E-Learning Cyber Security

Schützen Sie Ihr Unternehmen, sensibilisieren Sie Ihre Mitarbeiterinnen und Mitarbeiter.

E-Learning Cyber Security

Risiken erkennen

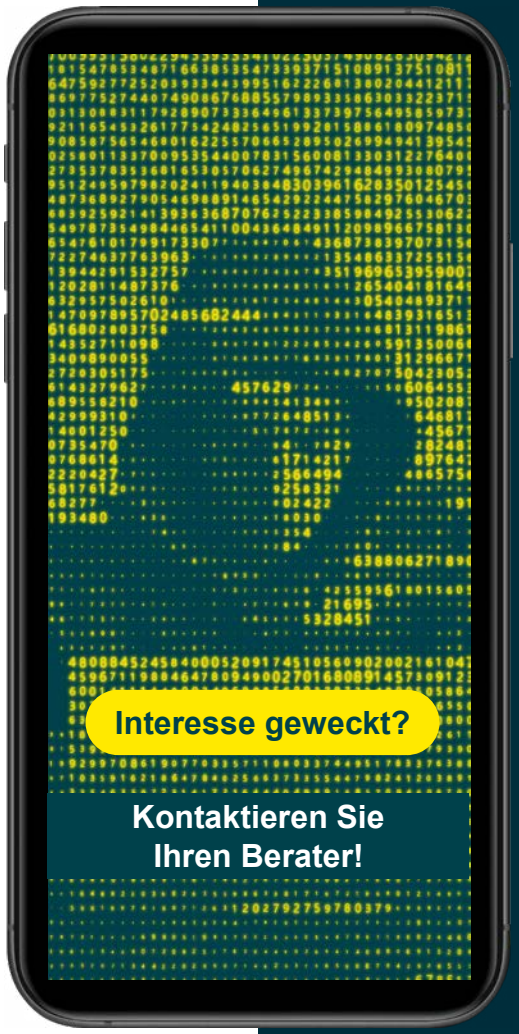
Cyberkriminelle nutzen zunehmend die „Schwachstelle Mensch“. Durch professionelle Täuschung und Beeinflussung von Mitarbeitenden gelangen sie in Unternehmensnetzwerke, greifen sensible Daten ab bzw. lassen hohe Zahlungen autorisieren.

Mitarbeitende schulen

Schützen Sie sich durch Sensibilisierung Ihrer Mitarbeitenden. Auf Basis unseres hohen Erfahrungsschatzes aus Betrugsversuchen und -fällen haben wir für Sie das passende E-Learning für die Cyber Security erstellt: eine digitale Schulung, die durch ausgewählte Praxisbeispiele Lerninhalte zum Thema Betrugsbekämpfung vermittelt.

Vorteile nutzen

- ✓ **Kostengünstige Schulung** (im Vergleich zu Präsenzkursen oder eigener Konzeption)
- ✓ **Sensibilisierung Ihrer Mitarbeitenden**
- ✓ **Ortsunabhängiger digitaler Zugang und flexible Lernzeit**
- ✓ **Erhalt eines Abschlusszertifikats**



CEO Fraud

Umleitung von Zahlungsströmen

Krypto-Trojaner

Fernwartungs-software

Alle Themen der Schulung auf einen Blick

Schulungsinhalte: Grundlagen & Praxis

Technische Bedrohungen
Würmer, Trojaner, Viren

Menschliche Bedrohungen
Social Engineering, Phishing, Manipulation

Cyber Security in der Praxis
Kryptotrojaner, Fernwartungssoftware, Umleitung von Zahlungsströmen, CEO-Fraud

Das E-Learning auf einen Blick

Zusatzleistung & Lernerfolg

Wissens-Check
Im Anschluss an die Schulung wird eine Lernkontrolle in Form eines Quiz durchgeführt.

Handlungsempfehlungen
Nützliche Tipps und Tricks für den Notfall

Zertifikat
Nach erfolgreicher Beendigung des Wissens-Checks wird dem Mitarbeitenden ein Zertifikat ausgestellt.

Ihnen werden die Grundlagen der Cybersicherheit dargelegt und anschließend echte Praxisbeispiele vorgestellt.

Unser E-Learning ist interaktiv

Unser E-Learning ist eine interaktive Schulung.

Ihre Mitarbeiter werden durch unser multimediales Konzept mit Animationen, Quizfragen, Audios und weiteren abwechslungsreichen Formaten spielerisch durch die praxisnahe Schulung geführt.

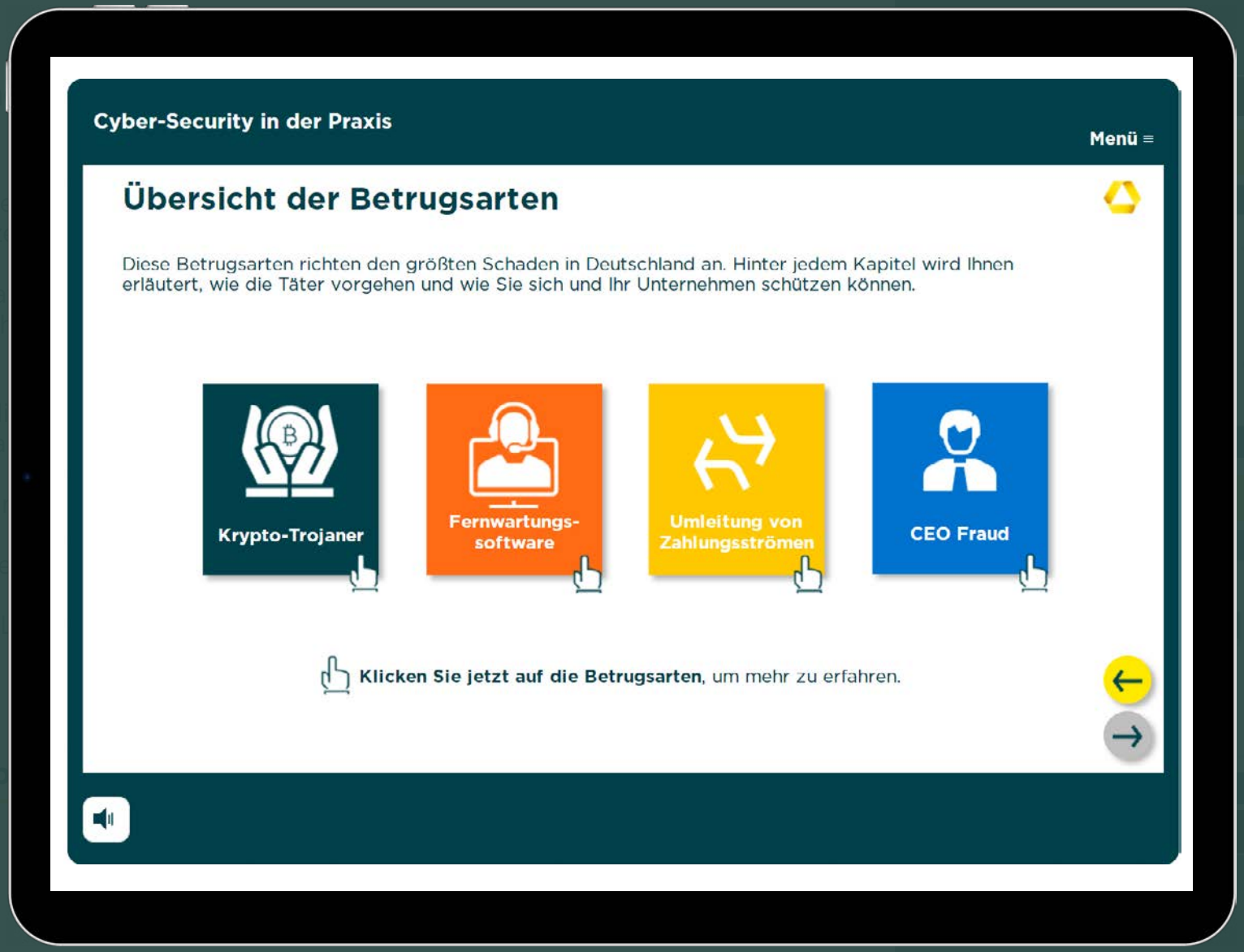
- Kein langweiliges stundenlanges Anschauen von Videomaterial
- Keine abgefilmten Vorträge
- Keine ermüdenden Onlineseminare
- Keine festen Lerntermine

„Kurzweilig, spannend, nicht öde.“

Kundenzitat

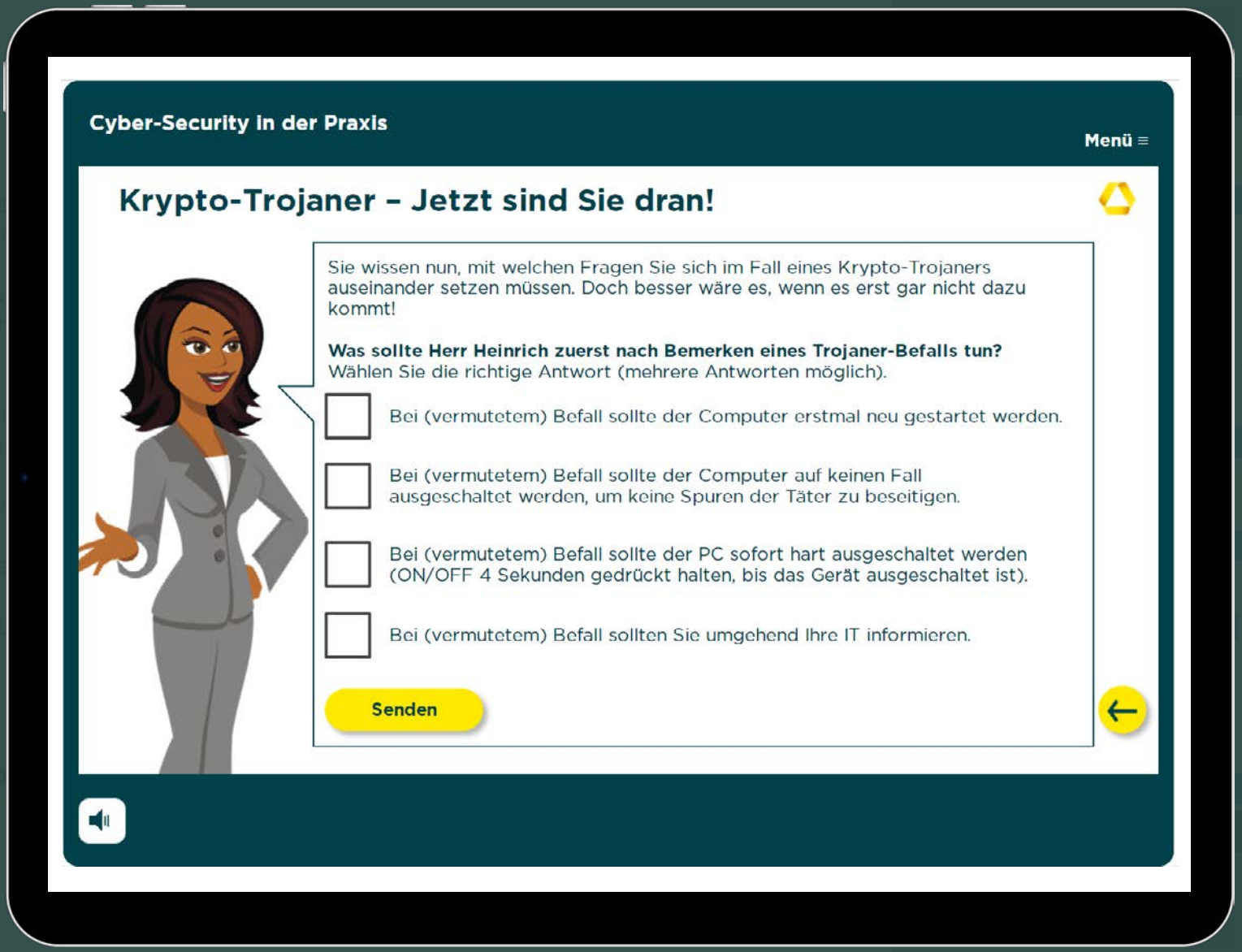
Klicken Sie auf ein Thema für die Detailansicht.

Übersichtliche Gestaltung



Reale Beispiele

Quizfragen


Cyber-Security in der Praxis
Menü ≡
Krypto-Trojaner – Jetzt sind Sie dran!
Sie wissen nun, mit welchen Fragen Sie sich im Fall eines Krypto-Trojaners auseinander setzen müssen. Doch besser wäre es, wenn es erst gar nicht dazu kommt!
Was sollte Herr Heinrich zuerst nach Bemerken eines Trojaner-Befalls tun?
Wählen Sie die richtige Antwort (mehrere Antworten möglich).
Bei (vermutetem) Befall sollte der Computer erstmal neu gestartet werden.
Bei (vermutetem) Befall sollte der Computer auf keinen Fall ausgeschaltet werden, um keine Spuren der Täter zu beseitigen.
Bei (vermutetem) Befall sollte der PC sofort hart ausgeschaltet werden (ON/OFF 4 Sekunden gedrückt halten, bis das Gerät ausgeschaltet ist).
Bei (vermutetem) Befall sollten Sie umgehend Ihre IT informieren.
Senden

Klick-Schulung

Unsere Zusatzleistungen

Das Abschlusszertifikat:
Das Zertifikat gilt als Nachweis für die bestandene Schulung.

Einfacher Download:
Jeder Ihrer Mitarbeitenden kann das erworbene Zertifikat einfach und schnell online herunterladen – zu Zwecken der Dokumentation.

Die Handlungsempfehlungen:
Ihre Mitarbeitenden erhalten im Anschluss an die Schulung kurze Handlungsempfehlungen für Notfälle.

Ihr Ansprechpartner:
Sie erhalten mit den Handlungsempfehlungen neben Ihrem Firmenkundenbetreuer oder CTS-Sales den Namen eines Ansprechpartners der Commerzbank für Betrugsfälle.

Das Abschlusszertifikat

Die Handlungsempfehlungen

Unsere Zusatzleistungen

Das Abschlusszertifikat:
Das Zertifikat gilt als Nachweis für die bestandene Mitarbeiterschulung.

Einfacher Download
Jeder Ihrer Mitarbeiter*innen kann das erworbene Zertifikat einfach und schnell online herunterladen – zu Zwecken der Dokumentation.

Die Handlungsempfehlungen:
Ihre Mitarbeiter*innen erhalten im Anschluss an die Schulung eine kurze Handlungsempfehlung für Notfälle.

COMMERZBANK

Max Mustermann

hat am 6. August 2021 das

E-Learning Cyber-Security

- Grundlagen
- Cybercrime in der Praxis
- Handlungsempfehlungen & Prävention

der Commerzbank AG erfolgreich abgeschlossen.

Frank-Oliver Wolf
Global Head of Sales Germany

Commerzbank AG
Corporate Banking
Transaction Banking

Klicken Sie auf ein Thema für die Detailansicht

Cyber-Security - Handlungsempfehlungen

COMMERZBANK

Wie können Sie sich am besten schützen? – Tipps & Tricks

Kommunikationskultur

- Überlegen Sie im Vorfeld, wer in der Firma welche Verantwortung für die interne Kommunikation und Reaktion im Schadensfall trägt.
- Machen Sie sich Gedanken darüber, wer innerhalb und außerhalb des Unternehmens unmittelbar informiert werden sollte.
- **Tipp:** Sprechen Sie Ihre Geschäftsleitung oder IT-Abteilung an, welche Maßnahmen es für die Prävention und den Ernstfall gibt.

Schadsoftware / Krypto-Trojaner

- Öffnen Sie keine Datei-Anhänge von unerwarteten E-Mails, vor allem keine ZIP-Dateien mit Passwortschutz.
- Aktivieren Sie in geöffneten, verdächtigen Office-Dateien nicht den Bearbeitungsmodus und folgen Sie keinen Systemmeldungen.
- Nutzen Sie für Bewerbungen einen Rechner (oder Tablet) außerhalb Ihres Firmennetzwerks. Auch PDFs können Schadcode enthalten.
- Klicken Sie nicht auf Links in einer verdächtigen E-Mail. Öffnen Sie die entsprechende Internetseite in einem neu geöffneten Internetbrowser durch Eingabe der bekannten Internetadresse.
- Überdenken Sie den Einsatz von USB-Sticks am Arbeitsplatz.

Fernwartung

- Haben Sie technische Hilfe erbeten und es ruft Sie hierzu ein erwarteter Ansprechpartner Ihrer Firma an, dann ist ein Betrug unwahrscheinlich.
- Drängt Ihnen jemand Software auf und versucht Ihnen Probleme glaubhaft zu machen, wird es vermutlich Betrug sein!
- Verweigern Sie den Zugriff, bieten Sie einen Rückruf an und notieren Sie sich die Rufnummer. Gehen Sie dann auf Ihre IT und/oder Ihren Vorgesetzen zu, um den Vorfall zu validieren.

1

COMMERZBANK