

# Proofpoint Security Awareness Training-Inhalte:

## Das Anwenderverhalten ändern, um Risiken zu minimieren

### WICHTIGE FUNKTIONEN

#### Content-Bibliothek

Suche nach Inhalten basierend auf Bedrohungen, Anwendern, Regionen und Formaten

#### Grundlagenschulungen

CISO/SME-orientierte Lernpfade, um die Implementierung zu beschleunigen und das Onboarding neuer Anwender zu vereinfachen

#### Beurteilung der Anwender

Einblick in die Stärken und Schwächen von Anwendern, Gruppen und Abteilungen

#### Schulungsmodule

Vielfältige Themen und Formate, die zahlreiche Sicherheits- und Datenschutzthemen sowie unterschiedliche Präferenzen der Anwender abdecken

#### Inhaltsanpassung und Bereitstellung

Sorgen Sie für ein personalisiertes Lernerlebnis für Ihre Anwender und stellen Sie, falls gewünscht, Inhalte über Ihr Lern-Management-System (LMS) bereit

#### Materialien zur Steigerung des Sicherheitsbewusstseins

Sofort einsetzbare Materialien unterstützen effektive und effiziente Kampagnen zur Sensibilisierung sowie schnell verfügbare Bedrohungswarmmeldungen und Berichte

#### Übersetzungen

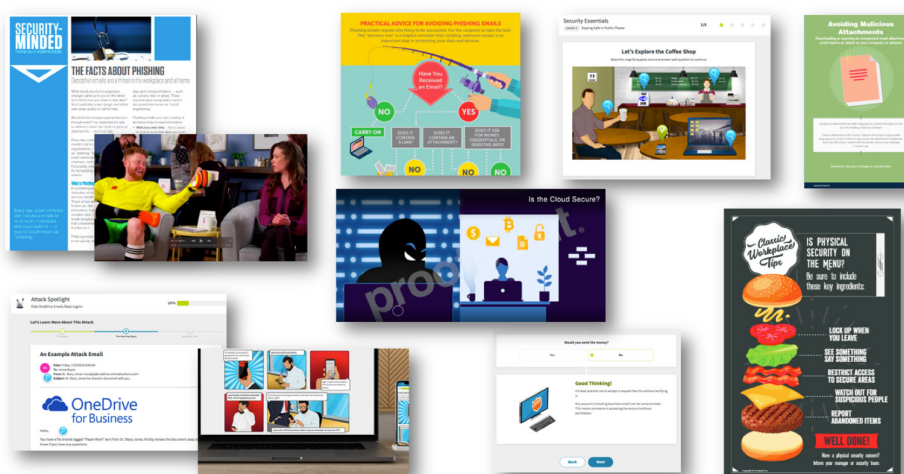
Grundlagenschulungen in 40 Sprachen und alle Inhalte in mindestens 6 Sprachen verfügbar

#### Simulationen

Vollständige Bibliothek mit simulierten Bedrohungen, mit denen Sie testen können, wie gut Ihre Anwender Social-Engineering-Angriffe erkennen

Die Inhalte von Proofpoint Security Awareness Training (PSAT) haben sich dabei bewährt, riskantes und unbedachtes Verhalten von Anwendern messbar zu ändern. Zudem bieten unsere Lösungen die Möglichkeit, den richtigen Personen zum richtigen Zeitpunkt die richtigen Schulungen bereitzustellen, sodass Ihre Anwender bei sicherheits- oder datenschutzbezogenen Bedrohungen richtig reagieren und die Richtlinien einhalten. Unsere Lösungen bieten folgende Vorteile:

- Bewertung und Schulung von Anwendern
- Bereitstellung informativer Materialien für Kampagnen zur Steigerung des Sicherheitsbewusstseins
- Automatische Erstellung von Berichten
- Meldung verdächtiger E-Mails



Die Proofpoint Security Awareness Training-Inhalte umfassen eine große Bandbreite an Schulungsmaterialien und anderen Ressourcen.

## Grundlegendes Curriculum, Lernpfade und Übersetzungen

Beschleunigen Sie Verhaltensänderungen mit CISO/SME-geführten Lehrplänen und Lernpfaden. Grundlegende Lehrpläne vermitteln grundlegendes Wissen und helfen ihnen, von grundlegenden zu fortgeschrittenen Kenntnissen zu gelangen. In Verbindung mit rollenspezifischen Lernpfaden können Unternehmen die Anleitung von Experten nutzen, um das Lernen der Anwender und die Trainingsverwaltung zu beschleunigen.

Alle Basiskurse sind in mehr als 40 Sprachen übersetzt und zusätzliche Kurse und Awareness-Materialien sind in mehr als sechs Sprachen verfügbar.

## Inhalt der Wissenstests: Verstehen, was Ihre Anwender benötigen

Damit Sie geeignete Sicherheits- und Datenschutz-Praktiken etablieren können, müssen Sie die Wissenslücken Ihrer Mitarbeiter kennen. Wir unterstützen Sie dabei, personalisierte Sicherheitsschulungen bereitzustellen und grundlegende Sicherheitsrisiken für Ihr Unternehmen zu identifizieren.

Mit unseren ThreatSim-Simulationen, die als Phishing- und USB-Angriffe umgesetzt werden können, wird die Anfälligkeit Ihrer Mitarbeiter für reale Bedrohungen getestet, während die CyberStrength-Wissenstests das Wissen Ihrer Anwender über wichtige Sicherheitsthemen bewerten.

### SIMULIERTE THREATSIM-ANGRIFFE: PHISHING UND USB

#### Vorlagen für simulierte Angriffe

Testen Sie, wie wahrscheinlich Ihre Anwender verschiedenen Bedrohungstypen auf den Leim gehen, zum Beispiel schädliche Anhänge öffnen, auf schadhafte Links klicken, infizierte USB-Sticks verwenden und Anfragen zur Weitergabe personenbezogener Daten Folge leisten. Dabei können Sie aus tausenden Vorlagen in mehr als 36 Sprachen wählen.

#### Vorlagenkategorien:

- Cloud
- Werbung
- Verbraucherbezogen
- Unternehmensbezogen
- Proofpoint-Bedrohungsdaten
- Saisonal
- USB
- Branchenbezogen

#### Landing Pages mit Lerneffekt

Sie können „Just-in-Time-Teaching“ in dem Moment einsetzen, in dem ein Mitarbeiter mit einer fingierten Phishing-E-Mail interagiert. Diese Landing Pages erklären, was passiert ist. Sie weisen auch auf die Gefahren hin, die mit echten Angriffen verbunden sind. Zudem bieten sie Ratschläge zur Vermeidung zukünftiger Angriffe.

#### Arten von lehrreichen Momenten:

- Individuell
- Eingebettet
- Fehlermeldungen
- Interaktiv
- Video

### CYBERSTRENGTH-WISSENSTESTS

#### Individuell erstellte und vordefinierte Wissenstests

Testen Sie das Wissen Ihrer Anwender jenseits der simulierten Angriffe. Wählen Sie aus mehr als 400 bereits im System hinterlegten Fragen oder fügen Sie eigene hinzu. Außerdem stehen Ihnen 17 vordefinierte Wissenstests in vielen verschiedenen Kategorien zur Verfügung.

#### Vordefinierte Wissenstests:

- Allgemeine Tests mit 55, 33 und 22 Fragen
- Datenschutz-Grundverordnung (DSGVO)
- Bedrohungen durch Insider
- Online-Sicherheit
- Kennwortschutz
- Zahlungskartendaten
- Phishing
- Personenbezogene Daten
- Verhinderung von Kompromittierungen
- Geschützte Gesundheitsdaten
- Schutz personenbezogener Daten
- Absicherung Ihrer E-Mails (für Fortgeschrittene)
- Absicherung Ihrer E-Mails (Grundlagen)
- Sicherheitsmaßnahmen
- Sicherheit unterwegs

## Proofpoint-Schulungsmodule

Unsere flexiblen, preisgekrönten Schulungsmodule umfassen Videos, Interaktionen und Gamification-Elemente. Sie wurden mithilfe wissenschaftlich bestätigter Lernprinzipien entwickelt und sind darauf ausgelegt, das Verhalten nachhaltig zu verändern. Zudem basieren sie auf Proofpoint-Bedrohungsdaten, um sicherzustellen, dass sie in Anbetracht der sich stetig weiterentwickelnden Bedrohungslandschaft immer höchst relevant sind.

### Informationen zu den Modulen

- Alle Lektionen sind kurz gehalten und erfordern die volle Konzentration des Lernenden. Es sind jeweils nur 5 bis 15 Minuten erforderlich. Dadurch bleiben die Anwender während der Schulung aufmerksam. Zudem ist es wahrscheinlicher, dass sie die Schulungsinhalte nicht wieder vergessen.
- Der Inhalt kann für Ihre Anwender angepasst werden. Mittels des Customization Centers können Sie Text, Bilder, Fragen, Antworten und die Reihenfolge der Inhalte selbst ändern.
- Anwendern können im Anschluss an einen Test automatisch Schulungsmodule zugewiesen werden. So wird gewährleistet, dass die richtigen Personen zum richtigen Zeitpunkt die richtigen Schulungen erhalten.
- Schulungsmodule sind für Mobilgeräte geeignet und für leichte Zugänglichkeit optimiert. Sie entsprechen dem Standard U.S. Section 508 sowie den internationalen Web Content Accessibility Guidelines (WCAG) 2.0 AA.

### Themen der Schulungsmodule

- Application Security (Anwendungssicherheit)
- Anti-Fraud and Bribery (Schutz vor Betrug und Bestechung)
- Anti-Money Laundering (Schutz vor Geldwäsche)
- Avoiding Dangerous Attachments (Vermeidung gefährlicher Anhänge)
- Avoiding Dangerous Links (Vermeidung gefährlicher Links)
- Business Email Compromise (BEC, auch Chefmasche genannt)
- Compromised Devices (Kompromittierte Geräte)
- Data Protection and Destruction (Datensicherheit und Datenzerstörung)
- Email Security (E-Mail-Sicherheit)
- Email Security on Mobile Devices (E-Mail-Sicherheit für Mobilgeräte)
- FERPA
- GDPR (DSGVO)
- Healthcare (Gesundheitswesen)
- Insider Threats (Bedrohungen durch Insider)
- Phishing
- Malware
- Mobile Security
- Passwords (Kennwörter)
- PCI
- Physical Security (Physische Sicherheit)
- PII and Personal Data Protection (Schutz für personenbezogene und persönliche Daten)
- Privileged Access Awareness (Sensibilisierung für privilegierte Zugriffe)

- Ransomware
- Rollenbasierte Module für Kundendienst, Finanzabteilung und Management
- Safe Social Networking (Sichere Nutzung sozialer Netzwerke)
- Safe Web Browsing (Sicheres Surfen im Web)
- Secure Printing (Sicheres Drucken)
- Security Beyond the Office (Sicherheit jenseits des Büros)
- Security Essentials (Grundlegende Sicherheit)
- Travel Security (Sicherheit auf Reisen)
- URL Training (URL-Schulung)
- USB Device Safety (USB-Gerätesicherheit)
- Working From Home (Arbeit im Home Office)
- Workplace Security in Action (Arbeitsplatzsicherheit in der Praxis)
- Video: Arbeitsplatzsicherheit in der Praxis

## TeachPrivacy-Schulungsmodule

Wir arbeiten mit TeachPrivacy zusammen, um die Bandbreite und Vielfalt der verfügbaren Schulungen zu erweitern. Alle Inhalte wurden von unseren Schulungs- und Entwicklungs-Teams überprüft.

TeachPrivacy verfügt über umfassende Erfahrung bei Vorschriften und Anforderungen in Bezug auf Datenschutz. Sie können die umfangreichen Inhalte der Datenschutz- und Compliance-Schulungen an Ihre individuellen Anforderungen und Ihre Kultur anpassen.

### Themen von TeachPrivacy

- California Health Privacy (Datenschutz bei Gesundheitsdaten in Kalifornien)
- CCPA
- FERPA
- FTC Red Flags (Warnzeichen der Federal Trade Commission)
- GDPR (DSGVO)
- GLBA
- HIPAA
- Malware and Privacy (Malware und Datenschutz)
- PCI
- Privacy for Federal Government Contractors (Datenschutz für Vertragspartner von Bundesbehörden)
- Texas Health Privacy (Datenschutzbestimmungen im Gesundheitswesen in Texas)
- Ransomware

## Inhaltsanpassung und -bereitstellung

Mit unserem Self-Service Customization Center können Sie die Relevanz der Inhalte mit Blick auf Ihre Anwender bewahren. Einfaches Anpassen der Schulung mit Worten, Bildern und Fragen, die für Ihre Anwender relevant sind. Klonen und modifizieren Sie schnell Module, Lektionen und Seiten, um die notwendigen Änderungen vorzunehmen – alles in Echtzeit. Module können sogar mit einem „Schalter“ von Schulungsmodulen (mit Fragen) auf Awareness-Module umgeschaltet werden.

Um die Wirksamkeit aufrechtzuerhalten, hält unser Learning Science Evaluator Sie auf dem Laufenden und gibt Feedback. Wenn zum Beispiel Länge, Menge des Inhalts auf dem Bildschirm oder die Anzahl der Fragen in einer Challenge von der Norm abweicht, lassen wir Sie das wissen.

Bei Unternehmen, die mit einem eigenen Learning Management System (LMS) arbeiten, welches SCORM-basierte Dateien verwendet, können deren Administratoren einfach Schulungsmodule anpassen und in ihr LMS exportieren. Sie können mehrere Module zu einem zusammenfassen und sogar die Reihenfolge festlegen, in der Benutzer sie absolvieren sollen.

## Materialien zur Steigerung des Sicherheitsbewusstseins

Wir bieten eine große Bandbreite an Modulen, Videos, Postern, Bildern, Newslettern, Artikeln, Infografiken und anderen Materialien zur Steigerung des Sicherheitsbewusstseins, die die Wirkung Ihrer Schulungsprogramme verstärken und so gestaltet sind, dass Cybersicherheit für Ihre Endnutzer ein ständig präsent Thema ist. Wenn sich Ihre Mitarbeiter dieser Gefahren stets bewusst sind, können Sie die Risiken für Ihr Unternehmen reduzieren.

- Sie können die meisten Materialien zur Steigerung des Sicherheitsbewusstseins mit dem Logo Ihres Unternehmens ergänzen. Die Originaldateien können von unserem Portal heruntergeladen werden.
- Viele unserer Materialien sind in 20 Sprachen verfügbar.

### Attack Spotlight und Warnmeldungen zu Bedrohungen

Basierend auf unseren marktführenden Bedrohungsdaten können Sie ein besseres Verständnis dafür entwickeln, wer in Ihrem Unternehmen wie angegriffen wird. Außerdem können wir gewährleisten, dass die betreffenden Personen entsprechende Schulungen erhalten. Zudem erhalten Sie dank der kontinuierlich bereitgestellten Bedrohungsdaten einen optimalen Einblick in neue und sich ausbreitende Bedrohungen. Dadurch können Sie die Anwender mit Schulungen und Sensibilisierungsmaßnahmen sofort darauf vorbereiten, neue Gefahren zu erkennen und zu vermeiden.

**Attack Spotlight:** Schulen Sie Ihre Anwender mit diesen monatlich veröffentlichten Inhalten zu aktuellen Themen, die auf realen Phishing-Angriffen, Techniken und Ködern aus den Proofpoint-Bedrohungsdaten basieren.

- COVID-19 (Coronavirus)
- DocuSign Phishing (DocuSign-Phishing)
- Domain Fraud (Domänenbetrug)
- Dridex
- Fake Browser Updates (Gefälschte Browser-Updates)
- Fake OneDrive Emails Steal Logins (Gefälschte OneDrive-E-Mails stehlen Login-Daten)
- Fraudulent Shipping Notifications (Gefälschte Versandbenachrichtigungen)

- Look-Alike Websites Trick Users (Doppelgänger-Websites täuschen Anwender)
- Microsoft Office 365 Credential Phishing (Anmeldedaten-Phishing bei Microsoft 365 (Office 365))
- OneDrive Phishing Campaign (OneDrive-Phishing-Kampagne)
- Phishing Campaign Delivers Dangerous Trojan (Phishing-Kampagne überträgt gefährlichen Trojaner)
- Scammers Mimic Real Banking Emails (Betrüger imitieren reale Bank-E-Mails)
- Malicious Cloud Applications (Schädliche Cloud-Anwendungen)

**Bedrohungswarmmeldungen:** Warnen Sie Ihre Anwender schnell zu bestimmten Angriffen, die von den Proofpoint-Bedrohungsdaten erfasst wurden.

- COVID-19 Credential Phishing (U.S. Retailers) (COVID-19-Anmeldedaten-Phishing: US-Einzelhändler)
- COVID-19 Phish Spreading Malware (U.S. Infrastructure) (COVID-19-Phishing, das Malware verbreitet: US-Infrastruktur)
- WebEx Credential Phishing Lures (Köder für Anmeldedaten-Phishing bei WebEx)
- Zoom Credential Phishing Lures (Köder für Anmeldedaten-Phishing bei Zoom)
- Zoom Phishing Attacks Spread Malware (Zoom-Phishing-Angriffe, die Malware verbreiten)
- Wöchentlich neue Inhalte

**Awareness-Videos:** Verdeutlichen Sie Ihren Mitarbeitern mit diesen ansprechenden und unterhaltsamen Videos den Grund, warum ein hohes Sicherheitsbewusstsein sowohl für Ihr Unternehmen aber auch für sie persönlich so wichtig ist. Proofpoint Security Awareness Training bietet aktuell eine Auswahl von mehr als 50 Videos:

- Awareness-Video: Think Before You Click (Great Saves) (Erst denken, dann klicken (Eine starke Abwehr))
- Awareness-Video: Is the Cloud Secure? (Ist die Cloud sicher?)
- Awareness-Video: Use Caution on Public Wi-Fi (Vorsicht bei öffentlichen WLANs)
- The Defence Works-Video: Not Particularly High Tech (Nicht wirklich Hightech)
- The Defence Works-Video: Oh... My Password! (Oh, mein Kennwort!)
- The Defence Works-Video: Swiped Right Into Trouble (Ein Wisch direkt ins Unglück)
- 60 Seconds to Better Security: What Is Smishing? (60 Sekunden für mehr Sicherheit: Was ist Smishing?)
- 60 Seconds to Better Security: What is Phishing? (60 Sekunden für mehr Sicherheit: Was ist Phishing?)
- 60 Seconds to Better Security: What is BEC? (60 Sekunden für mehr Sicherheit: Was ist BEC?)
- und mehr

**Infografiken:** Festigen Sie mit diesen eindrücklichen Materialien die Grundlagen für sicheres Arbeiten im Cyberzeitalter:

- Business Email Compromise-Angriffe
- Internet of Things (Internet der Dinge)
- Phishing Decision Tree (Phishing-Entscheidungsbaum)
- Phishing: A Scammer's Sinister Scheme (Phishing: Eine gemeine Taktik von Betrügern) (normale und erweiterte Version)
- Tax-Related Schemes (Steuerbezogene Taktiken)
- Grundlegendes zu Ransomware
- und mehr

#### Newsletter und Artikel

- Sicherheitsorientierte Newsletter und Artikel zu verschiedenen Themen: gefährliche Links und Anhänge, Bedrohungen durch Insider, Kennwörter, Phishing, Physische Sicherheit, Sicherheit auf Reisen und mehr

**Poster:** Sorgen Sie dafür, dass die Botschaft immer sichtbar ist und gelerntes Wissen festigt.

- Vermeidung schädlicher Anhänge
- Be Smart About Mobile Security (Optimale Mobilgeräte-Sicherheit)
- URL-Ziel unbekannt
- Dangerous USB Devices (Gefährliche USB-Geräte)
- Is Physical Security on the Menu? (Physische Sicherheit à la carte?)
- Not All Offers Are as Sweet as They Seem (Nicht alle Angebote sind wirklich süß)
- und mehr

#### Verschiedenes

- Grafiken und Anleitung zur Erstellung weiterer Inhalte
- Spiel: „Cybersecurity Consequences“ (Folgen von Cybersicherheit)
- Notizzettel: „Lock Before You Walk“ (Schließen Sie vor dem Verlassen des Tisches alles ein)
- Meme
- Postkarten
- und mehr

## Materialien zum Schulungsprogramm

Damit ein Programm erfolgreich sein kann, müssen alle Beteiligten verstehen, warum sie teilnehmen und was von ihnen erwartet wird. Deshalb enthält unsere Security Awareness Training-Lösung auch umfangreiche Materialien für Administratoren, sodass diese die Programme zur Steigerung des Sicherheitsbewusstseins in ihrem Unternehmen höchst effektiv umsetzen können. Zudem bieten wir gezielte Kommunikation für wichtige Verantwortliche und Anwender. Unsere Materialien zum Programm sind in mehrere Kategorien gruppiert:

- Bewährte Methoden
- Schlüssel zum Erfolg
- Kampagnen

Mit diesen Informationen können Ihre Programm-Administratoren Vertrauen aufbauen und eine sicherheitsbewusste Kultur pflegen.

**Bewährte Methoden:** Unsere Dokumentation zu bewährten Methoden unterstützt Programm-Administratoren bei der Durchsetzung möglichst effektiver Verhaltensänderungen. Ganz gleich, ob Ihr Programm neu eingerichtet wird oder bereits eine Weile läuft, finden Sie hier Informationen zu Zeitplänen, bewährten Methoden sowie Empfehlungen zur Programmdurchführung.

**Kampagnen:** Unsere Kampagnen vereinfachen die Verwaltung und unterstützen Sie bei der Erstellung kuratierter Anwendererlebnisse. Sie enthalten alle internen Kommunikationsressourcen und Inhalte, mit denen Sie Programme zur Steigerung des Sicherheitsbewusstseins in Ihrem Unternehmen auf mehreren Kanälen bereitstellen können.

**Schlüssel zum Erfolg:** Diese Podcasts, Webinare, Forschungs- und andere Inhalte sind für Ihre Administratoren gedacht und helfen dabei, die Vorteile der Schulungen zur Sensibilisierung für wichtige Zielgruppen zu verdeutlichen, Unterstützung für weitere Schulungen zu erhalten, Gespräche zu Konsequenzmodellen zu führen usw. Diese vorab aufgezeichneten Präsentationen decken verschiedene Themen ab, zum Beispiel Phishing, Identitätsdiebstahl und Social Engineering. Administratoren können sie für persönliche und Online-Schulungen nutzen.

## WEITERE INFORMATIONEN

Testen Sie Demoversionen unserer Schulungsmodule und sehen Sie sich unsere Materialien zur Steigerung des Sicherheitsbewusstseins unter <https://www.proofpoint.com/de/resources/try-security-awareness-training> an.

#### INFORMATIONEN ZU PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT) ist ein führendes Unternehmen für Cybersicherheit und Compliance. Im Fokus steht für Proofpoint dabei der Schutz der Mitarbeiter, denn diese bedeuten für ein Unternehmen sowohl das größte Kapital als auch das größte Risiko. Mit einer integrierten Suite von Cloud-basierten Lösungen unterstützt Proofpoint Unternehmen auf der ganzen Welt dabei, gezielte Bedrohungen zu stoppen, ihre Daten zu schützen und ihre IT-Anwender für Risiken von Cyberangriffen zu sensibilisieren. Führende Unternehmen aller Größen, darunter mehr als die Hälfte der Fortune-1000-Unternehmen, setzen auf die personenzentrierten Sicherheits- und Compliance-Lösungen von Proofpoint, um ihre größten Risiken in den Bereichen E-Mail, Cloud, soziale Netzwerke und Web zu minimieren. Weitere Informationen finden Sie unter [www.proofpoint.de](http://www.proofpoint.de).

© Proofpoint, Inc. Proofpoint ist eine Marke von Proofpoint, Inc. in den USA und anderen Ländern. Alle weiteren hier genannten Marken sind Eigentum ihrer jeweiligen Besitzer.