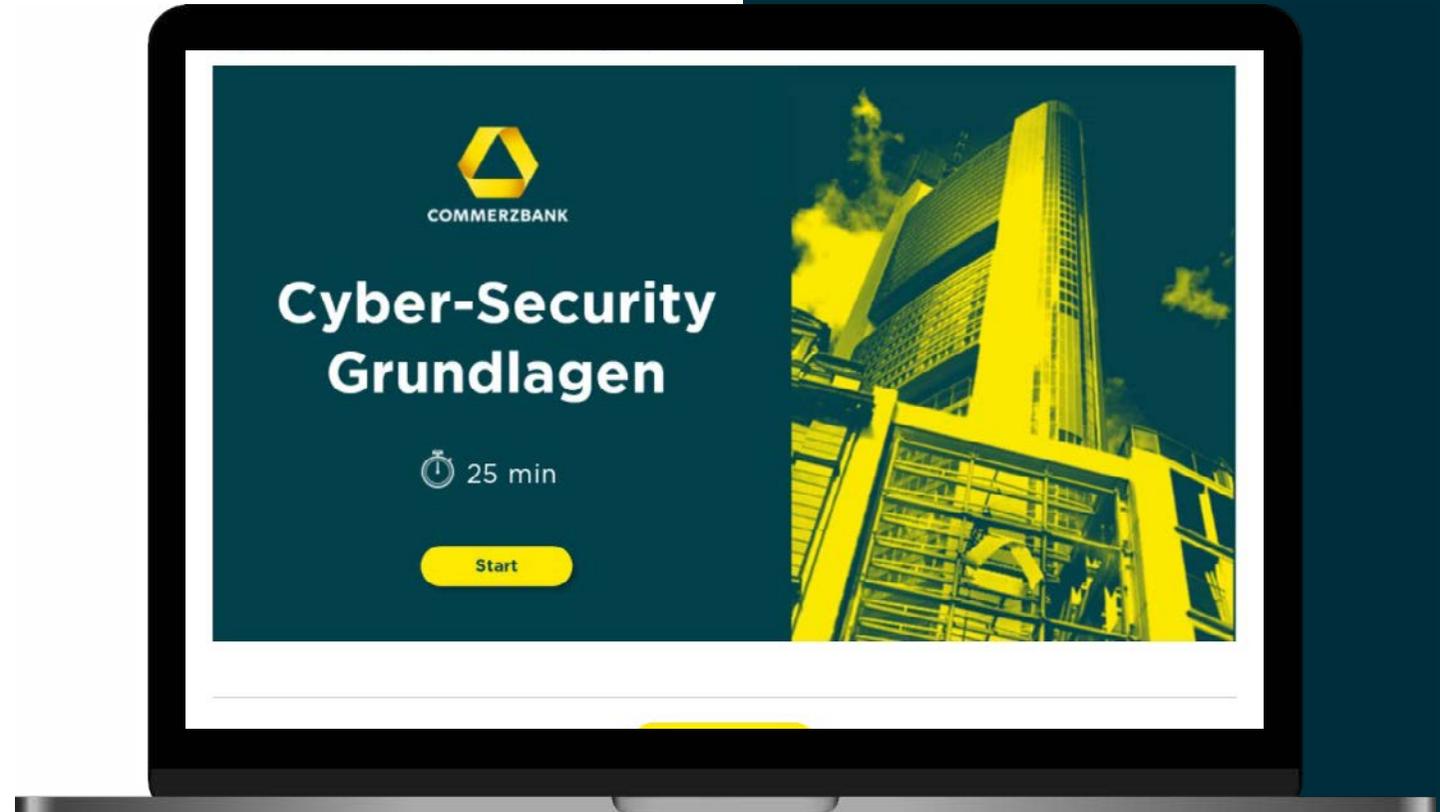


E-Learning Cyber Security



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



Fernwartungssoftware

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

Übersichtliche Gestaltung

Cyber-Security in der Praxis

Übersicht der Betrugsarten

Diese Betrugsarten richten den größten Schaden in Deutschland an. Hinter jedem Kapitel wird Ihnen erläutert, wie die Täter vorgehen und wie Sie sich und Ihr Unternehmen schützen können.

Krypto-Trojaner Fremdwort-Software Umleitung von Zahlungsverbindungen CEO Fraud

Klicken Sie jetzt auf die Betrugsarten, um mehr zu erfahren.

Reale Beispiele

Cyber-Security in der Praxis

Umleitung von Zahlungsströmen

Monika ist Mitarbeiterin der Muster GmbH. Sie bearbeitet aktuell einen Auftrag an Jeff, einem bekannten Zulieferer. Die Kommunikationen zwischen den beiden erfolgt per E-Mail.

Monika: monika@muster.de Jeff: jeff@zulieferer.com

ADK: jeff@zulieferer.com

Auftragsbestätigung

Hiermit bestätigen wir den Auftrag

GIAN DE12 3334 5566 7788 9900 33

BIC: H2483333

Warenbestellung

Auftragsbestätigung

Quiz Fragen

Cyber-Security in der Praxis

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 hier Heinrich zuerst nach Bemerkten eines Trojaner-Befalls tun? Wählen Sie die richtige Antwort (mehrere Antworten möglich).

- Bei (vermutetem) Befall sollte der Computer erstmalig 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 (Ctrl+Shift+4 Sekunden gedrückt halten, bis das Gerät ausgeschaltet ist).
- Bei (vermutetem) Befall sollten Sie umgehend Ihre IT informieren.

Senden

Klick-Schulung

Cyber-Security in der Praxis

Krypto-Trojaner

Welche Fragen sollten sich die Geschäftsleitung und IT-Spezialisten stellen?

Muss ich die Polizei einschalten? Oder lieber noch warten?

Wann informiere ich meine Bank?

Sollte meine eigene IT das Problem lösen?

Klicken Sie jetzt auf die Fragen, um mehr zu erfahren.

Klicken Sie auf ein Thema für die Detailsicht.



Übersichtliche Gestaltung



Reale Beispiele

Cyber-Security in der Praxis Menü ≡

Umleitung von Zahlungsströmen

Monika ist Mitarbeiterin der Muster GmbH. Sie bearbeitet aktuell einen Auftrag an Jeff, einem bekannten Zulieferer. Die Kommunikation zwischen den beiden erfolgt per E-Mail.

Warenbestellung →

Auftragsbestätigung ←

Monika
monika@einkäuferin.de

Jeff
jeff@zulieferer.com

Abs.: jeff@zulieferer.com

Auftragsbestätigung
Hiermit bestätigen wir den Auftrag

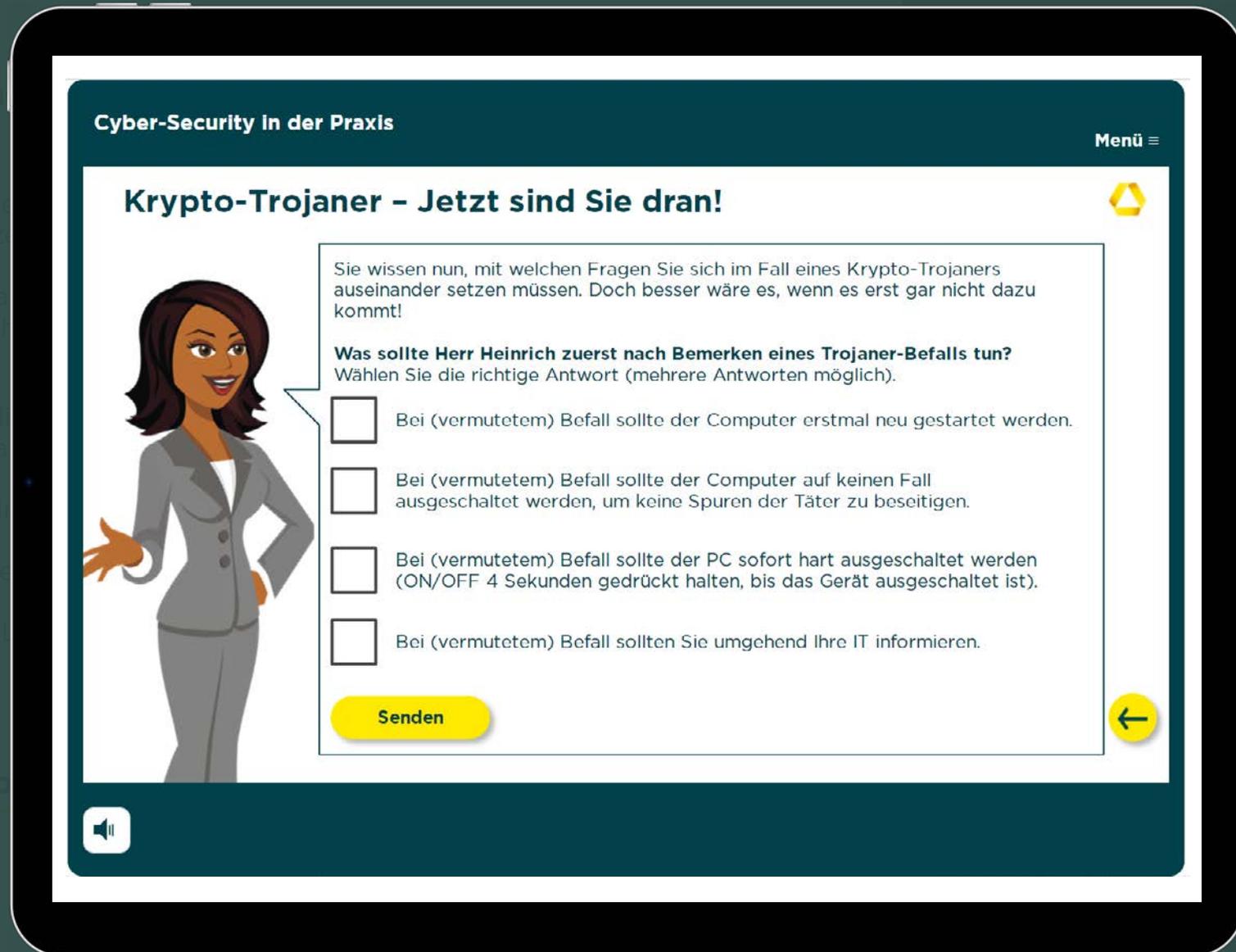
IBAN: DE12 3334 5566 7788 9900 33
BIC: HZUJBNZW

Navigation: ← →

Speaker icon: 🔊



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 ←



Unser E-Learning
Schulung.

Ihre Mitarbeiter im
multimediales Kon-
Quizfragen, Audio-
lungsreichen Form-
und spielerische Sch-

✓ Kein langweil-
Videomaterial

✓ Keine abgefil-

✓ Keine ermüd-

✓ Keine festen

„kurzweilig, sp-

Klick-Schulung



The screenshot shows an interactive e-learning interface. At the top, it says 'Cyber-Security in der Praxis' and 'Menü ='. The main title is 'Krypto-Trojaner'. Below the title, a question asks: 'Welche Fragen sollten sich die Geschäftsleitung und IT-Spezialisten stellen?'. There are three interactive buttons with question marks and hand icons: 'Muss ich die Polizei einschalten? Oder lieber noch warten?', 'Wann informiere ich meine Bank?', and 'Sollte meine eigene IT das Problem lösen?'. On the left, there is an illustration of a man with glasses sitting at a desk with a computer. On the right, there is an illustration of a man in a suit thinking. At the bottom, there is a speaker icon, a hand icon pointing to the text 'Klicken Sie jetzt auf die Fragen, um mehr zu erfahren.', and two navigation arrows (left and right).

Cyber-Security in der Praxis

Menü =

Krypto-Trojaner

Welche Fragen sollten sich die Geschäftsleitung und IT-Spezialisten stellen?

Muss ich die Polizei einschalten? Oder lieber noch warten?

Wann informiere ich meine Bank?

Sollte meine eigene IT das Problem lösen?

Klicken Sie jetzt auf die Fragen, um mehr zu erfahren.

Unser E-Learning
Schulung.

Ihre Mitarbeiter im
multimediales Kon-
Quizfragen, Audio-
lungsreichen Form-
und spielerische Sch-

✓ Kein langweil-
Videomaterial

✓ Keine abgefil-

✓ Keine ermüde-

✓ Keine festen

„kurzweilig, sp-

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.

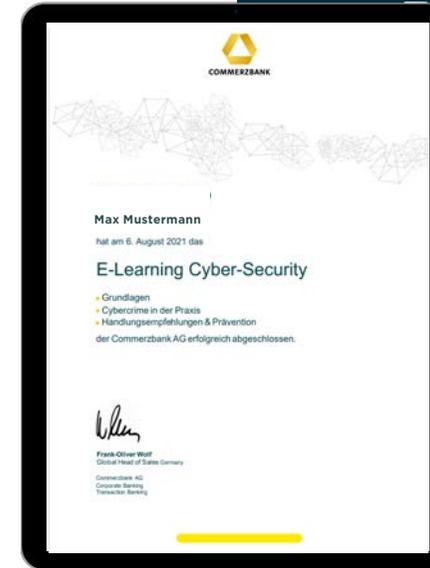


Ihr Ansprechpartner:

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.



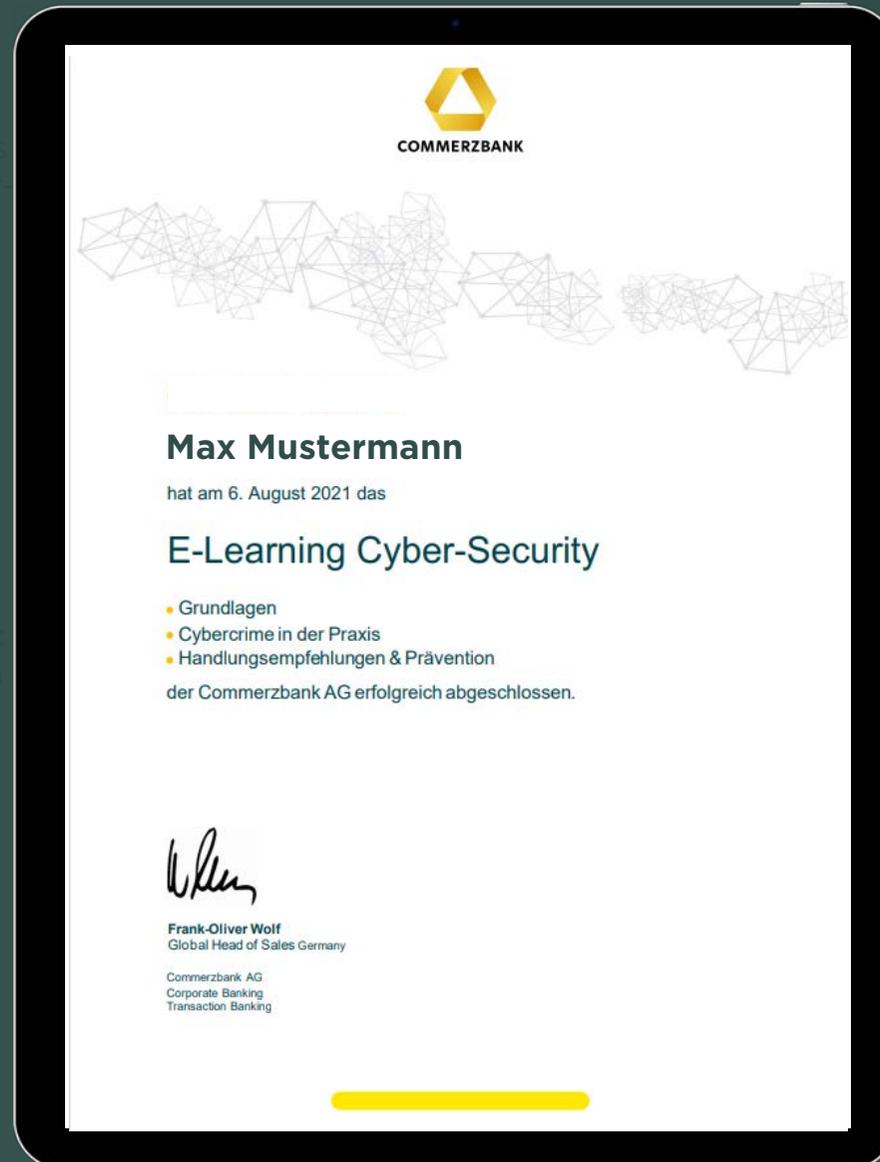
Einfacher Download

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.



Klicken Sie auf ein Thema für die Detailansicht.



Das Abschluss
Das Zertifikat
für die bester
schulung

Einfacher De
Jeder Ihrer M
kann das erw
einfach und s
herunterlader
der Dokument

Die Handlung
ihre Mitarbei
im Anschluss
eine kurze Ho
lung für Notf

Cyber-Security - Handlungsempfehlungen



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 Vorgesetzten zu, um den Vorfall zu validieren.



COMMERZBANK