IT-Sicherheit am Arbeitsplatz

Grundlagenwissen für Mitarbeitende

Die Schulung sensibilisiert Mitarbeitende für IT-Sicherheitsrisiken, die durch menschliches Fehlverhalten wie Phishing oder schwache Passwörter entstehen. Ziel ist es, das Bewusstsein zu schärfen und praxisnahe Strategien für sicheres Arbeiten zu vermitteln. Mit fundierten wissenschaftlichen Erkenntnissen und praxisnahen Beispielen lernen die Teilnehmenden, Risiken frühzeitig zu erkennen, bewusste Entscheidungen zu treffen und geeignete Maßnahmen zur Risikominimierung zu ergreifen.

Sicherheitsbewusstsein stärken, Risiken erkennen, richtig handeln

IT-Angriffe zielen oft auf menschliches Fehlverhalten, etwa durch Phishing, schwache Passwörter oder den unachtsamen Umgang mit sensiblen Daten.

Solche Risiken entstehen nicht nur durch technische Lücken, sondern vor allem durch mangelndes Bewusstsein und fehlendes Wissen im Umgang mit modernen IT-Gefahren.

Genau hier setzt dieser Kurs an: Er sensibilisiert Mitarbeitende für die zahlreichen Gefahren der digitalen Welt und vermittelt konkrete, praxisnahe Strategien für sicheres Arbeiten.

Ziel ist es, nicht nur Wissen zu vermitteln, sondern auch das Verständnis für Sicherheit im Arbeitsalltag nachhaltig zu schärfen.

Kursdetails auf einen Blick

- Für Mitarbeitende in operativen Bereichen von Unternehmen und Organisationen
- Inhouse Training
- Dauer: nach Bedarf. Standardmäßig 2 Stunden.
- Format: Präsenz oder Online
- Kosten: 200,00 Euro (zzgl. MwSt.)

Risiken der digitalen Welt – erklärt auf Basis von Praxis und Forschung

Basierend auf langjähriger Praxiserfahrung und fundierten wissenschaftlichen Erkenntnissen beleuchtet der Kurs die grundlegenden Unterschiede zwischen der analogen und digitalen Welt.

Dabei wird das Verhalten der Teilnehmenden hinterfragt, insbesondere typische Denkmuster, die unbewusst zu riskanten Entscheidungen führen können. Durch anschauliche Beispiele und leicht verständliche Erklärungen wird vermittelt, wie solche Risiken erkannt und vermieden werden können.

Die Teilnehmenden lernen, potenzielle Gefahren frühzeitig zu identifizieren, bewusste Entscheidungen zu treffen und geeignete Maßnahmen zur Risikominimierung zu ergreifen.

Ein weiterer Schwerpunkt liegt auf praktischen Anleitungen, die sich direkt in den Arbeitsalltag integrieren lassen. Dabei werden bewährte Strategien vermittelt, die sowohl auf allgemeine IT-Sicherheitsprinzipien als auch auf spezifische Herausforderungen zugeschnitten sind.

Ziel ist es, Mitarbeitende nicht nur zu informieren, sondern sie auch zu selbstbewusstem Handeln in schwierigen oder ungewöhnlichen Situationen zu befähigen.

Nach dem Seminar können Sie:

- **Typische Vorgehensmuster** von **IT-Angriffen** besser **erkennen** und entsprechend reagieren,
- **Ungewöhnliche Vorkommnisse** in Ihren Arbeitsabläufen richtig einschätzen und passende Maßnahmen ergreifen.
- **Verstehen, wie Denkmuster und Stereotypen entstehen** und wie Angreifer*innen diese gezielt ausnutzen.

Alle Kursdetails und die Anmeldung finden Sie hier:

https://shorturl.at/D21hs

Kursinhalte.

Das Spektrum der behandelten Fragestellungen umfasst:

- Wie entwickelt sich die aktuelle Bedrohungslage im Bereich der Cybersicherheit?
- Warum besitzt Informationssicherheit für Unternehmen und sonstige Organisationen einen derart hohen Stellenwert?
- Welche Motivationen haben Cyberkriminelle und durch welche Angriffsvektoren führen sie Angriffe durch?
- Welche Trends und Muster in Bezug auf Angreiferaktivitäten sind in der jüngsten Zeit zu beobachten?
- Wie können Mitarbeiter verantwortungsvoll und sicher mit Informationen und Arbeitsmitteln umgehen, um präventiv gegen Cyberangriffe vorzugehen?
- Woran erkenne ich, ob meine Arbeitsgeräte möglicherweise kompromittiert wurden?
- Welche Schritte sollte ich unternehmen, wenn ich einen Cybersicherheitsvorfall vermute oder feststelle?

Weitere Informationen.

Es besteht die Möglichkeit, die Inhouse-Schulung an Ihre spezifischen Bedürfnisse anzupassen. Dabei können Sie insbesondere vorgeben, in welcher Ausführlichkeit die oben genannten Fragestellungen behandelt werden sollen oder ob zusätzliche, für Sie relevante Aspekte erörtert werden sollen.

Auch die Dauer der Schulung kann individuell gestaltet werden, wobei die Mindestdauer einer Schulung 2 Zeitstunden beträgt.

Fachlicher Ansprechpartner am Fraunhofer FOKUS

Sebastian Wedell
Tel. +49 30 3463-7544
sebastian.wedell@fokus.fraunhofer.de

Fraunhofer FOKUS
Kaiserin-Augusta-Allee 31
10589 Berlin
www.fraunhofer.de

Lernlabor
Cybersicherheit