SOLUTION BRIEF

Proofpoint Security Awareness and Training Content

Change User Behaviour to Reduce Risk

KEY FEATURES

Content Library

Locate content bases on threats, users, regions and formats

Foundational Curriculums

CISO/SME driven learning paths to fast track implementation and the onboarding of new users

User Assessment

Understand the strengths and weaknesses of users, groups and departments

Training Modules

A broad variety of topics and formats to cover security and privacy and also accommodate user preferences

Content Customisation and Delivery

Ensure a personalised learning experience for your users and deliver content via your Learning Management System (LMS) if desired.

Security Awareness Materials

Ready to use materials facilitate effective and efficient awareness campaigns and timely Threat Alerts and Reports

Translations

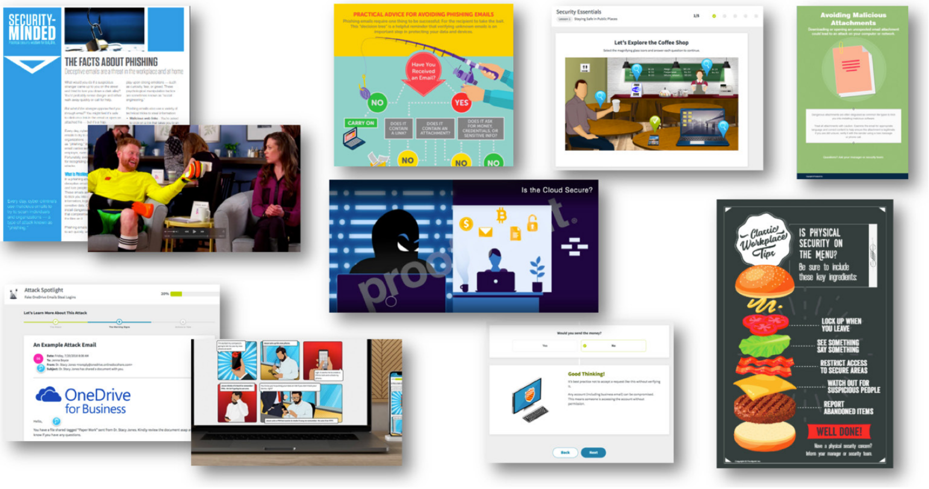
40 translations for foundational curriculum and a minimum of six for all content

Simulations

A full library of simulated threats to help assess user recognition of social engineering attacks

Proofpoint Security Awareness Training (PSAT) provides proven content to your employees to drive behavioural change. Our solutions enable you to deliver the right training to the right people at the right time. This ensures the right response to security and privacy threats and requirements. With our solutions, you can:

- Assess and train users
- Access robust materials for security awareness campaigns
- Automate reporting
- Monitor suspicious emails



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

Foundational curriculum, learning paths and translations

Accelerate behaviour change with CISO/SME guided curriculums and learning paths. Foundational curriculums provide essential knowledge for users and help them progress from basic to advanced proficiency. Coupled with role-specific learning paths, organisations can leverage expert guidance to fast track user learning and training administration.

All foundational courses are translated into more than 40 languages and additional courses and awareness materials are available in more than six languages.

Assessment content: Understand what your users need

When it comes to security and privacy practices, it’s important to understand your employee knowledge gaps. We help you deliver personalised security awareness training and identify broader security risks for your organisation.

Our ThreatSim Simulated Attacks help you assess how susceptible your employees are to real-world threats. These simulated attacks include phishing and USB attacks. With CyberStrength Knowledge Assessments you can gauge your employees’ knowledge on a wide range of key security topics.

THREATSIM SIMULATED PHISHING AND USB ATTACKS

Simulated Attack Templates

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

Categories of Templates:

- Cloud
- Commercial
- Consumer
- Corporate
- Proofpoint Threat Intel
- Seasonal
- USB
- Vertical

Teachable Moment Landing Pages

You can use “just-in-time teaching” the moment an employee interacts with a mock phishing email. Our 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

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

Predefined Knowledge Assessments:

- 55, 33 and 22-question broad assessments
- 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 flexible, award-winning training modules are available in gaming, interactive and video formats. They are based on learning science principles that lead to changes in behaviour. 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 customisable 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 on the training modules from an assessment. This ensures that they're getting the right training at the right time.
- The training modules are mobile friendly, easily accessible and conform to the U.S. Section 508 standard and the Web Content Accessibility Guidelines (WCAG) 2.0 AA standard.

Training Modules Topics

- Application Security
- Anti-Fraud and Bribery
- Anti-Money Laundering
- Avoiding Dangerous Attachments
- Avoiding Dangerous Links
- Business Email Compromise
- Compromised Devices
- Data Protection and Destruction
- Email Security
- Email Security on Mobile Devices
- FERPA
- GDPR
- Healthcare
- Insider Threats
- Phishing
- Malware
- Mobile Security
- Passwords
- PCI
- Physical Security
- PII and Personal Data Protection
- Privileged Access Awareness
- Ransomware
- Role-based modules for customer service, finance and management
- Safe Social Networking
- Safe Web Browsing
- Secure Printing
- Security Beyond the Office
- Security Essentials
- Travel Security
- URL Training
- USB Device Safety
- Working From Home
- Workplace Security in Action
- Video: Workplace Security in Action

TeachPrivacy training modules

We work with TeachPrivacy 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.

Teach Privacy are experts on privacy regulations and requirements. With its rich privacy content, you can tailor privacy and compliance training to fit your unique challenges and culture.

TeachPrivacy Topics

- California Health Privacy
- CCPA
- FERPA
- FTC Red Flags
- GDPR
- GLBA
- HIPAA
- Malware and Privacy
- PCI
- Privacy for Federal Government Contractors
- Texas Health Privacy
- Ransomware

Content customisation and delivery

With our self-service Customization Center, you can improve content relevance with your users in mind. 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. Modules can even be toggled from training modules (with questions) to awareness modules with one switch.

To maintain efficacy our Learning Science Evaluator will keep you on-track, providing feedback. For example, if length, amount of content on screen, or number of questions in a challenge gets off track we will let you know.

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

Security awareness materials

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

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

Attack Spotlights and Threat Alerts

With our market leading threat intelligence, we help you understand who will be attacked and how, and ensure they receive the appropriate training. Our continuous threat intelligence also gives you the best view of new and emerging threats so that training and awareness can immediately prepare users to recognise and avoid new dangers.

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

- COVID-19 (Coronavirus)
- DocuSign Phishing
- Domain Fraud
- Dridex
- Fake Browser Updates
- Fake OneDrive Emails Steal Logins
- 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
- Malicious Cloud Applications

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 engaging and entertaining videos. Here is a sample of over 50 videos:

- Awareness Video: Think Before You Click (Great Saves)
- Awareness Video: Is the Cloud Secure?
- Awareness Video: Use Caution on Public Wi-Fi
- The Defence Works Video: Not Particularly High Tech
- The Defence Works Video: Oh… My Password!
- The Defence Works Video: Swiped Right Into Trouble
- 60 Seconds to Better Security: What is Smishing?
- 60 Seconds to Better Security: What is Phishing?
- 60 Seconds to Better Security: What is BEC?
- And More

Infographics: Use these sparklers for reinforcing fundamentals of safe computing:

- 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: Keep the message clear and reinforce learning.

- 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

Programme materials

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

- Best Practices
- Keys to Success
- Campaigns

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

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

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 organisation.

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, gain employee buy-in for further training, guide consequence model discussions and more. Scripted and pre-recorded presentations that cover various topics such as phishing, identity theft and social engineering are available. System administrators can make use of these presentations 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/uk/resources/try-security-awareness-training**.