CYBERDISE-Schulungen Inhalt 2025

Ein einzigartiger, modularer und anpassbarer Ansatz für Cybersicherheits-Schulungen für Unternehmen mit komplexen Anforderungen

Wesentliche Vorteile

- Basierend auf einem klar definierten didaktischen Konzept für maximale Konsistenz des Portfolios.
- Vollständig anpassbare Module: Bearbeiten, Ändern oder Hinzufügen von benutzerdefinierte Inhalten, um sie an die Anforderungen und Richtlinien ihres Unternehmens anzupassen.
- Whitelabelling: Fügen Sie ihre CI/CD und White-Label-Inhalte hinzu, um sie an das Design ihres Unternehmens anzupassen.
- Flexible Schulungsformate: Wählen Sie zwischen Text, Video oder einer Mischung aus beidem, um den Vorlieben ihrer Mitarbeiters gerecht zu werden.
- Strukturierter Lernpfad: Theorie ➔ Spiel ➔ Test für ansprechende und messbare Schulungen.
- Immer auf dem neuesten Stand: Greifen Sie auf die neuesten Inhalte für 2025 zu, um den neuen Bedrohungen immer einen Schritt voraus zu sein.
- Integration benutzerdefinierter Inhalte: Schulen Sie Mitarbeiter nach firmeneigenen Richtlinien und Materialien.
- Kurze, fokussierte Lektionen: Knappe, 5-15-Minuten-Module, um lange Unterbrechungen kurz zu halten.
- Globale Reichweite: Professionell übersetzte und lokalisierte Inhalte in über 12 Sprachen.
- Mobilfreundliches Design: Schulungen jederzeit, überall und auf jedem Gerät.
- Über 20 Kernthemen, die sowohl Grund- als auch Fortgeschrittenenstufen abdecken – entwickelt zur leichteren Einarbeitung von neuen Mitarbeitern, regelmäßigen Nachschulungen und Compliance, mit anpassbaren Pfaden für jedes Unternehmen.

Das CYBERDISE-Portfolio für Cybersicherheits-Schulungen basiert auf einem didaktisch und pädagogisch fundierten Rahmenkonzept, das sicherstellt, dass die Lerninhalte nicht nur ansprechend sind, sondern auch tatsächlich zu Verhaltensänderungen führen.
Die Module gewährleisten, dass Unternehmen mit komplexen Sicherheitsanforderungen die Schulungen an ihre spezifischen Herausforderungen, Richtlinien und Risikoprofile anpassen können. Dies hilft ihnen dabei, die Gründe für Sicherheitsrichtlinien zu vermitteln und ihre Mitarbeiter zu befähigen, proaktiv gegen Cyberbedrohungen vorzugehen.

Hier finden Sie eine Liste der Themen unseres Schulungsangebots, das darauf abzielt, das Sicherheitsbewusstsein zu schärfen, eine Sicherheitskultur aufzubauen und ihr Team zu befähigen, intelligente, sicherheitsbewusste Entscheidungen zu treffen:

Umfassender Lehrplan für Cybersicherheit mit über 20 Themen von der Grundstufe bis zum Fortgeschrittenenlevel

Bewusstsein für Cybersicherheit

- Auswirkungen eines Cyberangriff auf Unternehmen, Mitarbeiter und Einzelpersonen
- Rolle der Mitarbeiter bei der Verhinderung von Sicherheitsverletzungen

Sicherheitsbewusstsein und Verhaltensweise

- Sicherheitsdenken, Erkennen von Anomalien und Bewusstsein für physische Sicherheit
- Meldeprozesse und Reaktionsverhalten

Grundlegende Konzepte der Cybersicherheit

- Integrität, Verfügbarkeit, Authentifizierung, Autorisierung, Risiko, Verschlüsselung, Schwachstellen, Reaktion auf Vorfälle

Next Gen Security Awareness Training

Gold Winner-Company of the Year

Cybersecurity Learning Management System

„Diese moderne Lösung erfüllt alle unsere Anforderungen. Sie ist ein wesentlicher Bestandteil unseres Schutzes im IT-Bereich, reduziert Kosten und trägt erheblich zur Mitarbeiter-Sensibilisierung bei. Wir können CYBERDISE nur wärmstens empfehlen.“
Ismael Aemisegger, Leiter IT-Support bei GLB

„Als Systemingenieur konnte ich die erste Phishing-Kampagne innerhalb von 30 Minuten starten, die Installation bereits inkludiert. Ich habe das System eingerichtet, Domains hinzugefügt, SSL-Zertifikate generiert, auf Basis einer Vorlage die Phishing-Simulation erstellt, Benutzer hinzugefügt und schon konnte es losgehen. Besonders gut gefallen haben mir die Kampagnenchecks!“
Norman Umbach, Senior Consultant bei DSS-CONNECT

Häufige Arten von Cyberbedrohungen

- Malware, Phishing, Ransomware, DDoS, Insider-Bedrohungen, Deep Fakes, Zero-Day-Exploits

Cyber-Risikomanagement

- Risikobewertung, Bedrohungsinformationen, Schwachstellenmanagement, Analyse der Auswirkungen auf das Geschäft, Compliance

Grundlagen der Cybersicherheit

- Definitionen, Bedrohungen, Risiken und Schutzmaßnahmen

Angriffsvektoren

- Phishing, Smishing, Deep-Fake-Videoanrufe, unsichere QR-Codes, USB-Geräte, Chat-Tools

Passwortsicherheit

- Erstellen und Verwalten sicherer Passwörter, Zwei-Faktor-Authentifizierung

Schutz vor Malware

- Erkennen und Vermeiden von Viren, Trojanern und anderen Schadprogrammen

Sicheres Surfen im Internet

- Gefährliche Websites und Downloads vermeiden

Datenschutz und Privatsphäre

- Umgang mit personenbezogenen Daten, Datenschutzgrundsätze, regulatorische Anforderungen
- Daten mit erhöhten Schutzanforderungen

Personenbezogene Daten

- Arten personenbezogener Daten und Schutzstrategien

Physische Sicherheit und Besucher

- Zugangskontrolle, unbefugte Anwesenheit, Meldeverfahren
- Aufgeräumter Schreibtisch

Netzwerksicherheit

- Sichere WLAN-Nutzung, VPNs, Firewalls

Sicherheit auf Reisen und im Homeoffice

- Geräteschutz und Datensicherheit auf Geschäftsreisen
- Risiken bei Remote-Arbeit und sicheres Verhalten außerhalb des Büros

Mobile Geräte

- Sicherheitsvorkehrungen für Smartphones und Tablets, BYOD (Nutze das eigene Gerät)

Reaktion auf Vorfälle

- Verfahren zur Erkennung, Meldung, Eindämmung und Eskalation

Compliance und gesetzliche Vorschriften

- DSGVO, nDSG, CCPA (Kalifornisches Verbraucherschutzgesetz) und andere rechtliche Rahmenbedingungen

Sicherheitsrichtlinien und interne Dokumente

- Interne Richtlinien, verbindliche Leitlinien und Umgang mit Dokumenten

KI-Sicherheit

- Risiken der KI-Manipulation, Deepfake-Erkennung, Sicherheit von KI-Tools

Videos zum Thema Sicherheitsbewusstsein

Als Ergänzung zu ihren Schulungsinitiativen, bieten wir eine große Auswahl an Videos zum Thema Sicherheitsbewusstsein. Diese Videos wurden erstellt, um zusätzliche, einprägsame Inhalte zu vermitteln, die den Teilnehmern auch noch lange nach Abschluss der Schulung im Gedächtnis bleiben. Indem das Thema Sicherheit stets im Auge behalten wird, schaffen Sie eine Kultur des Sicherheitsbewusstseins und reduzieren das Bedrohungsrisiko für ihr Unternehmens.

- Video zur Sensibilisierung für KI-Sicherheit
- Video zur Sensibilisierung für Deepfake-Sicherheit
- Video zur Sensibilisierung für E-Mail-Sicherheit Video
- zur Sensibilisierung für Malware-Sicherheit Video zur
- Sensibilisierung für mobile Sicherheit Video zur
- Sensibilisierung für Passwortsicherheit Video zur
- Sensibilisierung für Phishing
- Video zur Sensibilisierung für Social-Media
- WFH-Video

Und mehr

Mehr erfahren

Weitere Informationen finden Sie unter www.cyberdise-awareness.com/