TREESOLUTION

SECURITY AWARENESS SINCE 2005

E-Learning Lösungen

Inhaltsübersicht

Version 4.9

TREESOLUTION
SECURITY AWARENESS SINCE 2005

Inhaltsverzeichnis

1. Informationssicherheit

1.1. Arbeiten unterwegs

Wenn Sie diesen Kurs beendet haben, werden Sie im Stande sein, die Risiken zu erkennen, die mit dem Arbeiten unterwegs und zuhause verbunden sind, und vorbeugende Massnahmen zu ergreifen, um sicher zu bleiben und Ihre Daten zu schützen.

Technisches:

Sprachen: Deutsch (formell & informell), Englisch, Französisch, Italienisch

Dauer: 10-15 Minuten

Format: SCORM, cmi5, xAPI oder über unser Learning Center

Anpassbar an das Unternehmen: Ja. Zum Beispiel: Vorgaben, Begriffe, Farben, Schrift, Logo, Kontaktdaten und verlinkte Dokumente.

Lernziele:

- Sie kennen die Risiken vom Arbeiten von unterwegs und können sie benennen
- Sie verstehen die Risiken und Massnahmen und können Sie wiedergeben
- Sie können vorbeugende Massnahmen ergreifen und die Regeln für das Arbeiten von unterwegs anwenden

Lerninhalte:

- Video-Clip
- Risiken
- Szenarien - Mehrteilige, interaktive Kurzgeschichte
- Regeln für das Arbeiten ausserhalb des Büros
- Sichere Netzwerk-Verbindungen
- Interaktive Übungen
- Wissenstest
- Abschluss

Anzahl Lektionen: 14

Zielgruppe:

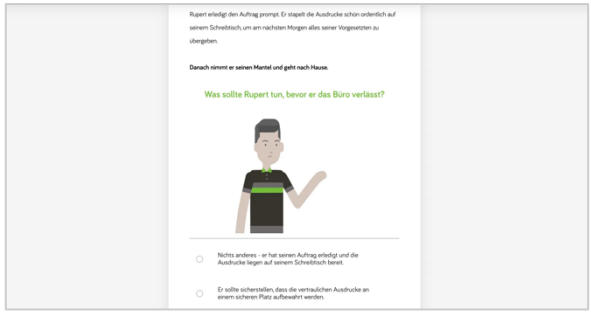
Jegliche Mitarbeitende in Ihrem Unternehmen, die von unterwegs arbeiten können.

Zusätzliche Materialien:

- Informationsblatt
- Optionen: Animationsfilm, Poster, Quiz, E-Mail und Intranet Informationen

1.2. Wichtiges zu Clear Desk und Clear Screen

In diesem Kurs lernen Sie, wie die Umsetzung einer Clear Desk und Clear Screen Weisung unerlaubten Zugriff oder Diebstahl von wichtigen Firmeninformationen verhindert.



Technisches:

Sprachen: Deutsch (formell & informell), Englisch, Französisch, Italienisch

Dauer: 10-15 Minuten

Format: SCORM, cmi5, xAPI oder über unser Learning Center

Anpassbar an das Unternehmen: Ja. Zum Beispiel: Vorgaben, Begriffe, Farben, Schrift, Logo, Kontaktdaten und verlinkte Dokumente.

Lernziele:

- Sie kennen die Risiken von Clear Desk & Clear Screen und können sie benennen
- Sie verstehen die Verhaltensregeln und können Sie wiedergeben
- Sie können die Verhaltensregeln für Clear Desk & Clear Screen anwenden

Lerninhalte:

- Video-Clip
- Risiken
- Szenarien - Mehrteilige, interaktive Kurzgeschichte
- Verhaltensregeln
- Interaktive Übungen
- Wissenstest
- Abschluss

Anzahl Lektionen: 11

Zielgruppe:

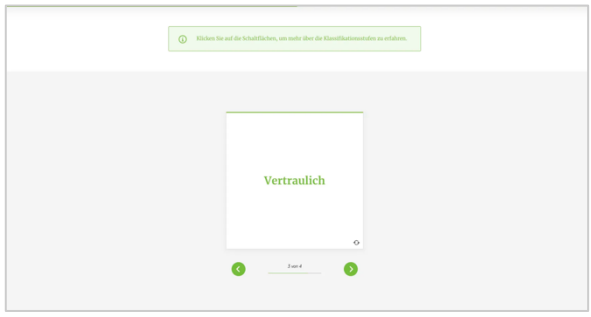
Jegliche Mitarbeitende in Ihrem Unternehmen, die regelmässig oder unregelmässig an einem Schreibtisch und am Computer arbeiten.

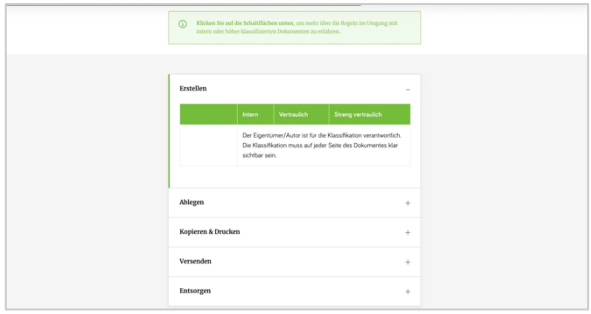
Zusätzliche Materialien:

- Informationsblatt
- Optionen: Animationsfilm, Poster, Quiz, E-Mail und Intranet Informationen

1.3. Kennzeichnung und Klassifizierung von Informationen

In diesem Kurs zeigen wir Ihnen, wie wichtig es ist sowohl gedruckte als auch elektronische Dokumente sicher handzuhaben. Ausserdem werden Sie lernen, wie Sie Ihre Informationen durch korrekte Klassifikation schützen können.





Technisches:

Sprachen: Deutsch (formell & informell), Englisch, Französisch, Italienisch

Dauer: 10-15 Minuten

Format: SCORM, cmi5, xAPI oder über unser Learning Center

Anpassbar an das Unternehmen: Ja. Zum Beispiel: Vorgaben, Begriffe, Farben, Schrift, Logo, Kontaktdaten und verlinkte Dokumente.

Lernziele:

- Sie können die Risiken benennen, wenn man nicht auf die Klassifizierung achtet
- Sie können die Schutzklassen der Klassifizierung in unserem Unternehmen beschreiben
- Sie können den Umgang mit klassifizierten Informationen wiedergeben
- Sie können Dokumente mit richtiger Klassifizierung erstellen

Lerninhalte:

- Video-Clip
- Risiken
- Szenarien - Mehrteilige, interaktive Kurzgeschichte
- Schutzklassen
- Umgang mit klassifizierten Informationen
- Interaktive Übungen
- Wissenstest
- Abschluss

Anzahl Lektionen: 14

Zielgruppe:

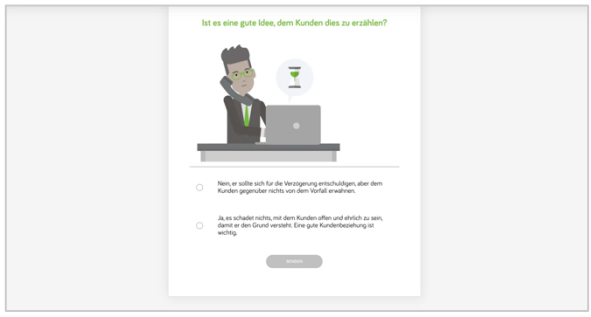
Jegliche Mitarbeitende in Ihrem Unternehmen, die mit unterschiedlichen Daten in Berührung kommen.

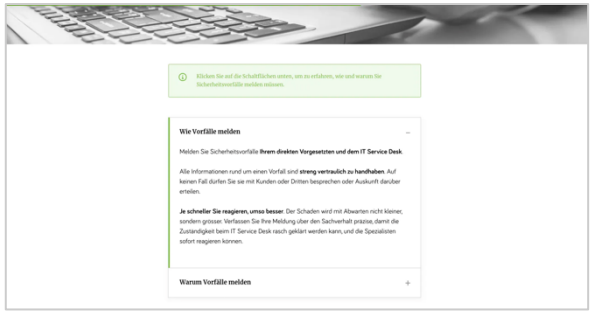
Zusätzliche Materialien:

- Microlearning «Sichere Nutzung von KI-Tools»
- Informationsblatt
- Optionen: Animationsfilm, Poster, Quiz, E-Mail und Intranet Informationen.

1.4.Melden von Sicherheits-vorfällen

Lernen Sie in diesem Kurs, warum es so wichtig ist, Sicherheitsvorfälle zu melden, und wie und wann Sie das tun sollten.





Technisches:

Sprachen: Deutsch (formell & informell), Englisch, Französisch, Italienisch

Dauer: 10-15 Minuten

Format: SCORM, cmi5, xAPI oder über unser Learning Center

Anpassbar an das Unternehmen: Ja. Zum Beispiel: Vorgaben, Begriffe, Farben, Schrift, Logo, Kontaktdaten und verlinkte Dokumente.

Lernziele:

- Sie kennen verschiedene Arten von Sicherheitsvorfällen und können diese aufzählen
- Sie wissen, weshalb Sie Sicherheitsvorfälle rasch melden sollten
- Sie verstehen, wann ein Sicherheitsvorfall vorliegt, und können diesen einordnen
- Sie wissen, wo Sie Sicherheitsvorfälle melden müssen

Lerninhalte:

- Video-Clip
- Beispiele von Sicherheitsvorfällen
- Szenarien - Mehrteilige, interaktive Kurzgeschichte
- Was sollten Sie tun?
- Interaktive Übungen
- Wissenstest
- Abschluss

Anzahl Lektionen: 11

Zielgruppe:

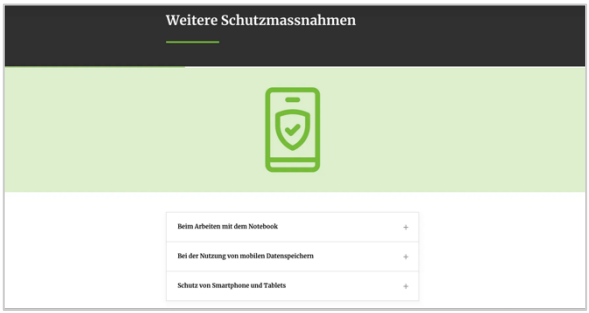
Alle Mitarbeitende in Ihrem Unternehmen.

Zusätzliche Materialien:

- Informationsblatt
- Optionen: Animationsfilm, Poster, Quiz, E-Mail und Intranet Informationen.

1.5. Umgang mit mobilen Geräten

In diesem Kurs lernen Sie, wie Sie verhindern können, dass Daten von mobilen Geräten wie Notebooks, Tablets und Smartphones gestohlen werden.



Technisches:

Sprachen: Deutsch (formell & informell), Englisch, Französisch, Italienisch

Dauer: 10-15 Minuten

Format: SCORM, cmi5, xAPI oder über unser Learning Center

Anpassbar an das Unternehmen: Ja. Zum Beispiel: Vorgaben, Begriffe, Farben, Schrift, Logo, Kontaktdaten und verlinkte Dokumente.

Lernziele:

- Sie können die Risiken, die mit mobilen Geräten und Datenträgern verbunden sind, benennen
- Sie kennen die Schutzmassnahmen für mobile Geräte und Speichermedien und können diese beschreiben
- Sie verstehen, wie man mobile Geräte und Speichermedien schützt
- Sie können die Regeln für den Umgang mit mobilen Geräten und Datenträgern anwenden
- Sie wissen, wie Sie mit mobilen Datenträgern und Geräten umgehen müssen

Lerninhalte:

- Video-Clip
- Risiken
- Szenarien - Mehrteilige, interaktive Kurzgeschichte
- Schutz von mobilen Geräten und Speichermedien
- Weitere Schutz-Massnahmen
- Interaktive Übungen
- Wissenstest
- Abschluss

Anzahl Lektionen: 13

Zielgruppe:

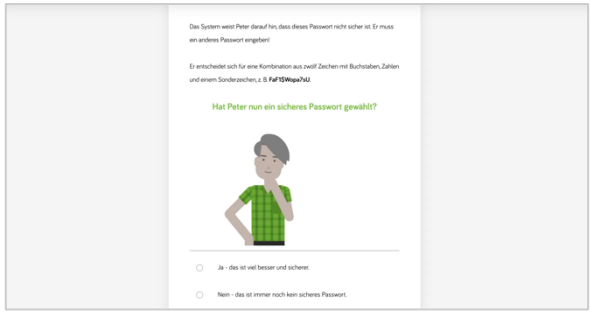
Jegliche Mitarbeitende in Ihrem Unternehmen, die mit mobilen Geräten und Datenspeichern arbeiten.

Zusätzliche Materialien:

- Informationsblatt
- Optionen: Animationsfilm, Poster, Quiz, E-Mail und Intranet Informationen.

1.6. Umgang mit Passwörtern

In diesem Kurs lernen Sie, wie wichtig sichere Passwörter sind und es werden Ihnen einige Tipps aufgezeigt, wie Sie sich Ihre Passwörter problemlos merken können.



Technisches:

Sprachen: Deutsch (formell & informell), Englisch, Französisch, Italienisch

Dauer: 10-15 Minuten

Format: SCORM, cmi5, xAPI oder über unser Learning Center

Anpassbar an das Unternehmen: Ja. Zum Beispiel: Vorgaben, Begriffe, Farben, Schrift, Logo, Kontaktdaten und verlinkte Dokumente.

Lernziele:

- Sie kennen die Wichtigkeit von sicheren Passwörtern und den Umgang damit
- Sie können die wichtigen Komponenten von Passwörtern wiedergeben
- Sie kennen die wichtigsten Merkhilfen für Passwörter und können diese nutzen
- Sie können die Passwortregeln anwenden

Lerninhalte:

- Video-Clip
- Passwörter und PINs
- Szenarien - Mehrteilige, interaktive Kurzgeschichte
- Sichere Passwörter
- Merkhilfe für Passwörter
- Sicherer Umgang mit Passwörtern und PINs
- Interaktive Übungen
- Wissenstest
- Abschluss

Anzahl Lektionen: 16

Zielgruppe:

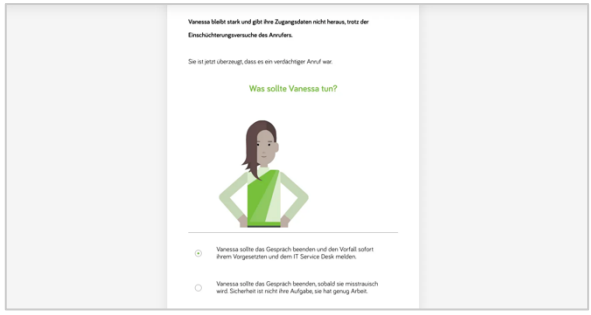
Jegliche Mitarbeitende in Ihrem Unternehmen, die auf passwortgeschützte Systeme zugreifen müssen.

Zusätzliche Materialien:

- Microlearning «Was ist Multi-Faktor-Authentifizierung (MFA)»
- Microlearning «Was ist Prompt Bombing»
- Informationsblatt
- Optionen: Animationsfilm, Poster, Quiz, E-Mail und Intranet Informationen.

1.7. Schutz vor Social Engineering

In diesem Kurs wird das Konzept des Social Engineerings behandelt. Es wird aufgezeigt, wie wertvolle Informationen von ahnungslosen Personen gestohlen werden können. Sie lernen auch Massnahmen kennen, die Sie treffen können, um zu verhindern, dass Sie Opfer eines Social Engineers werden.



Technisches:

Sprachen: Deutsch (formell & informell), Englisch, Französisch, Italienisch

Dauer: 10-15 Minuten

Format: SCORM, cmi5, xAPI oder über unser Learning Center

Anpassbar an das Unternehmen: Ja. Zum Beispiel: Vorgaben, Begriffe, Farben, Schrift, Logo, Kontaktdaten und verlinkte Dokumente.

Lernziele:

- Sie kennen die Risiken von Social Engineering und können sie aufzählen
- Sie verstehen, wie ein Social Engineer vorgeht und können das beschreiben
- Sie können die Massnahmen zum Schutz vor Social Engineering anwenden

Lerninhalte:

- Video-Clip
- Risiken
- Szenarien - Mehrteilige, interaktive Kurzgeschichte
- Methoden des Social Engineerings
- Interaktive Übungen
- Wissenstest
- Abschluss

Anzahl Lektionen: 11

Zielgruppe:

Alle Mitarbeitende in Ihrem Unternehmen, besonders wenn sie mit sensiblen Daten in Berührung kommen wie Finanzen, HR oder Geschäftsleitung.

Zusätzliche Materialien:

- Microlearning «Risiken und Gefahren der KI»
- Informationsblatt
- Optionen: Animationsfilm, Poster, Quiz, E-Mail und Intranet Informationen.

1.8.Arbeiten im Homeoffice

Wenn Sie diesen Kurs beendet haben, werden Sie im Stande sein, die Risiken zu erkennen, die mit dem Arbeiten von zuhause verbunden sind und vorbeugende Massnahmen ergreifen, um sicher zu bleiben und Ihre Daten zu schützen. Sie kennen die Clear Desk und Clear Screen Regeln sowie den Umgang mit mobilen Geräten und Speichermedien.

Technisches:

Sprachen: Deutsch (formell & informell), Englisch, Französisch, Italienisch

Dauer: 10-15 Minuten

Format: SCORM, cmi5, xAPI oder über unser Learning Center

Anpassbar an das Unternehmen: Ja. Zum Beispiel: Vorgaben, Begriffe, Farben, Schrift, Logo, Kontaktdaten und verlinkte Dokumente.

Lernziele:

- Sie kennen die Risiken vom Arbeiten zuhause und können sie benennen
- Sie verstehen die Risiken und Massnahmen und können Sie wiedergeben
- Sie können vorbeugende Massnahmen ergreifen und die Regeln für das Arbeiten von zuhause anwenden

Lerninhalte:

- Video-Clip
- Risiken
- Regeln für das Arbeiten von zuhause
- Schutz von mobilen Speichermedien
- Sichere Netzwerk-Verbindungen
- Interaktive Übungen
- Wissenstest
- Abschluss

Anzahl Lektionen: 12

Zielgruppe:

Jegliche Mitarbeitende in Ihrem Unternehmen, die von zuhause arbeiten können.

Zusätzliche Materialien:

- Informationsblatt
- Optionen: Animationsfilm, Poster, Quiz, E-Mail und Intranet Informationen.

2. Cyber Security

2.1. Vorsicht vor Schadprogrammen

In diesem Kurs werden Sie lernen, was Schadprogramme sind und wie sie die Arbeitsprozesse einer Firma stören können. Sie werden auch erfahren, wie Schadprogramme dazu benutzt werden, sensitive Informationen zu stehlen.

Technisches:

Sprachen: Deutsch (formell & informell), Englisch, Französisch, Italienisch

Dauer: 10-15 Minuten

Format: SCORM, cmi5, xAPI oder über unser Learning Center

Anpassbar an das Unternehmen: Ja. Zum Beispiel: Vorgaben, Begriffe, Farben, Schrift, Logo, Kontaktdaten und verlinkte Dokumente.

Lernziele:

- Sie kennen die Typen und Risiken von Schadprogrammen und können sie benennen
- Sie verstehen die Verfahren, die Hacker einsetzen, um an Informationen zu gelangen und können diese wiedergeben
- Sie können die Regeln zum Schutz vor Malware anwenden

Lerninhalte:

- Video-Clip
- Risiken
- Szenarien - Mehrteilige, interaktive Kurzgeschichte
- Arten von Malware
- Absatzwege
- Schutzmassnahmen
- Interaktive Übungen
- Wissenstest
- Abschluss

Anzahl Lektionen: 14

Zielgruppe:

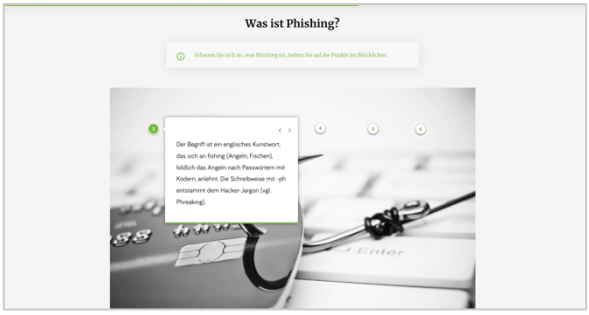
Alle Mitarbeitende in Ihrem Unternehmen.

Zusätzliche Materialien:

- Microlearning «Schutz vor Ransomware»
- Microlearning «Vorsicht vor Ransomware»
- Informationsblatt
- Optionen: Animationsfilm, Poster, Quiz, E-Mail und Intranet Informationen.

2.2.Schutz vor Phishing

In diesem Kurs lernen Sie, um was es bei Phishing geht und worauf es ganz speziell ankommt. Nach einer Einführung lernen Sie Phishing Angriffe zu erkennen und abzuwehren.



Technisches:

Sprachen: Deutsch (formell & informell), Englisch, Französisch, Italienisch

Dauer: 10-15 Minuten

Format: SCORM, cmi5, xAPI oder über unser Learning Center

Anpassbar an das Unternehmen: Ja. Zum Beispiel: Vorgaben, Begriffe, Farben, Schrift, Logo, Kontaktdaten und verlinkte Dokumente.

Lernziele:

- Sie wissen, um was es sich bei Phishing handelt und können dies benennen
- Sie kennen die Risiken von Phishing und können sie aufzählen
- Sie kennen die verschiedenen Arten von Phishing und können diese wiedergeben
- Sie kennen die typischen Merkmale von Phishing E-Mails und können diese beschreiben
- Sie können Phishing E-Mails von richtigen E-Mails unterscheiden

Lerninhalte:

- Video-Clip
- Was ist Phishing und was geht es mich an?
- Szenarien - Mehrteilige, interaktive Kurzgeschichte
- Verschiedene Arten von Phishing
- Wie erkennt man Phishing?
- Was kann man gegen Phishing tun?
- Wissenstest
- Abschluss

Anzahl Lektionen: 20

Zielgruppe:

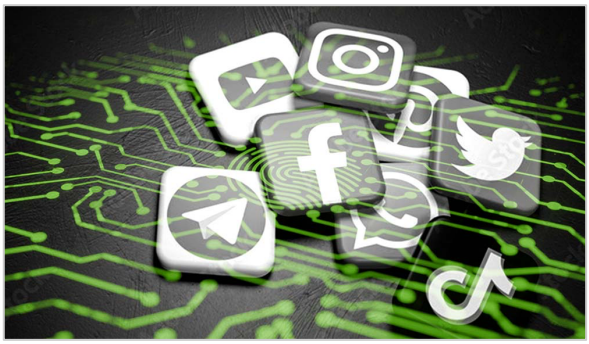
Jegliche Mitarbeitende in Ihrem Unternehmen, die mit E-Mail und Internet arbeiten.

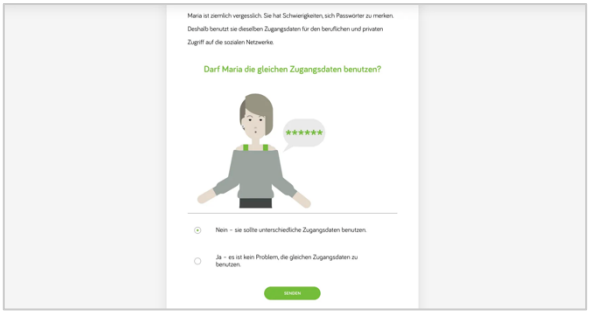
Zusätzliche Materialien:

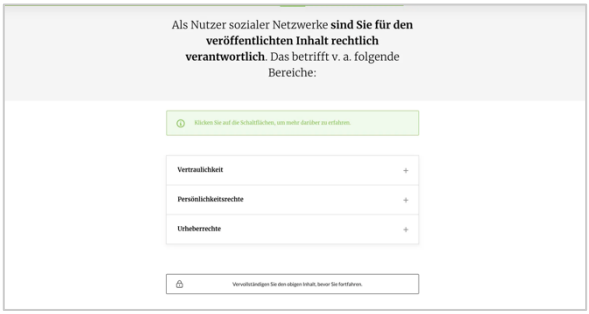
- Microlearning «Phishing-Methoden und grundlegende Schutzmassnahmen»
- Microlearning «Sichere URLs erkennen»
- Informationsblatt
- Optionen: Animationsfilm, Poster, Quiz, E-Mail und Intranet Informationen.

2.3.Umgang mit Social Media

In diesem Kurs werden die Risiken behandelt, die mit sozialen Medien verbunden sind und die gesetzlichen Vorschriften, die Sie bei Veröffentlichungen im Web beachten müssen.







Technisches:

Sprachen: Deutsch (formell & informell), Englisch, Französisch, Italienisch

Dauer: 10-15 Minuten

Format: SCORM, cmi5, xAPI oder über unser Learning Center

Anpassbar an das Unternehmen: Ja. Zum Beispiel: Vorgaben, Begriffe, Farben, Schrift, Logo, Kontaktdaten und verlinkte Dokumente.

Lernziele:

- Sie kennen die Risiken von sozialen Medien und können sie benennen
- Sie verstehen die Regeln beim Umgang mit sozialen Medien und können sie wiedergeben
- Sie können die Regeln und gesetzlichen Grundlagen für soziale Medien anwenden

Lerninhalte:

- Video-Clip
- Risiken
- Szenarien - Mehrteilige, interaktive Kurzgeschichte
- Regeln im Umgang mit sozialen Medien
- Gesunder Menschenverstand
- Rechtsgrundlage
- Interaktive Übungen
- Wissenstest
- Abschluss

Anzahl Lektionen: 14

Zielgruppe:

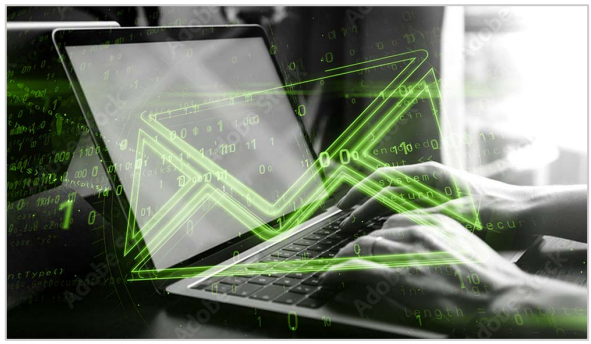
Alle Mitarbeitende in Ihrem Unternehmen.

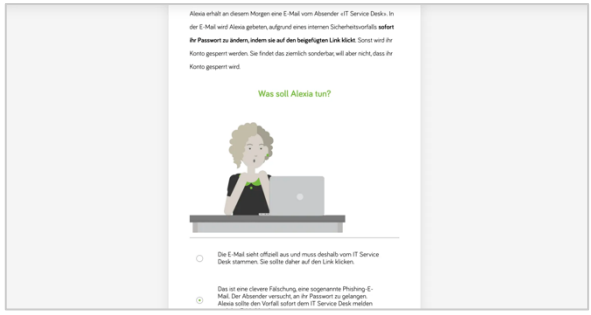
Zusätzliche Materialien:

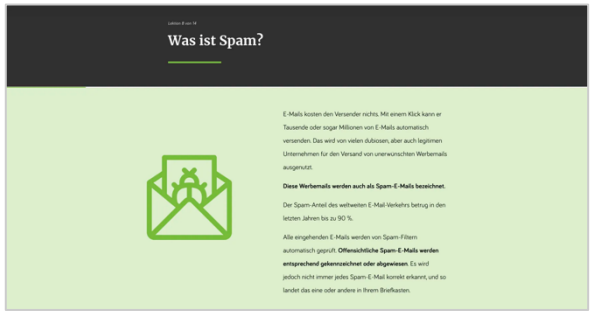
- Informationsblatt
- Optionen: Animationsfilm, Poster, Quiz, E-Mail und Intranet Informationen.

2.4.Umgang mit E-Mail

In diesem Kurs wird Ihnen gezeigt, wie zweifelhafte Personen mit Spam unerwünschte E-Mails verteilen und wie Angreifer Phishing benutzen, um unrechtmässig Informationen von ahnungslosen Opfern zu erhalten.







Technisches:

Sprachen: Deutsch (formell & informell), Englisch, Französisch, Italienisch

Dauer: 10-15 Minuten

Format: SCORM, cmi5, xAPI oder über unser Learning Center

Anpassbar an das Unternehmen: Ja. Zum Beispiel: Vorgaben, Begriffe, Farben, Schrift, Logo, Kontaktdaten und verlinkte Dokumente.

Lernziele:

- Sie kennen die Risiken, die von E-Mails ausgehen können und können sie benennen
- Sie verstehen den Unterschied von Spam und Phishing, und können diese wiedergeben
- Sie können die Schutzmassnahmen für E-Mails anwenden

Lerninhalte:

- Video-Clip
- Risiken
- Szenarien - Mehrteilige, interaktive Kurzgeschichte
- Was ist Spam?
- Was ist Phishing?
- Schutzmassnahmen im Umgang mit E-Mails
- Interaktive Übungen
- Wissenstest
- Abschluss

Anzahl Lektionen: 13

Zielgruppe:

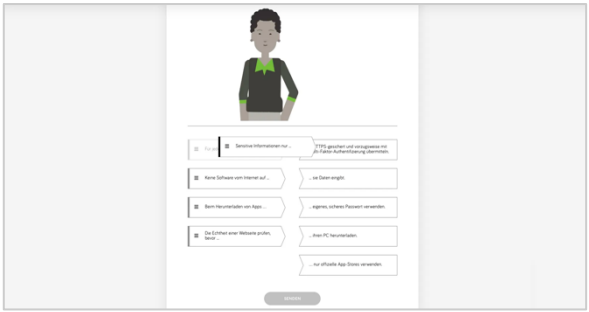
Jegliche Mitarbeitende in Ihrem Unternehmen, die eine E-Mail-Adresse haben oder einen E-Mail-Account verwalten.

Zusätzliche Materialien:

- Informationsblatt
- Optionen: Animationsfilm, Poster, Quiz, E-Mail und Intranet Informationen.

2.5.Verhalten im Internet

In diesem Kurs lernen Sie, wie Sie sich und sensitive Informationen schützen können, wenn Sie auf das Web zugreifen.



Technisches:

Sprachen: Deutsch (formell & informell), Englisch, Französisch, Italienisch

Dauer: 10-15 Minuten

Format: SCORM, cmi5, xAPI oder über unser Learning Center

Anpassbar an das Unternehmen: Ja. Zum Beispiel: Vorgaben, Begriffe, Farben, Schrift, Logo, Kontaktdaten und verlinkte Dokumente.

Lernziele:

- Sie kennen die Risiken des Internets und können sie benennen
- Sie verstehen, worauf Sie achten müssen und können die Schutzmassnahmen wiedergeben
- Sie können die Schutzmassnahmen anwenden

Lerninhalte:

- Video-Clip
- Risiken
- Szenarien - Mehrteilige, interaktive Kurzgeschichte
- Schützen Sie die Verbindung
- Schützen Sie die Passwörter
- Schützen Sie die Informationen
- Schützen Sie den PC
- Interaktive Übungen
- Wissenstest
- Abschluss

Anzahl Lektionen: 13

Zielgruppe:

Jegliche Mitarbeitende in Ihrem Unternehmen, die auf das Web zugreifen können.

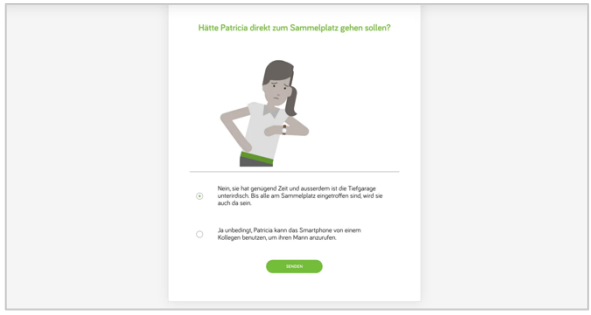
Zusätzliche Materialien:

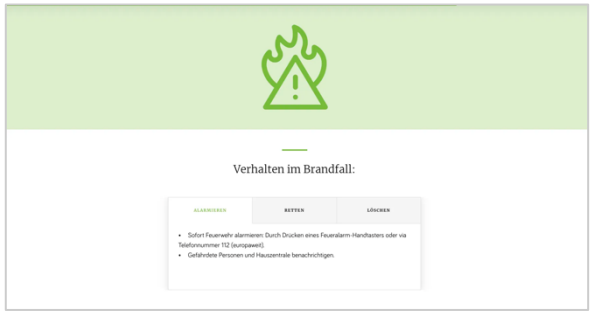
- Informationsblatt
- Optionen: Animationsfilm, Poster, Quiz, E-Mail und Intranet Informationen.

3. Physische Sicherheit

3.1. Erste Hilfe, Feuer & Evakuierung

In diesem Kurs behandeln wir den Evakuierungsprozess und die Massnahmen, die Sie treffen sollten, um sich und Ihre Kollegen zu schützen. Lernen Sie, was Sie im Falle eines Unfalls oder Feuers am Arbeitsplatz tun sollten.





Technisches:

Sprachen: Deutsch (formell & informell), Englisch, Französisch, Italienisch

Dauer: 10-15 Minuten

Format: SCORM, cmi5, xAPI oder über unser Learning Center

Anpassbar an das Unternehmen: Ja. Zum Beispiel: Vorgaben, Begriffe, Farben, Schrift, Logo, Kontaktdaten und verlinkte Dokumente.

Lernziele:

- Sie kennen die Massnahmen zum Schutz von Leib und Leben und können sie benennen
- Sie können die Abläufe bei Unfall oder Brand aufzählen
- Sie verstehen den Evakuierungsprozess und können diesen wiedergeben
- Sie können die Abläufe bei Evakuierung, Brand oder Unfall anwenden

Lerninhalte:

- Video-Clip
- Risiken
- Szenarien - Mehrteilige, interaktive Kurzgeschichte
- Evakuierung
- Feuer
- Unfälle – gute Vorbereitung ist wichtig
- Unfälle – was sollten Sie tun?
- Interaktive Übungen
- Wissenstest
- Abschluss

Anzahl Lektionen: 14

Zielgruppe:

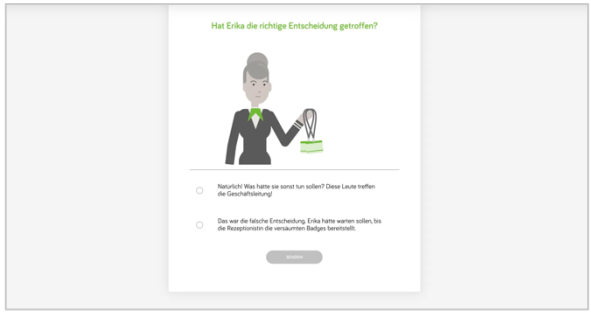
Alle Mitarbeitende in Ihrem Unternehmen.

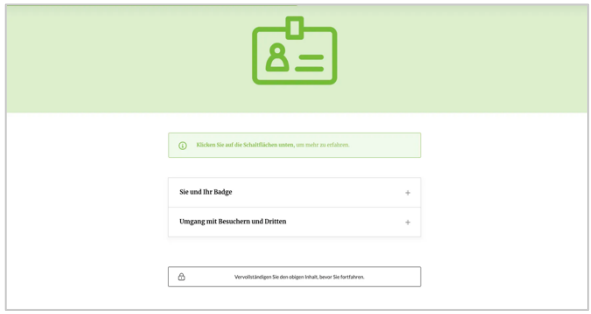
Zusätzliche Materialien:

- Microlearning «Herzdruckmassage & Defibrillator - wie Sie Leben retten können»
- Informationsblatt
- Optionen: Animationsfilm, Poster, Quiz, E-Mail und Intranet Informationen.

3.2.Gebäudezutritte und Umgang mit Besuchern

Dieser Kurs behandelt die Notwendigkeit, einen Personalausweis zu tragen und die Sicherheitsrisiken, die mit nicht autorisierten Personen in Geschäftsräumlichkeiten verbunden sind.





Technisches:

Sprachen: Deutsch (formell & informell), Englisch, Französisch, Italienisch

Dauer: 10-15 Minuten

Format: SCORM, cmi5, xAPI oder über unser Learning Center

Anpassbar an das Unternehmen: Ja. Zum Beispiel: Vorgaben, Begriffe, Farben, Schrift, Logo, Kontaktdaten und verlinkte Dokumente.

Lernziele:

- Sie können die Sicherheitsrisiken, welche mit nicht autorisierten Personen in unseren Räumlichkeiten verbunden sind, benennen
- Sie verstehen die Wichtigkeit, einen Ausweis zu tragen und können die Handhabung mit demselben wiedergeben
- Sie können die Regeln im Umfang mit Besuchern anwenden

Lerninhalte:

- Video-Clip
- Risiken
- Szenarien - Mehrteilige, interaktive Kurzgeschichte
- Was wird von Ihnen erwartet?
- Interaktive Übungen
- Wissenstest
- Abschluss

Anzahl Lektionen: 10

Zielgruppe:

Jegliche Mitarbeitende in Ihrem Unternehmen, die einen Mitarbeiterausweis haben und Besuchern begegnen könnten.

Zusätzliche Materialien:

- Informationsblatt
- Optionen: Animationsfilm, Poster, Quiz, E-Mail und Intranet Informationen.

4. Compliance

4.1.Einführung in den Datenschutz

Dieser Kurs bietet Antworten auf Fragen über den Datenschutz und nützliche Tipps für Ihre tägliche Arbeit. Zudem lernen Sie die verschiedenen Kategorien von Personendaten kennen und welche Formen der «Bearbeitung» es gibt. Eine besondere Beachtung finden dabei auch die Anforderungen an die Datenbearbeitung durch Dritte oder im Ausland.

Technisches:

Sprachen: Deutsch (formell & informell), Englisch, Französisch, Italienisch

Dauer: 20-25 Minuten

Format: SCORM, cmi5, xAPI oder über unser Learning Center

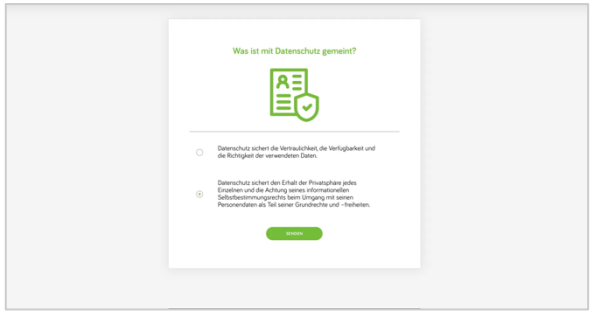
Anpassbar an das Unternehmen: Ja. Zum Beispiel: Vorgaben, Begriffe, Farben, Schrift, Logo, Kontaktdaten und verlinkte Dokumente.

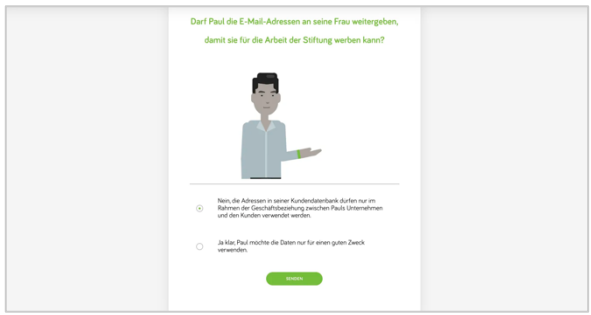
Lernziele:

- Sie können die Ziele des Datenschutzes benennen
- Sie kennen die Kategorien von personenbezogenen Daten
- Sie können die Grundsätze für eine sichere und datenschutzkonforme Verarbeitung personenbezogener Daten anwenden
- Sie kennen die Rechte von Personen, deren Daten verarbeitet werden und können diese aufzählen
- Sie wissen, welche Massnahmen für eine Weitergabe von personenbezogenen Daten an Dritte im In- oder ins Ausland notwendig sind

Lerninhalte:

- Video-Clip
- Was bringt mir Datenschutz?
- Szenarien - Mehrteilige, interaktive Kurzgeschichte
- Kontext und Ziel des Datenschutzes
- Rechtliche Grundlagen (Schweiz/Europa)





- Kategorien personenbezogener Daten
- Verarbeitung personenbezogener Daten
- Rechte der betroffenen Person
- Schutzmassnahmen
- Interaktive Übungen
- Wissenstest
- Abschluss

Anzahl Lektionen: 12

Zielgruppe:

Jegliche Mitarbeitende in Ihrem Unternehmen, die mit unterschiedlichen Daten in Berührung kommen.

Zusätzliche Materialien:

- Informationsblatt
- Optionen: Animationsfilm, Poster, Quiz, E-Mail und Intranet Informationen.

5. Spezifische Zielgruppen

5.1. Sicherheit für Führungskräfte

Dieses Modul gibt Hinweise, wichtige Regeln und nützliche Tipps für den verantwortungsvollen Führungsalltag. Dabei werden Führungsaufgaben und -verantwortung im Hinblick auf die Sicherheit adressiert und anhand des Employee Life Cycles dargelegt. Einer besonderen Rolle kommt dabei der Vorbildfunktion und der Mitarbeiterbefähigung zu.

Technisches:

Sprachen: Deutsch (formell & informell), Englisch, Französisch, Italienisch

Dauer: 10-15 Minuten

Format: SCORM, cmi5, xAPI oder über unser Learning Center

Anpassbar an das Unternehmen: Ja. Zum Beispiel: Vorgaben, Begriffe, Farben, Schrift, Logo, Kontaktdaten und verlinkte Dokumente.

Lernziele:

- Sie kennen Ihre Führungsaufgaben betreffend Sicherheit
- Sie erkennen, dass Ihnen eine wichtige Vorbildfunktion zukommt
- Sie wissen, welche Aufgaben Sie im Employee Life Cycle erfüllen müssen
- Sie kennen die Angebote von Security und die wichtigen Kontaktstellen
- Sie können mit Notfällen richtig umgehen

Lerninhalte:

- Video-Clip
- Risiken
- Führungsverantwortung (Klassifizierung, Datenschutz, Vorbildfunktion)
- Ihre Aufgabe im Employee Life Cycle
- Mitarbeiterbefähigung (Physische Sicherheit, Mitarbeiter Trainings, Melden von Sicherheitsvorfällen)
- Kontaktstellen
- Interaktive Übungen
- Wissenstest
- Abschluss

Anzahl Lektionen: 11

Zielgruppe:

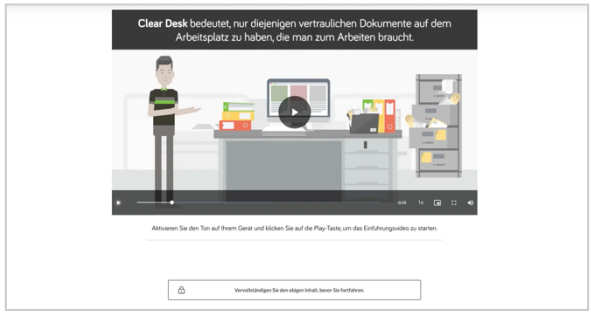
Mitarbeitende mit Führungs- oder Projektleitungsfunktion.

Zusätzliche Materialien:

- Informationsblatt
- Optionen: Animationsfilm, Poster, Quiz, E-Mail und Intranet Informationen.

5.2.Grundschulung Informationssicherheit

Dieses Modul ist für die Grundschulung von allen Mitarbeitenden geeignet. Dazu zählen auch Lernende und Externe. In diesem Modul werden sieben Informationssicherheitsthemen in verkürzter Form behandelt, um die Mitarbeitenden nach Abschluss in die jeweiligen Kampagnen zu integrieren.



Technisches:

Sprachen: Deutsch (formell & informell), Englisch, Französisch, Italienisch

Dauer: 20-25 Minuten

Format: SCORM, cmi5, xAPI oder über unser Learning Center

Anpassbar an das Unternehmen: Ja. Zum Beispiel: Vorgaben, Begriffe, Farben, Schrift, Logo, Kontaktdaten und verlinkte Dokumente.

Lernziele:

- Sie wissen, welche Themen Informationssicherheit u. a. beinhaltet und kennen die damit verbundenen Risiken.
- Sie verstehen die Risiken und Massnahmen dieser Themen und können diese wiedergeben.
- Sie können vorbeugende Massnahmen ergreifen und die Verhaltensregeln anwenden.

Lerninhalte:

- Risiken
- Sichere Passwörter
- Der korrekte Umgang mit Daten
- Verhaltensregeln zu Clear Desk/Clear Screen
- Umgang mit E-Mail bzw. Phishing
- Das korrekte Verhalten im Internet
- Arbeiten unterwegs
- Sicherheitsvorfälle melden
- Richtlinien
- Interaktive Übungen
- Wissenstest

Anzahl Lektionen: 24

Zielgruppe:

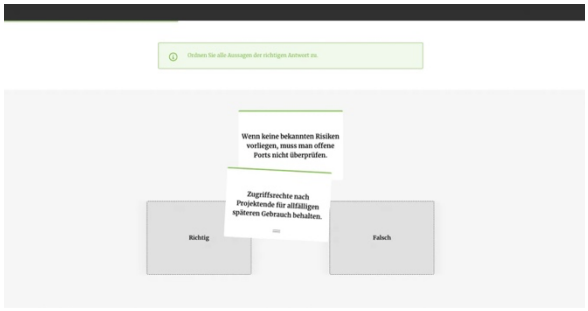
Alle Mitarbeitende in Ihrem Unternehmen.

Zusätzliche Materialien:

- Informationsblatt
- Optionen: Animationsfilm, Poster, Quiz

5.3.Informationssicherheit für IT-Administratoren: Wichtige Konzepte

In diesem Lernmodul erfahren Sie die wichtigsten Konzepte für IT-Administratoren in Bezug auf Informationssicherheit. Es werden die Risiken erläutert, welche durch eine unsachgemässe Handhabung entstehen können. Die Konzepte und damit verbundenen Verhaltensweisen werden aufgezeigt, welche IT-Administratoren umsetzen sollten, um sich und das Unternehmen zu schützen.



Technisches:

Sprachen: Deutsch (formell & informell), Englisch, Französisch, Italienisch

Dauer: 12-16 Minuten

Format: SCORM, cmi5, xAPI oder über unser Learning Center

Anpassbar an das Unternehmen: Ja. Zum Beispiel: Vorgaben, Begriffe, Farben, Schrift, Logo, Kontaktdaten und verlinkte Dokumente.

Lernziele:

- Sie kennen die für IT-Administratoren wichtigen Konzepte der Informationssicherheit und die damit verbundenen Risiken.
- Sie verstehen die Risiken und Massnahmen dieser Themen und können diese wiedergeben.
- Sie können vorbeugende Massnahmen ergreifen und die Verhaltensregeln anwenden.

Lerninhalte:

- Risiken
- Verantwortlichkeiten und Anlaufstelle
- Privilegien und Verantwortung
- Passwortanforderungen für Admin- und Dienstkonten
- Sicherheit als Standard (Security by Default)
- Minimale Rechte
- Verarbeitung personenbezogener Daten
- Melden von Sicherheitsvorfällen
- Wissenstest
- Szenarien
- Übungen

Anzahl Lektionen: 17

Zielgruppe:

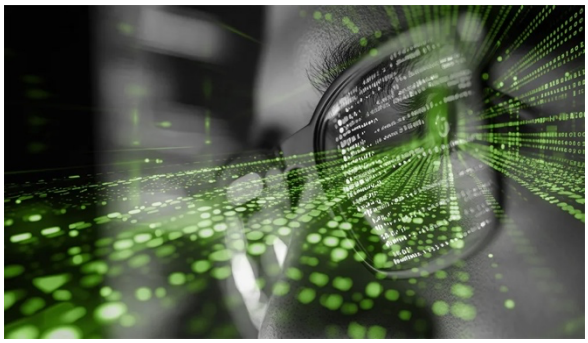
IT-Administratoren und IT-Administratorinnen

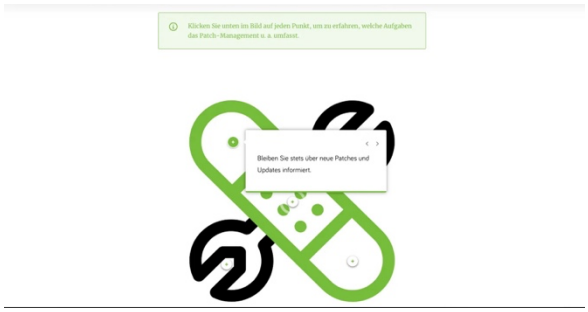
Zusätzliche Materialien:

- Keine

5.4.Informationssicherheit für IT-Administratoren: Sichere IT-Dienste

In diesem Lernmodul erfahren Sie, auf was Sie achten müssen, um sichere IT-Dienste zu gewährleisten. Es werden die Risiken erläutert, welche durch eine unsachgemässe Handhabung entstehen können. Es wird aufgezeigt, wie Sie IT-Dienste sicherer machen und auf was Sie achten müssen, um sich und das Unternehmen zu schützen.





Technisches:

Sprachen: Deutsch (formell & informell), Englisch, Französisch, Italienisch

Dauer: 12-16 Minuten

Format: SCORM, cmi5, xAPI oder über unser Learning Center

Anpassbar an das Unternehmen: Ja. Zum Beispiel: Vorgaben, Begriffe, Farben, Schrift, Logo, Kontaktdaten und verlinkte Dokumente.

Lernziele:

- Sie kennen die mit der Tätigkeit als IT-Administrator/-in verbundene Verantwortung in Bezug auf Sicherheit und können diese anwenden.
- Sie verstehen die Risiken, die mit unsicheren IT-Diensten verbunden sind und können diese wiedergeben.
- Sie können vorbeugende Massnahmen ergreifen, um sichere IT-Dienste bereitzustellen und die Sicherheitspraktiken anwenden.

Lerninhalte:

- Risiken
- Sichere Bereitstellung
- Tiefenverteidigung
- Patching und Behebung von Schwachstellen
- Planung für den Fall des Scheiterns
- Forensische Bereitschaft, Protokollierung und Alarmierung
- Ziele und Nutzen von Audits und Kontrollen
- Melden von Sicherheitsvorfällen
- Wissenstest
- Szenarien
- Übungen

Anzahl Lektionen: 16

Zielgruppe:

IT-Administratoren und IT-Administratorinnen

Zusätzliche Materialien:

- Keine

6. Gamifizierte Kurse (Superhelden)

6.1.Soziale Medien

In diesem game-based Kurs werden wir über die Risiken sprechen, die mit sozialen Medien verbunden sind und über die gesetzlichen und firmenspezifischen Vorschriften, die Sie bei Veröffentlichungen im Web beachten müssen.

Technisches:

Sprachen: Deutsch (formell & informell), Englisch, Französisch, Italienisch

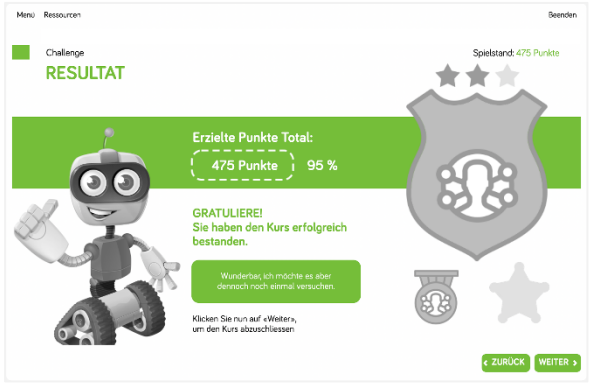
Dauer: 15-20 Minuten

Format: SCORM, cmi5, xAPI oder über unser Learning Center

Anpassbar an das Unternehmen: Ja. Zum Beispiel: Vorgaben, Begriffe, Farben, Schrift, Logo, Kontaktdaten und verlinkte Dokumente.

Lernziele:

- Sie kennen die Gefahren von sozialen Medien und können sie aufzählen
- Sie verstehen die Regeln beim Umgang mit sozialen Medien und können sie wiedergeben
- Sie können die Regeln und gesetzlichen Grundlagen für soziale Medien anwenden
- Sie wissen, wie Sie Geschäftsdaten schützen müssen
- Sie sind in der Lage, bei einem Vorfall rasch und richtig zu reagieren



Lerninhalte:

- Video-Clip
- Risiken
- Szenarien - Mehrteilige, interaktive Kurzgeschichte
- Regeln für soziale Medien
- Ihre Profile auf sozialen Medien
- Rechtsgrundlage
- Umgang mit schwierigen Situationen
- Challenges und Resultate
- Abschluss

Zusätzliche Materialien:

- Informationsblatt
- Optionen: Animationsfilm, Poster, Quiz, E-Mail und Intranet Informationen.

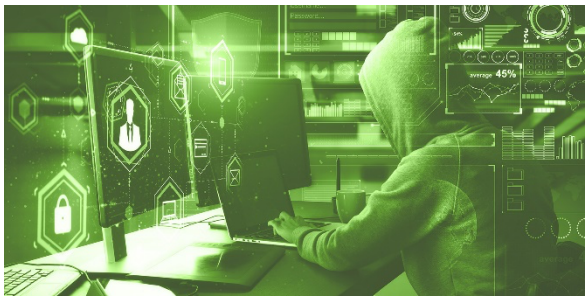
Anzahl Lektionen: 20

Zielgruppe:

Alle Mitarbeitende in Ihrem Unternehmen.

6.2.Social Engineering

In diesem game-based Kurs lernen Sie, um was es bei Social Engineering geht und worauf es ganz speziell ankommt. Nach einer Einführung lernen Sie in einer Game Challenge, Social Engineering Angriffe zu erkennen und abzuwehren.



Technisches:

Sprachen: Deutsch (formell & informell), Englisch, Französisch, Italienisch

Dauer: 15-20 Minuten

Format: SCORM, cmi5, xAPI oder über unser Learning Center

Anpassbar an das Unternehmen: Ja. Zum Beispiel: Vorgaben, Begriffe, Farben, Schrift, Logo, Kontaktdaten und verlinkte Dokumente.

Lernziele:

- Sie kennen die Risiken von Social Engineering und können sie aufzählen
- Sie verstehen, wie ein Social Engineer vorgeht und können das beschreiben
- Sie kennen den Ablauf einer Social Engineering Attacke und können diese erklären
- Sie können die Massnahmen zum Schutz vor Social Engineering anwenden

Lerninhalte:

- Einleitung und Anweisungen
- Das ist unser Social Engineer Guy Fawkes
- Stufe 1: Informationen sammeln und Quiz
- Stufe 2: E-Mails verschicken und Quiz
- Stufe 3: Anrufen und Quiz
- Stufe 4: Persönliches Treffen und Quiz
- Stufe 5: Loslegen und Quiz
- Stufe 6: Die Früchte ernten und Quiz
- Zusammenfassung und Gesamtpunktzahl

Anzahl Lektionen: 21

Zielgruppe:

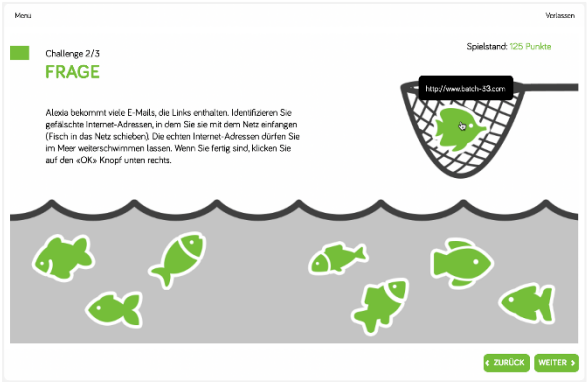
Alle Mitarbeitende in Ihrem Unternehmen, besonders wenn sie mit sensiblen Daten in Berührung kommen wie Finanzen, HR oder Geschäftsleitung.

Zusätzliche Materialien:

- Informationsblatt
- Optionen: Animationsfilm, Poster, Quiz, E-Mail und Intranet Informationen.

6.3.Schutz vor Phishing

In diesem game-based Kurs lernen Sie, um was es bei Phishing geht und worauf es ganz speziell ankommt. Nach einer Einführung lernen Sie in einer Game Challenge, Phishing Angriffe zu erkennen und abzuwehren.



Technisches:

Sprachen: Deutsch (formell & informell), Englisch, Französisch, Italienisch

Dauer: 15-20 Minuten

Format: SCORM, cmi5, xAPI oder über unser Learning Center

Anpassbar an das Unternehmen: Ja. Zum Beispiel: Vorgaben, Begriffe, Farben, Schrift, Logo, Kontaktdaten und verlinkte Dokumente.

Lernziele:

- Sie wissen, um was es sich bei Phishing handelt, und können dies benennen
- Sie kennen die Risiken von Phishing und können sie aufzählen
- Sie kennen die verschiedenen Arten von Phishing und können diese wiedergeben
- Sie kennen die typischen Merkmale von Phishing E-Mails und können diese beschreiben
- Sie können Phishing E-Mails von richtigen E-Mails unterscheiden

Lerninhalte:

- Video-Clip
- Was ist Phishing und was geht es mich an?
- Szenarien - Mehrteilige, interaktive Kurzgeschichte
- Verschiedene Arten von Phishing
- Wie erkennt man Phishing?
- Was kann man gegen Phishing tun?
- Challenges und Resultate
- Abschluss

Anzahl Lektionen: 20

Zielgruppe:

Jegliche Mitarbeitende in Ihrem Unternehmen, die mit E-Mail und Internet arbeiten.

Zusätzliche Materialien:

- Informationsblatt
- Optionen: Animationsfilm, Poster, Quiz, E-Mail und Intranet Informationen.

TreeSolution Security Awareness AG
+41 58 510 98 00
info@treesolution.com
www.treesolution.com