

IT-Sicherheit verstehen

Dein Einstieg in die digitale
Selbstverteidigung



Für Schule, Ausbildung & Alltag
Mit interaktiven Links & Tests

💡 Dein Einstieg in die digitale Selbstverteidigung

🎓 Für Schule, Ausbildung & Alltag

💻 Mit interaktiven Links & Tests

👤 Autor: Konrad Rennert, ECDL-Trainer, <https://konrad-rennert.de/profil>

Inhalt.....	2
Einleitung.....	3
Kapitel 1 – Daten ≠ Informationen.....	4
Was sind Daten eigentlich?	4
✅ Prüf dich selbst:.....	4
🔗 Link-Tipp:.....	4
Kapitel 2 – Backups als Lebensversicherung für Daten!.....	4
Kapitel 3 – Cybergefahren erkennen.....	5
⚠️ Bekannte Methoden:.....	5
💬 Praxisbeispiel aus dem echten Leben:	5
🔗 Link-Tipp:.....	6
Kapitel 4 – Passwörter & Verschlüsselung.....	6
🔑 Gute Passwörter.....	6
🔒 Verschlüsselung.....	6
🔗 Link-Tipp:.....	6
Kapitel 5 – Schutz vor Schadsoftware.....	6
🛡️ Schutzmaßnahmen:	6
🧠 Prüfungswissen:.....	6
🔗 Link-Tipp:.....	6
Kapitel 6 – Sicher im Internet	7
🌐 Tipps für sicheres Surfen:	7
🔗 Link-Tipp:.....	7
Kapitel 7 – E-Mail & Soziale Netzwerke.....	7
📧 E-Mail-Sicherheit.....	7
👥 Soziale Netzwerke.....	7
🔗 Link-Tipp:.....	7
Kapitel 8 – Netzwerke & WLAN absichern.....	7
🏠 Heimnetzwerke schützen	7
🌐 WLAN-Tipps:	8
🔗 Link-Tipp:.....	8

Kapitel 9 – Mobile Geräte schützen.....	8
📱 Schutztipps:.....	8
🔗 Link-Tipp:.....	8
Kapitel 10 – Datenschutz & Urheberrecht.....	8
🔒 Datenschutz in Kürze:.....	8
⚖️ Urheberrecht beachten:.....	8
🔗 Link-Tipp:.....	9
📘 Glossar der wichtigsten Begriffe	10
Backup.....	10
Phishing.....	10
Malware.....	10
Firewall.....	10
Verschlüsselung	10
HTTPS.....	10
Passwort-Manager.....	10
VPN	10
Social Engineering.....	10
Zwei-Faktor-Authentifizierung.....	10
🎯 Mini-Quiz: Teste dein Wissen	11
🎯 Lösungen zum Mini-Quiz: Teste dein Wissen – Mit Kommentaren	12
Anhang	13
Konrads Angebot – IT-Sicherheit mit Unterstützung.....	13
Bearbeitbare PDF-Dokumente für Bildung und Weiterbildung	14
Zusammenfassung der Funktionen in der Werkzeugleiste.....	16
Haftungsausschluss für Schulungsformate.....	16
Impressum	17

Einleitung

Warum IT-Sicherheit dich betrifft – egal ob Schüler, Azubi oder Digital Native

In einer Welt voller Daten, Clouds, WLANs und Smartphones ist IT-Sicherheit kein

Spezialwissen mehr – sondern Grundbildung. Dieses eBook zeigt dir einfach und verständlich, wie du dich, deine Geräte und deine Daten schützt.

Mit vielen Beispielen, Quizfragen, Linktipps und Praxisfällen!

Kapitel 1 – Daten ≠ Informationen

Was sind Daten eigentlich?

- Daten = Fakten (z. B. 32 °C in Berlin, 1500 € Umsatz)
- Informationen = Bedeutung (z. B. „Heute ist es heiß“ oder „Das Geschäft läuft gut“)
- Wissen = Handeln („Ich zieh heute was Leichtes an“ oder „Ich investiere weiter“)



Merksatz:

„Daten sind wie Zutaten. Informationen sind das fertige Gericht.“



Prüf dich selbst:

Was ist der Unterschied zwischen Daten und Wissen?



Link-Tipp:

→ <https://www.easy4me.info/modul-8>



Kapitel 2 – Backups als Lebensversicherung für Daten!

Daten können durch Diebstahl, Feuer, Überspannung oder Fehler verloren gehen. Ein Backup ist die beste Vorsorge.



Warum ein Backup?

- Schutz vor Datenverlust
- Schnelle Wiederherstellung
- Sicherheit bei wichtigen Dokumenten (z. B. Abschlussarbeit)

Wie sichern?

- USB-Stick, externe Festplatte
- Cloud-Dienste (OneDrive, Google Drive, Dropbox)
- NAS-Systeme
- Automatische Sicherung mit Zeitplan

📌 **Link-Tipp:** <https://www.bsi.bund.de> – Suchbegriff (Lupe): "Empfehlungen zur Datensicherung" - Es werden mehrere hundert relevante Stellen angezeigt, die dann gefiltert werden können.

Kapitel 3 – Cybergefahren erkennen

Nicht nur Technik ist eine Gefahr – auch Menschen sind ein Risiko. Social Engineering, Phishing und Identitätsdiebstahl sind ernste Bedrohungen.

Bekannte Methoden:

- Phishing: gefälschte Mails mit gefährlichen Links
- Skimming: Datenklau am Bankautomaten
- Shoulder Surfing: jemand schaut beim Eintippen zu
- Pretexting: Betrüger geben sich als jemand anderes aus

Praxisbeispiel aus dem echten Leben:

Eine Nachbarin erhielt eine WhatsApp-Nachricht: 'Hallo Mama, mein Handy ist kaputt, überweise bitte Geld.' Sie tat es. Es war ein Betrug.

Details: Das ist eine bekannte Betrugsmasche, die oft als **WhatsApp-Enkeltrick** bezeichnet wird. Dabei geben sich Kriminelle als nahe Angehörige aus und behaupten, ihr Handy sei kaputt oder sie hätten eine neue Nummer. Kurz darauf folgt eine Bitte um eine dringende Geldüberweisung, oft mit einer erfundenen Notlage.

Viele Menschen fallen darauf herein, weil sie glauben, ihrem Kind oder einem anderen Familienmitglied zu helfen. Besonders ältere Personen sind gefährdet, da sie möglicherweise weniger misstrauisch gegenüber solchen Nachrichten sind.

Falls du oder jemand in deinem Umfeld eine solche Nachricht erhält, ist es wichtig, **nicht sofort zu reagieren**. Stattdessen sollte man die angebliche neue Nummer ignorieren und den echten Angehörigen über die alte Nummer oder auf anderem Wege kontaktieren.

 Link-Tipp:

➔ <https://www.bka.de> – Im Suchfeld (Lupe) „**Aktuelle Warnungen**“ eingeben. Es werden mehrere Dutzend relevante Stellen angezeigt, die dann gefiltert werden können.

Kapitel 4 – Passwörter & Verschlüsselung

 Gute Passwörter

Ein starkes Passwort ist wie ein guter Schlüssel – es schützt deinen digitalen Raum.

- Mindestens 12 Zeichen
- Mischung aus Buchstaben, Zahlen und Sonderzeichen
- Niemals Geburtstage oder Namen verwenden

 Verschlüsselung

- Emails, Dateien und Festplatten sollten verschlüsselt sein
- Tools wie VeraCrypt oder BitLocker helfen
- HTTPS zeigt dir: Diese Seite ist verschlüsselt

 Link-Tipp:

➔ <https://www.bsi.bund.de> – „**Verschlüsselung leicht erklärt**“ in das Suchfeld (Lupe) eingeben. Es werden ca. zweihundert relevante Stellen angezeigt, die dann gefiltert werden können.

Kapitel 5 – Schutz vor Schadsoftware

Schadsoftware oder „Malware“ sind Programme, die Schaden anrichten. Dazu gehören Viren, Würmer, Trojaner und Spyware.

 Schutzmaßnahmen:

- Antivirus-Programme regelmäßig aktualisieren
- Keine unbekannten Anhänge öffnen
- Vorsicht bei Downloads aus inoffiziellen Quellen
- Betriebssystem und Programme aktuell halten

 Prüfungswissen:

Der Quarantäne-Ordner ist ein spezieller Speicherort für verdächtige Dateien.

 Link-Tipp:

➔ <https://de.wikipedia.org/wiki/Malware>

Kapitel 6 – Sicher im Internet

Das Internet ist praktisch – aber nicht ungefährlich. Mit ein paar einfachen Regeln surfst du sicherer.

Tipps für sicheres Surfen:

- Nur auf Webseiten mit HTTPS einkaufen oder Online-Banking nutzen
- Achte auf Impressum, Kontaktmöglichkeiten und aktuelle Inhalte
- Keine persönlichen Daten in öffentlichen WLANs preisgeben
- Werbeanzeigen und Pop-ups mit Vorsicht behandeln

Link-Tipp:

➔ <https://www.klicksafe.de> – Im Suchfeld (Lupe) „**Surfen lernen**“ eingeben. Es werden ca. 16 relevante Stellen angezeigt, die dann gefiltert werden können.

Kapitel 7 – E-Mail & Soziale Netzwerke

E-Mail-Sicherheit

- Öffne keine unbekannten Anhänge
- Phishing-Mails erkennen: falsche Logos, Aufforderung zu schnellen Aktionen
- Digitale Signatur nutzen, um Echtheit zu bestätigen

Soziale Netzwerke

- Poste keine sensiblen Daten (Adresse, Urlaub, Geburtsdaten)
- Einstellungen zu Privatsphäre regelmäßig prüfen
- Fremde Freundschaftsanfragen ablehnen
- Achte auf Fake-Profile und Kettenbriefe

Link-Tipp:

➔ <https://www.bsi.bund.de/> – „**Sicherheit in sozialen Medien**“ in das Suchfeld (Lupe) eingeben. Es werden ca. zweihundert relevante Stellen angezeigt, die dann gefiltert werden können.

Kapitel 8 – Netzwerke & WLAN absichern

Heimnetzwerke schützen

- Router-Passwort ändern
- WPA2 oder WPA3-Verschlüsselung nutzen
- Geräte im Netzwerk regelmäßig prüfen

WLAN-Tipps:

- Netzwerkname (SSID) nicht öffentlich sichtbar machen
- Gastzugang aktivieren statt Hauptnetz nutzen
- VPN verwenden für sicheres Arbeiten unterwegs

Link-Tipp:

➔ <https://www.bsi.bund.de> – „**WLAN richtig sichern**“ in das Suchfeld (Lupe) eingeben. Es werden ca. 138 relevante Stellen angezeigt, die dann gefiltert werden können.

Kapitel 9 – Mobile Geräte schützen

Smartphones sind kleine Computer – mit vielen privaten Daten. Deshalb brauchen sie Schutz.

Schutztipps:

- Geräte mit Fingerabdruck oder PIN sichern
- Apps nur aus offiziellen App-Stores laden
- Berechtigungen regelmäßig prüfen
- Bei Verlust: Fernsperrung und Ortung aktivieren

Link-Tipp:

➔ <https://www.bsi.bund.de> Im Suchfeld (Lupe) „**Smartphone & Co absichern**“ eingeben. Es werden ca. 34 relevante Stellen angezeigt, die dann gefiltert werden können.

Kapitel 10 – Datenschutz & Urheberrecht

Nicht alles, was du im Netz siehst, darfst du einfach speichern oder teilen. Und deine Daten haben einen Wert.

Datenschutz in Kürze:

- Nur notwendige Daten weitergeben
- Auf sichere Aufbewahrung achten (Cloud & lokal)
- Persönliche Daten nie unverschlüsselt verschicken

Urheberrecht beachten:

- Bilder, Texte und Musik sind geschützt
- Quelle immer angeben, wenn erlaubt
- Privatkopie nie öffentlich teilen
- Creative Commons Lizenzen prüfen

 Link-Tipp:

 <https://www.bpb.de> – Im Suchfeld (Lupe) „**Urheberrecht einfach erklärt**“ eingeben. Es werden ca. 70 relevante Stellen angezeigt, die dann gefiltert werden können

Glossar der wichtigsten Begriffe

Backup

Sicherungskopie deiner Daten, um sie bei Verlust wiederherstellen zu können.

Phishing

Versuch, über gefälschte Mails an persönliche Daten zu kommen.

Malware

Sammelbegriff für schädliche Software wie Viren, Trojaner oder Spyware.

Firewall

System, das den ein- und ausgehenden Datenverkehr überwacht und unerwünschte Zugriffe blockiert.

Verschlüsselung

Technik, um Daten so zu codieren, dass sie nur von Befugten gelesen werden können.

HTTPS

Sicheres Internetprotokoll mit verschlüsselter Verbindung.

Passwort-Manager

Programm, das starke Passwörter erstellt und sicher verwaltet.

VPN

Virtuelles privates Netzwerk – schützt deine Daten in öffentlichen Netzwerken und kann deine IP-Adresse verschleiern. Deine Netzwerkverbindung ist von Unbeteiligten nicht einsehbar.

Social Engineering

Trickbetrug, bei dem Menschen manipuliert werden, um Zugang zu Daten zu bekommen.

Zwei-Faktor-Authentifizierung

Sicherheitsmethode mit zwei getrennten Zugangswegen (z. B. Passwort + SMS).

Mini-Quiz: Teste dein Wissen

1. Was ist ein sicheres Passwort?

- a) 12345678
- b) MeinGeburtsdatum
- c) Xf9\$g7L@3pZ

2. Woran erkennst du eine sichere Webseite?

- a) Sie hat bunte Bilder
- b) Sie nutzt HTTP
- c) Sie beginnt mit HTTPS

3. Was ist Phishing?

- a) Eine Angeltechnik
- b) Betrug mit gefälschten Nachrichten
- c) Schutzprogramm gegen Viren

4. Welche Aussage stimmt?

- a) Eine Firewall löscht E-Mails
- b) Eine Firewall blockiert unerlaubte Zugriffe
- c) Eine Firewall braucht man nicht

🔗 Lösungen zum Mini-Quiz: Teste dein Wissen – Mit Kommentaren

1. Was ist ein sicheres Passwort?

- a) 12345678
- b) MeinGeburtsdatum
- ☒ c) Xf9\$g7L@3pZ

Kommentar: Ein sicheres Passwort ist lang, enthält Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen – und hat **keinen Bezug zu persönlichen Daten**.

2. Woran erkennst du eine sichere Webseite?

- a) Sie hat bunte Bilder
- b) Sie nutzt HTTP
- ☒ c) Sie beginnt mit HTTPS

Kommentar: Das „S“ in HTTPS steht für „secure“ – es bedeutet, dass deine Verbindung zur Webseite **verschlüsselt** ist.

3. Was ist Phishing?

- a) Eine Angeltechnik
- ☒ b) Betrug mit gefälschten Nachrichten
- c) Schutzprogramm gegen Viren

Kommentar: Beim Phishing versuchen Kriminelle, über E-Mails oder Webseiten **deine Daten zu stehlen** – z. B. Passwörter oder Bankinformationen.

4. Welche Aussage stimmt?

- a) Eine Firewall löscht E-Mails
- ☒ b) Eine Firewall blockiert unerlaubte Zugriffe
- c) Eine Firewall braucht man nicht

Kommentar: Eine Firewall schützt dein Gerät oder Netzwerk, indem sie **verdächtigen Datenverkehr filtert oder blockiert** – sie ist ein wichtiger Baustein der IT-Sicherheit.

Anhang

Konrads Angebot – IT-Sicherheit mit Unterstützung

Auf <https://news.konrad-rennert.de/ebook-support> findest Du meine frei verfügbaren eBooks.

Ergänzend dazu biete ich individuelle Unterstützung und Schulung:



Lernunterstützung und Weiterbildung:

- IT-Sicherheitsschulungen auf Basis des eBooks
- Workshops und Videokonferenzen mit praktischen Übungen und Fallbeispielen
- Bereitstellung bearbeitbarer PDFs, Kursmaterialien und Lernvideos



Didaktische Beratung für Lehrkräfte:

- Unterstützung bei der Nutzung von Moodle, WordPress, alfaview, MS Teams, Zoom



Zielgruppen:

- Lehrkräfte und Bildungseinrichtungen
- Multiplikatoren der Erwachsenenbildung
- IT-Verantwortliche in Organisationen und Initiativen



Kontakt & Umsetzung:

- Schulungsanfragen: flipped-classroom@konrad-rennert.de
- Allgemeine Fragen: info@konrad-rennert.de
- Weitere Infos: <https://konrad-rennert.de/?s=learninglounge>



Flexibilität: Die Angebote sind modular, flexibel und auf Ihre Bedürfnisse zugeschnitten – vom einstündigen Impuls bis zur mehrtägigen Fortbildung.



Spendenbasierter Zugang zur erweiterten Lernplattform:

- Ab 10 € Spende erhält man eine Benutzerrolle mit 3 Monaten Zugriff auf zusätzliche Inhalte via <https://news.konrad-rennert.de>
- Die Überweisung der Spende gilt zugleich als Identitätsnachweis für den Spender, um auf der Plattform kommentieren zu können und an Videokonferenzen teilzunehmen.

Bearbeitbare PDF-Dokumente für Bildung und Weiterbildung

Wie können Lernende das meiste aus einem bearbeitbaren PDF herausholen – insbesondere mit den Werkzeugen, die direkt im Edge-Browser oder im PDF-Viewer zur Verfügung stehen?

Die KI **ChatGPT-4** erklärt die Symbole in der Werkzeugleiste Schritt für Schritt – jeweils mit einer praxisbezogenen Anwendung für Weiterbildung oder Videokonferenzen:

 **Symbolleiste – Funktionen & Anwendungsbeispiele**

 **Zeichnen** (Freihand-Werkzeug)

 Damit kannst du per Maus, Stift oder Finger direkt ins PDF schreiben oder skizzieren.

 Anwendung:

Markiere mit einem Tablet-Stift zentrale Begriffe während einer Live-Erklärung in der Videokonferenz – wie auf einem Whiteboard.

 Text hervorheben (**Markieren**)

 Zum Hervorheben wichtiger Textstellen, wie mit einem Textmarker auf Papier.

 Anwendung:

Lernende markieren z. B. Begriffe wie „Vertraulichkeit“ oder „Pharming“ und notieren in einer separaten Datei eine Definition – ideal zur Prüfungsvorbereitung.

 Textfeld hinzufügen

 Mit einem Klick kannst du **eigene Notizen als Textbox** direkt ins PDF einfügen.

 Anwendung:

Schreibe unter jeden Abschnitt deine eigene Zusammenfassung – oder eine Frage, die du im nächsten Online-Treffen stellen willst.

 **Vorlesen** lassen (z. B. mit Immersive Reader in Edge)

 Edge bietet eine Vorlesefunktion, die Texte in natürlicher Sprache wiedergibt.

 Anwendung:

Perfekt für DaF-Lernende oder Menschen mit Sehschwäche: Lass dir Inhalte auf Deutsch oder Englisch abschnittsweise vorlesen, um Aussprache und Verständnis zu trainieren.

 **Übersetzen** (via Kontextmenü oder Microsoft Edge-Add-on)

 Rechtsklick → „Übersetzen in...“ oder Browsererweiterung nutzen.

 Anwendung:

Markiere ein schwieriges Wort oder einen Absatz – und lasse dir die Bedeutung in deiner Muttersprache anzeigen, z. B. als Unterstützung für DaF-Lernende in Videokursen.

 Kommentar hinzufügen

 Kommentare einfügen wie in Word – ohne das Original zu verändern.

 Anwendung:

Trainer*innen können individuelle Hinweise oder Reflexionsfragen einfügen („Was bedeutet dieser Begriff für deine tägliche Online-Nutzung?“). Oder: Teilnehmende kommentieren gegenseitig.

 Suchen (Suchfeld rechts oben) **Volltextsuche** durch das gesamte Dokument. Anwendung:

Schnell nach „Verschlüsselung“ oder „Passwort“ suchen – ideal, wenn du ein Thema wiederholen willst.

 Drucken & Speichern (Diskette/Druckersymbol) Änderungen speichern oder direkt **mit eigenen Ergänzungen ausdrucken**. Anwendung:

Fertig bearbeitetes Arbeitsblatt ausdrucken oder zur Hausaufgabenkontrolle im Online-Kurs einsenden.

 Seitenanzeige (z. B. „9 von 21“)

→ Navigation durch das Dokument.

 Anwendung:

Ermöglicht gezielten Zugriff auf das gerade im Online-Meeting besprochene Kapitel – z. B. „Gehe bitte alle auf Seite 12“.

 Online-Kurs-Szenario: Das PDF im Einsatz

- ◆ Vorbereitung: Teilnehmer laden das PDF im Browser, markieren und kommentieren vor dem Meeting
- ◆ Live: Trainer teilt Bildschirm und erklärt Inhalte – Teilnehmer ergänzen Notizen direkt ins PDF
- ◆ Nachbereitung: Lernende senden ihre Version mit Kommentaren oder Rückfragen ein oder tauschen sich in Gruppenräumen (Breakout-Rooms) aus

✓ Fazit

Ein bearbeitbares PDF ist viel mehr als ein statisches Dokument. In Verbindung mit den integrierten Werkzeugen – insbesondere in Microsoft Edge – wird es zum interaktiven Arbeits- und Lernheft. Es fördert:

- Selbstständiges Arbeiten
- Sprachliches Verständnis
- Digitale Kompetenz
- Kollaboratives Lernen im Online-Unterricht

Zusammenfassung der Funktionen in der Werkzeugleiste



Symbol / Funktion	Einsatz im Bildungsalltag
Zeichnen	Freihand schreiben oder skizzieren – ideal für Hervorhebungen mit einem Stift.
Text markieren	Wichtige Begriffe oder Definitionen hervorheben wie mit einem Textmarker.
Textfeld	Eigene Notizen direkt ins Dokument einfügen – z. B. Zusammenfassungen oder Rückfragen.
Vorlesen	Texte automatisch vom System vorlesen lassen – ideal für DaF-Lernende.
Übersetzen	Abschnitte in deine Muttersprache übersetzen lassen – per Rechtsklick oder Add-on.
Kommentar	Kommentare einfügen, ohne das Original zu verändern – ideal zur Reflexion.
Suchen	Begriff im gesamten Dokument finden – z. B. „Phishing“ oder „Verschlüsselung“.
Speichern & Drucken	Bearbeitete Seiten sichern oder als Lernnachweis ausdrucken.
Navigation	Gezielt zu Kapiteln springen – z. B. für Besprechung im Online-Meeting.

Haftungsausschluss für Schulungsformate

Die Inhalte aller Webinare, Online-Kurse und Workshops dienen ausschließlich der allgemeinen Information und Weiterbildung. Trotz sorgfältiger Vorbereitung übernehmen Referenten und Veranstalter keine Gewähr für die Aktualität, Richtigkeit oder Vollständigkeit der vermittelten Informationen.

Die Veranstaltungen stellen keine individuelle Rechts-, IT- oder Sicherheitsberatung dar. Die Teilnehmenden sind selbst verantwortlich für die Umsetzung der vermittelten Inhalte in ihrer jeweiligen Organisation oder Praxis.

Für etwaige Schäden oder Verluste, die durch die Anwendung von Inhalten aus der Schulung entstehen, wird keine Haftung übernommen.

Impressum

Titel des Werks: IT-Sicherheit verstehen

Autorenschaft & Projektverantwortung:

Dieses Werk wurde fachlich konzipiert und inhaltlich betreut von:

Konrad Rennert, ECDL-Trainer, Diplom-Physiker, E-Learning-Trainer

<https://konrad-rennert.de/profil>

E-Mail: info@konrad-rennert.de

Redaktionelle und visuelle Ausarbeitung mit Unterstützung künstlicher Intelligenz:

Die Erstellung der Inhalte, Illustrationen und didaktischen Aufbereitung erfolgte unter aktiver Einbindung von ChatGPT-4 und DALL·E, zwei KI-gestützten Tools der Firma OpenAI.

Was wurde erstellt?

- Ein Mini eBook – mit Hinweisen zur sicheren digitalen Kommunikation, angepasst für Lernende aller Altersgruppen

Wie wurde es erstellt?

- Fachlich begleitet durch einen zertifizierten ECDL/ICDL-Trainer
- Generiert mit Unterstützung generativer KI (Text & Bild) und manuell redigiert
- Quellenrecherche aus öffentlich verfügbaren Inhalten (z. B. BSI, Wikipedia, Verbraucherzentralen)
- Ausrichtung an den Zielen von Computerführerschein für das Modul „IT-Security“

Wann wurde es erstellt?

Erarbeitet im Zeitraum April – Mai 2025

Warum wurde es erstellt?

Zur verständlichen Vermittlung von IT-Sicherheitswissen anhand frei zugänglicher Quellen. Ziel ist es, digitale Kompetenzen und Medienverantwortung ab dem Schulalter zu stärken.

Wo darf das Werk verwendet werden?

- In beliebigen Weiterbildungsangeboten

Rechtlicher Hinweis zur Verwendung generativer KI

Die Inhalte wurden mithilfe generativer KI erstellt und redaktionell überprüft.

Es besteht urheberrechtliche Schutzfähigkeit gemäß § 2 UrhG, da Struktur, Auswahl, Didaktik und Präsentation menschlich kuratiert wurden.

Rechtlicher Hinweis zur Verwendung generativer KI:

Die Texte und Bilder in diesem Werk wurden unter aktiver redaktioneller Aufsicht mit Unterstützung künstlicher Intelligenz erzeugt. Eine eigenständige urheberrechtliche Schutzfähigkeit gemäß §2 UrhG besteht, da die Inhalte menschlich kuratiert, strukturiert und finalisiert wurden.

Haftungsausschluss:

Trotz größter Sorgfalt bei der Erstellung übernimmt der/die Herausgeber/in keine Gewähr für die Richtigkeit, Vollständigkeit und Aktualität der Inhalte. Die Nutzung erfolgt auf eigene Verantwortung.

Bildnachweise & Tools:

Titel- und Kapitelbilder erstellt mit DALL·E (OpenAI)

Inhalte erstellt mit ChatGPT-4 (OpenAI)

Lizenzhinweis (CC BY 4.0)

Dieses Werk steht unter einer Lizenz. Bei Verwendung folgenden Vermerk angeben:

Creative Commons Namensnennung 4.0 International (CC BY 4.0)

<https://creativecommons.org/licenses/by/4.0/deed.de>

Namensnennung gemäß Lizenz:

Dieses Werk „IT-Sicherheit verstehen“ ist erstellt von Konrad Rennert mit Unterstützung durch KI (ChatGPT & DALL·E) und lizenziert unter CC BY 4.0

Du darfst:

- ✅ das Werk teilen – also kopieren und weiterverbreiten,
- ✅ es bearbeiten – remixen, verändern und darauf aufbauen, auch kommerziell,
- ❌ unter der Bedingung, dass du den Namen des Autors nennst und auf die Lizenz verweist.