



**WISSEN
MACHT
ERFOLG**

Grundlagen der IT- Security

Kurs zur Verbesserung der IT-
Sicherheit

Seminar-ID: 31024

Kursinfo: **BEGINNER**

Veranstaltungsformat: Seminar

🔊 Darum lohnt sich der Kurs

Geben Sie Cyberkriminellen keine Chance und erfahren Sie, wie Sie Ihre Computer und Netzwerke effektiv gegen Einwirkung von außen schützen, Sicherheitslücken erkennen und Cyberattacken vermeiden. Inklusive Live-Demo: Hacking für Laien.

Das nehmen Sie mit

Sie möchten als Nicht-IT-Fachmann Themen wie Datei- und E-Mail-Verschlüsselungen, Cookies, Social Engineering Methoden, Multi-Faktor-Authentifizierungen oder Bedrohungsszenarien wie Ransomware oder SQL Injections einfach erklärt bekommen?

Verschaffen Sie sich umfassendes Einsteigerwissen über die wichtigsten IT-Begriffe sowie Schutz- und -Verteidigungseinrichtungen zur Bewältigung von Cyberrisiken.

Nach dem Seminar kennen Sie die Gefahren des Internets, Sie wissen, wie Angreifer an Daten Ihres Netzwerks / Computers gelangen und wie Sie Sicherheitsvorfälle rechtzeitig erkennen und vermeiden. Zahlreiche Praxisbeispiele & Live Demos zeigen, wie man als Laie Dateien hackt oder Verschlüsselungen richtig anwendet und veranschaulichen Ihnen zusätzlich die Inhalte.

Ihr Programm im Überblick

- Sichere Passwörter einfach handhaben
 - Auswahl | Tools
 - Live Demo: Hacking für Laien
- Verschlüsselung
 - Aktuelle Technologien einfach erklärt (TLS, SSL, AES, RSA...)
 - Verschlüsselungsmethoden | E-Mails & Daten verschlüsseln – inkl. Demo
 - Asymmetrische / Symmetrische
 - Sicher Surfen im Internet (HSTS, HTTPS...)
- Aktuelle Bedrohungsszenarien
 - Viren / Würmer / Trojaner | SQL Injections | Cross Site Scripting
 - Spam | Sabotage / Diebstahl | DDOs / Botnetze
- Elektronische Signatur
 - Einfach / Qualifiziert | Signatur- und Vertrauensdienstegesetz (SVG) / eIDAS-Verordnung der EU
 - Bürgerkarte / Amtssignatur
- Tracking-Technologien
 - Cookies | Web Beacons | Local Shared Objects
 - HTML5 Storage | Browser Fingerprinting | Gegenmaßnahmen

- Authentifikationsmethoden
 - Single / Multifaktor | Zugriffsmanagement
 - Single sign-on (SSO)
- Social Engineering inkl. Beispielen
 - Erkennen, Handhaben, Vorbeugen | Phishing | Spear-Phishing
 - Vishing | Malware & Ransomware | CEO Frauds
- Umgang mit Sicherheitsvorfällen
 - Erkennen – Bewerten – Verhindern
- Funk-Technologien

Interessant für

- Datenschutzbeauftragte / Datenschutzverantwortliche
- Mitglieder der Geschäftsführung | Führungskräfte
- Mitarbeiter der Abteilungen Recht, Compliance, HR, Revision, Marketing
- Unternehmens-Juristen
- Rechtsanwälte / Rechtsanwaltsanwärter
- Öffentliche Verwaltung
- Wirtschaftsprüfer / Steuerberater

Referent*in



Univ.-Lekt. Nicolas Nagel LL.M., CIPP/E, CIPM,
Experte im Datenschutzmanagement

Termine & Optionen

DATUM	DAUER	ORT	FORMAT	PREIS
06.11.2024	1 Tag	Virtual Classroom	Online	€ 630,-
06.11.2024	1 Tag	Wien	Präsenz	€ 630,-

Beratung & Buchung



Jeffrey Müller-Büchse
 ☎ +43 1 713 80 24-38 ✉ jeffrey.mueller-buechse@ars.at