



## IT-Awareness für Windows-User

### Sicher agieren und Gefahren erkennen

*Erhöhen Sie Ihre IT-Sicherheit mit einfachen, praxisnahen Maßnahmen für den Umgang mit Windows-Rechnern. In diesem interaktiven Kurs lernen Sie, Bedrohungen zu verstehen und Schutzmaßnahmen anzuwenden. Es gibt zudem wertvolle Tipps zur Schadensbegrenzung und zur dauerhaften Sensibilisierung.*

#### Cyber-Sicherheit verstehen und anwenden – Grundwissen für Alltag

IT-Sicherheit – ein Begriff der oft genannt wird und unter dem sich eine Vielzahl an Facetten verbirgt. Egal ob zuhause oder im Berufsleben: Die Forderungen nach Grundkenntnissen der IT-Sicherheit wachsen mit der fortschreitenden Digitalisierung.

Fast jeden Tag wird in den Nachrichten über Begriffe aus der Welt der IT-Sicherheit berichtet.

Doch wer kann mit diesen Begriffen etwas anfangen? Was verbirgt sich dahinter? Was bedeutet dies für mein Unternehmen oder für mich privat?

In diesem interaktiven Seminar erhalten Sie das notwendige Wissen, um die Cyber-Sicherheit bei Ihrem täglichen Umgang an einem Arbeitsplatz- oder Privatrechner zu erhöhen.

#### Kursdetails auf einen Blick

- Für Mitarbeitende bei täglichem Umgang mit Windows-Rechner
- Offene Schulung oder Inhouse Training
- Dauer: 1 Tag à 4 Stunden
- Format: Online
- Kosten: 350,00 Euro (zzgl. MwSt.)

## Cyber-Bedrohungen erkennen, handeln und vorbeugen – praxisnah und interaktiv

Ihnen werden im Rahmen des Seminars fundierte Inhalte vermittelt, die Ihnen helfen, typische Bedrohungen für einen Windows-Rechner besser zu verstehen und einzuordnen.

Dabei lernen Sie, wie Sie Schwachstellen erkennen, potenzielle Angriffsvektoren identifizieren und einfache, aber wirkungsvolle Überprüfungs- und Vorsichtsmaßnahmen sicher und routinemäßig in Ihren Alltag integrieren können.

Alle vorgestellten Maßnahmen werden nicht nur theoretisch erklärt, sondern praxisnah und interaktiv direkt am System demonstriert. In realitätsnahen Szenarien üben Sie die Umsetzung der Inhalte, um das Gelernte effektiv in der Praxis anwenden zu können.

Darüber hinaus erhalten Sie konkrete Hinweise zur ersten Hilfe im Falle eines Schadensvorfalls – also was zu tun ist, wenn es bereits zu einem sicherheitsrelevanten Ereignis gekommen ist.

### Nach dem Seminar können Sie:

- **Phishing-Mails und gefälschte Websites erkennen:** Sie lernen, wie Sie betrügerische E-Mails und täuschend echte Websites identifizieren können, die darauf abzielen, persönliche Daten oder Zugangsinformationen zu stehlen.
- **Sich vor Social Engineering schützen:** Sie erfahren, wie Angreifer durch gezielte Manipulation versuchen, an vertrauliche Informationen zu gelangen – und wie Sie sich effektiv gegen solche Täuschungsversuche wappnen.
- **Sichere Passwörter erstellen und verwalten:** Es wird gezeigt, wie starke, individuelle Passwörter erstellt werden und mit welchen Methoden oder Tools diese sicher und benutzerfreundlich verwaltet werden können.
- **Gefahren beim Surfen und E-Mail-Verkehr vermeiden:** Sie erhalten praktische Hinweise, wie Sie sich sicher im Netz bewegen, unseriöse Inhalte erkennen und typische Risiken im Umgang mit E-Mails vermeiden.
- **Angriffe und Schadsoftware richtig einschätzen:** Sie lernen die häufigsten Arten von Malware und Cyberangriffen kennen und wie man die potenziellen Gefahren einschätzen und frühzeitig erkennen kann.
- **Im Notfall schnell und richtig reagieren:** Es werden erste Schritte vermittelt, die Sie bei einem IT-Sicherheitsvorfall einleiten sollten – ob im privaten Umfeld oder im beruflichen Kontext.

## Kursinhalte

### Einblicke in die Themen:

- Wie erkenne ich Phishing E-Mails?  
Anti-Phishing-Maßnahmen
- Was ist Social Engineering und wie erkenne ich Betrüger
- Web-/ Internetsicherheit
- Malware und typische Angriffe
- Bedrohungen und Risikoanalyse; Checklisten vom BSI
- Passwortverwaltung – Passwortsicherheit  
- Passwortrichtlinie
- Verschlüsselung / Zertifikate / digitale Unterschrift /  
Multi-Faktor-Authentifizierung / eMail-Verschlüsselung /  
Festplattenverschlüsselung
- Was ist zu tun, wenn's dann passiert? Was nutzen Angreifende zu ihrem Vorteil - einblicke in die Schwachstellen der menschlichen Natur

Alle Kursdetails und die Anmeldung finden Sie hier:



<https://shorturl.at/KrF3u>

### Fachlicher Ansprechpartner

Prof. Dr. Thomas Meuser  
Tel. +49 228 9435-0  
[thomas.meuser@fkie.fraunhofer.de](mailto:thomas.meuser@fkie.fraunhofer.de)

Hochschule Bonn-Rhein-Sieg  
Grantham-Allee 20  
53757 Sankt Augustin  
[www.fraunhofer.de](http://www.fraunhofer.de)



Lernlabor  
Cybersicherheit