



IT-Sicherheit für Anwender – Prävention und Schutz im digitalen Alltag

Untertitel: Praxisnahe Strategien zur Vermeidung von Cyberangriffen im Berufs- und Privatleben

Arbeitszeit:

09:00–12:00 Uhr und 13:00–16:00 Uhr (6 Zeitstunden)

Pause: 12:00–13:00 Uhr

Tag 1 (Montag)

Zeit	Lerninhalte
09:00–10:00	Einführung, Bedrohungslage im Berufs- und Privatalltag
10:00–12:00	Phishing & Social Engineering erkennen und vermeiden
13:00–14:00	Passwörter, MFA und sichere Authentifizierung
14:00–15:30	Verantwortung im Umgang mit IT-Sicherheit im Unternehmen und Alltag
15:30–16:00	Wiederholung und Reflexion der Inhalte

Tag 2 (Dienstag)

Zeit	Lerninhalte
09:00–10:30	Malware, Anhänge und Downloads im Alltag
10:30–12:00	Sicherer Umgang mit E-Mails, Links und Dateien
13:00–14:30	Updates, Rechte und sichere Systeme
14:30–15:30	Umgang mit Sicherheitsvorfällen und richtiges Verhalten
15:30–16:00	Wiederholung und Vertiefung

Tag 3 (Mittwoch)

Zeit	Lerninhalte
09:00–10:30	Kontoübernahmen und typische Angriffsszenarien
10:30–12:00	Absicherung von Accounts und Cloud-Diensten
13:00–14:00	Backup-Strategien und Datensicherheit
14:00–15:30	Praxisfall: Cyberangriff im Berufs- und Privatkontext
15:30–16:00	Wiederholung und Reflexion

Tag 4 (Donnerstag)

Zeit	Lerninhalte
09:00–10:30	Sicheres Arbeiten unterwegs
10:30–12:00	Mobile Security und Geräteschutz
13:00–14:30	Sichere Kommunikation und Datenaustausch
14:30–15:30	Auswirkungen von Cyberangriffen auf Unternehmen und Gesellschaft
15:30–16:00	Wiederholung und Vertiefung

Tag 5 (Freitag)

Zeit	Lerninhalte
09:00–10:30	Sichere Routinen im digitalen Alltag
10:30–12:00	Phishing-Simulation und Auswertung
13:00–14:00	Individueller Maßnahmenplan (Beruf & Privatleben)
14:00–15:30	Regeln, Verantwortung und Mitwirkung bei IT-Sicherheit
15:30–16:00	Wiederholung und Abschlussreflexion