



Cyber Security Awareness – „Firewall Mensch“ statt „Risiko Mensch“

Mit uns bekommen Sie HanseSecure Expertenwissen zu Cyber Security Awareness

Aus intensivem Austausch entstand die Idee zu einer einzigartigen Zusammenarbeit:

Florian Hansemann, Geschäftsführer von HanseSecure, gilt als weltweit führender Experte und Berater für IT Security Awareness und Phishing Attacken. Zusammen mit der langjährigen Expertise und lernpsychologischen Kompetenz von soluzione42 bieten wir das Beste aus beiden Welten, denn **nur Experten machen Experten!**



Awareness

- kontinuierliche Awareness-Bildung auf Basis von:
 - modularen Lerninhalten
 - Phishing-Simulationen
 - begleitenden Kampagnen Awareness-Nuggets
- aufeinander aufbauende Kurse festigen betriebl. Sicherheitskultur

Resilienz des Unternehmens stärken



Expertise

- lernpsychologisch fundiert für nachhaltige Lernerfahrung
- motivierendes Storytelling
- Best Practices
- relevante Handlungsempfehlungen
- animierte, unterhaltsame Lernvideos

Inhalte nachhaltig im Gedächtnis verankern



Methodik

- Multi-Channel-Lernerfahrung
- Phishingwellen
- Monitoring und Analysen
- unterstützende Kampagnen:
 - Tipps & Tricks
 - Videosnippets
 - interaktive Quizze
 - aktuelle Cybervorfälle

Schwachstellen aufdecken und beheben



Lernverwaltung

- 100% DSGVO-konform
- Daten werden ausschließlich in EU verarbeitet
- geringer technischer Aufwand
- Userfreundliche Lernplattform
- unmittelbarer Lernprozess

Stets aktuelle und sichere Lernplattform

E-Learning-Kurse gibt es viele, was macht unsere Kursmodule so besonders?

Cyber-Security-Angriffe werden immer gerissener und Hacker ändern immer schneller ihre Methoden - herkömmliche Trainings hinken dieser Entwicklung hinterher. Wir bieten dagegen eine stets aktuelle Plattform, damit Ihre Mitarbeiter auch gegen künftige Bedrohungen gewappnet sind. Dabei unterstützt Sie unser Customer Success Team vom Onboarding bis zur Auswertung, um für Sie das Beste aus den Awareness-Kursen herauszuholen.

Nach dem Prinzip des verteilten Lernens wechseln kontextbasierte, modulare Lerninhalte mit Phishing-Simulationen und motivierenden Kampagnenelementen.

Unser Erfolgsversprechen:

- schnelle Nutzeraktivierung
- einfache Umsetzung in den Arbeitsalltag
- hohe Akzeptanz bei den Mitarbeitenden
- Aufbau nachhaltiger Gewohnheiten





soluzione Kursmodul Datenschutz

Das wichtige und komplexe Thema Datenschutz befasst sich damit, wie personenbezogene Daten vor unbefugtem Zugriff, Missbrauch oder Verlust geschützt werden können.

In unserem Kurs erfahren Sie, welche gesetzlichen Vorgaben zum Datenschutz bestehen, welche Pflichten beim Umgang mit personenbezogenen Daten zu beachten sind und wer bei Datenschutzverletzungen haftet. Wir grenzen Datenschutz von Datensicherheit ab und zeigen anhand von anschaulichen Beispielen auf, wie mit Dienstleistern, Personaldaten oder bei der werblichen Nutzung von Daten umgegangen werden soll. Zudem beleuchten wir die Rolle des Datenschutzbeauftragten und erklären, wie Datenschutz in Unternehmen organisiert wird.

In unserem Kurs erfahren Sie – in 26 Lernmodulen – alles Wissenswerte rund um das Thema „Schutz personenbezogener Daten“

(Gesamtdauer: 102 Minuten)

Kurskapitelübersicht Datenschutz:

- Einleitung: Datenschutz
- Was ist Datenschutz?
- Was sind personenbezogene Daten?
- Wichtige Abgrenzung zu Datensicherheit
- Die gesetzlichen Vorgaben:
 - Verbotprinzip und die Ausnahmen
 - Einwilligung
 - Vertragsdurchführungserlaubnis
- Wer haftet wofür?
- Begleitpflichten:
 - Intro
 - Pflicht zu Datenschutzhinweisen
 - Löschpflicht
 - Verfahrenspflicht
- Einschaltung von Dienstleistern, die Daten verarbeiten
- Umgang mit Personaldaten:
 - Intro
 - Einwilligung vermeiden
 - DSGVO verwenden
 - Ausführliche Datenschutzhinweise
 - Daten löschen
 - HR-Datentransfer regeln
 - Sensible, leistungs- und verhaltensrelevante Daten
- Datenschutz-Organisation in Unternehmen
- Die Rolle des Datenschutzbeauftragten
- Werbung
 - Datenschutzrecht und Werbung
 - Wettbewerbsrecht
 - Folgefragen und typische Fälle aus der Praxis
- Betroffenenrechte
 - Intro
 - Informationspflicht
 - Recht auf Datenauskunft & Berechtigung
 - Recht auf Löschung & Sperrung
 - Recht auf Datenübertragbarkeit
 - Recht auf Widerruf und Widerspruch
 - Recht, nicht automatisierten Entscheidungen unterworfen zu werden
 - Auf Betroffenenanfragen reagieren

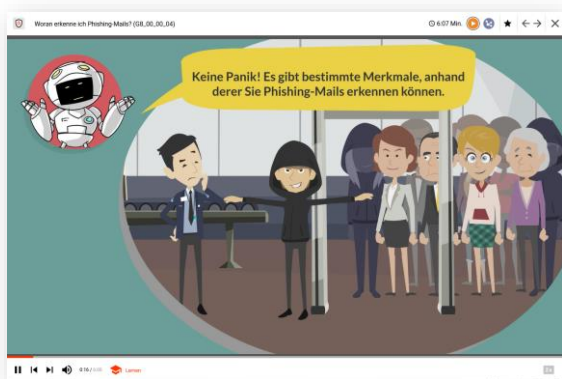




soluzione Kursmodul Phishing

Der Kurs erklärt, wie Sie Phishing-Mails oder gefälschte Login-Seiten anhand von aktuellen Beispielen erkennen. Wir geben Tipps zum Schutz und zeigen, wie Sie handeln sollen, wenn Sie auf eine Phishing-Mail reagiert haben.

In unserem Kurs erfahren Sie - kompakt in neun Lernmodulen - alles Wissenswerte zum Thema „Phishing & IT-Security“ (Gesamtdauer: 62 Minuten).



Kurskapitelübersicht:

- Was ist Phishing?
- Wie gefährlich sind Phishing-Mails?
- Woran erkenne ich Phishing-Mails? Formale Kriterien
- Woran erkenne ich Phishing-Mails? Sprachliche Kriterien
- Woran erkenne ich Phishing-Mails? Social Engineering
- Woran erkenne ich gefälschte Login-Seiten?
- Was soll ich tun, wenn ich eine Phishing-Mail geöffnet oder darauf reagiert habe?
- Wie kann ich mich schützen?
- Aktuelle Beispiele für Phishing-Mails?
- Was ist Spear-Phishing?
- Was ist Quishing?
- Was ist Vishing?
- Was ist Technischer Support Scam?

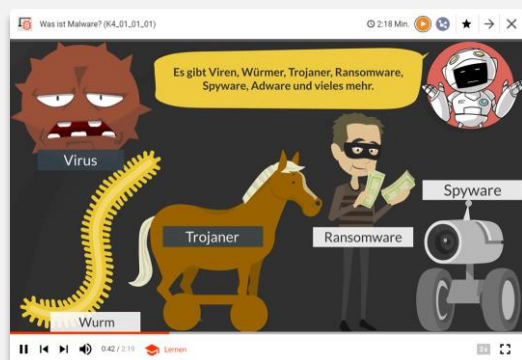
soluzione Kursmodul Malware

Die Abkürzung Malware bezeichnet allgemein jede Art von schädlicher Software. Sie zielt darauf ab, Computer, Netzwerke und Daten zu beschädigen oder zu manipulieren. Dieser Kurs erklärt genau, welche verschiedenen Formen Malware annehmen kann, wie diese auf Ihr Gerät gelangt und welche Schäden sie dort verursacht. Außerdem erhalten Sie wertvolle Tipps, um Anzeichen von Malware zu erkennen und die richtigen Schritte einzuleiten, wenn Sie Malware auf Ihrem Gerät vermuten.

In unserem Kurs erfahren Sie – kompakt in 20 Lernmodulen – alles Wissenswerte rund um das Thema „Was ist Malware und wie gehe ich damit um“ (Gesamtdauer: 81 Minuten).

Kurskapitelübersicht:

- Was ist Malware?
- Welche Schäden verursacht Malware?
- Wie gelangt Malware auf mein Gerät?
- Was ist ein Virus?
- Was ist ein Wurm?
- Was ist ein Trojaner?
- Was ist Ransomware?
- Was ist Spyware?
- Was sind PUPs und insbesondere Adware?
- Was mache ich bei Malware auf meinem Gerät?
- Kann ich Opfer von Malware werden?
- Woran erkenne ich Phishing-Mails? Formale Kriterien
- Woran erkenne ich Phishing-Mails? Sprachliche Kriterien
- Woran erkenne ich Phishing-Mails? Social Engineering
- Passwortsicherheit



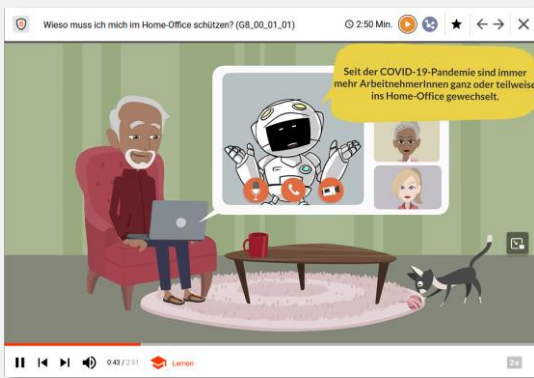
- Sicheres Surfen: Login-Seiten
- Sicheres Downloaden aus dem Netz
- Warnsysteme von Browsern
- Sicheres Downloaden von E-Mail Anhängen
- Sicheres Senden von E-Mail Anhängen



soluzione Kursmodul Sicherheit im Büro und Home-Office

Beim Arbeiten im Büro – egal ob Großraumbüro oder Einzelzimmer – werden oft solche Risikostellen übersehen, an denen unbefugte Personen Einblick in sensible Daten erhalten. Und auch im Home-Office bestehen Gefahren, wenn Räume geteilt werden oder private Geräte zum Einsatz kommen. Der Kurs erklärt, wie Sie Ihren Arbeitsplatz mit technischen Mitteln und durch eigenes umsichtiges Vorgehen schützen. Wir geben Tipps zum Erkennen von Bedrohungen und zeigen, wie Sie bei Verdacht von Schadsoftware-Übergriffen handeln sollen. Außerdem informieren wir Sie, was Sie bei Online-Meetings und beim mobilen Arbeiten von unterwegs beachten können.

In unserem Kurs erfahren Sie – kompakt in neun Lernmodulen – alles Wissenswerte rund um das Thema „Büroarbeitsplatz, Home-Office und IT-Security“ (Gesamtdauer: 35 Minuten).



Kurskapitelübersicht:

- Sicherheit am Büroarbeitsplatz
- Wieso muss ich mich im Home-Office schützen?
- Wie schütze ich meinen Arbeitsplatz?
- Wie schütze ich meine Geräte?
- Wie schütze ich mich und andere während eines Meetings?
- Wie werden Teams-Meetings sicher?
- Woran erkenne ich akute Bedrohungen auf meinem Gerät?
- Was soll ich bei akuten Bedrohungen tun?
- Wie schütze ich mich beim mobilen Arbeiten?

soluzione Kursmodul Passwortsicherheit & MFA

Aufgrund der großen Nachfrage haben wir ein ausführliches E-Learning-Video zur Passwortsicherheit erstellt. Darin zeigen wir bekannte Angriffsmethoden zum Hacken von Passwörtern auf und geben konkrete Hilfestellungen, wie Sie sichere, aber dennoch merkbare Passwörter erstellen können. Außerdem beleuchten wir das Thema der Wiederauffindbarkeit von Passwörtern und zeigen Do's und Don'ts, die mit dem Speichern von Passwörtern verbunden sind. Ergänzt wird der Kurs durch das Thema Multi-Faktor-Authentifizierung. Sie erfahren, welche Authentifizierungsmethoden es gibt und wie sich Hacker Sicherheitslücken zu Nutze machen.

In unserem Kurs erfahren Sie – kompakt in drei Lernmodulen – alles Wissenswerte rund um das Thema „Passwortsicherheit und MFA“

(Gesamtdauer: 17 Minuten).

Kurskapitelübersicht:

- Passwortsicherheit
- Multi-Faktor-Authentifizierung (MFA)
- MFA Bombing

