

Proofpoint Security Awareness Training Content

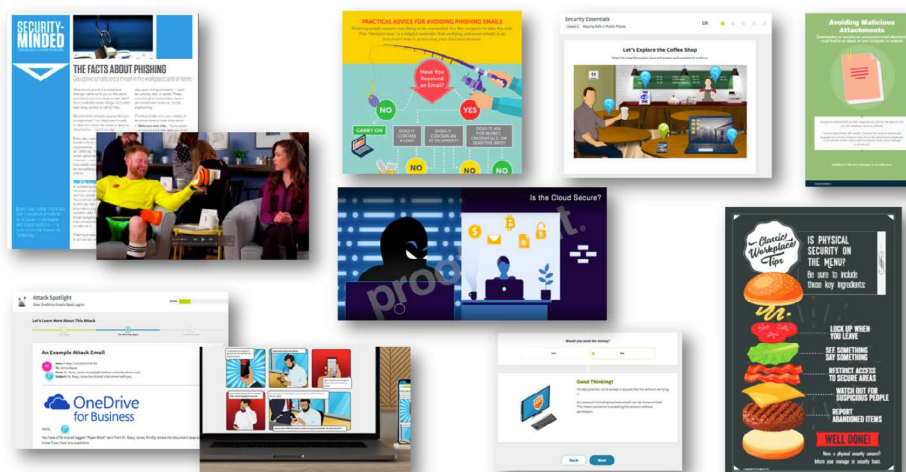
Efficiently Train Employees to Recognize and Avoid Security Risks

KEY BENEFITS

Reduce People-Centric Risk

- Assess users' vulnerabilities with simulated attacks to identify your risk
- Provide on-the-spot training to help avoid future attacks
- Test users' security knowledge
- Drive positive change with easy-to-access training modules
- Localize training for employees all over the world
- Raise security awareness with customizable materials and communications

Proofpoint Security Awareness Training provides training content based on proven learning science principles that improve the effectiveness of security education. Our ThreatSim® Simulated Attacks and CyberStrength® Knowledge Assessments give you a deeper understanding of your people-centric risk. Proofpoint customers across all industries have positive things to say about our training modules. These help you deliver the right training to the right people to create the right response. This ultimately reduces your people-centric risk. We also offer security awareness materials to reinforce the training content.



Proofpoint Security Awareness Training content includes a wide range of training and other resources.

Assessment Content

Understanding where your employees are vulnerable is essential. This information will help you deliver personalized security awareness training and identify broader security risks for your organization. Our ThreatSim Simulated Attacks help you assess how susceptible your users are to real-world threats. These simulated attacks include phishing, USB and text-message attacks. CyberStrength Knowledge Assessments help you gauge how well your employees understand a wide range of key security topics.

THREATSIM SIMULATED PHISHING, USB AND TEXT MESSAGE ATTACKS

Simulated Attack Templates

Assess users on multiple threat types. These include malicious attachments, embedded links, USB attacks and requests for personal data. Choose from thousands of templates in more than 36 languages.

Categories of Templates:

- Cloud
- Commercial
- Consumer
- Corporate
- Proofpoint Threat Intel
- Seasonal
- Text Message (SMS)
- USB
- Vertical

Teachable Moment Landing Pages

Use “just-in-time teaching” the moment an employee interacts with a mock phishing email. These landing pages explain what happened. They also outline the dangers associated with real attacks. And, they offer advice about avoiding future attacks.

Types of Teachable Moments:

- Custom
- Embedded
- Error Messages
- Interactive
- Video

CYBERSTRENGTH KNOWLEDGE ASSESSMENTS

Custom and Predefined Knowledge Assessments

Evaluate users on a wide variety of topics beyond simulated attacks. Choose from more than 400 built-in questions or add your own. You can also choose from 17 predefined knowledge assessments in many different categories.

Predefined Knowledge Assessments:

- 55-question broad assessment
- 33-question broad assessment
- 22-question broad assessment
- GDPR
- Insider Threats
- Online Safety
- Password Protection
- Payment Card Industry
- Phishing
- Personally Identifiable Information (PII)
- Preventing Compromise
- Protected Health Information (PHI)
- Protecting Personal Data
- Securing Your Email Advanced
- Securing Your Email Fundamentals
- Security Safeguards
- Security on the Go

Proofpoint Training Modules

Our customizable, award-winning training modules are available in gaming, interactive and video formats. They are based on learning science principles which are meant to drive changes in behavior. Our modules are derived from Proofpoint threat intelligence to ensure relevancy based on the changing threat landscape.

About the Modules

- The lessons are brief and focused. Modules take only five to 15 minutes to complete on average. This keeps users engaged throughout the training, so they are more likely to learn and retain the content.
- Content is customizable to ensure it's tailored for your users. The self-service Customization Center allows you to edit text, screens, images, questions, answers and even reorder content.
- Users can be auto-enrolled into the training modules from an assessment. This ensures that they're getting the right training at the right time.
- The training modules are designed for mobile devices. Users can take training anytime, anywhere, on any connected device.
- Interactive modules conform to the U.S. Section 508 standard and the Web Content Accessibility Guidelines (WCAG) 2.0 AA standard.
- Employees all over the world can take advantage of the training. Modules are available in more than 35 languages and can be customized for each locale. Content is professionally translated and localized with regional references.

Training Modules

- Avoiding Dangerous Attachments
- Video: Avoiding Dangerous Attachments
- Avoiding Dangerous Links
- Video: Avoiding Dangerous Links
- Beyond Passwords
- Business Email Compromise
- Video: Business Email Compromise
- Awareness Video: Confidential Information
- Attack Spotlight: COVID-19 (Coronavirus) Phishing Scams
- Data Entry Phishing
- Video: Data Entry Phishing
- Data Protection and Destruction
- Attack Spotlight: DocuSign Phishing Campaign
- Awareness Video: Don't be Jan
- Email Protection Tools
- Email Security
- Email Security on Mobile Devices
- Attack Spotlight: Fake OneDrive Emails Steal Logins
- FERPA For Higher Education
- Attack Spotlight: Fraudulent Shipping Notifications
- GDPR in Action
- GDPR Overview
- Healthcare Data Protection
- Healthcare Privacy Data Overview
- Healthcare Privacy Violations
- Awareness Video: How to Report a Phish
- Insider Threat Overview
- Video: Insider Threat Overview
- Introduction to Phishing
- Video: Introduction to Phishing
- Awareness Video: Is the Cloud Secure?
- Awareness Video: Lock Before You Walk – Dr.
- Awareness Video: Lock Before You Walk – Human Resources
- Malicious Insider Threat
- Mitigating Compromised Devices
- Mobile App Permissions
- Mobile App Security
- Mobile Device Security
- Video: Mobile Device Security
- Multi-Factor Authentication (MFA)
- OWASP Fundamentals
- Password Management
- Password Policy
- PCI DSS
- Physical Security
- Video: Physical Security
- PII Fundamentals
- Video: PII Fundamentals
- PII in Action
- Video: PIN and Password Protection
- Protected Health Information (PHI)
- Protecting Against Ransomware
- Safe Social Networking
- Video: Safe Social Networking
- Safer Web Browsing
- Security Beyond the Office
- Security Essentials
- Video: Security Essentials
- Security Essentials (Executive)
- Social Engineering
- Spear-Phishing Threats
- Awareness Video: Think Before You Click (Great Saves)
- Awareness Video: Think Before You Click
- Awareness Video: Think Before You Post (Social Media)
- Travel Security
- Video: Travel Security
- Unintentional Insider Threat
- URL Training
- USB Device Safety

- Awareness Video: Use Caution on Public Wi-Fi
- Awareness Video: What is Email Fraud?
- Awareness Video: Why Your Security Awareness Training Program is Important
- Workplace Security in Action

Partner Training Modules

We work with a handful of leading vendors to expand our variety of content and types of training available. All content is vetted by our learning and development teams to ensure consistent guidance for your users.

- The Defence Works was acquired by Proofpoint in May 2020. It provides a diverse selection of entertaining and humorous content that helps you engage users in new ways.
- Teach Privacy has deep expertise on privacy regulations and requirements. With its rich privacy content, you can tailor privacy and compliance training for your unique challenges and culture.

The Defence Works content

- The Defence Works Video: A Sneaking Suspicion
- The Defence Works Video: A Step Too Far
- The Defence Works Video: Agent Smith
- The Defence Works Video: An Unexpected Call
- The Defence Works: Anti-Fraud and Bribery
- The Defence Works: Anti-Money Laundering
- The Defence Works Video: Backup Bob
- The Defence Works: BEC Scams
- The Defence Works Video: Behind Closed Doors
- The Defence Works Video: Behind Your Back
- The Defence Works Video: Cooking with a Con!
- The Defence Works Video: Deadline Demands
- The Defence Works Video: Don't Bet on It
- The Defence Works Video: Don't Click on That!
- The Defence Works Video: Double "Oh... No"
- The Defence Works Video: Fake It 'Til You Make It
- The Defence Works: Freedom of Information
- The Defence Works: GDPR Awareness (Global)
- The Defence Works: GDPR Awareness (UK)
- The Defence Works: Incident Reporting
- The Defence Works: Insider Threats
- The Defence Works Video: Internet-Enabled Nightmare
- The Defence Works: Introduction to Phishing Emails and Websites
- The Defence Works: Malware & Ransomware
- The Defence Works: Mobile Device Defence
- The Defence Works: Modern Slavery

- The Defence Works Video: Nerves of Steel
- The Defence Works Video: Oh... My Password!
- The Defence Works: PCI DSS
- The Defence Works: Perfect Your Password
- The Defence Works: Personally Identifiable Information
- The Defence Works Video: Phishing Emails in Real Life
- The Defence Works: Physical Security
- The Defence Works Video: Prison Break... In?
- The Defence Works: Privileged Access Awareness
- The Defence Works: Protecting Data
- The Defence Works: Secure Printing
- The Defence Works: Security Beyond the Office
- The Defence Works: Shielding Against Spear Phishing
- The Defence Works Video: Sleepy Security
- The Defence Works Video: So Much Data!
- The Defence Works: Social Engineering
- The Defence Works Video: Social Media Roller Coaster
- The Defence Works: Social Networking
- The Defence Works: Spotting Invoice Scams
- The Defence Works: Surfing the World Wide Web
- The Defence Works Video: Swiped Right Into Trouble
- The Defence Works Video: TAKEOVER: BEC Scams
- The Defence Works Video: TAKEOVER: Digging for Data
- The Defence Works: The Hazards of Hacking
- The Defence Works Video: Under Surveillance
- The Defence Works Video: What Is It, My Child?
- The Defence Works: Working From Home
- The Defence Works: Working From Home (COVID-19)
- The Defence Works: You, Me & Data Protection (GDPR Recap)

TeachPrivacy content

- TeachPrivacy Video: California Health Privacy
- TeachPrivacy: CCPA
- TeachPrivacy: CCPA – Interactive Whiteboard
- TeachPrivacy Video: FERPA (for Higher Education)
- TeachPrivacy: FERPA (K-12)
- TeachPrivacy: FERPA – Interactive Whiteboard
- TeachPrivacy: FTC Red Flags
- TeachPrivacy Video: GDPR
- TeachPrivacy: GDPR – Interactive Whiteboard
- TeachPrivacy: GLBA
- TeachPrivacy: Global Privacy and Data Protection
- TeachPrivacy: HIPAA – Interactive Whiteboard
- TeachPrivacy Video: HIPAA Overview
- TeachPrivacy Video: HIPAA Privacy for Covered Entities
- TeachPrivacy Video: Malware

- TeachPrivacy Video: PCI
- TeachPrivacy: Privacy Training for Federal Government Contractors
- Teach Privacy: Secure Workplace: Game
- TeachPrivacy: Texas Health Privacy
- TeachPrivacy: The Ransomware Attack

Security Awareness Materials

We offer a wide selection of awareness modules, videos, posters, images, newsletters, articles, infographics and more to reinforce your training initiatives. These are designed to make cybersecurity an ongoing topic of conversation with your users. By keeping security top of mind, you can help reduce your organization's risk.

- You can customize most awareness materials with your organization's logo. Access original files from the Security Awareness Materials portal.
- Many of our awareness materials are available in 20 languages.

Attack Spotlight: Teach your users about current threats. This timely content comes from real-world phishing attacks, techniques and lures being seen by Proofpoint threat intelligence.

- COVID-19 (Coronavirus)
- DocuSign Phishing
- Domain Fraud
- Fake Browser Updates
- Fraudulent Shipping Notifications
- Look-Alike Websites Trick Users
- Microsoft Office 365 Credential Phishing
- OneDrive Phishing Campaign
- Phishing Campaign Delivers Dangerous Trojan
- Scammers Mimic Real Banking Emails

Threat Alerts: Quickly alert your users to specific attacks being seen in the wild by Proofpoint threat intelligence.

- COVID-19 Credential Phishing (U.S. Retailers)
- COVID-19 Phish Spreading Malware (U.S. Infrastructure)
- WebEx Credential Phishing Lures
- Zoom Credential Phishing Lures
- Zoom Phishing Attacks Spread Malware
- More Every Week

Awareness Videos: Introduce your employees to the importance of security awareness with these videos.

- Make a Great Save series
- Don't Let Thieves In series
- Don't Be a Jan series
- Is the Cloud Secure?

- What Are BEC Attacks?
- What Is Email Fraud?
- What Is Phishing?
- What Is Ransomware?
- What Is Smishing?
- What Is the IoT?
- What Is Vishing?
- Why Is your Security Training Important?

Infographics

- Business Email Compromise Attacks
- Internet of Things
- Phishing Decision Tree
- Phishing: A Scammer's Sinister Scheme (Regular and Expanded)
- Tax-Related Schemes
- Understanding Ransomware
- And More

Newsletters and Articles

- Security-minded newsletters and articles explaining many different topics: back to school, dangerous links and attachments, holiday shopping, insider threats, passwords, phishing, physical security, travel tips and more

Posters

- Avoiding Malicious Attachments
- Be Smart About Mobile Security
- Destination Unknown URL Security
- Dangerous USB Devices
- Is Physical Security on the Menu?
- Not All Offers Are as Sweet as They Seem
- And More

Miscellaneous

- Artwork and direction to create additional content
- "Cybersecurity Consequences" game
- "Lock Before You Walk" post-it notes
- Memes
- Postcards
- Word search
- And More

Program Materials

For a program to be successful, everyone involved needs to understand why they are participating and what is expected of them. That's why our security awareness programs include expert guidance for administrators on how to most effectively run their program. We also provide targeted communications to key stakeholders and users. Our program materials are organized into four categories:

- Best Practices
- Keys to Success
- Campaigns
- Presentations

This information helps your program administrators build trust and foster a culture of security awareness.

Best Practices: Our best practices documentation helps program administrators drive the most effective behavior change. It doesn't matter if your program is new or has been in place for a while. This content provides information about schedules, best practices and suggested plans for running a program.

Campaigns: Campaigns simplify administration and help you create curated user experiences. They include all the internal communication resources and content you need to deliver a multichannel security awareness initiative in your organization.

Keys to Success: These podcasts, webinars, research and other content are created for your administrators. This helps them explain the value of security awareness training to key audiences, get buy-in for more training, guide consequence model discussions and more.

Presentations: These scripted and pre-recorded presentations cover various topics such as phishing, identity theft and reporting suspicious emails. Administrators can use these for in-person or online training sessions.

LEARN MORE

Try demo versions of our training modules and view our security awareness materials at <https://www.proofpoint.com/us/resources/try-security-awareness-training>.

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ: PFPT) is a leading cybersecurity 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.

©Proofpoint, Inc. Proofpoint is a trademark of Proofpoint, Inc. in the United States and other countries. All other trademarks contained herein are property of their respective owners. Proofpoint.com