IT-Sicherheit

leicht erklärt – Datenschutz, Netzwerksicherheit und Schutz vor Cybergefahren – Ein E-Book auf Basis von 12 YouTube-Videos

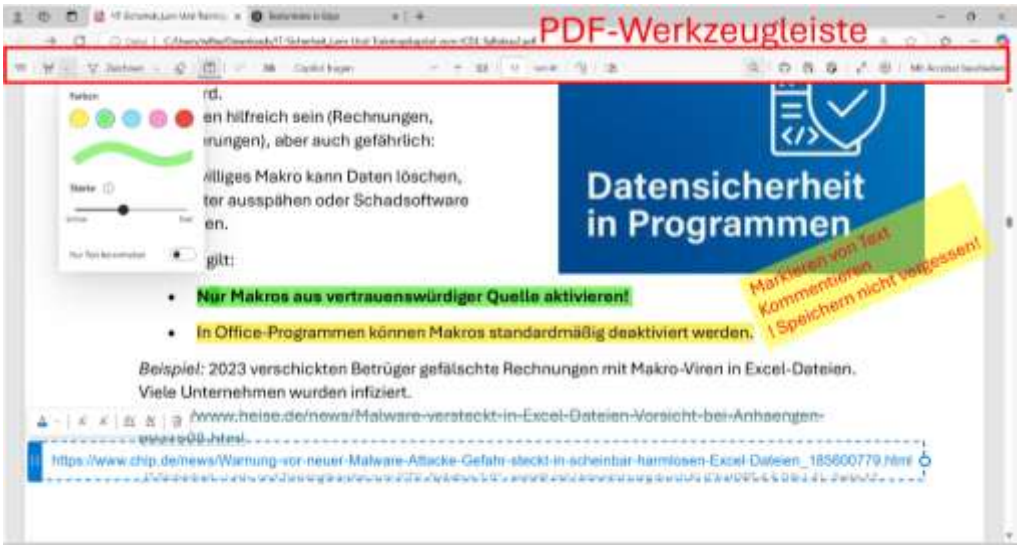
Konrad Rennert
ECDL-Trainer & Autor

Erstellt mit Unterstützung durch KI
(ChatGPT-4 & DALLE)

KI

Tipp zur aktiven Nutzung und Bearbeitung des pdf-Dokuments

In modernen Browsern wie **Microsoft Edge** kannst man mit der automatisch eingeblendeten **PDF-Werkzeugleiste** eigene Notizen oder Ergänzungen direkt im PDF-Dokument hinterlegen – z. B. für Recherche-Ergebnisse oder alternative Quellen. Nach dem Speichern bleiben diese Ergänzungen erhalten.



Video 1: IT- Sicherheit - Empfohlene Materialien zum Online-Kurs

https://www.youtube.com/watch?v=Lf4jyxH7Ebg

YouTube-Video wie oben, aber zusätzlich mit Fragen zum Selbsttest (ggf. mit Login):

https://news.konrad-rennert.de/it-sicherheit-01-h5p-selbsttest/

Inhaltsangabe

Das Video, präsentiert von Konrad Rennert, behandelt empfohlene Lernmaterialien für den Online-Kurs DSS01 IT-Security. Es richtet sich an Teilnehmer von geförderten Weiterbildungsmaßnahmen sowie an allgemein Interessierte. Vorgestellt werden primär zwei Anbieter: Herdt-Verlag und Easy4Me.

Die Materialien des Herdt-Verlags sind als gedrucktes Buch oder als eBook erhältlich. Hervorgehoben wird insbesondere das eBook, da es preisgünstiger, interaktiv nutzbar und durchsuchbar ist. Es enthält jedoch nicht die neuesten Entwicklungen (z.B. Datenschutzgrundverordnung von 2018), sodass Aktualisierungen durch den Dozenten erfolgen.

Die österreichische Plattform Easy4Me bietet kostenlose und kompakte Zusammenfassungen, Glossare, Quizze, interaktive Inhalte sowie weiterführende Materialien zur Vorbereitung auf den Computerführerschein (ECDL/ICDL). Zusätzlich wird eine Schullizenz angeboten, die weitere Nutzungsmöglichkeiten eröffnet. Die Materialien sind praxisnah und enthalten auch aktuelle Fallbeispiele und Sicherheitshinweise.

Der Dozent wird im weiteren Verlauf des Kurses diese Materialien ergänzen, aktuelle Entwicklungen integrieren und praxisrelevante Beispiele geben.

Glossar zum Video:

- **Datensicherheit:** Schutz vor Verlust, Manipulation und unbefugtem Zugriff auf Daten 1.
- **Skimming:** Betrugsverfahren zum illegalen Auslesen von Bank- und Kreditkartendaten 2.
- **Shoulder-Surfing:** Ausspähen vertraulicher Daten durch Schulterblick 3.
- **Malware:** Schadsoftware zur Störung oder Übernahme eines Computersystems 4.
- **Rootkit:** Software, die es Angreifern erlaubt, unerkannt Zugriff auf Systeme zu erhalten 5.
- **Multifaktor-Authentifizierung:** Sicherheitsverfahren, das mehrere unabhängige Identifikationsnachweise verlangt 6.
- **Phishing:** Betrügerisches Erlangen sensibler Daten über gefälschte E-Mails oder Webseiten 7.
- **Authentifizierung:** Überprüfung der Identität einer Person oder eines Systems 8.
- **Daten:** Rohmaterialien, die gesammelt und gespeichert werden 9.
- **Informationen:** Interpretierte und kontextualisierte Daten 10.

Weiterführende Links

- **Wikipedia:** Datenschutz, Malware, Rootkit, Phishing 11.
- **Bundesamt für Sicherheit in der Informationstechnik (BSI):** Suchbegriffe „IT-Sicherheit“, „Datenschutz“, „Phishing“, „Malware“ (bsi.bund.de) 12.
- **Bundeskriminalamt (BKA):** Suchbegriffe „Phishing“, „Cyberkriminalität“, „BKA-Warnungen“ (bka.de) 13.
- **Wikipedia Suche:** „Authentifizierung“, „Malware“, „Multifaktor-Authentifizierung“ 14.
- **Bundesamt für Sicherheit in der Informationstechnik (BSI):** Suche „Datenschutzgrundverordnung“, „Skimming“, „Malware“ 15.
- **Bundeskriminalamt (BKA):** Suche „Computerkriminalität“, „Phishing“, „gefälschte E-Mails“ 16.

Fragen zum Mini-Abschlusstest:

1. Nenne zwei Vorteile der eBook-Version der Herdt-Materialien.
2. Was versteht man unter dem Begriff „Shoulder-Surfing“?
3. Welche Materialien stellt Easy4Me kostenlos zur Verfügung?

4. Wofür steht die Abkürzung „DSGVO“ und wann trat sie in Kraft?
5. Was sind Vorteile des eBooks gegenüber dem gedruckten Buch des Herdt-Verlags? a) Volltextsuche und Markierbarkeit b) Billiger Preis und interaktive Nutzung c) Aktuellere Inhalte d) Nur in Papierform erhältlich 21.
6. Welche Aussage beschreibt am besten den Unterschied zwischen Daten und Informationen? a) Daten sind interpretierte Fakten, Informationen sind Rohdaten. b) Informationen sind interpretierte Daten, Daten sind Rohfakten. c) Daten sind unwichtig, Informationen sind wesentlich.
7. Was bedeutet der Begriff „Skimming“? a) Erstellen sicherer Passwörter b) Illegales Auslesen von Kartendaten c) Sichere Speicherung von Passwörtern.

Lösungen: 5: a, b | 6: b | 7: b.

Video 2 IT-Sicherheit - Datenbedrohung und Datenschutz

https://www.youtube.com/watch?v=6jar_w_a9HE

YouTube-Video wie oben, aber zusätzlich mit Fragen zum Selbsttest (ggf. mit Login):

https://news.konrad-rennert.de/it-sicherheit-02-h5p-selbsttest/

Inhaltsangabe

Das zweite Video, ebenfalls präsentiert von Konrad Rennert, erläutert zentrale Begriffe und Konzepte rund um die Bedrohung, den Schutz und die Sicherheit von Daten. Es richtet sich weiterhin an Personen, die sich beruflich oder privat mit IT-Sicherheit beschäftigen wollen.

Zunächst wird die Unterscheidung zwischen Daten, Informationen und Wissen erläutert: Daten bilden die Basis (z.B. Wetterdaten), Informationen sind aus Daten gewonnene interpretierte Fakten (z.B. Wetterbericht), und Wissen beschreibt die Fähigkeit, aus diesen Informationen Entscheidungen abzuleiten (z.B. Erntezeitpunkt).

Ein Schwerpunkt liegt auf der Datensicherung und ihren Methoden, um vor Verlust durch Hardwarefehler, Diebstahl oder Naturkatastrophen zu schützen. Empfohlen werden einfache Backups auf externe Datenträger für Privatanwender bis hin zu komplexeren Lösungen wie NAS-Systeme oder RAID-Systeme für Unternehmen. Besonders sensible Bereiche wie Banken sichern Daten oft durch räumlich getrennte, redundante Rechenzentren ab.

Neben physischer Datensicherung thematisiert Rennert auch Maßnahmen gegen kriminelle Handlungen und unbefugten Zugriff, wie Verschlüsselung, Zugangskontrollen mittels Passwörtern und die Nutzung digitaler Zertifikate zur Sicherstellung der Authentizität und Integrität elektronischer Dokumente.

Ein weiterer wichtiger Themenkomplex des Videos ist die Datenschutzgrundverordnung (DSGVO). Diese fordert Datensparsamkeit, Transparenz und Schutz besonders sensibler persönlicher Daten wie Religion oder sexueller Orientierung. Verstöße dagegen können hohe Strafen nach sich ziehen.

Zum Abschluss erwähnt Rennert noch kurz das Urheberrecht, das digitale Inhalte schützt und unerlaubte Verbreitung unterbindet.

Glossar zum Video:

- **Backup:** Sicherheitskopie von Daten zur Wiederherstellung nach Datenverlust.
- **NAS (Network-Attached Storage):** Netzwerkspeicher zur gemeinsamen Nutzung.
- **RAID (Redundant Array of Independent Disks):** Datenspeicherung auf mehreren Festplatten, um Datenverlust zu verhindern.
- **Digitale Zertifikate:** Elektronischer Nachweis zur Sicherstellung der Authentizität und Integrität von Daten.
- **Datenschutzgrundverordnung (DSGVO):** EU-Richtlinie zum Schutz personenbezogener Daten.
- **Datensparsamkeit:** Prinzip, nur notwendige Daten zu sammeln und zu speichern.

Weiterführende Links

- Wikipedia Suche: „RAID-System“, „NAS-System“, „Digitale Zertifikate“, „Datenschutzgrundverordnung“ https://de.wikipedia.org

BSI-Suche: „Verschlüsselung“, „Datensicherung“, „Digitale Zertifikate“

Fragen zum Mini-Abschlusstest:

1. Welche Methode schützt NICHT gegen Datenverlust? a) RAID-Systeme b) Verschlüsselung c) Backup auf externe Datenträger
2. Was versteht man unter Datensparsamkeit? a) Daten regelmäßig löschen b) Nur notwendige Daten sammeln c) Daten für Marketing sammeln
3. Welcher Begriff beschreibt die Sicherstellung der Integrität und Authentizität digitaler Dokumente? a) Datensicherung b) Digitales Zertifikat c) Datensparsamkeit

Lösungen: 1: b | 2: b | 3: b

- https://www.bsi.bund.de
- BKA-Suche: „Datendiebstahl“, „Cyberkriminalität“ https://www.bka.de

Video 3 IT-Sicherheit – Urheberrecht und Copyright

https://www.youtube.com/watch?v=1ibkQT5TDIE

YouTube-Video wie oben, aber zusätzlich mit Fragen zum Selbsttest (ggf. mit Login):

https://news.konrad-rennert.de/it-sicherheit-03-h5p-selbsttest/

Inhaltsangabe:

In diesem Erklärvideo von Konrad Rennert geht es um das Thema IT-Security mit einem besonderen Schwerpunkt auf Urheberrecht und Copyright. Der Sprecher richtet sich insbesondere an Lernende, die sich auf Computerführerscheine vorbereiten, aber auch an

Personen, die Webseiten betreiben oder Inhalte über soziale Medien veröffentlichen wollen. Das Video bietet eine Einführung in die Grundlagen des Urheberrechts, erklärt zentrale Begriffe und beschreibt, welche Materialien genutzt werden dürfen, und welche rechtlichen Konsequenzen drohen, wenn Regeln missachtet werden.

Zur Veranschaulichung verweist der Sprecher auf Materialien wie die Seite Easy4Me sowie die Bundeszentrale für politische Bildung, die umfangreiche und leicht verständliche Informationen über Urheberrecht bereitstellt. Insbesondere wird darauf eingegangen, dass Werke wie Fotos, Texte oder Musik grundsätzlich geschützt sind und nur unter bestimmten Bedingungen verwendet werden dürfen. Er erläutert auch die Bedeutung von Creative-Commons-Lizenzen und diskutiert kritisch die Einschränkungen für Bildungszwecke.

Persönliche Erfahrungen des Sprechers, wie ein Gerichtsverfahren gegen ihn wegen der Nutzung eines Fotos vom Leipziger Bahnhof, verdeutlichen die Praxisrelevanz der Thematik. Er gewann das Verfahren, da das Gericht seine Nutzung als zulässige Werksbenutzung einstufte. Diese Anekdote dient als Beispiel dafür, wie wichtig das Verständnis von Urheberrechtsregelungen ist.

Besonders hervorgehoben wird die Panoramafreiheit im deutschen Recht, die es erlaubt, Aufnahmen von öffentlichen Plätzen zu machen und zu veröffentlichen, solange keine schutzwürdigen Interessen abgebildeter Personen verletzt werden. Im Vergleich dazu erläutert der Sprecher Unterschiede zu anderen Ländern, etwa Frankreich, wo Aufnahmen des beleuchteten Eiffelturms nachts lizenzpflichtig sein können.

Zum Abschluss weist der Sprecher darauf hin, dass Urheberrechte auch nach dem Tod eines Künstlers noch bis zu 70 Jahre weiterbestehen können. Bei Datenbanken gilt eine Schutzfrist von 15 Jahren. Eigene Werke hingegen können grundsätzlich frei verwendet werden.

Schließlich bietet Konrad Rennert interessierten Personen die Möglichkeit an, mit ihm in Kontakt zu treten, um gemeinsam Projekte zu unterstützen, insbesondere im Bereich Deutsch als Fremdsprache.

Glossar zum Video:

- Urheberrecht: Schutzrecht für geistige Schöpfungen wie Texte, Bilder oder Musik.
- Copyright: Internationale Bezeichnung für das Urheberrecht.
- Creative Commons (CC): Lizenzmodell, das die Nutzung von Werken unter bestimmten Bedingungen erlaubt.
- CC BY-NC-ND: Lizenz, die Namensnennung, keine kommerzielle Nutzung und keine Bearbeitungen erlaubt.
- Panoramafreiheit: Recht, Aufnahmen von öffentlichen Plätzen ohne spezielle Genehmigung zu veröffentlichen.
- Privatkopie: Erlaubte Kopie eines Werkes für den persönlichen Gebrauch.
- Werksbenutzung: Nutzung eines bestehenden Werkes im Rahmen gesetzlicher Schranken.
- Gemeinfreiheit: Status eines Werkes, das ohne Einschränkung genutzt werden darf, meist nach Ablauf der Schutzfrist.

Weiterführende Links:

- Wikipedia: "Urheberrecht" - Suchbegriff: Urheberrecht
- Bundeszentrale für politische Bildung (bpb): "Urheberrecht" - Suchbegriff: Urheberrecht bpb
- Bundesamt für Sicherheit in der Informationstechnik (BSI): "Copyright und Sicherheit" - Suchbegriff: IT-Sicherheit Copyright BSI
- Bundeskriminalamt (BKA): "Cybercrime und Urheberrecht" - Suchbegriff: BKA Cybercrime Urheberrecht

Mini-Abschlusstest:

1. Was versteht man unter Panoramafreiheit?
    - a) Fotografieren und Veröffentlichen von Privatwohnungen ohne Erlaubnis
    - b) Fotografieren und Veröffentlichen öffentlicher Plätze ohne spezielle Erlaubnis
    - c) Fotografieren von öffentlichen Plätzen nur mit Genehmigung
2. Wie lange besteht der Urheberschutz nach dem Tod eines Künstlers?
    - a) 50 Jahre
    - b) 70 Jahre
    - c) 100 Jahre
3. Was bedeutet die Lizenz "CC BY-NC-ND"?
    - a) Nutzung und Bearbeitung für kommerzielle Zwecke erlaubt
    - b) Nutzung erlaubt, aber keine Bearbeitung und keine kommerzielle Nutzung
    - c) Nutzung und Bearbeitung für private Zwecke erlaubt
4. Was darf man laut Deutschem Urheberrecht ohne Erlaubnis verwenden?
    - a) Eigene Fotos von öffentlichen Plätzen
    - b) Jede Musikdatei aus dem Internet
    - c) Alle Texte unabhängig vom Alter
5. Was ist eine Privatkopie?
    - a) Eine öffentliche Aufführung eines Werkes
    - b) Eine private Nutzung eines kopierten Werkes ohne Weitergabe
    - c) Das Hochladen von Werken auf Streamingplattformen

Lösungen:

1. b) Fotografieren und Veröffentlichen öffentlicher Plätze ohne spezielle Erlaubnis
2. b) 70 Jahre
3. b) Nutzung erlaubt, aber keine Bearbeitung und keine kommerzielle Nutzung

4. a) Eigene Fotos von öffentlichen Plätzen
5. b) Eine private Nutzung eines kopierten Werkes ohne Weitergabe

Video 4 IT-Sicherheit - Cybercrime

https://www.youtube.com/watch?v=gkGiJZ62QDk

YouTube-Video wie oben, aber zusätzlich mit Fragen zum Selbsttest (ggf. mit Login):

https://news.konrad-rennert.de/it-sicherheit-04-h5p-selbsttest/

Inhaltsangabe:

In diesem vierten Erklärvideo von Konrad Rennert dreht sich alles um das Thema Cybercrime bzw. Internetkriminalität, ein zunehmend wichtiges Gebiet im Bereich IT-Security und Datenschutz. Der Sprecher richtet sich an Teilnehmer seiner Online-Seminare sowie an Personen, die sich für die Computerführerschein-Prüfung oder berufliche Weiterentwicklung vorbereiten. Er erklärt, dass Cybercrime den Einsatz von Computern und IT-Systemen zu illegalen Zwecken umfasst und gibt praxisnahe Beispiele.

Das Video hebt hervor, dass YouTube über eine leistungsfähige automatische Spracherkennung verfügt, die die Inhalte in über 100 Sprachen übersetzen kann. Zudem bietet der Sprecher eine Excel-Arbeitsmappe an, die das Transkript, Vokabellisten und Quellangaben enthält. Insbesondere werden Materialien wie Kursunterlagen vom Herdt-Verlag und die Plattform EASY4ME empfohlen, die wichtiges Basiswissen vermitteln.

Ein zentraler Bestandteil des Videos ist die Empfehlung, sich umfassend über Cybercrime beim Bundeskriminalamt (BKA) zu informieren. Die Webseite des BKA bietet aktuelle und praxisrelevante Hinweise, unter anderem zu Betrugsmaschen wie Messenger-Betrug, Digital Skimming, betrügerische BKA-Mails und Sextortion. Der Sprecher illustriert die Risiken anhand von Beispielen aus seinem privaten Umfeld, etwa einem Fall von Messenger-Betrug bei einer Nachbarin.

Ein weiteres Beispiel ist die Sextortion-Erpressung via E-Mail, bei der mit angeblichen Videoaufnahmen erpresst wird. Zudem wird erläutert, dass betrügerische Jobangebote und falsche E-Mails im Namen des BKA im Umlauf sind. Der Sprecher betont, wie wichtig es ist, misstrauisch zu sein und niemals unüberlegt Geldforderungen nachzugeben.

Abschließend verweist der Sprecher auf weiterführende Informationsquellen wie die Wikipedia und gibt ein aktuelles Fallbeispiel: den Hackerangriff auf den Landkreis Anhalt-Bitterfeld, der gravierende Folgen hatte. Zum Schluss bietet Konrad Rennert seine Unterstützung an, insbesondere für Personen, die Deutsch als Fremdsprache lernen oder lehren.

Glossar zum Video:

- **Cybercrime**: Straftaten, die unter Nutzung von IT-Systemen oder über das Internet begangen werden.
- **Social Engineering**: Manipulative Methoden, um Menschen zur Preisgabe vertraulicher Informationen zu bewegen.
- **Phishing**: Versuch, sensible Daten wie Passwörter oder Kreditkartennummern durch gefälschte E-Mails oder Webseiten zu stehlen.

- **Skimming**: Ausspähen von Daten auf Kreditkarten oder Bankautomaten.
- **Digital Skimming**: Datendiebstahl über manipulierte Onlineshops.
- **Sextortion**: Erpressung durch angebliche intime Aufnahmen.
- **Messenger-Betrug**: Betrugsversuch per Messenger-Apps, oft unter Vortäuschung einer Notlage.

Weiterführende Links:

- Wikipedia: "Cybercrime" - Suchbegriff: Cybercrime
- Bundesamt für Sicherheit in der Informationstechnik (BSI): "Cyber-Sicherheit" - Suchbegriff: BSI Cyber-Sicherheit
- Bundeskriminalamt (BKA): "Cybercrime" - Suchbegriff: BKA-Cybercrime

Mini-Abschlusstest:

1. Was beschreibt der Begriff Cybercrime?
    - a) Legale Computernutzung
    - b) Illegale Nutzung von IT-Systemen
    - c) Entwicklung von Sicherheitssoftware
2. Was ist Digital Skimming?
    - a) Kopieren von Webseiten
    - b) Manipulieren von Onlineshops zum Datendiebstahl
    - c) Fotografieren von Kreditkarten
3. Wie sollte man auf eine angebliche BKA-E-Mail reagieren?
    - a) Sofort antworten und Daten übermitteln
    - b) Löschen oder ignorieren
    - c) Die angegebene Telefonnummer anrufen
4. Was versteht man unter Messenger-Betrug?
    - a) Phishing über Banken
    - b) Betrugsversuche über Messenger-Dienste
    - c) Erpressung per E-Mail
5. Wie lange wurde der Landkreis Anhalt-Bitterfeld laut Bericht vor dem Hackerangriff ausgespäht?
    - a) Eine Woche
    - b) Ein Monat
    - c) Ein halbes Jahr

Lösungen:

1. b) Illegale Nutzung von IT-Systemen
2. b) Manipulieren von Onlineshops zum Datendiebstahl
3. b) Löschen oder ignorieren
4. b) Betrugsversuche über Messenger-Dienste
5. c) Ein halbes Jahr

Video 5 IT-Sicherheit - Verschlüsselung und Passwortschutz

https://www.youtube.com/watch?v=9WEt0lDjnjE

YouTube-Video wie oben, aber zusätzlich mit Fragen zum Selbsttest (ggf. mit Login):

https://news.konrad-rennert.de/it-sicherheit-05-h5p-selbsttest/

Inhaltsangabe:

Das fünfte Video von Konrad Rennert aus der Reihe über IT-Security widmet sich dem Thema "Verschlüsselung und Passwortschutz". Es richtet sich an Teilnehmer seiner Onlinekurse, insbesondere an jene, die Deutsch als Fremdsprache lernen oder sich auf den Computerführerschein vorbereiten. Neben der Vermittlung technischer Inhalte fördert das Video zugleich sprachliche Kompetenzen.

Zu Beginn stellt der Sprecher die begleitende Excel-Arbeitsmappe vor, die Links zu relevanten Materialien, ein Transkript und eine Vokabelliste umfasst. Besonders betont wird die Bedeutung moderner Browserfunktionen zur Übersetzung von Inhalten in über 100 Sprachen, was das Video fächerübergreifend nutzbar macht.

Inhaltlich wird auf Kursunterlagen des Herdt-Verlags und die Plattform Easy4Me verwiesen, die Grundlagenwissen zur Verschlüsselung und Passwortsicherheit vermitteln. Wichtige Aspekte wie sichere Passwörter und Passwort-Manager werden angesprochen.

Ein zentraler Schwerpunkt liegt auf den Materialien des Bundesamts für Sicherheit in der Informationstechnik (BSI). Es wird erklärt, wie Datenverschlüsselung funktioniert, welche Arten von Verschlüsselung es gibt – insbesondere asymmetrische Verschlüsselung – und wie die Public Key Infrastruktur zur sicheren Kommunikation beiträgt. Beispiele aus der Praxis, wie E-Mail-Verschlüsselung mit GPG und Schutzmechanismen für WLAN-Netze (WPA2/WPA3), verdeutlichen die Bedeutung sicherer Systeme.

Zudem wird auf die Bedeutung sicherer Passwörter eingegangen. Kurze, einfache Passwörter gelten als große Sicherheitslücke. Tipps für die Erstellung starker und leicht merkbarer Passwörter werden vorgestellt. Abschließend werden biometrische Verfahren wie Fingerabdruck- oder Iris-Erkennung als die aktuell sichersten Methoden zum Schutz persönlicher Daten hervorgehoben.

Das Video motiviert dazu, sich intensiver mit IT-Security auseinanderzusetzen und verweist auf weiterführende Quellen für tiefergehende Informationen.

Glossar zum Video:

- **Datenverschlüsselung**: Verfahren zur Umwandlung von Daten in eine unlesbare Form zum Schutz vor unbefugtem Zugriff.
- **Asymmetrische Verschlüsselung**: Verschlüsselungsverfahren mit öffentlichem und privatem Schlüssel.
- **Public Key Infrastruktur (PKI)**: System zur Verwaltung digitaler Zertifikate und Schlüsselpaare.
- **WLAN-Sicherheit (WPA2/WPA3)**: Standards zum Schutz drahtloser Netzwerke vor unbefugtem Zugriff.
- **E-Mail-Verschlüsselung (GPG)**: Technik zur sicheren Kommunikation per E-Mail mittels Verschlüsselung.
- **Passwort-Manager**: Programme zur sicheren Verwaltung komplexer Passwörter.
- **Biometrische Verfahren**: Authentifizierung über einzigartige körperliche Merkmale wie Fingerabdruck oder Iris.

Weiterführende Links:

- Wikipedia: "Datenverschlüsselung" - Suchbegriff: Datenverschlüsselung
- Bundesamt für Sicherheit in der Informationstechnik (BSI): "Passwortschutz" - Suchbegriff: BSI Passwortschutz
- Bundeskriminalamt (BKA): "Cybercrime" - Suchbegriff: BKA-Cybercrime

Mini-Abschlusstest:

1. Was ist asymmetrische Verschlüsselung?
    - a) Verschlüsselung mit nur einem gemeinsamen Schlüssel
    - b) Verschlüsselung mit einem öffentlichen und einem privaten Schlüssel
    - c) Verschlüsselung ohne Schlüssel
2. Was bedeutet WPA2/WPA3 im Zusammenhang mit WLAN?
    - a) WLAN-Netzwerke ohne Passwort
    - b) Sicherheitsstandards für drahtlose Netzwerke
    - c) Offene Hotspots ohne Verschlüsselung
3. Was ist ein Passwort-Manager?
    - a) Ein Programm zur Erzeugung von Computerviren
    - b) Ein Programm zur Verwaltung sicherer Passwörter
    - c) Ein Online-Forum für Passwörter
4. Warum sind biometrische Verfahren besonders sicher?
    - a) Sie sind einfacher zu merken als Passwörter

- b) Sie beruhen auf einzigartigen körperlichen Merkmalen
- c) Sie benötigen keine Technik zur Nutzung

5. Was ist der Vorteil der automatischen Spracherkennung und Übersetzung in modernen Browsern?
    - a) Schnellere Internetverbindung
    - b) Zugang zu Lernmaterialien in vielen Sprachen
    - c) Kostenloser Download von Programmen

Lösungen:

1. b) Verschlüsselung mit einem öffentlichen und einem privaten Schlüssel
2. b) Sicherheitsstandards für drahtlose Netzwerke
3. b) Ein Programm zur Verwaltung sicherer Passwörter
4. b) Sie beruhen auf einzigartigen körperlichen Merkmalen
5. b) Zugang zu Lernmaterialien in vielen Sprachen

Video 6 IT-Sicherheit - Netzwerkstrukturen und -sicherheit 1

https://www.youtube.com/watch?v=438fr3oyq1Q

YouTube-Video wie oben, aber zusätzlich mit Fragen zum Selbsttest (ggf. mit Login):

https://news.konrad-rennert.de/it-sicherheit-06-h5p-selbsttest/

Inhaltsangabe:

Im sechsten Video der Serie zu IT-Security, Datenschutz und Sicherheit von Konrad Rennert dreht sich alles um Netzwerkstrukturen und Netzwerksicherheit. Der Sprecher erklärt zunächst die Vorteile von mehrsprachigen Untertiteln und bereitgestellten Vokabellisten, die insbesondere für Deutschlernende nützlich sind. Er erläutert, wie moderne Browserfunktionen wie automatische Übersetzungen und Vorlesefunktionen helfen, sprachliche Barrieren zu überwinden. Ergänzend bietet er eine Excel-Arbeitsmappe mit Transkripten, Übersetzungen und Vokabular zu IT-relevanten Begriffen an.

Anschließend geht das Video auf verschiedene Quellen für Kursunterlagen ein, darunter die Materialien des Herdt-Verlages und die Plattform Easy4Me. Beide dienen zur Vorbereitung auf Prüfungen im Bereich IT-Sicherheit, insbesondere auf den Computerführerschein.

Kerninhalt des Videos sind die Grundlagen von Netzwerkstrukturen. Begriffe wie LAN, WLAN, VPN, MAN und globale Netzwerke werden anschaulich erklärt. Praxisbeispiele wie das heimische WLAN, Firmennetzwerke, globale Satellitennetzwerke (z.B. Starlink im Ukrainekrieg) und regionale Metropolnetze (z.B. NetCologne) machen die Theorie greifbar.

Ein weiteres Thema ist die Rolle von Netzwerkadministratoren, ihre Bedeutung für die Sicherheit von Datennetzen und die Risiken, die entstehen, wenn Administratoren ihre Zugriffsrechte missbrauchen. Beispiele wie Edward Snowden und Datendiebstähle aus Schweizer Banken

verdeutlichen die Problematik. Abschließend wird auf die Wichtigkeit von Schutzmaßnahmen, insbesondere VPNs, zum Schutz der Datenkommunikation eingegangen.

Das Video richtet sich sowohl an Anfänger als auch an Fachkräfte und bietet Grundlagenwissen, praktische Beispiele und Hinweise auf vertiefende Quellen wie das BSI und die Wikipedia.

Glossar zum Video:

- **LAN (Local Area Network)**: Lokales Netzwerk, meist innerhalb eines Gebäudes, z.B. in Haushalten oder Firmen.
- **WLAN (Wireless Local Area Network)**: Drahtloses lokales Netzwerk.
- **VPN (Virtual Private Network)**: Virtuelles Netzwerk, das sichere, verschlüsselte Verbindungen über unsichere Netze ermöglicht.
- **MAN (Metropolitan Area Network)**: Großräumiges Stadtnetzwerk.
- **Globale Netzwerke**: Netzwerke, die Kontinente verbinden, wie das Internet oder Starlink.
- **Netzwerkadministrator**: Person, die Netzwerke einrichtet, verwaltet und schützt.
- **ARPANET**: Vorläufer des Internets, ursprünglich militärisch motiviertes Projekt.
- **Starlink**: Satellitengestütztes Internetprojekt von SpaceX für weltweite Vernetzung.
- **VPN-Dienstleister**: Anbieter von VPN-Verbindungen für sichere Internetnutzung.

Weiterführende Links:

- Wikipedia: „Datennetz“ – Suchbegriff: Datennetz
- Bundesamt für Sicherheit in der Informationstechnik (BSI): „Netzwerksicherheit“ – Suchbegriff: BSI Netzwerksicherheit
- Bundeskriminalamt (BKA): „Cybercrime“ – Suchbegriff: BKA Cybercrime

Mini-Abschlusstest:

1. Was beschreibt ein VPN?
    - a) Ein öffentlich zugängliches Netzwerk
    - b) Ein sicheres, verschlüsseltes virtuelles Netzwerk
    - c) Ein WLAN-Zugangspunkt in Cafés
2. Was ist ein MAN?
    - a) Ein privates Heimnetzwerk
    - b) Ein weltweites Kommunikationsnetz
    - c) Ein Stadtnetzwerk für Telekommunikation
3. Wer war Edward Snowden?
    - a) Entwickler von WLAN-Technologie

- b) Netzwerkadministrator, der Geheimdaten veröffentlichte
- c) Gründer von NetCologne

4. Welche Schutzmaßnahme hilft beim sicheren Zugriff auf Firmennetzwerke im Ausland?
    - a) WLAN-Repeater
    - b) VPN-Verbindungen
    - c) WLAN ohne Passwortschutz
5. Wofür wurde das ARPANET ursprünglich entwickelt?
    - a) Für private Haushalte
    - b) Für Forschung und militärische Kommunikation
    - c) Für Online-Shopping

Lösungen:

1. b) Ein sicheres, verschlüsseltes virtuelles Netzwerk
2. c) Ein Stadtnetzwerk für Telekommunikation
3. b) Netzwerkadministrator, der Geheimdaten veröffentlichte
4. b) VPN-Verbindungen
5. b) Für Forschung und militärische Kommunikation

Video 7 IT-Sicherheit - Netzwerkstrukturen und -sicherheit 2

https://www.youtube.com/watch?v=rcwmA_skeMg

YouTube-Video wie oben, aber zusätzlich mit Fragen zum Selbsttest (ggf. mit Login):

https://news.konrad-rennert.de/it-sicherheit-07-h5p-selbsttest/

Inhaltsangabe:

Im siebten Video der Reihe zu IT-Security, Datenschutz und Sicherheit beschäftigt sich Konrad Rennert mit den Bedrohungen durch Cyberkriege, persönlichen Risiken durch Hackerangriffe und den wichtigsten Schutzmaßnahmen für Netzwerke. Das Video ist eine direkte Fortsetzung von Teil 1 und richtet sich an Kursteilnehmer sowie alle Interessierten an IT-Sicherheit.

Zunächst wird erläutert, was unter Cyberkrieg verstanden wird: gezielte Angriffe auf kritische Infrastrukturen wie Wasserwerke und Elektrizitätsnetze. Diese Angriffe erfolgen oft über das Internet und können ganze Regionen lahmlegen, wie aktuelle Beispiele aus dem Ukraine-Konflikt zeigen. Ein besonderer Fokus liegt auf der Bedrohung durch den Einsatz chinesischer 5G-Komponenten und Hackergruppen aus Nordkorea, die Milliardenbeträge zur Finanzierung von Atomprogrammen erbeuten.

Danach geht Rennert auf persönliche Bedrohungen durch die Nutzung von Smartphones ein. Beispiele wie die Ortung russischer Soldaten durch Handys in der Ukraine, die zu schweren

Verlusten führten, sowie Schadsoftware wie der WannaCry-Virus verdeutlichen, wie gefährlich ungeschützte Geräte sein können. Auch alltägliche Risiken wie Datenverluste durch Ransomware werden thematisiert.

Abschließend werden wichtige Schutzmaßnahmen erklärt. Dazu gehört die Zugriffskontrolle, die in administrative, physische und technische Zugriffssicherung unterteilt wird. Ebenso werden die Funktionen von Firewalls erläutert, sowohl extern (z.B. FritzBox) als auch intern (z.B. Windows Defender Firewall). Besonders hervorgehoben wird die Wichtigkeit der WLAN-Verschlüsselung mit WPA2 oder WPA3 sowie der bewusste Umgang mit Bluetooth-Sicherheitslücken.

Das Video nutzt zahlreiche Fallbeispiele und aktuelle Ereignisse, um die Bedeutung von IT-Sicherheit praxisnah zu vermitteln. Es richtet sich an Anfänger, Berufstätige und alle, die sich auf Prüfungen im Bereich IT-Security vorbereiten möchten.

Glossar zum Video:

- **Cyberkrieg**: Angriffe auf kritische Infrastrukturen mittels Computernetzwerken.
- **Kybernetik**: Wissenschaft von Steuerung und Regelung von Systemen.
- **Ransomware**: Schadsoftware, die Daten verschlüsselt und Lösegeld fordert.
- **WannaCry**: Eine weltweite Cyberattacke, die 2017 große Schäden verursachte.
- **Zugriffskontrolle**: Schutzmechanismus, um den Zugang zu Systemen auf berechtigte Benutzer zu beschränken.
- **Firewall**: Sicherheitssystem, das den Datenverkehr zwischen verschiedenen Netzwerken überwacht und filtert.
- **WPA2/WPA3**: Sicherheitsprotokolle zur Verschlüsselung von WLAN-Verbindungen.
- **Bluetooth**: Drahtlose Technologie zur Datenübertragung über kurze Entfernungen.

Weiterführende Links:

- Wikipedia – Suchbegriff: Cyberkrieg
- BSI – Suchbegriff: Netzwerksicherheit BSI
- BKA – Suchbegriff: Cybercrime BKA

Mini-Abschlusstest:

1. Was versteht man unter Cyberkrieg?
a) Betrug im Internet
b) Militärische Angriffe auf IT-Infrastrukturen
c) Das Hacken von E-Mail-Accounts

2. Was war der WannaCry-Virus?
a) Eine neue Art der Firewall
b) Ein Virus, der Daten verschlüsselte und Lösegeld forderte
c) Ein Sicherheitssystem für WLAN

3. Welche Schutzmaßnahme hilft gegen unerwünschte Netzwerkzugriffe?
a) Offenes WLAN ohne Passwort

b) Nutzung von VPN und Firewalls
c) Deaktivierung von Sicherheitsupdates

4. Was bewirkt ein elektromagnetischer Impuls (EMP) bei einem Angriff?
a) Er erhöht die WLAN-Reichweite
b) Er zerstört elektronische Geräte
c) Er verbessert die Netzwerksicherheit

5. Wofür steht die Abkürzung WPA2?
a) Wireless Password Access 2
b) Wi-Fi Protected Access 2
c) Web Protected Application 2

Lösungen:

1. b) Militärische Angriffe auf IT-Infrastrukturen
2. b) Ein Virus, der Daten verschlüsselte und Lösegeld forderte
3. b) Nutzung von VPN und Firewalls
4. b) Er zerstört elektronische Geräte
5. b) Wi-Fi Protected Access 2

Video 8 IT-Sicherheit - Malware

https://www.youtube.com/watch?v=6YooX6BdqOc

YouTube-Video wie oben, aber zusätzlich mit Fragen zum Selbsttest (ggf. mit Login):

https://news.konrad-rennert.de/it-sicherheit-08-h5p-selbsttest/

Inhaltsangabe:

Im achten Video der Reihe zur IT-Security, Datenschutz und Sicherheit beschäftigt sich Konrad Rennert mit dem Thema **Malware** – einer der größten Bedrohungen für IT-Systeme weltweit. Der Begriff „Malware“ setzt sich aus den englischen Wörtern „malicious“ (bösartig) und „software“ zusammen und wird im Deutschen als **schädliche Software** oder **Schadprogramme** übersetzt.

Das Video richtet sich an Kursteilnehmer, die sich auf die **Prüfung zum Computerführerschein** vorbereiten, aber auch an allgemein Interessierte im Bereich IT-Sicherheit. Es wird darauf hingewiesen, dass die Wahrscheinlichkeit, mit Malware in Kontakt zu kommen, hoch ist – sowohl für Privatnutzer als auch für Unternehmen. Der Schaden kann dabei existenzbedrohend sein.

Malware kann auf verschiedenste Arten auf Geräte gelangen, etwa durch **E-Mail-Anhänge**, **Links** oder **Drive-by-Downloads**. Ein Beispiel für die gravierenden Folgen ist die Nutzung von Schadsoftware durch Nordkorea zur Finanzierung seines Atomprogramms.

Für die Prüfungsvorbereitung empfiehlt der Vortragende Materialien vom **Herdt Verlag** sowie die Plattform **Easy4Me**. Während die Herdt-Unterlagen grundlegende Inhalte abdecken, sei insbesondere die Aktualität von Quellen wie Wikipedia und die Empfehlungen des **Bundesamts für Sicherheit in der Informationstechnik (BSI)** hervorzuheben.

Im weiteren Verlauf erläutert Rennert unterschiedliche Arten von Malware:

- **Spyware** dient der heimlichen Informationsbeschaffung.
- **Adware** zeigt unerwünschte Werbung an und wird meist mit kostenloser Software gebündelt.
- **Trojaner** tarnen sich als nützliche Programme, um Zugang zu vertraulichen Informationen zu erhalten.
- **Makroviren** verstecken sich in Office-Dokumenten und können beim Öffnen Schaden anrichten.

Beispiele wie der **Bundestrojaner**, der zur Überwachung von Schwerverbrechern eingesetzt wird, sowie Angriffe auf Politiker und Unternehmen zeigen die reale Bedrohungslage. Das Video betont die Bedeutung von Vorsicht beim Herunterladen unbekannter Dateien und sensibilisiert für die Erkennung von Malware.

Zum Abschluss weist Rennert darauf hin, dass weitere Informationen und Transkripte in der bereitgestellten Excel-Arbeitsmappe verfügbar sind, um das Gelernte zu vertiefen.

Glossar zum Video:

- **Malware**: Allgemeiner Begriff für bösartige Software, die Schäden auf Computern verursacht.
- **Spyware**: Programm zur heimlichen Ausspähung und Weiterleitung von Nutzerdaten.
- **Adware**: Software, die unerwünschte Werbung einblendet, oft mit kostenloser Software gekoppelt.
- **Trojaner**: Schadprogramm, das sich als nützliches Programm tarnt, aber im Hintergrund schädliche Aktionen ausführt.
- **Makrovirus**: Virus, der sich in Makros von Office-Dokumenten versteckt und beim Öffnen aktiviert wird.
- **Bundestrojaner**: Von Strafverfolgungsbehörden eingesetzte Software zur Überwachung von Verdächtigen.
- **Drive-by-Download**: Automatisches Herunterladen von Schadsoftware beim Besuch infizierter Webseiten.

Weiterführende Links:

- Wikipedia – Suchbegriff: Malware
- BSI – Suchbegriff: Schadsoftware BSI
- BKA – Suchbegriff: Cybercrime BKA

Mini-Abschlusstest:

1. Was versteht man unter Malware?
a) Eine Art Schutzsoftware
b) Schädliche Software, die Schaden verursacht
c) Werbung im Internet

2. Wie kann Malware auf ein Gerät gelangen?
a) Über WLAN-Verbindungen
b) Über das einfache Anschalten des Geräts
c) Über E-Mail-Anhänge und Drive-by-Downloads

3. Was ist ein Trojaner?
a) Ein Programm, das Schutz vor Viren bietet
b) Ein nützliches Programm ohne Gefahren
c) Ein schädliches Programm, das sich als harmlos tarnt

4. Wofür wird der Bundestrojaner eingesetzt?
a) Zur Verbreitung von Werbung
b) Zur Überwachung von Schwerverbrechern
c) Zum Schutz privater Daten

5. Was kann ein Makrovirus infizieren?
a) Nur Webseiten
b) Microsoft Office-Dokumente
c) E-Mail-Postfächer

Lösungen:

1. b) Schädliche Software, die Schaden verursacht
2. c) Über E-Mail-Anhänge und Drive-by-Downloads
3. c) Ein schädliches Programm, das sich als harmlos tarnt
4. b) Zur Überwachung von Schwerverbrechern
5. b) Microsoft Office-Dokumente

Video 9 IT-Sicherheit - Malwareschutz

https://www.youtube.com/watch?v=EZ0Shoegwsc

YouTube-Video wie oben, aber zusätzlich mit Fragen zum Selbsttest (ggf. mit Login):

https://news.konrad-rennert.de/it-sicherheit-09-h5p-selbsttest/

Inhaltsangabe:

Im neunten Teil der Video-Reihe zu IT-Security, Datenschutz und Sicherheit widmet sich Konrad Rennert dem Thema **Schutz vor Malware**. Die Zielgruppe sind Kursteilnehmer, insbesondere solche, die Deutsch als Fremdsprache sprechen und sich auf die Prüfung zum **Computerführerschein** vorbereiten. Das Video bietet zudem praktische Hinweise zur Nutzung von YouTube-Funktionen wie verlangsamter Abspielgeschwindigkeit und mehrsprachigen Untertiteln.

Malware, also Schadsoftware, stellt eine ernsthafte Bedrohung für Computer und IT-Infrastrukturen dar. Antivirenprogramme sind die erste Verteidigungslinie: Sie sollen verhindern, dass Malware auf Geräte gelangt, diese erkennen und bestenfalls entfernen. Neue Schadprogramme entstehen täglich, jedes mit einer eigenen „Signatur“, die wie ein digitaler Fingerabdruck funktioniert. Diese Signaturen werden von Antivirenprogrammen erkannt, die dafür regelmäßig aktualisiert werden müssen.

Der Dozent betont, dass trotz Virenschutzprogramme weiterhin Vorsicht geboten ist, insbesondere bei E-Mail-Anhängen und Links. Selbst scheinbar vertrauenswürdige Absender könnten gefälscht sein. Verdächtige Dateien werden von Antivirenprogrammen häufig in einen **Quarantäne-Ordner** verschoben – ein Begriff, der auch prüfungsrelevant ist.

Besonders hervorgehoben wird, dass moderne Betriebssysteme wie Windows 10 und 11 bereits integrierte Antivirensoftware wie den **Microsoft Defender** mitliefern. Diese Lösungen bieten zuverlässigen Grundschutz ohne zusätzliche Kosten oder komplizierte Konfiguration.

Zur Vertiefung stellt Rennert verschiedene zusätzliche Lernmaterialien und Links zur Verfügung: Dazu zählen Unterlagen vom Herdt Verlag, Easy4Me, Wikipedia-Artikel und Informationen des Bundesamts für Sicherheit in der Informationstechnik (BSI). Außerdem erklärt er, wie sich Nutzer bei einem Malware-Verdacht verhalten sollten: Gerät vom Netz trennen, Virenscan durchführen, Passwörter ändern und gegebenenfalls das System neu aufsetzen.

Im praktischen Teil zeigt Rennert die wichtigsten Funktionen des Windows Defenders, etwa die Durchführung vollständiger und benutzerdefinierter Virenscans. Abschließend verweist er auf die zugehörige Excel-Arbeitsmappe, die Transkripte, Vokabular und Linklisten enthält.

Glossar zum Video:

- **Malware**: Oberbegriff für Schadprogramme, die Computersysteme schädigen oder manipulieren.
- **Antivirenprogramm**: Software zur Erkennung, Verhinderung und Beseitigung von Malware.
- **Signatur**: Erkennungsmerkmal eines Schadprogramms, ähnlich einem digitalen Fingerabdruck.
- **Quarantäne-Ordner**: Speicherort, in den verdächtige Dateien isoliert werden, um Schaden zu verhindern.
- **Microsoft Defender**: In Windows integriertes Antivirenprogramm.
- **Drive-by-Download**: Infektion eines Rechners durch den bloßen Besuch einer manipulierten Website.
- **Passwortänderung**: Sicherheitsmaßnahme nach Verdacht auf einen Malware-Angriff.

Weiterführende Links:

- Wikipedia – Suchbegriff: Antivirenprogramm
- BSI – Suchbegriff: Virenschutz BSI
- BKA – Suchbegriff: Cybercrime BKA

Mini-Abschlusstest:

1. Was ist das Hauptziel eines Antivirenprogramms?
a) Softwareinstallation vereinfachen
b) Schadsoftware erkennen und entfernen
c) Werbung blockieren

2. Was passiert mit verdächtigen Dateien in Antivirenprogrammen?
a) Sie werden sofort gelöscht
b) Sie werden in einen Quarantäne-Ordner verschoben
c) Sie werden öffentlich geteilt

3. Was sollte man tun, wenn man Malware auf dem Gerät vermutet?
a) Gerät weiter nutzen
b) Gerät vom Netzwerk trennen und Passwörter ändern
c) Den Rechner sofort ausschalten und liegen lassen

4. Welches Antivirenprogramm ist bei Windows 10/11 bereits integriert?
a) Norton Antivirus
b) Kaspersky
c) Microsoft Defender

5. Warum sollten Antivirenprogramme regelmäßig aktualisiert werden?
a) Um neue Musik herunterzuladen
b) Um neue Malware-Signaturen erkennen zu können
c) Um die Internetverbindung zu verbessern

Lösungen:

1. b) Schadsoftware erkennen und entfernen
2. b) Sie werden in einen Quarantäne-Ordner verschoben
3. b) Gerät vom Netzwerk trennen und Passwörter ändern
4. c) Microsoft Defender
5. b) Um neue Malware-Signaturen erkennen zu können

Video 10 IT-Sicherheit - SafeInternet

https://www.youtube.com/watch?v=EwDh_133MAw

YouTube-Video wie oben, aber zusätzlich mit Fragen zum Selbsttest (ggf. mit Login):

https://news.konrad-rennert.de/it-sicherheit-10-h5p-selbsttest/

Inhaltsangabe:

Im zehnten Video seiner Reihe zu IT-Security, Datenschutz und Sicherheit thematisiert Konrad Rennert die sichere Internetnutzung und den verantwortungsvollen Umgang mit persönlichen Daten im Internet. Das Video richtet sich an Kursteilnehmer, insbesondere an jene, die Deutsch als Fremdsprache sprechen, und nutzt Untertitel in über 100 Sprachen sowie die Möglichkeit, die Abspielgeschwindigkeit zu verringern.

Der zentrale Gedanke des Videos ist, dass das Internet nichts vergisst. Anhand der Archivierung alter Webseiten demonstriert Rennert, wie einfach frühere Internetinhalte wiedergefunden werden können. Daraus ergibt sich eine wichtige Warnung: Kompromittierende oder leichtfertig geteilte Inhalte – wie peinliche Partyfotos oder intime Nachrichten – können noch Jahre später schwerwiegende Folgen haben. Rennert verweist auf reale Fälle von Mobbing und Erpressung, bis hin zu dramatischen Konsequenzen wie Selbstmord. Erwachsene und Jugendliche sind gleichermaßen gefährdet, insbesondere im Kontext von Sexting und Sextortion.

Ein weiteres zentrales Thema ist der Identitätsdiebstahl. Anhand von Beispielen zeigt Rennert, wie gestohlene personenbezogene Daten genutzt werden können, um Waren auf fremde Namen zu bestellen oder Kreditwürdigkeit zu ruinieren. Er weist auf die Bedeutung von Achtsamkeit bei der Weitergabe persönlicher Daten hin und empfiehlt, sich im Falle eines Verdachts an die Schufa oder andere seriöse Stellen zu wenden.

Rennert erläutert zudem, wie man seriöse Websites erkennt: HTTPS-Verschlüsselung, das Vorhandensein eines SSL-Zertifikats und ein vollständiges Impressum sind wichtige Indizien. Gleichzeitig thematisiert er, dass die Impressumspflicht auch Nachteile haben kann, da sie Kriminellen Zugang zu persönlichen Daten bietet.

Abschließend geht Rennert auf den Umgang mit E-Mails ein. Besonders warnt er davor, emotional aufgeladene Nachrichten vorschnell abzusenden. Der Rat lautet, erst am nächsten Tag über solche Nachrichten zu reflektieren, da einmal gesendete Inhalte unwiderruflich im Netz verbleiben können.

Das Video bietet darüber hinaus weiterführende Materialien wie eine Arbeitsmappe, automatische Übersetzungen und eine umfangreiche Sammlung an themenbezogenen Begriffen und Links.

Glossar zum Video:

- **Wayback Machine**: Internet-Archiv, das alte Versionen von Webseiten speichert.
- **Sexting**: Versenden von intimen Bildern oder Texten über digitale Medien.
- **Sextortion**: Erpressung unter Androhung der Veröffentlichung intimer Inhalte.
- **Identitätsdiebstahl**: Missbrauch persönlicher Daten zur Täuschung oder zum Betrug.
- **HTTPS**: Sicheres Übertragungsprotokoll für Webseiten, erkennbar am Schlosssymbol.
- **SSL-Zertifikat**: Digitale Bescheinigung über die Sicherheit und Identität einer Website.
- **Impressumspflicht**: Gesetzliche Pflicht für Betreiber von Webseiten, bestimmte Kontaktdaten öffentlich zugänglich zu machen.

Weiterführende Links:

- Wikipedia – Suchbegriff: Wayback Machine
- BSI – Suchbegriff: Sextortion BSI
- BSI – Suchbegriff: Identitätsdiebstahl BSI
- BKA – Suchbegriff: Cybercrime BKA

Mini-Abschlusstest:

1. Was zeigt die Wayback Machine?
a) Zukünftige Versionen von Webseiten
b) Alte Versionen von Webseiten
c) Neue Trends im Internet

2. Was versteht man unter Sexting?
a) Versand von Werbemails

b) Austausch intimer Inhalte über digitale Medien
c) Virenverschickung über E-Mail

3. Wie erkennt man eine seriöse Webseite?
a) Nur am modernen Design
b) An HTTPS, Schloss-Symbol und vollständigem Impressum
c) An der Anzahl der Besucher

4. Was sollte man tun, bevor man eine verärgerte E-Mail absendet?
a) Sie sofort abschicken
b) Den Empfänger informieren
c) Einen Tag warten und erneut überdenken

5. Was ist ein typisches Risiko bei Identitätsdiebstahl?
a) Man verliert automatisch seine Zugangsdaten
b) Fremde bestellen Waren auf den eigenen Namen
c) Man kann keine E-Mails mehr verschicken

Lösungen:

1. b) Alte Versionen von Webseiten
2. b) Austausch intimer Inhalte über digitale Medien
3. b) An HTTPS, Schloss-Symbol und vollständigem Impressum
4. c) Einen Tag warten und erneut überdenken
5. b) Fremde bestellen Waren auf den eigenen Namen

Video 11 IT-Sicherheit - Sichere Kommunikation

https://www.youtube.com/watch?v=xkPTBXWqOzo

YouTube-Video wie oben, aber zusätzlich mit Fragen zum Selbsttest (ggf. mit Login):

https://news.konrad-rennert.de/it-sicherheit-11-h5p-selbsttest/

Inhaltsangabe:

Im elften Teil seiner Reihe über IT-Security, Datenschutz und Sicherheit erklärt Konrad Rennert die Prinzipien und Techniken sicherer Kommunikation. Er beginnt mit einem historischen Vergleich: Früher sicherten Brief und Siegel die Authentizität und Unverfälschtheit von Dokumenten, heute übernehmen digitale Signaturen und Verschlüsselungen diese Aufgaben im Internet. Anhand eines alten Adelsbriefs illustriert Rennert die Bedeutung von Vertraulichkeit, Authentizität und Integrität, die damals wie heute essenziell sind.

In der Gegenwart werden ähnliche Anforderungen an die elektronische Kommunikation gestellt. Besonders bei E-Mails besteht ein hohes Risiko, da standardmäßig nur eine Transportverschlüsselung erfolgt, die auf den Servern der Provider nicht durchgehend schützt. Wirklich sicher ist Kommunikation nur bei einer Ende-zu-Ende-Verschlüsselung, die beispielsweise bei Messenger-Diensten wie WhatsApp oder bei behördlichen Online-Diensten wie Elster eingesetzt wird.

Das Video erläutert die grundlegenden Begriffe Vertraulichkeit, Authentizität und Integrität: Nur durch starke Verschlüsselung und digitale Signaturen kann sichergestellt werden, dass Nachrichten weder abgefangen noch manipuliert oder falsch dargestellt werden. Symmetrische und asymmetrische Verschlüsselungsverfahren sowie hybride Ansätze werden vorgestellt, wobei insbesondere die Vorteile asymmetrischer Verfahren bei der sicheren Übermittlung betont werden.

Praktische Beispiele wie die Steuererklärung über Elster oder das Online-Banking veranschaulichen den alltäglichen Einsatz verschlüsselter Kommunikation. Hier wird deutlich: Vertrauliche Informationen sollten niemals über ungesicherte E-Mail-Kommunikation verschickt werden. Außerdem werden Risiken wie Phishing durch gefälschte E-Mails betont.

Zum Schluss gibt Rennert Hinweise auf weiterführende Quellen, wie die Seiten des Bundesamts für Sicherheit in der Informationstechnik (BSI), und erläutert die Bedeutung von Zertifikaten und Online-Ausweisfunktionen. Auch der Hinweis auf Schwächen bei Messenger-Diensten wie WhatsApp fehlt nicht, trotz ihrer Ende-zu-Ende-Verschlüsselung.

Glossar zum Video:

- **Vertraulichkeit**: Sicherstellung, dass Informationen nur von den vorgesehenen Empfängern gelesen werden können.
- **Authentizität**: Garantie, dass der Absender einer Nachricht tatsächlich derjenige ist, der er vorgibt zu sein.
- **Integrität**: Gewährleistung, dass eine Nachricht auf dem Übertragungsweg nicht verändert wurde.
- **Transportverschlüsselung**: Verschlüsselung der Datenübertragung zwischen Client und Server; schützt nicht auf dem Server selbst.
- **Ende-zu-Ende-Verschlüsselung**: Verschlüsselung von Absender bis Empfänger ohne zwischengeschaltete Entschlüsselungspunkte.
- **Symmetrische Verschlüsselung**: Verfahren, bei dem Sender und Empfänger denselben Schlüssel zum Ver- und Entschlüsseln nutzen.
- **Asymmetrische Verschlüsselung**: Verfahren mit einem Schlüsselpaar aus privatem und öffentlichem Schlüssel.
- **Digitale Signatur**: Elektronische Bestätigung der Authentizität und Integrität eines digitalen Dokuments.

Weiterführende Links:

- Wikipedia – Suchbegriff: Digitale Signatur
- BSI – Suchbegriff: Verschlüsselt kommunizieren
- BKA – Suchbegriff: Cybercrime Kommunikation BKA

Mini-Abschlusstest:

1. Was sicherte früher Brief und Siegel?
a) Die Versanddauer eines Briefes

b) Die Echtheit und Unverfälschtheit eines Dokuments
c) Den Preis einer Urkunde

2. Wann ist eine E-Mail wirklich sicher?
a) Wenn sie Transportverschlüsselung nutzt
b) Wenn sie Ende-zu-Ende-verschlüsselt und signiert ist
c) Wenn sie eine große Dateigröße hat

3. Was garantiert die Authentizität einer Nachricht?
a) Der Dateiname
b) Die Absenderadresse
c) Die digitale Signatur

4. Was beschreibt das Prinzip der Vertraulichkeit?
a) Der Inhalt ist öffentlich einsehbar
b) Nur der vorgesehene Empfänger kann den Inhalt lesen
c) Der Text darf verändert werden

5. Welche Technik kombiniert symmetrische und asymmetrische Verschlüsselung?
a) Hash-Verfahren
b) Hybride Verschlüsselung
c) Blockchain-Technik

Lösungen:

1. b) Die Echtheit und Unverfälschtheit eines Dokuments
2. b) Wenn sie Ende-zu-Ende-verschlüsselt und signiert ist
3. c) Die digitale Signatur
4. b) Nur der vorgesehene Empfänger kann den Inhalt lesen
5. b) Hybride Verschlüsselung

Video 12 IT-Sicherheit - Datensicherheitsmanagement

https://www.youtube.com/watch?v=Y74-BNTSiNs

YouTube-Video wie oben, aber zusätzlich mit Fragen zum Selbsttest (ggf. mit Login):

https://news.konrad-rennert.de/it-sicherheit-12-h5p-selbsttest/

Inhaltsangabe:

Im zwölften Video der Reihe zu IT-Security, Datenschutz und Sicherheit behandelt Konrad Rennert die essenzielle Bedeutung der Datensicherung im persönlichen Bereich. Anhand einer Anekdote aus seiner Studienzeit erklärt er, wie mühsam Datenverlust schon früher war, als Programme noch auf Lochkarten gespeichert wurden. Heute ist die Problematik ähnlich: Der Verlust eines Laptops ohne Datensicherung kann Monate an Arbeit vernichten.

Rennert erklärt die Risiken, wenn Daten nur auf derselben Festplatte gesichert werden. Gerätediebstahl, Defekte wie ein Headcrash oder Schadsoftware wie Ransomware können sämtliche Inhalte vernichten. Externe Speicherlösungen wie SD-Karten, USB-Sticks oder externe

Festplatten werden als einfache und kostengünstige Alternativen vorgestellt, besonders für private Nutzer oder kleinere Unternehmen.

Für sehr große Datenmengen empfiehlt Rennert Datensicherungsbänder oder professionelle Cloud-Dienste. Allerdings weist er auf Risiken bei Cloud-Speicherung hin, insbesondere auf die Möglichkeit, dass Geheimdienste wie die NSA auf gespeicherte Daten zugreifen könnten. Besonders sensible oder vertrauliche Daten sollten daher lokal gesichert werden.

Er gibt praktische Tipps: Regelmäßige Backups, idealerweise auf mehreren Medien und Geräten, die sichere Lagerung der Datenträger und die Übertragung wichtiger Inhalte von mobilen Geräten auf zentral gesicherte Systeme. Zudem wird auf forensische Datenrettung hingewiesen: Selbst beschädigte Festplatten können von Spezialisten oft noch ausgelesen werden – allerdings zu hohen Kosten.

Abschließend verweist Rennert auf ein umfassendes Kompendium des Bundesamts für Sicherheit in der Informationstechnik (BSI), das für tiefergehende Informationen über professionelles Datensicherheitsmanagement geeignet ist.

Glossar zum Video:

- **Datensicherung (Backup)**: Erstellung von Kopien wichtiger Daten, um sie vor Verlust oder Beschädigung zu schützen.
- **Headcrash**: Physische Beschädigung der Festplatte, bei der der Schreib-/Lesekopf die Plattenoberfläche berührt.
- **Ransomware**: Schadsoftware, die Daten verschlüsselt und für deren Freigabe Lösegeld fordert.
- **Cloud-Speicher**: Internetbasierter Speicherdienst, bei dem Daten auf externen Servern abgelegt werden.
- **Datenforensik**: Wissenschaftliche Methoden zur Wiederherstellung und Analyse beschädigter oder gelöschter Daten.
- **Sicherungsbänder**: Magnetband-Speichermedien, die große Datenmengen archivieren können.
- **Externe Festplatte**: Speichergerät, das unabhängig vom Computer betrieben und häufig für Backups genutzt wird.

Weiterführende Links:

- Wikipedia – Suchbegriff: Datensicherung
- BSI – Suchbegriff: Datensicherung und Backup-Strategien (speziell im IT-Grundschutz-Kompendium)
- BKA – Suchbegriff: Cybercrime und Datenverlust

Mini-Abschlusstest:

1. Was ist ein Headcrash?
a) Der Verlust eines USB-Sticks
b) Eine physische Beschädigung der Festplatte
c) Ein Hackerangriff auf E-Mail-Konten

2. Warum reicht eine Datensicherung auf der gleichen Festplatte nicht aus?
a) Weil sie zu teuer ist
b) Weil sie verloren geht, wenn das Gerät gestohlen oder beschädigt wird
c) Weil sie zu langsam ist

3. Was ist ein Vorteil von Sicherungsbändern?
a) Sie sind sehr kompakt und günstig
b) Sie können extrem große Datenmengen speichern
c) Sie benötigen keine spezielle Hardware

4. Welche Risiken bestehen bei der Nutzung von Cloud-Diensten zur Datensicherung?
a) Die Daten könnten schneller gelöscht werden
b) Geheimdienste oder Dritte könnten Zugriff auf die Daten bekommen
c) Die Übertragungsgeschwindigkeit ist immer sehr hoch

5. Welche Empfehlung gibt Rennert für besonders sensible Daten?
a) Speicherung ausschließlich in der Cloud
b) Speicherung auf einem öffentlichen Server
c) Lokale Sicherung außerhalb der Cloud

Lösungen:

1. b) Eine physische Beschädigung der Festplatte
2. b) Weil sie verloren geht, wenn das Gerät gestohlen oder beschädigt wird
3. b) Sie können extrem große Datenmengen speichern
4. b) Geheimdienste oder Dritte könnten Zugriff auf die Daten bekommen
5. c) Lokale Sicherung außerhalb der Cloud

Ergänzung zu den Inhalten der 12 Videos

Niemand ist perfekt! Ein von der KI durchgeführter Vergleich des ICDL-Lernzielplans mit den Texten der 12 Video-Transkripte hat acht Lücken identifiziert. Die folgenden Ergänzungen sind wichtig, wenn die ICDL-Lernziele wegen anstehender Prüfungen vollständig abgedeckt werden müssen. Die im Lernzielplan beschriebenen Gefahren durch Dialer und Skimming nehmen ab, da moderne Technik die früheren Szenarien nicht mehr zulässt.

1. Naturgefahren als Bedrohung für Daten (ICDL 1.1.4)

Ergänzung:
Neben Cyberangriffen stellen auch Naturkatastrophen eine erhebliche Gefahr für IT-Infrastrukturen dar. Feuer, Überschwemmungen oder Erdbeben können Serverräume zerstören oder Hardware dauerhaft beschädigen. Daher sind Offsite-Backups, Cloud-Speicher mit Geo-Redundanz und feuerfeste Safes für externe Speichermedien wichtige Schutzmaßnahmen.

2. Makro-Sicherheit (ICDL 1.4.1)

Ergänzung:
Makros in Office-Dokumenten können automatisierte Aufgaben ausführen – sie sind jedoch auch ein Einfallstor für Malware. In Programmen wie Microsoft Word oder Excel sollten Makros nur aktiviert werden, wenn die Quelle vertrauenswürdig ist. Die Standardeinstellung "Makros deaktivieren mit Benachrichtigung" bietet einen guten Schutz.

3. Botnetze, Keystroke-Logger, Dialer (ICDL 2.1.3)

Ergänzung:

- **Botnetze:** Zusammenschlüsse infizierter Geräte, die aus der Ferne gesteuert werden – z. B. für DDoS-Angriffe.
- **Keylogger:** Zeichnen Tastatureingaben auf, um Passwörter und PINs zu stehlen.
- **Dialer:** (Ehemalige) Kostenfalle für Modem- und ISDN-Nutzer, sie wählen ohne Wissen des Nutzers teure Sondernummern an.

4. WLAN-Sicherheit (WEP, WPA, WPA2 etc.) (ICDL 3.2.1)

Ergänzung:

- **WEP:** Veraltet, unsicher
- **WPA:** Verbesserung, aber heute ebenfalls angreifbar
- **WPA2/WPA3:** Aktuelle Standards mit robustem Schutz – WPA3 bietet z. B. Forward Secrecy.
  SSID sollte nicht öffentlich sichtbar sein. MAC-Filterung bietet zusätzlichen Schutz, ist aber leicht umgehbar.

5. Einmalpasswort (OTP) (ICDL 4.1.2)

Ergänzung:
Einmalpasswörter (One-Time Passwords) sind temporäre Codes, z. B. aus einer Authenticator-App oder per SMS. Sie werden meist im Rahmen der Zwei-Faktor-Authentifizierung (2FA)

verwendet. Vorteil: Selbst, wenn das normale Passwort kompromittiert wird, ist ein Zugang ohne das OTP nicht möglich.

6. Pharming (ICDL 5.2.3)

Ergänzung:
Pharming ist eine raffinierte Angriffsmethode, bei der Nutzer unbemerkt auf gefälschte Webseiten umgeleitet werden – etwa durch Manipulation der lokalen Hosts-Datei oder von DNS-Servern. Schutzmaßnahmen sind aktuelle Betriebssysteme, DNSSEC und vertrauenswürdige Nameserver.

7. Gefahren in sozialen Netzwerken (ICDL 6.2.4)

Ergänzung:
Gefahren beinhalten:

- **Cybermobbing:** Persönliche Angriffe online
- **Grooming:** Kontaktaufnahme durch Erwachsene zu Minderjährigen
- **Fake-Profile und Betrug:** z. B. romantische oder finanzielle Absichten
  Nutzer sollten Privatsphäre-Einstellungen prüfen, keine sensiblen Daten teilen und verdächtige Profile melden.

8. Datenvernichtung (Shreddern, Degaussen etc.) (ICDL 7.2.4)

Ergänzung:
Normales Löschen entfernt Daten nicht endgültig – sie bleiben oft rekonstruierbar. Methoden für sichere Löschung:

- **Softwarebasiert:** Tools wie „DBAN“ oder „Eraser“ überschreiben Sektoren mehrfach.
- **Physikalisch:** Schreddern, Entmagnetisieren (Degaussing), thermisches Zerstören.
  Besonders bei sensiblen Daten (z. B. in Behörden) sind zertifizierte Verfahren erforderlich.

Zusammenfassung der Glossare der 12 Videolektionen

A – D

- **Adware**: Software, die Werbung einblendet, oft gekoppelt mit kostenloser Software.
- **Antivirenprogramm**: Software zur Erkennung und Beseitigung von Schadsoftware.
- **ARPANET**: Vorläufer des Internets, ursprünglich militärisches Projekt.
- **Asymmetrische Verschlüsselung**: Verschlüsselung mit einem öffentlichen und einem privaten Schlüssel.
- **Authentifizierung**: Prüfung der Identität eines Nutzers oder Systems.
- **Authentizität**: Sicherheit, dass eine Nachricht vom angegebenen Absender stammt.
- **Backup (Datensicherung)**: Sicherheitskopie zur Wiederherstellung verlorener Daten.
- **Biometrische Verfahren**: Identifikation durch Fingerabdruck, Gesichtserkennung etc.
- **Bluetooth**: Drahtlose Datenübertragung über kurze Distanzen.
- **Bundestrojaner**: Überwachungssoftware von Behörden zur Strafverfolgung.
- **Cloud-Backup/-Speicher**: Online-Speicherung von Daten auf externen Servern.
- **Copyright (Urheberrecht)**: International gebräuchlicher Begriff für geistiges Eigentum.
- **Creative Commons (CC)**: Lizenzsystem für die kontrollierte Nutzung kreativer Werke.
- **Cybercrime**: Kriminalität mithilfe digitaler Technologien.
- **Cyberkrieg**: Angriffe auf IT-Infrastrukturen mit politischen Zielen.
- **Daten**: Rohinformationen ohne Kontext.
- **Datensicherheit**: Schutz vor unbefugtem Zugriff, Verlust und Manipulation.
- **Datenschutz**: Schutz personenbezogener Daten.
- **Datenschutzgrundverordnung (DSGVO)**: EU-Verordnung zum Datenschutz.
- **Datensicherung**: Regelmäßige Speicherung von Datenkopien zur Absicherung.
- **Datensparsamkeit**: Nur notwendige Daten erfassen und speichern.
- **Datenverschlüsselung**: Unlesbar machen von Daten zum Schutz vor Fremdzugriff.
- **Datenforensik**: Analyse und Wiederherstellung digitaler Beweise.
- **Digitale Signatur**: Prüfung der Authentizität und Integrität digitaler Dokumente.
- **Digitale Zertifikate**: Elektronischer Nachweis zur Identitätsprüfung.
- **Drive-by-Download**: Unbemerktes Herunterladen von Schadsoftware beim Surfen.

E – M

- **E-Mail-Verschlüsselung (GPG)**: Schutz von E-Mail-Inhalten vor unbefugtem Zugriff.

- **Ende-zu-Ende-Verschlüsselung**: Daten werden nur beim Sender und Empfänger entschlüsselt.
- **Externe Festplatte**: Mobiles Speichermedium für z. B. Backups.
- **Fake News**: Absichtlich verbreitete Falschmeldungen.
- **Firewall**: Filtert Datenverkehr und schützt Netzwerke vor Angriffen.
- **Globale Netzwerke**: Weltumspannende Systeme wie das Internet.
- **Headcrash**: Hardwarefehler durch physische Beschädigung der Festplatte.
- **HTTPS**: Verschlüsselte Übertragung von Webseiteninhalten.
- **Identitätsdiebstahl**: Diebstahl personenbezogener Daten zur Täuschung oder zum Betrug.
- **Impressumspflicht**: Gesetzlich vorgeschriebene Transparenz für Webseitenbetreiber.
- **Informationen**: Interpretierte und kontextualisierte Daten.
- **Integrität**: Sicherstellung, dass Daten nicht verändert wurden.
- **LAN / WLAN / MAN**: Verschiedene Netzwerkgrößenordnungen (lokal, drahtlos, städtisch).
- **Malware**: Schadsoftware zur Beeinträchtigung oder Kontrolle eines Systems.
- **Makrovirus**: Schadcode in Office-Makros.
- **Messenger-Betrug**: Betrug über Nachrichten-Apps durch vorgetäuschte Notlagen.
- **Microsoft Defender**: Windows-eigene Schutzsoftware gegen Malware.
- **Multifaktor-Authentifizierung**: Identitätsprüfung durch mehrere unabhängige Merkmale.

N – S

- **NAS (Network-Attached Storage)**: Netzwerkspeicher für lokale Backuplösungen.
- **Netzwerkadministrator**: Zuständig für die Verwaltung und Sicherheit von Netzwerken.
- **Panoramafreiheit**: Recht, öffentliche Gebäude und Plätze zu fotografieren.
- **Passwort-Manager**: Verwaltung starker Passwörter in einer verschlüsselten Anwendung.
- **Passwortänderung**: Reaktion auf Verdacht eines Sicherheitsvorfalls.
- **Phishing**: Täuschung zur Herausgabe vertraulicher Daten per Mail oder Website.
- **Privatkopie**: Erlaubtes Kopieren von Werken für den eigenen Gebrauch.
- **Public Key Infrastruktur (PKI)**: System zur Verwaltung digitaler Zertifikate.
- **Quarantäne-Ordner**: Isolierter Speicherort für verdächtige Dateien.
- **RAID**: Technik zur redundanten Datenspeicherung auf mehreren Festplatten.
- **Ransomware**: Schadsoftware, die Daten verschlüsselt und Lösegeld fordert.

- **Rootkit**: Unsichtbare Schadsoftware mit Systemzugriffsrechten.
- **Sexting / Sextortion**: Versenden intimer Inhalte bzw. deren Erpressung.
- **Shoulder Surfing**: Ausspähen von Passwörtern durch Mitlesen.
- **Signatur**: Erkennungsmerkmal von Malware oder digitaler Herkunftsnachweis.
- **Skimming / Digital Skimming**: Datendiebstahl über Bankautomaten oder manipulierte Online-Shops.
- **Social Engineering**: Täuschungstechniken zur Erlangung vertraulicher Daten.
- **Spyware**: Spioniert Nutzerverhalten unbemerkt aus.
- **SSL-Zertifikat**: Verschlüsselungsnachweis für HTTPS-Webseiten.
- **Starlink**: Satellitenbasiertes Internet von SpaceX.
- **Sicherungsbänder**: Magnetbandarchivierung großer Datenmengen.
- **Symmetrische Verschlüsselung**: Verwendung eines einzigen Schlüssels zum Ver- und Entschlüsseln.

T – Z

- **Transportverschlüsselung**: Schutz der Datenübertragung, nicht aber der gespeicherten Inhalte.
- **Trojaner**: Schadsoftware, die sich als nützliches Programm tarnt.
- **Urheberrecht**: Gesetzlicher Schutz geistiger Schöpfungen.
- **Vertraulichkeit**: Schutz vor unberechtigtem Zugriff auf Informationen.
- **VPN / VPN-Dienstleister**: Verschlüsselter Internetzugang über externe Anbieter.
- **WannaCry**: Große weltweite Ransomware-Attacke (2017).
- **Wayback Machine**: Archiviertes Internet zur Einsicht alter Webseiten.
- **Werksbenutzung**: Nutzung bestehender Werke im Rahmen gesetzlicher Ausnahmen.
- **WPA2/WPA3**: Verschlüsselungsstandards für drahtlose Netzwerke.
- **Zugriffskontrolle**: Regelung, wer worauf im System zugreifen darf.

Anhang

Mein Angebot

Frei verfügbare eBooks: https://news.konrad-rennert.de/ebook-support

Optionaler Support:

- Durchführung von Schulungen auf Basis dieses E-Books zur IT-Sicherheit
- Workshops und Videokonferenzen mit interaktiven Aufgaben und Fallbeispielen
- Bereitstellung von bearbeitbaren PDFs, Kursmaterialien und Lernvideos
- Didaktische Beratung für Lehrkräfte, z. B. zu Moodle, WordPress, alfaview, MS Teams, Zoom

Zielgruppen

- Lehrkräfte und Bildungseinrichtungen
- Multiplikatoren in der Erwachsenenbildung
- IT-Beauftragte in Initiativen, Vereinen und Organisationen

Kontakt & Umsetzung

Alle Angebote sind modular, flexibel und individuell anpassbar – vom einstündigen Impuls bis zur mehrtägigen Fortbildung.

- Für Schulungen: **flipped-classroom@konrad-rennert.de**
- Allgemeine Anfragen: info@konrad-rennert.de
- Weitere Informationen: https://konrad-rennert.de/?s=learninglounge

Spendenbasierter Zugang zur erweiterten Lernplattform

Die Teilnahme erfolgt spendenbasiert:

- Ab 10 € Spende erhalten Sie eine Benutzerrolle und 3 Monate Zugriff auf geschützte Inhalte auf news.konrad-rennert.de mit weiteren Materialien zum Computerführerschein.
- Eine gültige E-Mail-Adresse genügt – kein Account, kein Passwort
- Die Spende gilt gleichzeitig als Identitätsnachweis

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 41“)**

➞ 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**

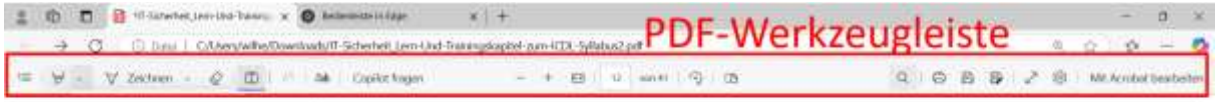
🔹 *Vorbereitung:* Teilnehmer laden das PDF im Browser, markieren und kommentieren vor dem Meeting
🔹 *Live:* Trainer teilt Bildschirm und erklärt Inhalte – Teilnehmer ergänzen Notizen direkt ins PDF
🔹 *Nachbereitung:* Lernende senden ihre Version mit Kommentaren oder Rückfragen ein oder tauschen sich 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 leicht erklärt - Datenschutz, Netzwerksicherheit und Schutz vor Cybergefahren - Ein E-Book auf Basis von 12 YouTube- Videos zum Thema IT-Security:
https://www.youtube.com/playlist?list=PLhGYp2d1_OXsH8W0GvIrhe70Pd-nqA7ZB

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?

- Kapiteltexte gemäß Titel der Erklärvideos

- Fallbeispiele und Quellenverweise
- Infografiken und Titelbilder im einheitlichen Layout
- Erklärungen für die Zielgruppen und Altersklassen von älteren Schülern bis zu Senioren

Wie wurde es erstellt?

- Fachlich begleitet durch einen zertifizierten ECDL/ICDL-Trainer
- Unterstützt durch generative KI (Text & Bild) mit manuellem Feinschliff
- Quellen aus öffentlicher Berichterstattung und Behördenportalen (z. B. BSI, Verbraucherzentralen, Heise, Tagesschau, Wikipedia)
- Struktur und Tiefe orientieren sich an frei verfügbaren Lehrplänen zum Computerführerschein

Wann wurde es erstellt?
Erarbeitet und aktualisiert im Zeitraum: **März – April 2025**

Warum wurde es erstellt?
Zur Vorbereitung auf das Modul *IT-Sicherheit* sowie zur Sensibilisierung für digitale Risiken in Alltag, Schule, Beruf und Gesellschaft.
Das Werk richtet sich ausdrücklich an alle Lernenden – unabhängig von Alter oder Vorwissen – und versteht sich als Beitrag zur digitalen Grundbildung.

Wo darf das Werk verwendet werden?

- Zur Vorbereitungen von Computerführerschein-Prüfungen
- Für schulische und berufliche Bildungsmaßnahmen
- In beliebigen Weiterbildungsprojekten

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)**

Namensnennung gemäß Lizenz:
Konrad Rennert, „IT-Sicherheit leicht erklärt - Datenschutz, Netzwerksicherheit und Schutz vor Cybergefahren - Ein E-Book auf Basis von 12 YouTube-Videos“

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.

Bei Verwendung bitte folgenden Vermerk angeben:

„Erstellt von Konrad Rennert, mit Unterstützung durch KI (ChatGPT & DALL·E), lizenziert unter CC BY 4.0“