Module
Proofpoint Security Awareness

Datenspeicherung- und zerstörung
Die Mitarbeiter lernen, wie sie Best Practices im Zusammenhang mit dem sicheren Umgang und der sicheren Speicherung sensibler Daten anwenden. Dieses Modul erläutert die Verwaltung physischer Dateien, Dokumente und tragbarer Speichermedien, sowie die technischen Schutzmaßnahmen für elektronische Geräte und Dateien. Dem Benutzer werden auch Techniken zur ordnungsgemäßen Entsorgung und Zerstörung vertraulicher Daten vermittelt.

E-Mail Sicherheit
Dem Mitarbeiter wird beigebracht, Köder und Fallen zu erkennen, die häufig in Phishing-Emails und Spear Phishing-Angriffen vorkommen. Die Benutzer lernen, manipulative Inhalte, böswillige und verschleierte Links, gefährliche Anhänge, unangemessene Datenanforderungen und andere Bedrohungen zu identifizieren und zu vermeiden. Zu diesem Thema werden zwei Arten der Ausbildung angeboten. Ein interaktives Trainingsmodul und ein charakterbasiertes Trainingsspiel. Beide zeigen Beispiele für Phishing-Emails und fordern Benutzer auf, potenzielle Fallen zu identifizieren.

DSGVO im Überblick
Endbenutzer müssen sich im Klaren sein, dass sie für die Einhaltung der in der Allgemeinen Datenschutzverordnung (DSGVO) festgelegten Datenschutzanforderung verantwortlich sind. In diesem Modul erfahren sie, warum sie aktiver Teilnehmer an der allgemeinen Einhaltung der DSGVO sein müssen. Ihnen wird vermittelt, wie man die richtigen Entscheidungen über die Daten trifft, die sie erstellen und verarbeiten und welche Konsequenzen die Nichteinhaltung für Ihr Unternehmen hat.

DSGVO in der Praxis
Die DSGVO betrifft viele Unternehmen auf der ganzen Welt. Dieser Kurs führt zuerst in die Regelung ein. Anschließend werden die Lernenden aufgefordert, die Anwendung der Verordnung in einer Vielzahl von Geschäftsfunktionen zu üben.

Insider-Bedrohungen
Cyber-Kriminelle verlassen sich weniger auf automatisierte Angriffe als vielmehr auf Taktiken wie Social Engineering, um die Menschen in Ihrem Unternehmen auszunutzen. Gleichzeitig haben viele Ihrer derzeitigen oder ehemaligen Mitarbeiter möglicherweise Zugriff auf einen Schatz an vertraulichen oder wertvollen Informationen und können diesen Zugriff zu persönlichen oder beruflichen Zwecken missbrauchen. Es ist wichtiger denn je, sich der Bedrohungen bewusst zu sein, die von Ihrem Unternehmen ausgehen. Die neuen interaktiven Insider-Bedrohungs-Schulungsmodule von Proofpoint untersuchen, ob Ihre eigenen Mitarbeiter absichtlich oder unbeabsichtigt Schaden anrichten können.

Schutz von Mobilgeräten
Unabhängig davon, ob Sie Ihren Mitarbeitern Mobilgeräte ausstellen oder eine BYOD-Organisation (Bring Your Own Device) sind, können Ihre Mitarbeiter von unseren interaktiven Schulungen und empfohlenen Best Practices für die sichere Verwendung von Mobilgeräten profitieren. Mit diesem auf Mobilgeräte reagierenden Modul erfahren Benutzer, wie wichtig physische und technische Sicherheitsvorkehrungen sind und wie sie die Sicherheit ihrer Mobilkommunikation und -verbindungen verbessern können.

Reihe zum Kennwortschutz

Diese Serie enthält die folgenden Module und Minimodule:

Kennwortrichtlinie
Erfahren Sie, wie Sie sicherere Kennwörter erstellen, die den Kennwortrichtlinien Ihres Unternehmens entsprechen. Enthält auch praktische Übungen zum Erstellen.

Jenseits von Passwörtern
Entdecken Sie Optionen zum Sichern von Geräten und Konten. Erfahren Sie, wie Sie sichere PINs erstellen, um Geräte und die darin enthaltenen Daten zu schützen. In diesem Modul wird auch die Verwendung von Passphrasen zum Erstellen sicherer Passwörter erläutert.

Passwortverwaltung
Benutzer benötigen sichere, eindeutige Passwörter für jedes Konto. Es kann schwierig sein, sich all diese Passwörter zu merken. In diesem Modul werden Strategien vermittelt, mit denen Benutzer ihre Kennwörter sicher verwalten können.

Multi-Faktor-Authentifizierung
In vielen Fällen reicht es nicht mehr aus, nur ein Kennwort zum Schutz unserer Konten zu verwenden. Erfahren Sie, wie Sie die Multi-Factor-Authentifizierung (MFA) effektiv einsetzen, um wichtige Konten zu schützen.

PCI DSS

Mit diesem Modul können Ihre Mitarbeiter Kreditkartendaten besser verwalten. PCI-DSS-Anforderungen verstehen, Datensätze und Konten sicher verwalten und Sicherheitsverletzungen erkennen und darauf reagieren.

PII (Personally Identifiable Information)-Grundlagen

Diese Serie enthält die folgenden Module und Minimodule:

PII-Grundlagen
Ihre Endbenutzer lernen bewährte Methoden für die Handhabung, Speicherung und Weitergabe von PII. Es behandelt die verschiedenen Arten von personenbezogenen Daten sowie Richtlinien zur Identifizierung, Erfassung und Verwendung von personenbezogenen Daten.

PII in Aktion
Ihre Endbenutzer werden verschiedene Szenarien untersuchen, um zu erfahren, wie sich unterschiedliche Entscheidungen auf unsere Fähigkeit auswirken, PII zu schützen.

Physische Sicherheit

Dieses Modul stellt die wichtigsten Komponenten der physischen Sicherheit vor und hilft Ihren Mitarbeitern, ihre Rolle bei der Aufrechterhaltung einer sicheren Arbeitsumgebung zu verstehen. Sie erfahren auch, wie sie physische Sicherheitsverletzungen und Best Practices verhindern und korrigieren können, um die Sicherheit Ihrer Mitarbeiter, Bereiche und Vermögenswerte zu gewährleisten.

Schutz vor Ransomware

Mit diesem Mini-Modul können Sie kurze, aber umfassende Schulungen zu Ransomware durchführen, einer bedeutenden und wachsenden Bedrohung in allen Märkten, einschließlich des Gesundheitswesens. Endbenutzer lernen, wie sie Ransomware-Angriffe erkennen und verhindern können, und die Best Practices, die sie erlernen, können bei der Bekämpfung anderer Arten von Phishing und Malware-basierten Bedrohungen angewendet werden.

Sichere Nutzung sozialer Netzwerke

Ihre Mitarbeiter lernen, wie sie auf Social-Networking-Websites sicher miteinander kommunizieren und kommunizieren können. Wir erklären häufige Fallen und Betrügereien, die auf diesen sehr öffentlichen Plattformen vermieden werden sollen. Dieses interaktive Training hilft den Mitarbeitern zu verstehen, was sie in sozialen Medien teilen sollten und was nicht. So werden Ihre Unternehmensinformationen sicherer.

Grundlegende Sicherheit

Diese Serie enthält die folgenden Module und Minimodule:

Einführung in Phishing
Bietet einen kurzen, aber aufschlussreichen Einblick in die Best Practices zum Erkennen und Behandeln verdächtiger E-Mails.

Vermeiden gefährlicher Links
Bietet Benutzern praktische Anleitungen zum Ermitteln des tatsächlichen Ziels einer URL und untersucht häufige visuelle Hinweise, anhand derer Benutzer feststellen können, ob eine Website legitim oder gefährlich ist.

Vermeiden gefährlicher Anhänge
Hilft Benutzern zu verstehen, warum sie E-Mail-Anhänge mit einem gesunden Verdacht behandeln sollten, und wie mit diesen Nachrichtentypen umgegangen wird.

Phishing bei der Dateneingabe
Erläutert die mit böswilligen Dateneingabeformularen verbundenen Gefahren und hilft Benutzern zu verstehen, warum sie bei E-Mails, die eine Anforderung von Anmeldeinformationen oder anderen vertraulichen Informationen enthalten, vorsichtig sein sollten.

Grundlegende Sicherheit für Führungskräfte

Dieses szenariobasierte, auf Mobilgeräten reagierende Training konzentriert sich auf Cybersicherheitsbedrohungen und -bedenken, die nur für leitende Angestellte, Führungskräfte gelten. In der Schulung werden bewährte Methoden in Bezug auf mobile Geräte, die Verwendung von Netzwerken außerhalb des Unternehmens, physische Sicherheit, interne und externe Besprechungen, soziale Medien und andere Themen vorgestellt. Dieses umfassende Modul hilft Führungskräften, potenzielle Bedrohungen zu erkennen, das Sicherheitsverhalten in ihrem Geschäfts- und Privatleben zu verbessern.

Social Engineering

Social Engineers bauen Beziehungen auf und nutzen die menschliche Tendenz, offen und hilfsbereit zu sein, um Daten zu stehlen, auf vertrauliche Netzwerke zuzugreifen und andere Betrügereien auszuführen. Dieses Modul geht über die Phishing-Bedrohung hinaus und erläutert die mit Smishing, Vishing, Social Media und persönlichen Angriffen verbundenen Gefahren. Ihre Mitarbeiter lernen, gängige Social-Engineering-Techniken zu erkennen und zu vermeiden und Ihre Mitarbeiter, Bereiche und Vermögenswerte zu schützen.

Sicherheit auf Reisen

Dieses Mini-Modul ist ein Muss für Mitarbeiter, die Unternehmensgeräte und -daten unterwegs mitnehmen. Unabhängig davon, ob sie häufig oder selten verreisen, ist es für Ihre Endbenutzer von Vorteil, Informationen zu Cybersicherheitsmaßnahmen zu erhalten, die sie auf Inlands- und Auslandsreisen schützen können.

URL-Schulung

Ihre Mitarbeiter erfahren, wie URLs erstellt werden, wie URL-Warnzeichen angezeigt werden und wie schädliche Links identifiziert und vermieden werden. Das Training behandelt manipulierte Domains, verkürzte URLs und andere gängige Tricks. Wir bieten zu diesem Thema zwei Arten der Ausbildung an, ein interaktives Trainingsmodul und ein charakterbasiertes Trainingsspiel. Beide Optionen fordern Benutzer auf, aus legitimen Links böswillige Links zu ermitteln.

USB-Gerätesicherheit

Infizierte USB-Geräte stellen eine häufig übersehene Bedrohung dar, und Endbenutzer müssen sich der Risiken bewusst sein, die mit Flash-Laufwerken und anderen IoT-Elementen verbunden sind, die über USB-Ports mit Strom versorgt werden. Dieses Mini-Modul informiert Ihre Mitarbeiter schnell und effektiv über die Gefahren, die mit unbekannten USB-Laufwerken verbunden sind, und erklärt, wie Benutzer ihre persönlichen und Unternehmensdaten und -systeme bei Verwendung von USB-basierten Geräten schützen können.

Sie haben Fragen? Sprechen Sie uns an:
T +49 2327 9912-336 | E proofpoint@adn.de