360	1%	80%

This is where we want to get your organization ⬆

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

Content Delivery

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

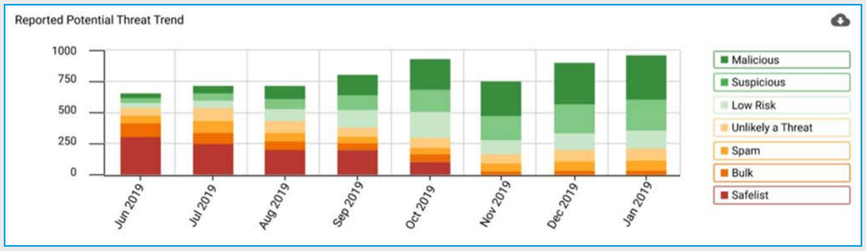
- Easily tailor the training using verbiage, images and questions that are relevant to your users
- Quickly clone and modify modules, lessons and pages to make the necessary changes—all in real-time
- Toggle training modules (with questions) to awareness modules with one switch
- Maintain efficacy with our Learning Science Evaluator as we will keep you on-track, providing feedback if length, amount of content on screen or number of questions in a challenge gets off track

For organizations with their own Learning Management System (LMS) that utilizes SCORM-based files, administrators can easily customize and export training modules to their LMS. They can combine multiple modules into one, and even prioritize the order users can take them.

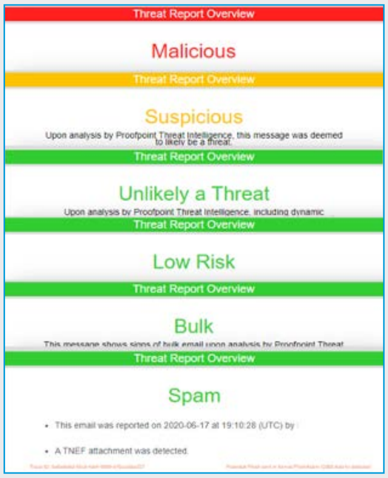
Reduce Exposure

Knowledgeable users report potential threats, which reduces attack surface

Empower your people to report suspicious messages with a single click using our PhishAlarm® email client add-in. After reporting an email, users get instant positive reinforcement in the form of a "thank you" pop-up message. This add-in eliminates the need to get headers and attachments from users who would otherwise forward emails to an abuse mailbox. Typical organizational reporting rates vary between 10-20%. With educated users, successful clients have consistently had more than 70% and sometimes even more than 80% of their users reporting simulated attacks.



Better understanding of user behaviour change with reported message types.



Threat Report Overview

Malicious

Threat Report Overview

Suspicious

Upon analysis by Proofpoint Threat Intelligence, this message was deemed to likely be a threat.

Threat Report Overview

Unlikely a Threat

Upon analysis by Proofpoint Threat Intelligence, including dynamic

Threat Report Overview

Low Risk

Threat Report Overview

Bulk

This message shows signs of bulk email upon analysis by Proofpoint Threat

Threat Report Overview

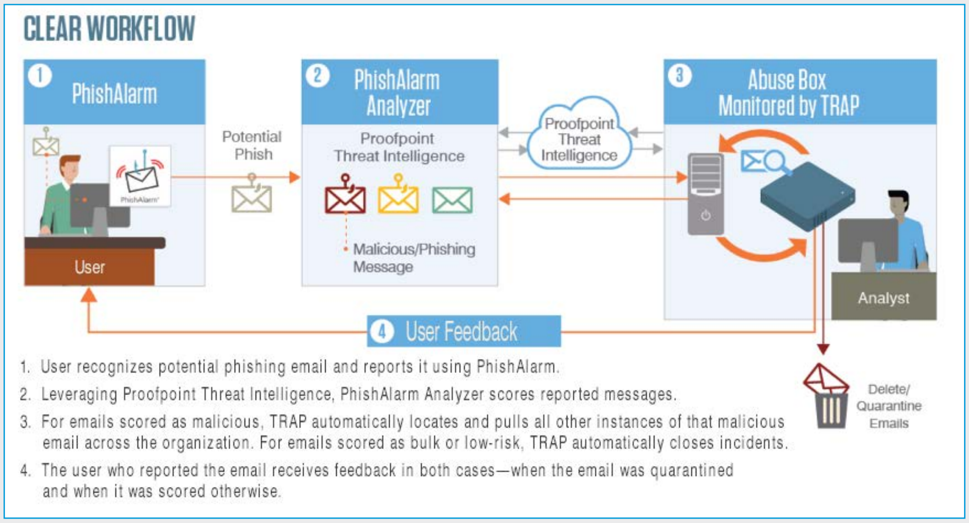
Spam

- This email was reported on 2020-06-17 at 19:10:28 (UTC) by
- A TNEF attachment was detected.

Provide incident response team with actionable information.

But simulated attacks are not risky like real threats in your environment. We have world-class threat intelligence including sandboxing. We'll automatically tell you which user-reported messages are malicious or not with a threat report overview. It includes specific details about what in the message is malicious. This saves your incident response teams time. And it provides insight into how your security awareness program is translating to decreased email-based risk. Our threat intelligence is based on the number one deployed solution across the Fortune 100, Fortune 1000 and Global 2000. It provides industry-leading aggregation and correlation of threat data across email, cloud, network and social media.

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


CLEAR WORKFLOW
1 PhishAlarm
User
Potential Phish
2 PhishAlarm Analyzer
Proofpoint Threat Intelligence
Malicious/Phishing Message
Proofpoint Threat Intelligence
3 Abuse Box Monitored by TRAP
Analyst
4 User Feedback
Delete/ Quarantine Emails

1. User recognizes potential phishing email and reports it using PhishAlarm.
2. Leveraging Proofpoint Threat Intelligence, PhishAlarm Analyzer scores reported messages.
3. For emails scored as malicious, TRAP automatically locates and pulls all other instances of that malicious email across the organization. For emails scored as bulk or low-risk, TRAP automatically closes incidents.
4. The user who reported the email receives feedback in both cases—when the email was quarantined and when it was scored otherwise.

Measure and Adapt

Understand how user behavior change is impacting key outcomes

Our comprehensive reporting helps you understand how user behavior is changing. And it shows how you're benchmarking compared to your peers. You can see employee interactions with:

- Assessments
- Simulated attacks
- Training assignments
- Email reporting and analysis (including dispositions)

Reports let you easily filter data, compare assessments, change measures and set up custom views.

Answer key questions such as:

- Who is most vulnerable to simulated phishing at my organization?
- Where are the knowledge gaps of key security and compliance topics in my user base?
- How well are my users performing in the training?
- How many and what kind of messages are users reporting (malicious, bulk, spam, etc.)?

You can download, export and set up automated delivery of reports to others. This makes it easy for your organization to track insights. And it lets you automatically communicate results to key stakeholders of your program.

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**.