

Phishing, Social Engineering und sichere E-Mails

Manipulationsversuche erkennen, verdächtige Nachrichten prüfen und bei Phishing-Verdacht richtig handeln.

DAUER

30 Minuten

NIVEAU

Grundlagen

SPRACHE

DE / EN

AKTUALISIERT

laufend

Fachlicher Bezug: Security-Awareness und betriebliche Meldeprozesse

KOMPETENZAUFBAU

Das lernen Mitarbeitende.

01

Signale erkennen

Typische sprachliche und technische Warnzeichen identifizieren.

02

Nachrichten prüfen

Absender, Links, Anhänge und Forderungen systematisch kontrollieren.

03

Manipulation stoppen

Zeitdruck und Autoritätsargumente bewusst unterbrechen.

04

Richtig melden

Verdächtige Kontakte ohne Eigenrisiko dokumentieren und eskalieren.

KURSAUFBAU

6 kompakte Kapitel.

01

Wie Phishing und Social Engineering funktionieren

02

Warnsignale in E-Mails erkennen

03

Links, Anhänge und Absender prüfen

04

CEO-Fraud, Telefon und Messenger

05

Bei Verdacht richtig reagieren

06

Praxischeck und Abschluss

FÜR DIE INTERNE ENTSCHEIDUNG

Erst prüfen, dann klicken: Angriffe im Postfach früh erkennen.

Zielgruppe: Alle Mitarbeitenden, Neue Mitarbeitende

Wiederholung: mindestens jährlich, ideal ergänzt durch kurze Refresher

Bereitstellung: SCORM 1.2, SCORM 2004, kijuno Cloud

kijuno.com/schulungen/phishing-social-engineering-sichere-emails

