

Finanz- und Rechnungsbetrug verhindern – im Zeitalter von KI

Seminar gegen CEO-Fraud für Mitarbeitende in den Bereich Finanzen und Controlling

Der Kurs richtet sich an Mitarbeitende im Finanzbereich. Sie lernen, Finanzbetrug – klassischen sowie KI-gestützten – frühzeitig zu erkennen und zu verhindern. Diese Schulung bereitet auf die speziellen Angriffe von Betrügern vor und stattet Controller mit besserem Bewusstsein und mehr Werkzeugen für sicheres Verhalten aus.

Praxisnahes Anti-Fraud-Wissen für Finanz- und Controlling-Teams

Mit vier Stunden Training 6-stellige Verluste vermeiden! Mitarbeitende lernen, wie sie ihre Wahrnehmung schärfen, Finanz- und Rechnungsbetrug frühzeitig erkennen und mit geeigneten Verhaltenstaktiken und Maßnahmen verhindern können.

Der Kurs richtet sich an Mitarbeitende im Finanz- und Controlling-Bereich, die ihre Fähigkeiten zur Erkennung und Abwehr von Betrugsversuchen verbessern möchten.

Die Weiterbildung vermittelt praxisnahe Kenntnisse, um Betrug frühzeitig zu identifizieren und durch gezielte Maßnahmen zu verhindern.

Im Jahr 2021 verursachte CEO-Betrug mehr Schaden bei den betroffenen Unternehmen als jede andere Form der Cyberkriminalität.

Mitarbeitende des Finanzbereichs stehen dabei besonders im Fokus, da sie direkt Gelder bewegen und somit ein Ziel für Angreifer sind.

Kursdetails auf einen Blick

- Für **Mitarbeitende der Abteilung Finanzen, inkl. Accountants, Controller**
- **Offene Schulung** oder **Inhouse Training**
- Dauer: **1 Tag à 4 Stunden**, aufgeteilt in 2 Blöcke
- Format: **Online**
- Kosten: 650,00 Euro (zzgl. MwSt.)

CEO-Fraud: Der Mensch als letzte Verteidigung

Oftmals können Mitarbeiter die verdächtigen Merkmale eines Angriffs nicht rechtzeitig erkennen und lösen Zahlungen aus. Unternehmen vertrauen häufig vergeblich auf rein technische Abwehrmaßnahmen. Angreifer nutzen gezielt die menschliche Natur, um ihre Ziele zu erreichen.

Mit dem Einzug von Künstlicher Intelligenz (KI) erreichen diese Angriffe eine neue Qualität: Täuschend echte E-Mails, nachgeahmte Stimmen oder sogar Deepfake-Videocalls machen es zunehmend schwer, Betrug rechtzeitig zu erkennen.

Daher ist es von entscheidender Bedeutung, die Mitarbeitenden auf solche Angriffe vorzubereiten und sie durch eine aktive Auseinandersetzung mit den Techniken der Angreifer in der Abwehr zu stärken. Das Training fokussiert auf erlebnisorientiertes Lernen von Gegenmaßnahmen, das den Transfer in den Arbeitsalltag schafft.

Die Mitarbeitenden des Finanzbereichs werden mit mehr Bewusstsein und Einblicken in die Abläufe von Angriffen, insbesondere auch KI-gestützter Bedrohungen, wodurch sie mehr Kontext und Hinweise erhalten, die es ihnen erleichtern, diese Betrügereien zu erkennen.

Nach dem Seminar können Sie:

- **Ihre Wahrnehmung schärfen**, klassischen sowie KI-unterstützten Finanz- und Rechnungsbetrug zu erkennen.
- **Geeignete Verhaltenstaktiken und Maßnahmen anwenden**, um Betrug zu verhindern.
- **Typische Betrugsmuster identifizieren** und adäquat darauf reagieren.

Alle Kursdetails und die Anmeldung finden Sie hier:



<https://s.fhg.de/ceo-fraud-verhindern>

Kursinhalte

Das Spektrum der behandelten Fragestellungen umfasst:

Einblicke in die Techniken der Angreifer:

- Was nutzen Angreifende zu ihrem Vorteil - einblicke in die Schwachstellen der menschlichen Natur
 - Open Source Intelligence: OSINT
 - Social Engineering-Techniken, die bei CEO Fraud eingesetzt werden
 - Analyse von wichtigen Finanz- und Rechnungsbetrugsarten
 - Gruppenübungen für immersives Lernen

Intuitive Angriffserkennung:

- Ausprobieren und Erleben von Angriffstechniken
 - Hinweise auf Betrug, die man erkennen sollte
- Verstehen von subtilen Hinweisen zwischen sicheren und unsicheren Transaktionen oder Angriffen
- Übungen, um die Erkennbarkeit von CEO-Betrügereien zu testen

Anwendung:

- Anwenden des Gelernten durch Übungen/Rollenspiele
- Umsetzung von Abwehrmaßnahmen
- Was wäre wenn? Richtige Reaktion auf eine falsche Geldüberweisung

Zugangsvoraussetzung:

Erfahrung mit der Durchführung von Transaktionen; kein spezielles IT-Sicherheits-Wissen erforderlich

Fachliche Ansprechpartnerin am Fraunhofer IAO

Dr. Mrudula Arunkumar
Tel. +49 711 970-5132
mrudula.arunkumar@iao.fraunhofer.de

Fraunhofer-Institut IAO
Nobelstr. 12
70569 Stuttgart



Lernlabor
Cybersicherheit