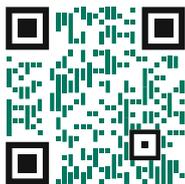


Trainerleitfaden zum DsiN-Digitalführerschein

Diese Anleitung steht auch
zum Download zur Verfügung:



Impressum

Trainerleitfaden, 1. Auflage, Januar 2023

Verantwortlich: Dr. Michael Littger

Projektleitung: Katharina Kunze

Redaktion: Gabriele Bruckmeier und Theresa Kuper

Gestaltung: Gabriele Bruckmeier (innen),
KRAUT & KONFETTI (außen)

Inhaltsangabe

Einführung: Warum ist dieser Kurs für Senior:innen sinnvoll?	4
Besonderheiten dieses Kurses	5
Kursaufbau und Themenbereiche	6
Kursmaterialien und Ablauf des Kurses	7
Zeitplanung, Kursstart und Kursende	9
Level 01	10
Level 02	40
Level 03	70
Glossar	100

Einführung

Die Digitalisierung geht in allen Lebensbereichen mit sehr großen Schritten voran. Die Generation 60+ ist mit Büchern, Bedienungsanleitungen und ohne YouTube-Tutorials aufgewachsen. Ältere Menschen haben echte Tasten und Schalter zu bedienen gelernt und sind mit WLAN, Updates, Online-Shopping oder Smart Home häufig überfordert. Sie haben Angst etwas falsch zu machen und dadurch Schaden zu verursachen.

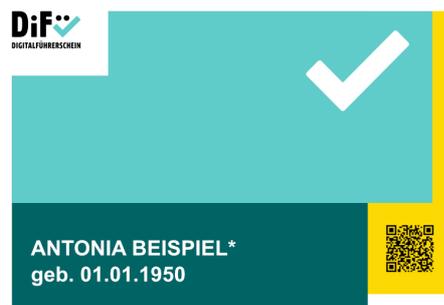
Der Digitalführerschein DiFü ist ein Angebot für alle Altersgruppen, dass diese Wissenslücke schließen möchte. Damit Seniorinnen und Senioren den Mut finden, den Digitalführerschein zu starten, hat der Digitale Engel einen Kurs dazu gestaltet. Mit diesem Trainerleitfaden bekommen Sie als Kursleiter:in alle Informationen, um einen erfolgreichen Digitalführerschein-Kurs mit einer Gruppe von Senior:innen durchzuführen.

Warum ist dieser Kurs für Senior:innen sinnvoll?

Das Internet bietet viele Chancen und Möglichkeiten, den Alltag zu bereichern und zu erleichtern. Hilfe bei Einkäufen, Behördengängen oder auch der Austausch mit Familie und Freunden. Digitalisierung ist kein Selbstzweck und sollte keinesfalls die realen Kontakte ersetzen. Die unzähligen Möglichkeiten des Internets kompetent, sicher und vor allem selbstbestimmt nutzen zu können, bedeutet aber auch ein Stück weit gesellschaftliche Teilhabe. Daher möchten wir älteren Menschen den Weg ins Internet so einfach wie möglich vorstellen.

Jeder wird in den nächsten Jahren mit digitalen Themen konfrontiert werden. Es ist besser, jetzt einzusteigen. Der DiFü stellt Chancen neuer Techniken vor, um den Alltag sicherer, einfacher und auch unterhaltsamer und sozialer zu gestalten.

Ob Entdecker:in, Erfahrener:in oder Alleskönner:in, der DiFü macht es Allen leicht, sich Digitalkompetenz aufzubauen. Wie beim Autoführerschein werden Grundkenntnisse vermittelt und nach erfolgreichem Abschluss erhält jede:r Kursteilnehmer:in ein Zertifikat.



hat **Level 1** des Lernangebots des DiIN-Digitalführscheins (DiFü) mit folgenden Schwerpunkten erfolgreich absolviert:

- A. Geräte
- B. Internet
- C. Kommunikation
- D. Datenwelt
- E. Gefahrenschutz
- F. Technologiealltag

15. Dezember 2022

M. Litterger

Dr. Michael Litterger
Geschäftsführung Deutschland sicher im Netz e.V.



*Dieses Zertifikat wurde verifiziert (Überprüfungsergebnis per QR-Code) oder per ID-Verfahren.
Der DiIN-Digitalführerschein ist ein Zertifikat von Deutschland sicher im Netz e.V., Lützenbrunnstraße 104, 10117 Berlin.

Besonderheiten dieses Kurses

Der DiFü ist ein Angebot von Deutschland sicher im Netz. Der sichere Umgang mit digitalen Medien und Geräten steht im Vordergrund. Zu allen Geräten, Programmen oder Netzwerken, die hier vorgestellt werden, gibt es ein Kapitel Sicherheit. Was sind mögliche Betrugsversuche und wie kann sich der Einzelne hier schützen? Es werden Anleitungen gegeben, wie sich Betroffene verhalten sollten und an wen sie sich wenden können.



Die Sprache der digitalen Welt ist Englisch. Das macht den Einstieg für die Generation 60+ teilweise schwieriger. Der DiFü berücksichtigt dies und erklärt mit Bildern und Videos auf einfache Weise die Bedeutung der meistgenutzten Begriffe.

Den Digitalführerschein gibt es als Website und als App. So können Personen mit einem Computer, Laptop, Tablet oder Smartphone teilnehmen.

Jedes Kapitel endet mit einer Teilprüfung. Das erscheint für ältere Menschen, die meist schon sehr lange keine Prüfung mehr absolviert haben, beängstigend. Die Besonderheit hier ist, dass jede Prüfung so oft wiederholt werden kann, wie man möchte. Jede:r wird hier ein Erfolgserlebnis mitnehmen. So wird Selbstvertrauen innerhalb der digitalen Welt aufgebaut.



Kursaufbau und Themenbereiche



Der DiFü teilt sich in privaten und beruflichen Kontext. Dieser Trainerleitfaden behandelt nur den privaten Kontext.

Der DiFü beinhaltet 3 Level. Das Level 1 ist für Entdecker:innen gedacht. In Level 2 und 3 wird Grundwissen aus Level 1 wiederholt, ergänzt und durch komplexere Sachverhalte erweitert. Am Anfang des Kurses gibt es online eine „Leveleinschätzung“.



Wir empfehlen, dass Sie alle drei Level durcharbeiten. So vermeiden Sie, dass sich einzelne in der Gruppe abgehängt fühlen und alle auf dem gleichen Wissensstand sind.

Ein Level besteht aus sechs Themenbereichen und hat zwischen vier und sechs Unterkapitel. Zusätzlich gibt es den Bereich „Fokusmodule“. Hier wird der DiFü fortlaufend durch neue und interessante Themen erweitert. Dieser Bereich wird in diesem Trainerleitfaden nicht berücksichtigt und ist auch kein Bestandteil der Prüfung zum Zertifikat.

Themenbereiche pro Level:

- A Geräte**
- B Internet**
- C Kommunikation**
- D Datenwelt**
- E Gefahrenschutz**
- F Technologiealltag**

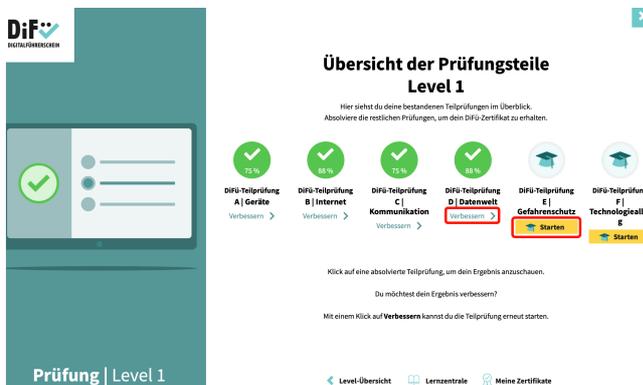


In Kursen für Senior:innen hat sich der Einstieg mit Themenbereich F, Technologiealltag, bewährt. Dieses Kapitel beinhaltet Themen, von denen Ältere bereits gehört haben könnten. Dadurch überfordern Sie Ihre Teilnehmenden nicht sofort. Danach könnten D Datenwelt und E Gefahrenschutz folgen und die drei anspruchsvollsten Themen heben Sie sich für den Schluss auf, wenn die Teilnehmer:innen schon Prüfungen bestanden haben und selbstbewusster und erfahrener sind.

Kursmaterialien und Ablauf des Kurses

Was brauchen Sie für diesen Kurs:

- Trainerleitfaden
- PowerPoint Präsentation DiFÜ
- Lernhefte für Kursteilnehmer:innen
<https://www.digitaler-engel.org/index.php/materialien>
- Erklärvideos (am besten vorher herunterladen)
- Internetzugang
- Tafel und/oder Projektionswand
- Teilnehmer:innen benötigen ein Gerät mit Internetverbindung



- ✚ Zur Vorbereitung des Kurses empfehlen wir Ihnen, alle Level und Teilprüfungen mehrmals selbst zu durchlaufen. Im Trainerleitfaden finden Sie alle Themenbereiche und anzusprechende Inhalte aufgeführt. Alle Video-Positionen sind markiert. So können Sie sich mit dem Trainerleitfaden im Kurs durch alle Themen und Begriffe durcharbeiten.

Im Kasten rechts sind jeweils Wörter, die (falls es keine Projektion gibt) Sie an die Tafel schreiben sollten. Dies betrifft vor allem englische Begriffe. Im Text sind manche Wörter „**fett**“ dargestellt. Das sind prüfungsrelevante Aussagen. Ermutigen Sie die Teilnehmer:innen, diese Punkte in ihr Lernheft zu schreiben.

1. Was ist WLAN und was ist LAN?

- Internetverbindung: **LAN WLAN**
- Router (Gleiche Übertragungsgeschwindigkeit)

WLAN - LAN
Wireless

2. Was ist besser, WLAN oder LAN?

- **WLAN bevorzugt:** Beweglichkeit, mobile Geräte
- **LAN bevorzugt:** Viele Geräte, viele Router im Umkreis, Hindernisse z.B. dicke Wände
- **Latenz**

Latenz
Kurze Reaktionszeit

Mein Wissen üben

Frage 1 | 5

Was kannst du zum Beispiel mit einem digitalen Personalausweis machen?

- A Du kannst dich an Bürgerterminals und Automaten elektronisch ausweisen.
- B Damit kannst du dir ein Profil in einem sozialen Netzwerk anlegen.
- C Damit kannst du online eine Essensbestellung aufgeben.

Am Ende jedes Unterkapitels gibt es ein kurzes Quiz. Diese 5 Fragen können Sie mit allen zusammen oder jeder:r für sich auf dem eigenen Gerät durchgehen. Weisen Sie darauf hin, dass manchmal mehrere Antworten möglich sind.

 <p>Information</p> <p>Erhalte alle wichtigen Infos zum DsiN-Digitalführerschein.</p>	 <p>Lernzentrale</p> <p>Eigne dir Wissen an und meistere die DiFü-Teilprüfungen.</p>	 <p>Zertifikat</p> <p>Erfahre mehr über die Vorteile des DiFü-Zertifikats.</p>	 <p>Jetzt Prüfung starten</p> <p>Starte direkt mit der DiFü-Gesamprüfung!</p>
---	--	--	---

Der Kurs kann als Präsenz- oder Online-Kurs durchgeführt werden. Die Teilnehmenden brauchen einen Zugang zur Lernzentrale. Das kann über einen Desktop-Computer, ein Laptop, ein Tablet oder ein Smartphone sein.

Mit den Teilnehmer:innen sollten Sie den Umgang und die Orientierung innerhalb der Lernzentrale üben. Dabei ist es egal, ob der Einzelne die Website oder die App nutzt. An manchen Stellen steht: „Siehe Lernzentrale“. Hier werden Anwendungen zu verschiedenen Geräten oder Programmen erklärt. An dieser Stelle bietet es sich an, die Lernzentrale auf den Geräten öffnen zu lassen, und die Anwendung zum eigenen Gerät zu finden. Erklären Sie dabei die Funktionsweise der Seitennavigation und der Brotkrümel-Navigation.

Dein Lernfortschritt

A Geräte	25%	0/4
B Internet	19%	0/5
B1 Mobiles Internet	<input type="checkbox"/>	
B2 Web & Web 2.0	<input type="checkbox"/>	
B3 Browser	<input type="checkbox"/>	
B4 Cookies	<input type="checkbox"/>	
B5 Suchmaschinen	<input type="checkbox"/>	
Teilprüfung starten		
C Kommunikation	0%	0/5
D Datenwelt	0%	0/5
E Gefahrenschutz	0%	0/6
F Technologiealltag	0%	0/4

[Start](#) > [DsiN-Digitalführerschein \(DiFü\)](#) > [Lernzentrale](#) > [Level 1 | Internet](#) > **Mobiles Internet**

2. Was ist ein starkes Passwort?



„12345“ ist kein starkes Passwort. Hacker:innen knacken einfache Passwörter wie dieses in Bruchteilen von Sekunden. Was ist also ein sicheres Passwort? Das ist ganz einfach erklärt. Es ist:

einmalig

Du solltest unterschiedliche Passwörter für verschiedene Konten nutzen – also verwende nicht das Passwort vom Online-Shop auch für das soziale Netzwerk. Das ist wichtig. Denn sollte tatsächlich mal jemand dein Passwort erraten, sind zumindest keine anderen Konten betroffen.

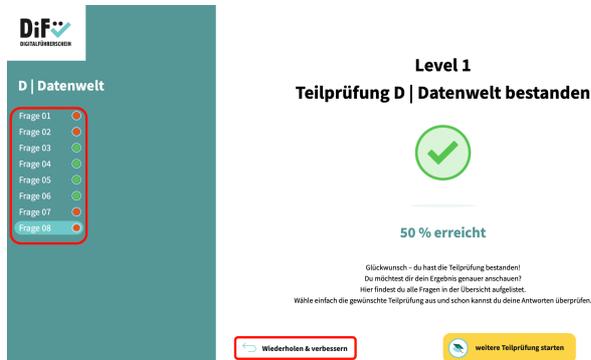
lang

komplex

kreativ

In der Lernzentrale wird ein sogenanntes Akkordion-Design genutzt. Dabei sieht man nur die Überschrift eines Punktes. Über einen kleinen Pfeil an der Seite der Zeile, kann man die Inhalte wie bei einem Akkordion aus- oder einklappen.

Zeitplanung



Pro Kurseinheit sollte ein Themenbereich behandelt und mit der Online-Teilprüfung abgeschlossen werden. Jede Teilprüfung hat 8 Fragen und erlaubt 10 Minuten zum Beantworten. Zum Bestehen der Prüfung braucht es 50 % richtige Antworten. Die Prüfung ist ein Mittel, das gelernte Wissen zu verfestigen. Ermutigen Sie die Teilnehmenden dazu, die Prüfung zu wiederholen. Je nach Gruppe und Zwischenfragen sollten Sie pro Themenbereich etwa 1,5 Stunden einplanen.

Kursstart

Alle Teilnehmer:innen sollten sich zu Beginn des Kurses auf der Website des DiFÜ registrieren, um Zugang zu den persönlichen Prüfungsergebnissen und dem Zertifikat zu bekommen. Jede:r sollte ein Lernheft erhalten. Es bietet Platz für Notizen zu allen 3 Level und enthält ein verkürztes Glossar. Alle Materialien finden Sie hier zum Download: <https://www.digitaler-engel.org/index.php/materialien>

Anmelden **Registrieren** **1**

meinname@mail.de **2**

.....

Optional: Für die Ausstellung von Zertifikaten kannst du deinen Namen und dein Geburtsdatum angeben.

Antonia Beispiel **3**

01.01.1950

Ich stimme den AGB des DsIn-Digitalführscheins zu und habe die Datenschutzrichtlinien gelesen.

4 Registrieren >

Kursende

Wenn alle Teilprüfungen bestanden sind, wird in der Übersicht „Zertifikat herunterladen“ angeboten. Darauf tippen und das Zertifikat herunterladen, per E-Mail senden lassen oder über „Teilen“ bei LinkedIn oder Bing einstellen. In der Anmeldung unter „Mein DiFÜ“ und „Meine Daten“ können Sie Ihr DiFÜ-Konto bei Bedarf löschen.

Übersicht der Prüfungsteile Level 1

Hier siehst du deine bestandenen Teilprüfungen im Überblick. Absolviere die restlichen Prüfungen, um dein DiFÜ-Zertifikat zu erhalten.



Klick auf eine absolvierte Teilprüfung, um dein Ergebnis anzuschauen.

Du möchtest dein Ergebnis verbessern?

Mit einem Klick auf **Verbessern** kannst du die Teilprüfung erneut starten.





Level 1

A | Geräte

A1 Router & (W)LAN

1. Was ist WLAN und was ist LAN?

- Internetverbindung: **LAN - WLAN**
- Router (Gleiche Übertragungsgeschwindigkeit)

*WLAN - LAN
Local Area Network
Wireless*

2. Was ist besser, WLAN oder LAN?

- **WLAN bevorzugt:** Beweglichkeit, mobile Geräte
- **LAN bevorzugt:** Viele Geräte, viele Router im Umkreis, Hindernisse z.B. dicke Wände
- **Latenz**

*Latenz
Kurze Reaktionszeit
Sender / Empfänger*

3. Was ist der Router?

- **Schnittstelle** zwischen Geräten und Internet
- Router = „Verteiler“ von Datenpakete

*Schnittstelle
Router*

4. Wie richte ich den Router ein? (Siehe Lernzentrale)

- Anschluss Stromquelle und DSL / Kabel
- Tipp: Auf Browser **Benutzeroberfläche Router** zugreifen: Netzwerkname und Passwort ändern, Update installieren

*Router
Benutzeroberfläche
IP Adresse: 192.168.0.1*

5. Wie verbinde ich meinen Router (sicher) mit den Geräten?

- Router-Informationen: **Aufkleber Rückseite**
- Anschluss LAN
- Anschluss WLAN



A2 PC & Laptop, Smartphone & Tablet

1. Was machen PCs und Laptops aus?

- Oberbegriff Computer
- **Desktop PC** mit **Bildschirm, Tastatur, Maus**
- Laptop
- Smartphone, Tablet

*Computer
Desktop PC
Laptop*

2. Was machen Smartphones und Tablets aus?

- Smartphone (Handy) / Tablet, Touch-Display
- **Hardware:** Drucker, Maus, Monitor, Tastatur, PC, Tablet, Smartphone
- **Software:** Programm, App Store, Betriebssystem, Virenschutzprogramm, Apps, PlayStore

*Mobile Datenverbindung
Touch Display
Hardware
Software*

3. Was ist ein Betriebssystem und welches läuft auf welchem Gerät?

- **Betriebssystem** „erweckt Hardware zum Leben“
- PC - Laptop: **Windows**
- MacBook - Apple Computer: **MacOS**
- Smartphone - Tablet: **Android**
- iPhone - iPad: **iOS**

*Betriebssystem
Windows - MacOS
Android - iOS*

4. Was genau macht ein Betriebssystem?

- **Gerätesteuerung**
- **Verwaltung:** Hardware, Software, Dateien, Rechte
- Internetverbindung zusammen mit Browser
- Schutz vor Gefahren durch **Updates** und **Firewall**
- Steuerung Betriebssystem über **Icons**

*Browser
Update
Firewall
Hacker
Icons*

A3 Apps & Programme

1. Was sind Apps und Programme?

- Software = Programm
- App, Application, Anwendungen

*App
Application*

2. Wo finde ich Apps und Programme? (Siehe Lernzentrale)

- **Virtueller Laden** = Store
- Microsoft Store - Mac App Store
- Google Play Store - App Store

*Microsoft Store -
Mac App Store
Play Store - App Store*

3. Was sind App-Berechtigungen?

- Kamera, Mikrophon, Standort, Adressbuch
- **Zugriffsrechte:** Ablehnen, Zulassen

*Berechtigungen
Zugriffsrechte*

4. Wie ändere ich App-Berechtigungen wieder? (Siehe Lernzentrale)

- Einstellungen
- Android: App Berechtigungen oder Liste der Apps
- Apple: Datenschutz oder Liste der Apps



*„Nur bei Nutzung der
App“*

3. Was muss ich also alles beachten?

- Vertrauenswürdigkeit: **PlayStore, AppStore**
- **Berechtigungsanfragen** kritisch betrachten (Standort, Kontakte, Kamera, Mikrophon)
- **Bewertungen** und Downloads prüfen
- **Kosten**
- **Datensicherheit**

A4 Smart Home

1. Was ist ein Smart Home?

- Video Smart Home: Länge 2:41
- Datenübertragung: **WLAN, Bluetooth, Funk**
- **Sprachassistenten**: Alexa, Siri, Hey Google
- Hub, Steuerungszentrale, Basisstation

*WLAN, Bluetooth, Funk
Steuerungszentrale,
Basisstation, Hub
Alexa, Siri, Google-Nest*

2. Was macht ein sicheres Smart Home aus?

- Sichere **Passwörter**
- Bei Steuerung mit App oder Browser auf **Verschlüsselung** achten
- Hersteller und **Updates**
- Datenschutz
- Verbindung zum Internet
- Nur Geräte von **seriösen Anbietern** nutzen
- Sparsames Internet: nur wenn nötig, mit dem Internet verbinden
- Tipp: Gastnetzwerk Router erstellen



B | Internet

B1 Mobiles Internet

1. Was ist das mobile Internet?

- Öffentliches WLAN (nicht verschlüsselt)
- Mobiles Internet (Deutschland fast abgedeckt)

Mobile Daten

2. Was brauche ich, um mobil zu surfen?

- Smartphone / mobilfunkfähiges Tablet
- Aktive **SIM-Karte**, Prepaid-Karte
- Mobilfunkanbieter = Provider
- **Netzanbieter:** Telekom, Vodafone, O2, Telefonica

*SIM-Karte
Prepaid-Karte
Provider*

3. Was muss ich beim Mobilfunkvertrag oder Prepaid-Kauf beachten? (Siehe Lernzentrale)

- Telefon-Flatrate, Datenvolumen
- **Kilobyte (KB), Megabyte (MB), Gigabyte (GB)**
- Datennutzung: Texte, Musik, Video, Datensparen

*Flatrate
Byte
KB, MB, GB*

4. Wie kann ich erkennen, wie gut mein Empfang ist?

- Statusleiste, Symbol WLAN, Symbol Telefonnetz
- **Funkstandard: 4G, 5G**



5. Wie kann ich zwischen WLAN und mobilem Internet wechseln?

- WLAN nutzen und mobile Daten sparen
- Umschalten: **Kontrollzentrum, Einstellungen**

*Kontrollzentrum
Statusleiste*

B2 Web & Web 2.0

1. Web & Web 2.0 – Was sind die Unterschiede?

- Web 1.0: Statische, passive Website
- Web 2.0: **User generated Content, nutzergenerierter Inhalt**

*User generated Content
Blogs*

2. Was kann man im Web 2.0 machen?

- **Kommunikation und Austausch**
- Bilder über soziale Netzwerke teilen
- Videos schauen, Musik oder Podcasts hören
- Kommentare und Likes (Daumen rauf oder runter)

*Soziale Netzwerke
Podcasts
Likes*

3. Welche wichtigen Grundbegriffe des Internets gibt es und was verbirgt sich dahinter?

- www, worldwideweb, URL, Hyperlink, Link
- Bereich im Internet: Domain, Top-Level-Domain

*www, URL, Hyperlink,
Link
Top-Level-Domain*

4. Was ist ein Download und was ist ein Upload?

- **Download:** Dateien aus Internet auf lokalem Gerät speichern (**herunter**)
- **Upload:** Dateien von lokalem Gerät im Internet verfügbar machen (**hoch**)

*Upload
Download*

5. Was ist beim Up- und Download zu beachten?

- **Urheberrecht**
- Datenschutz
- Schadsoftware
- Dateigröße, MB, GB

B3 Browser

1. Was ist ein Browser?

- Zugang zu Websites über die Website-Adresse

Browser

2. Welche Browser gibt es und für welchen sollte ich mich entscheiden? (Siehe Lernzentrale)

- Vor- und Nachteile von Browsern: Schnelligkeit, Sicherheit, Vertrauenswürdigkeit
- **Google Chrome, Mozilla Firefox, Microsoft Edge, Safari (Apple)**
- Browser auf Mobilgeräten: Apps
- Funktionen Browser: Websites öffnen (**surfen**), Suchverlauf speichern

*Google Chrome
Mozilla Firefox
Microsoft Edge
Safari*

3. Was ist der Cache und was sollte ich damit tun? (Siehe Lernzentrale)

- Speichern von Webadressen und Inhalten
- **Cache regelmäßig löschen:** Speicherplatz voll, Geschwindigkeit reduziert
- Cache löschen in: Google Chrome, Mozilla Firefox, Microsoft Edge, Safari

Cache

4. Was ist anonymes Surfen und wie geht es?

- Datenspuren im Internet reduzieren
- Privatsphäre schützen
- Keine Speicherung der im Browser besuchten Webadressen (Suchverlauf)
- **Keine Cache Speicherung:** Keine Inhalte von Website, keine Passwörter
- **Inkognito oder anonymer Modus** bieten alle Browser

*Inkognito oder anonymer
Modus*

B4 Cookies

1. Warum ploppt ständig ein Fenster auf, wenn ich eine Website öffne?

- Cookies akzeptieren, ablehnen oder anpassen
- Cookie-Einstellungen anpassen

Cookies

2. Was sind Cookies und welche Vor- und Nachteile haben sie?

- Video Cookies: Dauer 2:04 Minuten
- Cookies speichern Verhalten auf einer Website und passen so Werbung an
- **Tracking Cookies:** Verfolgen Surfen im Netz
- Spracheinstellung und Online Shopping

*Tracking Cookies
Online Shopping Login*

3. Welche Einstellungen sollte ich vornehmen?

- **Einstellungen anpassen**
- Browsereinstellungen: Cookies manuell oder automatisch löschen
- **Inkognito- oder anonym Modus** nutzen

B5 Suchmaschine

1. Was macht eine Suchmaschine und welche gibt es?

- Video Suchmaschine: Dauer 2:16 Minuten
- Nicht alle Ergebnisse passen zur Suche
- Finanzierung durch Werbung (advertisement)

Ad = Anzeige

2. Für welche Suchmaschine entscheide ich mich? (Siehe Lernzentrale)

- Datenschutz, soziales Engagement, genaue Suchergebnisse
- Größte ist Google: **googeln**
- Vor- und Nachteile von Suchmaschinen: **Google, Bing (Microsoft) DuckDuckGo, Ecosia (sozial)**
- Adresszeile Browser = Suchmaschine in Einstellungen festlegen

*Google
Bing
DuckDuckGo
Ecosia*

3. Welche Einstellungen kann ich vornehmen?

- **Filter-Suchergebnisse:** Format wie Video, Bilder, Karte, ...
- Einstellungen: Sprache oder Zeitraum auswählen
- Filter: z.B. anstößige Ergebnisse ausblenden

*Filter
Kebab Menü (Punkte)
Burger Menü (Striche)*

4. Wie kann ich Suchergebnisse einschätzen?

- Link prüfen
- Suchbegriffe in der Website-Beschreibung
- **Auf Anzeigen (Ad) / Werbung achten, ganz oben**

Link

C | Kommunikation

C1 E-Mail

1. Wofür brauche ich E-Mail?

- **Elektronischer Briefe** mit Text und Anhang

E-Mail

2. Wie erhalte ich eine E-Mail-Adresse?

- E-Mail Anbieter (Provider) outlook, gmail, web, gmx
- Ende-zu-Ende Verschlüsselung
- Server und Datenspeicherung
- Datensparsamkeit und Datenschutz

*E-Mail Adresse
...@gmail.com
Provider
Server*

3. Wie kann ich E-Mails sicher senden und empfangen?

- Login und **Passwort**
- **Spamfilter**, E-Mail Adresse nicht öffentlich teilen
- **Virenschutzprogramm, Verschlüsselung**
- Auf Absender und Betreffzeile achten

Spam

4. Was sind Spam-Mails und welche Arten von Spam-Mails gibt es?

- Video Spam: Dauer 3:16 Minuten
- **Spam** (send phenomenal amounts of mail), **Scam** (Betrug), Hoax (Scherz), Kettenbriefe, Phishing

*Spam, Scam, Hoax
Phishing*

5. Wie kann ich mich vor Spam-Mails schützen?

- **Datenanhang nicht öffnen (Schadsoftware)**
- **Datensparsamkeit**, Vorsicht mit **Zahlungsaufforderung**

*Datensparsamkeit
Schadsoftware*

C2 Messenger & SMS

1. Was ist der Unterschied zwischen SMS, MMS und Messengern?

- **SMS** (short message service), **160 Zeichen**
- **MMS** (multimedia message service)
- Messenger: WhatsApp, Signal, Telegram, Threema

*SMS
MMS
Messenger*

2. Welche Messenger gibt es? (Siehe Lernzentrale)

- **WhatsApp, Signal, Threema, Telegram**
- Ende-zu-Ende-Verschlüsselung
- Backup

*WhatsApp, Signal,
Threema, Telegram
Backup*

3. Wie installiere ich Messenger?

- App installieren, registrieren, einrichten (Profil)
- App Berechtigungen beachten

4. Wie nutze ich einen Messenger zum Chatten?

- Chatten = digitales Plaudern
- Internetverbindung
- Symbole: Video-Kamera, Telefonhörer, Häkchen, Doppelhäkchen, Büroklammer, Foto-Kamera, Mikrofon (Feststelltaste)

Chatten

C3 Videokonferenzen

1. Was sind Videokonferenzen und welche Anbieter gibt es?

- Videoanruf (auf WLAN Verbindung achten)
- **Kamera, Mikrofon, Internetzugang** nötig
- Anbieter: **Skype, Zoom**, Messenger (WhatsApp, Signal, Telegram)
- **Skypen** = Videoanruf

*Skype - skypen
Zoom
Messenger*

2. Wie wähle ich einen Anbieter aus? (Siehe Lernzentrale)

- Vor- und Nachteile: Skype, Zoom, Messenger
- **Funktionen: Chatten, Bildschirm teilen, Daten senden, Aufzeichnung, Tastenkürzel**
- **Datenschutz, AGB, Nutzungsbedingungen**
- **Kostenlose Version, nur Anmeldung und kein Programm nötig**

3. Wie gestalte ich einen sicheren Videoanruf?

- Datenschutz, Ende-zu-Ende-Verschlüsselung
- keine Weitergabe an Drittanbieter
- Sicheres Passwort, Zugriffsrechte, Updates
- **Einladung: E-Mail, Messenger**

Passwort, Ende-zu-Ende-Verschlüsselung

4. Wie bereite ich eine Videokonferenz gut vor?

- Kamera, Mikrofon angeschaltet
- Stabile Internetverbindung
- Ruhiger Ort
- Mit Programm vertraut machen

C4 Soziale Netzwerke

1. Welche sozialen Netzwerke gibt es und wie funktionieren sie?

- Video Soziale Netzwerke: Dauer 2:49 Minuten
- **Soziale Netzwerke: Facebook, Instagram, Snapchat, Twitter, TikTok**
- Nutzer haben Accounts (Nutzerkonten): E-Mail-Adresse
- **Posten:** Beitrag veröffentlichen
- **Adden:** Jemanden hinzufügen
- **Liken:** Daumen nach oben, Herz
- **# Hashtag:** Themen finden, Beitrag zuordnen

*Soziale Netzwerke:
Facebook, Instagram,
Snapchat, Twitter,
TikTok, YouTube*

*Posten, Adden, Liken
Accounts
Hashtag*

2. Was ist zu beachten?

- **Datensparsamkeit**
- Keine vertraulichen Daten teilen
- Anmeldung: Passwort, Profilname
- **Sicherheitsvoreinstellungen**
- **Persönlichkeitsrechte** beachten
- **Urheberrechte** beachten
- Zwei-Faktor-Authentisierung
- Bei **Beleidigung** in sozialen Netzwerken: blockieren, ignorieren, Beitrag melden, Beweise sammeln, zur Polizei gehen

*Sicherheits-
voreinstellungen
Datensparsamkeit*

C5 Belästigungen & Fake News

1. Welche Belästigungen gibt es?

- Video Belästigungen: Dauer 3:10 Minuten
- Hate Speech, Mobbing, Grooming, Stalking

*Hate Speech
Cyber = Internet*

2. Wie kann ich mich vor Belästigungen und Beleidigungen schützen?

- **Nicht provozieren lassen**
- **Sammle Beweise, melde den Beitrag**
- Nicht Alles teilen, Kontakte beschränken
- Aufklärung (Cyber-Grooming)

*Cyber: -Mobbing,
-Grooming, -Stalking
Screenshot*

3. Welche Angebote gibt es für Betroffene?

- Hate Aid, Weißer Ring, Polizei, Vertrauensperson

Hate Aid, Weißer Ring

4. Was sind Fake News und warum gibt es sie?

- **Fake News** (gefälschte Nachrichten)
- Desinformation, emotionale Sprache

Fake News

5. Wie erkenne ich Fake News?

- Autor:in, Impressum, Quellen, Überschrift
- Verifizierter Account (Häkchen), Follower
- Faktenfinder (Tagesschau, Mimikama, Hoaxmap)

*Quellen prüfen
Zahl der Follower
Verifizierte Accounts
Faktenfinder*

6. Was mache ich, wenn ich Fake News erkannt habe?

(Siehe Lernzentrale)

- Beitrag, Bild, News melden, Person einschränken, blockieren, melden

Cybermobbing: Polizei

D | Datenwelt

D1 Datenschutz

1. Was ist Datenschutz und wofür ist er gut?

- Video Datenschutz: Dauer 2:50 Minuten
- Europ. Datenschutzgrundverordnung **DSGVO**

DSGVO

2. Welche Daten gebe ich im Internet preis?

- Online-Händler: E-Mail-Adresse Newsletter
- Tracking durch Cookies
- App Berechtigungen: Standort, Kontakte

*Newsletter
Tracking*

3. Was steht in einer Datenschutzerklärung?

- **Welche personenbezogenen Daten** werden gespeichert
- **Zweck und Zeitraum** der Datenspeicherung
- Partnerunternehmen
- **Datenweitergabe an Dritte**
- **Sicherheitsmaßnahmen**, um vor Zugriff zu schützen
- **Datenschutzbeauftragter**

4. Wie prüfe ich, ob ein Online-Dienst meine Datenschutz-Rechte respektiert?

- Gibt es Datenschutzerklärung?
- Welche Daten werden gespeichert oder weitergegeben?
- Wird der Zweck der Datenerhebung genannt?
- Gibt es einen Datenschutzbeauftragten?
- Recherche im Netz ist hilfreich

D2 Datensparsamkeit

1. Was ist Datensparsamkeit und warum ist sie so wichtig?

- Verantwortungsbewusstes Umgehen mit persönlichen Daten
- **So wenig Daten wie möglich** bei Onlineanbietern speichern



2. Was sind Tipps für mehr Datensparsamkeit?

- Nur das Nötigste angeben, Pflichtfelder *
- Diskret verhalten, keine persönlichen Fotos
- Bleib so anonym wie möglich (**Pseudonyme**, Spitzname)
- Verschiedene E-Mail-Adressen nutzen
- Alle Anbieter dürfen nur die Daten abfragen und speichern, die für die Nutzung notwendig sind
- Datenzugriff von Apps in Einstellungen kontrollieren



3. Wie lösche ich meine Daten bei Online-Diensten endgültig?

- In **Profil Einstellungen „Löschen“** finden
- **justdeleteme.me: Zentrale Website, führt zu den Einstellungen und Löschen**
- Anbieter kontaktieren
- Daten vorher sichern
- Eine Stilllegung / Deaktivierung ist keine Löschung

justdeleteme.me

D3 Logins und Passwörter

1. Wozu dienen Logins und Passwörter?

- **Login - Einloggen:** Identifizierung als die Person, die berechtigt ist, auf persönliche und vertrauliche Daten zuzugreifen
- Schlüssel zum Safe

*Login
Einloggen*

2. Was ist ein starkes Passwort?

- **Einmalig, lang, komplex, kreativ**
- **Klein- und Großbuchstaben, Zahlen, Sonderzeichen**

iKGa#951_W

3. Wie bilde und merke ich mir ein starkes Passwort?

- Merksatzmethode (erster oder letzter Buchstabe) + App Verlängerung
- „**Passwort vergessen**“ nutzen

Merksatzmethode

4. Was ist die Zwei-Faktor-Authentisierung ?

- **Zwei Komponenten** zum Login
- Per: **SMS, Anruf, Authenticator App, Gesichtserkennung, Fingerabdrucksensor**

*Zwei-Faktor-
Authentisierung
Authenticator App*

5. Wo und wie richte ich die Zwei-Faktor-Authentisierung ein?

(Siehe Lernzentrale)

- Einstellungen
- Alternativ Authenticator App

D4 Backups

1. Warum sollte ich Sicherheitskopien von meinen Dateien machen?

- Schutz bei Verlust der Zerstörung
- Schutz vor Schadsoftware

BackUp

2. Wie mache ich Backups?

- Kopie auf **USB Stick** oder **externe Festplatte**
- Backup aktuell halten
- Backup-Medium nicht verbunden lassen:
Schaden bei Problemen der internen Festplatte oder USB Verlust
- **Synchronisation** heißt, alle Daten auf dem internen Speicher und dem Backup sind auf dem gleichen Stand

*USB Stick
drag&drop
Synchronisation*

3. Welche Programme kann ich nutzen, um Backups zu machen?

(Siehe Lernzentrale)

- Programme: GoodSync&Co, PureSync
- Microsoft Sicherungsfunktion
- MacOS Timemachine
- Backup von Betriebssystem: Schutz vor Schadsoftware

*GoodSync&Co
PureSync*

D5 Clouds

1. Was ist eine Cloud?

- Video Cloud: Dauer 2:21 Minuten
- Cloud-Backup
- Computer/Server (Rechenzentren) Standort

*Cloud, Server
Synchronisierung*

2. Worauf muss ich bei Clouds achten?

- Nie 100% Sicherheit (2FA)
- **Starkes Passwort, Datenschutzerklärung**
- Cloud Anbieter Recherche (Deutschland)

3. Welche Cloud-Dienste gibt es?

- USA: Dropbox, Microsoft OneDrive
- Deutschland: Hydrive, MagentaCloud, Open Telekom Cloud, GMX, Web.de, Drive, ownCloud

4. Wie bekomme ich meine Daten in die Cloud?

- Registrieren mit Bestätigung
- Einloggen, Cloud auf Website/App einrichten, eventuell Programm laden

5. Wie bekomme ich meine Dateien aus der Cloud wieder heraus?

- Leeren Ordner auf Computer erstellen
- Einloggen und Daten herunterladen

6. Wie funktioniert die Cloud auf Smartphones und Tablets?

- App installieren (iCloud, Google Drive), Einloggen,
- Zugriff erlauben und Daten hochladen

*Apple: iCloud
Android: Google Drive*

E | Gefahrenschutz

E1 Updates

1. Was sind Updates und warum sind sie wichtig?

- Aktualisierung Software, Apps und Programme
- **Sicherheitslücken, Schwachstellen schließen**

*Update
Hacker*

2. Wie aktualisiere ich mein Smartphone oder Tablet?

- iPhone/iPad: App Store (WLAN nutzen)
- Android Geräte: Play Store (WLAN nutzen)

*App Update
App Store - PlayStore*

3. Wie aktualisiere ich Programme auf meinem PC, Mac oder Laptop? (Siehe Lernzentrale)

- PC: Microsoft Store, (Drei-Punkte-Menü) Einstellungen, Downloads
- Mac: Apfel, App Store, Updates

4. Wie aktualisiere ich das Betriebssystem meines mobilen Gerätes?

- WLAN, Ladekabel, Login-Daten (Pin SIM-Karte)
- iPhone/iPad: Einstellungen, Allgemein, Softwareupdate
- Android: Einstellungen, System, Systemupdate

*Softwareupdate
Systemupdate*

5. Wie aktualisiere ich das Betriebssystem meines PCs oder Mac-Rechners? (Siehe Lernzentrale)

- Mac: Systemeinstellungen, Softwareupdate
- PC: Einstellungen, Update und Sicherheit

E2 Schadsoftware

1. Was ist Schadsoftware?

- Video Schadsoftware: Dauer 2:48 Minuten
- Datendiebstahl, Zerstörung Programme
- **Download, Öffnung Anhang, fremder USB-Stick, fremder Link, Werbebanner anklicken**

*Trojaner, Wurm
Malware
Adware (Werbung)*

2. Wie schütze ich mich vor Schadsoftware?

- Keine verdächtigen Links oder Anhänge öffnen
- Nur sichere Software installieren
- **Keine Werbebanner oder dubiose Angebote öffnen (X, Alt F4, nur Abbrechen hilft nicht)**
- Programme aktuell halten
- Sicherheitssoftware, Firewall und Bordmittel nutzen

*Sicherheitssoftware:
Firewall, Bordmittel
X tippen, Alt F4*

3. Wie erkenne ich, ob mein System infiziert ist?

- **Reagiert langsam**
- **Verhält sich komisch**
- **Seltsame E-Mails im Postausgang**
- System-Scan mit Schutzsoftware

4. Was muss ich tun, wenn doch etwas passiert ist?

- Virenalarm: Löschen oder Quarantäne-Lösung
- Informationen zu Malware im Internet suchen
- Rechner vom Netz trennen
- Rechner neu aufsetzen
- Hilfe beim Spezialisten suchen
- Rat holen: Bundesamt für Sicherheit in der Informationstechnik

BSI

E3 Social Engineering

1. Was ist Social Engineering?

- Oberbegriff Betrug und Täuschung
- Beispiele: Enkeltrick, Anruf Bankmitarbeiter, E-Mail-Anhang

*Social Engineering =
Soziale Manipulation*

2. Was ist Phishing?

- Passwort + Fishing
- **Vorsicht: Login-Daten werden abgefragt, Banking-Login, Zugangsdaten**
- Über Telefonanruf: **Vishing**

*Phishing
Vishing*

3. Wie erkenne ich Phishing?

- **E-Mail-Adresse, Betreff, Anhang beachten**
- **Erscheinungsbild, Ansprache, Links, Fehler**
- Verlockendes Angebot, kein Konto, keine Bestellung, Frage nach Zugangsdaten

4. Wie gehe ich mit Phishing um?

- Spam Filter, Spam-E-Mails löschen
- Phishing-E-Mails löschen
- Internetrecherche
- Person anrufen und nachfragen

Spam-Filter

5. Was, wenn doch etwas passiert ist?

- Andere informieren
- **Passwort ändern**, BankLogin 3x falsch
- **Anbieter informieren**, Anzeige erstatten

E4 Doxxing

1. Was ist Doxxing?

- **Negativ:** Persönliche, nicht veröffentlichte Daten und Dokumente werden im Internet veröffentlicht
- Folgen: E-Mail-Flut, Angriff Privatwohnung
- **Positiv:** Veröffentlichung von Missstände und Skandalen

Doxxing

2. Wie schütze ich mich vor Doxxing?

- **Datensparsamkeit**
- Social-Media-Einstellungen
- Sicherheitsvorkehrungen: **Zwei-Faktor-Authentisierung, Updates**
- Datenbroker:innen, Datenschnüffler:innen: gegen Bezahlung gezielt nach Daten suchen und zusammentragen

Datenbroker:innen

3. Was kann ich tun, wenn ich gedoxxed wurde?

- **Nur personenbezogenen Daten, die nicht frei zugänglich sind**
- Doxxing ist strafbar
- Sich mitteilen
- Beitrag melden
- Beweise sammeln
- Anzeige erstatten

E5 Identitätsdiebstahl

1. Was ist Identitätsdiebstahl?

- Jemand gibt sich online für jemand anderen aus
- Meistens **Geldbetrug** oder Online-Bestellungen, kostenpflichtige Abos
- Identity Leak Checker des Hasso-Plattner-Institutes

*Identitätsdiebstahl
Identity Leak Checker
Datenlecks*

2. Wie vermeide ich Identitätsdiebstahl?

- **Datensparsamkeit**
- **Privatsphäre-Einstellungen**
- **Auf Phishing-Versuche achten**

Datensparsamkeit

3. Was muss ich tun, wenn doch etwas passiert ist?

- Konto und Karten sperren (Login bei Bank 3x falsch eingeben)
- **Anzeige bei Polizei**
- **Passwörter ändern**
- Mahnung, Vollstreckungsbescheid oder Inkasso- Briefe sofort beantworten (Widerspruchsfrist)
- **Schufa** Meldung

E6 Scam

1. Was ist Scam?

- Video Scam: Dauer 2:29 Minuten
- Betrug: Vorschussbetrug, **Romance Scam** (vorgaukeln von **Gefühlen, Vertrauen** aufbauen)

*Scam
Romance Scam*

2. Wie erkenne ich Scamming?

- **Geldforderung**
- **Bauchgefühl**, „zu gut, um wahr zu sein“
- Anzeichen einer Fälschung, Umwege von Überweisung, Fehler
- Kommunikation über **andere Plattformen**
- **Persönliches Treffen abgelehnt**
- **Suche im Netz**

Geldforderung

3. Was muss ich tun, wenn ich Opfer von Scamming wurde?

- Nicht auf Forderungen eingehen und kein Geld überweisen
- Beweise sichern, Rückbuchung
- Anzeige bei Polizei
- Kontakt abbrechen

F | Technologiealltag

F1 Fitnessstracker & eHealth

1. Was steckt alles in eHealth?

- Video: Dauer 2:32 Minuten
- Wearables (**Kalorien, Schritte, Puls**), Krankenkassen-Apps

*eHealth
Wearables*

2. Welche Sicherheitsaspekte gibt es zu beachten?

- **Datensparsamkeit**, werden Daten geteilt?
- **Updates und Virenschutz**
- **Einwilligungen** überdenken, Server-Standort

3. Wie sieht eHealth im Gesundheitswesen aus?

- Elektronische Patientenakte (ePA)
- Elektronische Rezept, **E-Rezept**
- **Digitale Gesundheitsanwendung** DiGAs
- Medizintechnik, **Arztbesuch Videocall**
- Telematikinfrastruktur zur Sicherheit
- Termine: Doctolib, Doctena
- Krankenkassen-App: Boni, Impfnachweis, Übungen, digitale Sprechstunde

*ePA
E-Rezept
DiGAs
Telematikinfrastruktur*

4. Was ist digital detox?

- Digitales Fasten
- Zeit am Bildschirm reduzieren, Wecker stellen, Flugmodus nutzen
- Benachrichtigungen ausschalten
- Bildschirmzeit beobachten, Zeiten oder Orte festlegen

digital detox

F2 Digitaler Personalausweis

1. Was genau ist der digitale Personalausweis?

- Video: Dauer 2:34 Minuten
- eID: analoger Personalausweis (Symbol), Kartenlesegerät oder **AusweisApp2**, **6stellige Pin**
- Onlinezugangsgesetz: Ämter, Post, Rentenversicherung

*E-Government
eID
Onlinezugangsgesetz*

2. Welche Möglichkeiten bietet er?

- BAföG
- **Rentenkonto** bei Deutscher Rentenversicherung
- **Punktestand beim Kraftfahrt-Bundesamt**
- Bürgerämter: Dienste auf Anfrage
- Service Deutsche Post und Deutsche Bahn

Postident-Verfahren

3. Was muss ich beachten?

- Verbindung nach Nutzung trennen
- **Updates** und Virenschutz
- **Verlust** sofort melden (**Polizei, Bürgeramt**)
- Nutzung ist sicher

F3 Online-Banking

1. Wie genau funktioniert Online-Banking und was brauche ich dazu?

- **Website der Bank** gibt Kontozugriff
- Einmalige Anmeldung bei der Bank
- Daten per Post zugesendet, Sicherheitsstandards
- **Überweisung: Name und IBAN**
- Echtzeit Überweisung binnen kürzester Zeit

Überweisung: Name und IBAN

2. Wie kann ich sicher online Überweisungen tätigen?

- **Jeder Computer**
- Einloggen, **Zwei-Faktor-Authentisierung**
- Bestätigung mit **TAN** oder **App-Freischaltung**
- Ausloggen nicht vergessen

*Zwei-Faktor-Authentisierung
TAN
App-Freischaltung*

3. Wie bleibe ich beim Online-Banking geschützt?

- **Sichere Passwörter**
- **Phishing:** Banken fragen nie per E-Mail ab
- Kontoauszüge prüfen
- Sichere Verbindung (**https, Schlosssymbol**)
- Datensparsamkeit
- Betrüger nutzen ähnliche Websites, auf Kleinigkeiten achten
- NFC Hülle im Portemonnaie
- **Zahlungslimit** bei Bank

*Sichere Passwörter
Phishing
NFC Hülle*

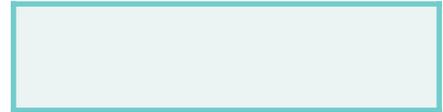
4. Und wenn doch etwas passiert ist?

- Bankverbindung sperren, **3 Mal hintereinander falsches Passwort eingeben, Anzeige**
- **Sperr-Notruf** anrufen, **Bank benachrichtigen**
- Belege sammeln, auf Schadsoftware achten

F4 Online-Shopping

1. Was ist Online-Shopping?

- Kauf von Waren im Internet
- Nutzung von Bring-Diensten



2. Welche Möglichkeiten gibt es?

- Großes Angebot und viele Anbieter
- Von Zuhause, ohne Öffnungszeiten
- Verschiedene Möglichkeiten für Bezahlung und Versand, **Click&Collect, Pick Up**

*Click&Collect
Pick Up*

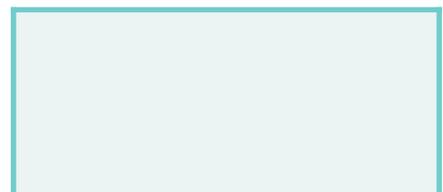
3. Wie kann ich bezahlen? (Siehe Lernzentrale)

- **Paypal:** Eigenes Konto eröffnen
- **Klarna:** Rechnung, Lastschrift, Vorkasse, Sofortüberweisung, Ratenkauf
- **Paydirekt:** Überweisung Bankkonto mit TAN
- **Kreditkarte**

*https
TAN*

4. Was sind die Vor- und Nachteile von Online-Bezahldiensten?

- Vorteil: Schnell, kostenlos, bequem
- Nachteil: weniger Kontrolle, Daten an Drittanbieter
- Achte auf Zwei-Faktor-Authentisierung



5. Was muss ich beachten?

- Website professionell, Preise transparent
- Gütesiegel: TÜV Süd, Trusted Shop, EHI, I Privacy
- Bewertungen, Auflistung Produkte, Abo-Kauf
- SOS-Karte Bundesamt Sicherheit in der Informationstechnik

*TÜV Süd, Trusted Shop,
Internet Privacy, EHI,
I Privacy*

SOS-Karte



Level 2

A | Geräte

A1 Router & (W)LAN

1. Was macht eigentlich ein Router?

- Video Router: Länge 2:22
- LAN = Local Area Network
- WLAN = **Wireless** Local Area Network
- Weltweites Netzwerk = Internet

*Router
LAN, WLAN
Internet*

2. Welche Routereinstellungen sind wichtig und wo passe ich sie an?

- Zugriff Router Internetbrowser: **IP Adresse**
- **Netzwerkname** und **Passwort** ändern
- Sichere **Verschlüsselung: WP2 - WP2/WP3**
- Welche Geräte dürfen sich verbinden
- Firmware Updates automatisch laden:
Sicherheitslücken schließen

*IP Adresse: 192.168.0.1
Verschlüsselung: WP2/
WP3*

3. Was bedeutet Mbit/s und Gigabit?

- **Bandbreite Mbit/s**
- 1000 Kilobit = 1 Megabit, 1000 MB = 1 GB
- Übertragungsgeschwindigkeit: 16Mbit/s - 1Gbit/s

*1000 Kilobit (KB)
= 1 Megabit (MB)
1000 MB =
1 Gigabit (GB)*

4. Wie schnell muss mein Internet sein?

- **Was mache ich im Internet und wie viele Personen** nutzen es?
- 2 Personen surfen, mailen, telefonieren: 50Mbit/s
- Große Datenmengen laden: Upload >10Mbit/s
- Surfgeschwindigkeit und Latenz online messen

*Upload
Download
Mbit/s
Latenz*

A2 PC & Laptop, Smartphone & Tablet

1. Was ist ein Betriebssystem? (Wiederholung Level 1)

- Oberbegriff **Computer**
- **Schnittstelle Betriebssystem**

*Computer
Betriebssystem*

2. Welches Betriebssystem läuft auf welchem Gerät?

- PC - Laptop: **Windows**
- MacBook - Apple Computer: **MacOS**
- Alternative: **Linux (open source)**
- Smartphone - Tablet: **Android**
- iPhone - iPad: **iOS**
- Andere wenig genutzt

*Windows
MacOS (Operating System)
Linux (open source)
Android
iOS*

3. Was genau macht ein Betriebssystem? (Wiederholung Level 1)

- **Gerätesteuerung**
- **Verwaltung:** Hardware, Software, Dateien, Rechte
- Internetverbindung zusammen mit Browser
- **Schutz** vor Gefahren / Hacker: **Updates** und **Firewall**
- Steuerung Betriebssystem über **Icons**

*Browser
Update
Firewall
Hacker
Icons*

A3 Apps & Programme

1. Was ist der Unterschied zwischen Apps und Programmen?

- Software = Programm
- Smartphone, Tablet = App (Application)
- Vertrauenswürdige Apps (**Bewertungen**)

*App, Application
Vertrauenswürdig,
Kosten*

2. Wo ist der Unterschied zwischen Microsoft, Apple und Android?

- **Windows** = Programme aus Stores/Websites
- **Apple:** nur hauseigenen Programme
- **Android / iOS-Geräte:** Nur aus den Stores

*Microsoft Store
Play Store - App Store*

3. Was sind App-Berechtigungen? (Wiederholung Level 1)

- Kamera, Mikrophon, Standort, Adressbuch
- **Zugriffsrechte:** ablehnen, zulassen

*Berechtigungen
Zugriffsrechte*

4. Wie ändere ich App-Berechtigungen wieder? (Wiederholung Level 1)

- Einstellungen
- Android: App-Berechtigungen oder Liste der Apps
- Apple: Datenschutz oder Liste der Apps
- „Nur bei Nutzung der App“



5. Welche alternativen Apps und Programme gibt es?

- Open-Source-Software: allen zugänglich
- Vorteile: Alle helfen mit es weiterzuentwickeln und sicherer zu machen (Peer-Review), günstiger
- Nachteile: kein Support, weniger intuitiv
- Libre-Office, Gimp, Audacity, Thunderbird, Firefox

*Open-Source-Software:
Libre-Office, Gimp,
Audacity, Thunderbird,
Firefox
Portal: GitHub*

A4 Smart Home

1. Was ist ein Smart Home? (Wiederholung Level 1)

- Video Smart Home: Länge 2:41
- Datenübertragung: **WLAN, Bluetooth, Funk**
- **Sprachassistenten**: Alexa, Siri, Google Pod
- Hub, Steuerungszentrale, Basisstation

*WLAN, Bluetooth, Funk
Steuerungszentrale,
Basisstation, Hub
Alexa, Siri, Google-Nest*

2. Was macht ein Smart Home aus?

- Nutzen **WLAN** oder **Bluetooth**
- Andere Funkstandards: ZigBee, Z-Wave
- Datenschutz
- Hub in der Cloud (Sprachassistent-
Lautsprecher)
- App-Steuerung: Router ist Schnittstelle

*Internet of Things (IoT)
WLAN, Bluetooth, ZigBee,
Z-Wave
Hub
App-Steuerung*

3. Was sind die Vor- und Nachteile eines Smart Home?

- Vorteile: machen das Leben leichter und sicherer (Wasserstandsmelder, smarte Steckdose, Heizungs-Thermostat), **reibungslose Kommunikation** (gleicher Hersteller)
- Nachteile: Austausch sensibler Daten über Server, **Sicherheitslücken, Funkstandards**

*WLAN, Bluetooth
Steuerungszentrale,
Basisstation = Hub
Funkstandards*

4. Wie halte ich mein Smart Home aktuell und sicher?

- **Passwort und Sicherheitseinstellungen**
- Virenschutzprogramme installieren
- Eigenes Gastnetzwerk erstellen
- **Nur bekannte Hersteller (Deutschland sicher)**
- Möglichst **ohne Internetverbindung** nutzen
- Datenschutz: Wo welche Daten gespeichert?
- **Verschlüsselte Kommunikation** zum Gerät

*Safety first
Sicherheitsupdates*

B | Internet

B1 Mobiles Internet

1. Was sind die Grundlagen des mobilen Internets

- Öffentliches WLAN, Mobiles Internet, **Mobilfunk**
- Mobilfunkantenne, Funkzelle, Radius, Funklöcher
- **3 Netzanbieter:** Telekom, Vodafone, O2
Telefonica (Alle Anbieter nutzen diese)

*Mobile Daten
Funkzelle,
Netzabdeckung
Provider*

2. Was muss ich beim Mobilfunkvertrag oder Prepaid-Kauf beachten?

- Netzanbieter, **Netzabdeckung**, Drosselung
- Tarif: **Kilobyte, Megabyte, Gigabyte**

*Tarif, Flatrate
Byte, KB, MB, GB*

3. Wie viel Datenvolumen (ver)brauche ich?

- Nur Textnachrichten: ca. 3 GB reicht
- Bilder und Videos: ca. 5 GB reicht
- Musik hören, Videotelefonat: min. 10GB

Datenvolumen

4. Wie gut ist mein Empfang?

- Netzabdeckung: Bestes Netz: LTE (4G), 5G
- 2G/Edge: schwach, kein Internet, 3G abgeschaltet
- Netzschwäche: Gebäude, Menschenmassen

*Funkstandard: 4G, 5G
Shared Medium=
Menschenansammlung*

5. Wie kann ich unterwegs Daten sparen?

- Qualität anpassen (Video, Musik)
- Downloads nutzen, Videoanrufe vermeiden
- Kein Bilder mit hoher Auflösung versenden

B2 Web & Web 2.0

1. Was ist das Web 2.0 und was kann man dort machen?

- **Web 2.0:** posten, liken, Blog; Web 1.0 statisch
- **User generated content, nutzergenerierter Inhalt**

*Posten, liken, Blog
User generated content*

2. Welche wichtigen Grundbegriffe des Internets gibt es und was verbirgt sich dahinter?

- URL der Website: Uniform Resource Locator
- http, https: Hypertext Transfer Protokol (Secure)
- www: World Wide Web (auch ohne www)
- Domain, Top-Level-Domain (.de, .org)
- Hyperlink (Textfarbe, anklickbar)

*www.sicher-im-netz.de
URL, http, https, www,
Domain, Top-Level-
Domain
Hyperlink*

3. Was ist beim Up- und Download zu beachten?

- **Urheberrecht**
- **Datenschutz, Schadsoftware**
- Dateigröße, MB, GB

*Server
Upload
Download*

4. Wie kann ich das Web 2.0 für mich nutzen?

- Inhalte **CMS** (Content-Management-Systeme)
- Video: YouTube, Twitch, Vimeo, DailyMotion
- Podcasts: Veröffentlichung auf Hosting-Sites

*CMS
Podcast
Hosting-Sites*

5. Was ist ein RSS-Feed?

- RSS (Really Simple Syndication), Feed = Füttern
- FeedReader Software
- Ständig die neuesten Inhalte sehen

*RSS-Feed
Browser-Plugin oder App*

B3 Browser

1. Welche Browser gibt es und für welchen sollte ich mich entscheiden? (Wiederholung Level 1)

- Vor- und Nachteile von Browsern: Schnelligkeit, Sicherheit, Vertrauenswürdigkeit
- **Google Chrome, Mozilla Firefox, Microsoft Edge (nicht Explorer), Safari (Apple)**
- Browser auf Mobilgeräten: Apps
- Funktionen Browser: Websites öffnen (**surfen**), Suchverlauf speichern

*Google Chrome
Mozilla Firefox
Microsoft Edge
Safari*

2. Was ist der Cache und was sollte ich damit tun? (Wiederholung Level 1)

- Speichern von Webadressen und Inhalten
- **Cache regelmäßig löschen:** Speicherplatz voll, Geschwindigkeit reduziert, Privatsphäre
- Cache löschen (*siehe Lernzentrale*)

Cache

3. Was ist anonymes Surfen und wie geht es? (Wiederholung Level 1)

- Datenspuren reduzieren, Privatsphäre schützen
- **Keine Cache Speicherung:** Keinen Suchverlauf speichern, keine Passwörter speichern
- **Inkognito oder anonymer Modus,** Browsereinstellungen

Inkognito oder anonymer Modus

4. Was kann meinen Browser sicherer machen?

- Regelmäßige Updates, **Add-Ons** (Erweiterungen), **Plugins** (eigenständige Software), Recherche!
- Zugriffsrechte, **SSL-Zertifikat** (Secure Socket Layer), **Sicherheitsstandard**

*Updates,
Add-Ons, Plugins
SSL-Zertifikat =
Schlosssymbol, https*

B4 Cookies

1. Warum ploppt ständig ein Fenster auf, wenn ich eine Website öffne? (Wiederholung Level 1)

- Cookies akzeptieren
- Einstellungen anpassen

Cookies

2. Was sind Cookies und welche Vor- und Nachteile haben sie? (Wiederholung Level 1)

- Video Cookies: Dauer 2:04 Minuten
- Cookies speichern **Surfverhalten** auf einer Website und passen so Werbung an
- **Tracking-Cookies**: Verfolgen Surfen im Netz
- Spracheinstellung und Onlineshopping

*Tracking-Cookies
Onlineshopping Login*

3. Welche Einstellungen sollte ich vornehmen?

- **Einstellungen anpassen**
- Browsereinstellungen: **Cookies** manuell oder automatisch **löschen**
- **Inkognito-Modus** nutzen
- Nutze **Anti-Tracking-Software**

Inkognito-Modus

4. Welche Anti-Tracking-Software gibt es für den Browser?

- **Anti-Tracking Plugins** (eigenständiges Zusatzprogramm) und **Add-Ons** (Erweiterung zu bestehendem Programm)
- Ghostery: kostenlos, für alle gängigen Browser
- uBlock Origin: für Chrome, Edge, Firefox, Safari verfügbar

*Plugins, Add-On
Ghostery
uBlock Origin*

B5 Suchmaschine

1. Wie funktioniert eine Suchmaschine?

- Algorithmus: Auswahl Suchergebnisse, **SERP**
- Nicht alle Ergebnisse passen zur Suche
- Finanzierung durch Werbung (advertisement)

*Algorithmus
SERP Search Engine
Result Page*

2. Warum gibt es mehrere Suchmaschinen und für welche entscheide ich mich? (Wiederholung Level 1)

- Unterschiede in Datenschutz, soziales Engagement oder genaue Suchergebnisse
- Unterschiede Suchmaschinen: **Google, Bing (Microsoft), DuckDuckGo, Ecosia (sozial)**
- Adresszeile Browser = Suchmaschine in Einstellungen festlegen

*Google
Bing
DuckDuckGo
Ecosia*

3. Wie kann ich meine Suche verfeinern?

- **Filter-Suchergebnisse:** Format wie Video, Bilder, Karte, ...
- Einstellungen: Sprachauswahl, Zeitraum
- Anstößige Ergebnisse ausblenden

*Filter
Kebab Menü (Punkte)
Burger Menü (Striche)*

4. Wie kann ich Suchergebnisse einschätzen? (Wiederholung Level 1)

- Link prüfen
- Suchbegriffe in der Website-Beschreibung
- **Auf Anzeigen (Ad) achten, ganz oben**

Link

5. Was sind Operatoren?

- **Genauere Ergebnisse:** AND, OR, **Minus (ohne Leerzeichen)**, Anführungszeichen, **site**

*Suchoperatoren: And,
OR= | Pipe-Operator, site*

C | Kommunikation

C1 E-Mail

1. Was gibt es grundsätzlich über E-Mails zu wissen?

- E-Mail Kommunikationsmittel #1

2. Was muss ich über E-Mail-Provider wissen?

- Kosten, Datenschutz und Datensicherheit

E-Mail-Provider, Beispiele

3. Wie steht es um den Datenschutz bei E-Mail-Providern?

- **DSGVO**, Ende-zu-Ende-Verschlüsselung
- Server-Standort, Datensparsamkeit

DSGVO, Ende-zu-Ende-Verschlüsselung

4. Wie kann ich meine E-Mails schützen?

- Sicheres Passwort, Virenschutz / Spamfilter
- Verschlüsselung, Absender / Betreff beachten

Virenschutz, Spamfilter

5. Was sind Spam-Mails und welche Arten von Spam-Mails gibt es? (Wiederholung Level 1)

- Video Spam: Dauer 3:16 Minuten
- **Spam** (send phenomenal amounts of mail), **Scam** (Betrug), Hoaxes (Scherz), Kettenbriefe, Phishing

Spam, Scam, Hoax, Phishing

6. Wie kann ich mich vor Spam-Mails schützen? (Wiederholung Level 1)

- **Datenanhang nicht öffnen, Datensparsamkeit**, Vorsicht bei **Zahlungsaufforderung**

Datensparsamkeit

C2 Messenger & SMS

1. Das 1x1 der Messenger

- **SMS** (short message service), **160 Zeichen, Zwei-Faktor-Authentisierung**
- **MMS** (multimedia message service), mobile Daten
- **Messenger:** App, WhatsApp, Signal, Telegram, Telefonat, Videoanruf, mobile Daten oder WLAN

*SMS
MMS
Messenger: App
installiert, beide
brauchen App, online*

2. Wie schützen die Messenger meine Daten?

- **DSGVO, AGB, Datenschutz**
- **WhatsApp:** Ende-zu-Ende-Verschlüsselung, Geräte und Verbindungsdaten, Facebook Kommunikation offen
- **Signal:** Ende-zu-Ende-Verschlüsselung, kein Daten sammeln
- **Threema:** Downloadgebühr, Ende-zu-Ende-Verschlüsselung, anonym (**ohne Telefonnummer**), europäischer Server
- **Telegram:** Ende-zu-Ende-Verschlüsselung deaktiviert, geheimer Chat, Daten werden gespeichert
- Auf Updates und Backup achten

*DSGVO, AGB,
Datenschutz
WhatsApp, Signal,
Threema, Telegram
Ende-zu-Ende-
Verschlüsselung,
anonym
Update, Backup*

3. Welche erweiterten Messenger-Funktionen gibt es?

- WhatsApp-Broadcast: ähnlich Gruppe, Mitglieder müssen Nummer speichern, Antwort an Sender
- Telegram-Kanal: öffentlich oder privat, **privat nur mit Einladung**
- Threema und Signal haben das nicht

*WhatsApp-Broadcast
Telegram-Kanal*

C3 Videokonferenzen

1. Was sind Videokonferenzen und welche Anbieter gibt es?

(Wiederholung Level 1)

- Videoanruf (auf WLAN Verbindung achten)
- **Kamera, Mikrofon, Internetzugang** nötig
- Anbieter: **Skype, Zoom**, Messenger (WhatsApp, Signal, Telegram)
- **Skypen** = Videoanruf

*Skype - skypen
Zoom
Messenger*

2. Wie wähle ich einen Anbieter aus? (Wiederholung Level 1)

- Vor- und Nachteile: Skype, Zoom, Messenger
- **Funktionen: Chatten, Bildschirm teilen, Daten senden, Aufzeichnung, Tastenkürzel**
- **Datenschutz, AGB, Nutzungsbedingungen**
- **Kostenlose Version, nur Anmeldung und kein Programm nötig**

3. Wie gestalte ich einen sicheren Videoanruf? (Wiederholung Level 1)

- Datenschutz, Ende-zu-Ende-Verschlüsselung
- keine Weitergabe an Drittanbieter
- Sicheres Passwort, Zugriffsrechte, Updates
- **Einladung: E-Mail, Messenger**

Passwort, Ende-zu-Ende-Verschlüsselung,

4. Wie teile ich Inhalte während des Videoanrufs?

- Ganzen **Bildschirm** teilen oder einzelnes **Fenster**
- Chat-Fenster nutzen, Büroklammer / Plus

Teilen, freigeben, Chat

5. Wie bereite ich eine Videokonferenz gut vor? (Wiederholung Level 1)

- Kamera, Mikrofon an, stabile Internetverbindung
- Ruhiger Ort, mit Programm vertraut machen

C4 Soziale Netzwerke

1. Welche sozialen Netzwerke gibt es? (Siehe Lernzentrale)

- Austausch: **posten, adden, liken**
- **Facebook:** auch Unternehmen, Verbände, Institutionen, Diskussionsgruppen, Meta
- **Instagram:** auch Restaurants, Bands usw., Follower, keine Links, Meta
- **Snapchat:** nur Fotos/Videos, privat oder Follower, nach 24 Stunden autom. gelöscht
- **Twitter:** Tweets max. 280 Zeichen, Fotos/Videos/Links, politisch, aktuell, Follower
- **TikTok:** nur Kurzvideos, Musik, Follower
- **YouTube:** Videos, Follower, Google
- **Twitch:** Livestream-Plattform, auf Kommentare live reagieren, Gamer, Amazon
- Vor allem Europa, Nordamerika
- China: SinaWeibo, Q-Zone, TencentQQ, WeChat; russisch VK

*Soziale Netzwerke:
Facebook, Instagram,
Snapchat, Twitter,
TikTok, YouTube
Posten, Adden, Liken
Accounts, Follower,
Gamer
Livestream, Plattform*

2. Wie kann ich ein soziales Netzwerk nutzen?

- **Registrierung: E-Mail, Passwort, Profilname**
- **Klarname** (Facebook)
- **Profil: Datensparsamkeit**
- **Follower:** folgen und gefolgt werden
- Themen sortieren mit **# Hashtag**

*Registrierung
Hashtag*

3. Welche Sicherheitsaspekte muss ich beachten?

- **Keine Anfragen von Unbekannten**
- **Datensparsamkeit**
- Veröffentlichung privater Inhalte überdenken
- **Persönlichkeitsrechte (Kinder), Urheberrechte**
- Keine Fotos/Videos von Kinder, **Jugendschutz**
- Auf **Social Login** verzichten, **Zugriffsrechte**

*Datensparsamkeit
Urheberrechte,
Verwertungsrecht,
Persönlichkeitsrechte
Finanzieller Vorteil
Social Login*

C5 Belästigungen & Fake News

1. Welche Belästigungen gibt es? (Wiederholung Level 1)

- Video Belästigungen: Dauer 3:10 Minuten
- Hate Speech, Cyber-Mobbing, Grooming, Stalking

*Hate Speech
Cyber = Internet*

2. Wie kann ich mich vor Belästigungen und Beleidigungen schützen?

- **Keine Provokation, Beweise, Beitrag melden**
- **Datensparsamkeit und Aufklärung**
- Sicherheitssoftware / Firewall aktuell halten

*Cyber-Mobbing-Grooming
-Stalking,
Blockieren
Firewall*

3. Welche Angebote gibt es für Betroffene? (Wiederholung Level 1)

- Hate Aid, Weißer Ring, Vertrauensperson

Hate Aid, Weißer Ring

4. Was sind Fake News und warum gibt es sie? (Wiederholung Level 1)

- **Fake News** (gefälschte Nachrichten)
- Emotional, reißerische Sprache

*Fake News
Desinformation*

5. Wie erkenne ich Fake News? (Wiederholung Level 1)

- **Autor:in**, Impressum, Überschrift prüfen
- Verifizierter Account mit Häkchen, Follower
- Faktenfinder (Tagesschau, Mimikama, Hoaxmap)

*Quellen prüfen
Followerzahl
Verifizierte Accounts*

6. Was mache ich, wenn ich Fake News erkannt habe? (Wiederholung Level 1)

- Beitrag, Bild, News: melden
- Person: einschränken, blockieren, melden

Cybermobbing: Polizei

D | Datenwelt

D1 Datenschutz

1. Welche Datenschutzrechte habe ich im Netz?

- Europ. Datenschutzgrundverordnung **DSGVO**
- Recht auf Selbstbestimmung und Sicherheit
- Datensicherheit: nur Daten, die nötig sind
- Sicherheitsmaßnahmen, Schutz vor Hacker
- Recht auf Auskunft, Recht auf Beschwerde

*DSGVO, informationelle
Selbstbestimmung
Datensicherheit:
Kontakt-, Login-,
Kommunikations-, Daten*

2. Respektieren Online-Anbieter meine Daten?

- **Datenschutzerklärung** übersichtlich, verständlich
- **Server-Standort** Europa, Sicherheitsmaßnahmen
- **Datenschutzbeauftragte, -behörde**

*Datenschutzerklärung
Datenschutzbeauftragte*

3. Welche persönlichen Daten sind auf meinem Smartphone gespeichert?

- Standort-, Bewegungs-, Kontaktdaten
- Kommunikations- und Gesundheitsdaten
- Analyse- und Statistikdaten, Pers. Daten

*Voreinstellungen
anpassen*

4. Was mache ich, wenn gegen den Datenschutz verstoßen wurde?

- App-Berechtigungen überprüfen
- Logindaten sichern, unbenutzte App löschen

*App-Berechtigungen
Log-in-Daten*

5. Wem kann ich Datenschutzverstöße melden?

- Datenschutzbeauftragte:n, oder Abmahnung
- Kontakt Datenschutzbehörde Bundesland

*Schutz personen-
bezogener Daten*

D2 Datensparsamkeit

1. Was bedeutet Datensparsamkeit? (Wiederholung Level 1)

- Verantwortungsbewusster Umgang mit persönlichen Daten
- **So wenig Daten wie möglich** bei Onlineanbietern speichern



2. Was sind Tipps für mehr Datensparsamkeit? (Wiederholung Level 1)

- Nur das Nötigste angeben, Pflichtfelder *
- Diskret sein, keine persönlichen Fotos
- Anonym bleiben (**Pseudonyme**, Spitzname)
- Verschiedene E-Mail-Adressen nutzen
- Alle Anbieter dürfen nur die Daten abfragen und speichern, die für die Nutzung notwendig sind
- Datenzugriff von Apps in Einstellungen kontrollieren



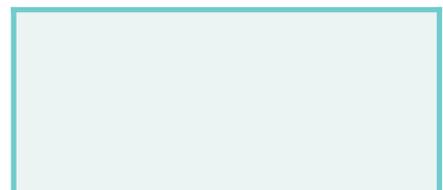
3. Wie kann ich meine Daten endgültig löschen?

- Konto kündigen, Hilfe durch justdeleteme.me
- **Anbieter** direkt kontaktieren, Kundenservice
- Kontakt **Datenschutzbeauftragte(r)** des Unternehmens oder **Datenschutzbehörde** Bundeslandes (eventuell Gebühren)



4. Wie erkenne ich, ob ein Online-Unternehmen Datensparsamkeit ernst nimmt? (Wiederholung Level 2)

- **Zweck** der Datenerhebung
- **Transparenz, Datenweitergabe**, wann werden Daten gelöscht
- Auflistung Nutzer-Rechte, **Datenspeicherung**



D3 Logins und Passwörter

1. Was ist ein starkes Passwort? (Wiederholung Level 1)

- Einmalig, lang, komplex, kreativ
- Klein- /Großbuchstaben, Zahlen, Sonderzeichen

iKGa#951_W

2. Wie bilde und merke ich mir ein starkes Passwort?

(Wiederholung Level 1)

- Merksatzmethode (erster oder letzter Buchstabe) + App Verlängerung
- „**Passwort vergessen**“ nutzen

Merksatzmethode

3. Was können Passwortmanager?

- **Passwörter nicht im Browser speichern**
- App- oder Plug-In-Passwortmanager, **Datenschutzerklärung lesen**
- Vorteil: nur 1 Masterpasswort (kein Zettel)
- Nachteil: Cloud, **Serverstandort** (Europa)

*Masterpasswort merken
Passwortmanager:
Enpass, LastPass,
NordPass*

4. Was ist die Zwei-Faktor-Authentisierung? (Wiederholung Level 1)

- **Zwei Komponenten** zum Login
- Per: **SMS, Anruf, Authenticator App, Gesichtserkennung, Fingerabdrucksensor**

*Zwei-Faktor-Authentisierung
Authenticator App*

5. Was sind U2F-Sticks und wie funktionieren sie?

- Universal Second Factor: Passwort + USB-Stick
- Im Handel alle Zertifikat Standard „FIDO“
- Account einrichten: Datenschutz/Sicherheit/Login
- Tipps: Ersatz-Stick einrichten, Smartphone-Sticks über NFC oder Bluetooth

*U2F-Sticks
2 Faktoren Login:
Passwort + USB-Stick*

D4 Backups

1. Was sind Backups?

- **Sicherheitskopie** der Daten, Programme
- Betriebssystem und Einstellungen
- Speicherort: Externer Speicher, Cloud
- Gründe für Datenverlust: USB-Stick bricht, Wasser-, Feuerschäden, versehentliches Löschen, Hackerangriff, Verlust

*Backup:
Externer Speicher, Cloud*

2. Wie erstelle ich ein Backup?

- Programmsynchronisierung: GoodSync, PurSync
- **Komplettes Backup**: BackItUp, Nova backUp PC, Cyber Protect Home Office
- **Sicherungsfunktion** Windows (Einstellungen)
- **TimeMachine** MacOS
- Backup-Medium nicht konstant verbinden
- **inkrementelle Datensicherung**

*Synchronisierung =
Abgleich
Windows:
Sicherungsfunktion
MacOS: TimeMachine
inkrementelle
Datensicherung*

3. Sollte ich meine Dateien verschlüsseln?

- Schutz bei Hacking oder Diebstahl
- Kinder-, Jugendschutz

Schlüssel = Passwort

4. Wie verschlüssele ich meine Dateien?

- Verschlüsselungssoftware: SteganoSafe, Gpg4Win, ArchiCrypt, VeraCrypt, TruPax
- Verschlüsselung Festplatte: Passwort
- Verschlüsselung Gehäuse mit Schloss
- Verschlüsselung Smartphone/Laptop: Gesichtserkennung, Fingerabdruck

*Software
Festplatte
Gehäuse*

D5 Clouds

1. Was ist eine Cloud? (Wiederholung Level 1)

- Video Cloud: Dauer 2:21 Minuten
- Cloud Backup auf Server über Internetverbindung
- Computer / Server in Rechenzentren In-/Ausland

*Cloud, Server
Synchronisierung*

2. Welchen Cloud-Anbieter sollte ich nutzen?

- Viele Anbieter: Dropbox und OneDrive (Microsoft), Hidrive (Strato), MagentaCloud (Telekom), OwnCloud
- Preise
- **Datenschutzerklärung**, Datensparsamkeit
- Sicherheitsmaßnahmen, Verschlüsselung
- **Zwei-Faktor-Authentisierung**
- Verschlüsselungstechnologie: **Tresor**
- **In Cloud keine persönl. Daten hochladen**

3. Wie funktioniert die Cloud auf Smartphones und Tablets?

(Wiederholung Level 1)

- App installieren (iCloud, Google Drive), einloggen,
- Zugriff erlauben und Daten hochladen

*Apple: iCloud
Android: Google Drive*

4. Welche Vorteile hat eine Cloud noch?

- Kein Versenden von Daten nötig
- **Auf Daten gemeinsam zugreifen und bearbeiten**
- Einsparung Hardware
- Bedenke: Wenn die Daten in der Cloud sind, sind sie nicht mehr nur auf dem eigenen Computer, sondern auf dem Computer/Server von jemand anderem.

E | Gefahrenschutz

E1 Updates

1. Was gibt es grundsätzlich über Updates zu wissen?

- Softwareaktualisierung: **Sicherheitslücke schließen, System stabil und sicher halten**

*Apps, Programme,
Betriebssystem*

2. Sollte ich Updates automatisch oder manuell einstellen?

(Siehe Lernzentrale)

- iOS / Androd, Windows - MacOS

*Ja, Einstellungen
Changelog*

3. Muss ich jedes Update sofort installieren?

- **Sofort:** Sicherheitsupdates, Bug-Fixes, Patches
- Funktions-Updates, Major-Updates umfassend

*Bug-Fixes, Patches
Major-Updates > Backup*

4. Woran erkenne ich, mit welcher Art von Update ich es zu tun habe?

- 4(**Major**).3(**Minor**).56(**Patch**)-384(Build-Nummer)
- je weiter rechts, desto kleiner Änderung, bei Major oder Minor folgen Nullen

*Versionsnummer
4.3.56-384*

5. Wie finde ich heraus, welche Neuerungen ein Update mit sich bringt? (Siehe Lernzentrale)

- iOS: App Store, Android: Play Store
- Windows: Einstellungen, MacOS: App Store
- Bei Apps aus anderen Quellen online suchen

*App Store
Website
Einstellungen der App*

E2 Schadsoftware

1. Was ist Schadsoftware? (Wiederholung Level 1)

- Video Schadsoftware: Dauer 2:48 Minuten
- Datendiebstahl, Zerstörung Programme
- **Download, Öffnung Anhang, fremder USB-Stick, fremder Link, Werbebanner anklicken**

*Trojaner, Wurm
Malware
Adware (Werbung)*

2. Wie schütze ich mich vor Schadsoftware? (Wiederholung Level 1)

- Keine verdächtigen Links oder Anhänge öffnen
- Nur sichere Software installieren
- **Keine Werbebanner oder dubiose Angebote öffnen (X, Alt F4, nur Abbrechen hilft nicht)**
- Programme aktuell halten
- Firewall und Bordmittel nutzen

*Sicherheitssoftware:
Firewall, Bordmittel
X tippen, Alt F4*

3. Was muss ich tun, wenn doch etwas passiert ist?

- Virenalarm: Löschen oder Quarantäne-Lösung
- In abgesichertem/sicherem Modus Virensan
- **Vom Netz trennen**, anderes Gerät für Hilfesuche
- Formatieren und neu aufsetzen
- Hilfe beim Spezialisten suchen

*Quarantäne-Lösung
abgesicherter/sicherer
Modus und Virensan*

4. Was sind interne Sicherheitseinstellungen?

- Windows: Sicherheitscenter, Bordmittel: Firewall, Viren- und Bedrohungsschutz
- Mac: Systemeinstellung, Sicherheit

E3 Social Engineering

1. Was ist Social Engineering? (Wiederholung Level 1)

- Oberbegriff Betrug und Täuschung
- Beispiele: Einzeltrick, Anruf Bankmitarbeiter, E-Mail Anhang

*Social Engineering =
Soziale Manipulation*

2. Was ist Phishing? (Wiederholung Level 1)

- Passwort + Fishing
- **Vorsicht: Login-Daten werden abgefragt, Banking Login, Zugangsdaten**
- Über Telefonanruf: **Vishing**

*Phishing
Vishing*

3. Wie erkenne ich Phishing? (Wiederholung Level 1)

- Achte auf: **E-Mail Adresse, Betreff, Anhang, Erscheinungsbild, Ansprache, Links, Fehler**
- Passe auf: Verlockendes Angebot, kein Konto, keine Bestellung, Frage nach Zugangsdaten

4. Wie gehe ich mit Phishing um?

- Spamfilter, Spam-E-Mails löschen
- Phishing-E-Mails löschen
- **E-Mail-Format von HTML auf nur Text ändern**
- Internetrecherche
- Person anrufen und nachfragen

*Spamfilter
E-Mail-Format :Text
ändern*

5. Was, wenn doch etwas passiert ist? (Wiederholung Level 1)

- Andere informieren
- **Passwort ändern**, Bank Login 3x falsch
- **Anbieter informieren**, Anzeige erstatten

E4 Doxxing

1. Was ist Doxxing? (Wiederholung Level 1)

- **Negativ:** Persönliche, nicht veröffentlichte Daten und Dokumente werden im Internet veröffentlicht
- Folgen: E-Mail-Flut, Angriff Privatwohnung
- **Positiv:** Veröffentlichung von Missständen und Skandalen

Doxxing

2. Wie schütze ich mich vor Doxxing? (Wiederholung Level 1)

- **Datensparsamkeit**
- Social Media Einstellungen
- Sicherheitsvorkehrungen: **Zwei-Faktor-Authentisierung, Updates**
- Datenbroker:innen, Datenschnüffler:innen: gegen Bezahlung gezielt nach Daten suchen und zusammentragen

Datenbroker:innen

3. Was kann ich tun, wenn ich gedoxxed wurde? (Wiederholung Level 1)

- **Nur personenbezogenen Daten, die nicht frei zugänglich sind**
- Doxxing ist strafbar
- Andere informieren
- Beitrag melden
- Beweise sammeln
- Anzeige erstatten

E5 Identitätsdiebstahl

1. Was ist Identitätsdiebstahl? (Wiederholung Level 1)

- Jemand gibt sich online für jemand anderen aus
- Meistens **Geldbetrug** oder Online-Bestellungen, kostenpflichtige Abos
- Identity Leak Checker

*Identitätsdiebstahl
Identity Leak Checker
Datenlecks*

2. Wie vermeide ich Identitätsdiebstahl? (Wiederholung Level 1)

- **Datensparsamkeit**
- **Privatsphäre-Einstellungen**
- **Auf Phishing-Versuche achten**

Datensparsamkeit

3. Was muss ich tun, wenn doch etwas passiert ist?

(Wiederholung Level 1)

- Konto und Karten sperren (**Bank** Login 3x falsch eingeben)
- Anzeige **Polizei**
- **Passwörter ändern**
- Mahnung, Vollstreckungsbescheid oder Inkasso- Briefe sofort beantworten (Widerspruchsfrist)
- **Schufa** Meldung

E6 Scam

1. Was ist Scam? (Wiederholung Level 1)

- Video Scam: Dauer 2:29 Minuten
- Betrug: Vorschussbetrug, **Romance Scam** (vorgaukeln von **Gefühlen, Vertrauen** aufbauen)

Scam
Romance Scam

2. Wie erkenne ich Scamming? (Wiederholung Level 1)

- **Geldforderung**
- **Bauchgefühl**, „zu gut, um wahr zu sein“
- Anzeichen einer Fälschung, Umwege von Überweisung, Fehler
- Kommunikation über **andere Plattformen**
- **Persönliches Treffen abgelehnt**
- **Suche im Netz**

Geldforderung

3. Was muss ich tun, wenn ich Opfer von Scamming wurde?

(Wiederholung Level 1)

- Nicht auf Forderungen eingehen und kein Geld überweisen
- Beweise sichern, Rückbuchung
- Anzeige bei Polizei
- Kontakt abbrechen

F | Technologiealltag

F1 Fitnessstracker & eHealth

1. Was steckt alles in eHealth? (Wiederholung Level 1)

- Video: Dauer 2:32 Minuten
- Wearables (**Kalorien, Schritte, Puls**), Krankenkassen-Apps

*eHealth
Wearables*

2. Welche Sicherheitsaspekte gibt es zu beachten?

(Wiederholung Level 1)

- **Datensparsamkeit**, wo werden Daten geteilt?
- **Updates und Virenschutz**
- **Einwilligungen** überdenken, Server-Standort

3. Wie sieht eHealth im Gesundheitswesen aus? (Wiederholung Level 1)

- Elektronische Patientenakte (ePA)
- Elektronische Rezept, **E-Rezept**
- **Digitale Gesundheitsanwendung** DiGAs
- Medizintechnik, **Arztbesuch Videocall**
- Telematikinfrastruktur zur Sicherheit
- Termine: Doctolib, Doctena
- Krankenkassen-App: Boni, Impfnachweis, Übungen, digitale Sprechstunde

*ePA
E-Rezept
DiGAs
Telematikinfrastruktur*

4. Was ist digital detox? (Wiederholung Level 1)

- Digitales Fasten
- Zeit am Bildschirm reduzieren, Wecker stellen, Flugmodus nutzen
- Benachrichtigungen ausschalten
- Bildschirmzeit beobachten, Zeiten oder Orte festlegen

digital detox

F2 Digitaler Personalausweis

1. Was genau ist der digitale Personalausweis? (Wiederholung Level 1)

- Video Personalausweis: Dauer 2:34 Minuten
- eID: analoger Personalausweis (Symbol), Kartenlesegerät oder **AusweisApp2**, **6stellige Pin**
- Onlinezugangsgesetz: Ämter, Post, Rentenversicherung

*E-Government
eID, Smart-e-ID
Onlinezugangsgesetz*

2. Welche Möglichkeiten bietet er? (Wiederholung Level 1)

- BAföG
- **Rentenkonto** bei Deutscher Rentenversicherung
- **Punktestand beim Kraftfahrt-Bundesamt**
- Bürgerämter Dienste auf Anfrage
- Service Deutsche Post und Deutsche Bahn

Postident-Verfahren

3. Was muss ich beachten? (Wiederholung Level 1)

- Verbindung nach Nutzung trennen
- **Updates** und Virenschutz
- **Verlust** sofort melden (**Polizei, Bürgeramt**)
- Nutzung ist sicher

F3 Online-Banking

1. Wie bleibe ich beim Online-Banking geschützt?

- **Sichere Passwörter**
- **Phishing:** Banken fragen nie per E-Mail ab
- Kontoauszüge prüfen
- Sichere Website (**https, Schlosssymbol**)
- Datensparsamkeit
- Auf Website Kleinigkeiten achten
- **Verschlüsseltes WLAN, WPA2,WPA3**
- **Zahlungslimit** bei Bank

*Sichere Passwörter
Phishing
NFC Hülle*

2. Und wenn doch etwas passiert ist? (Wiederholung Level 1)

- Bankverbindung sperren, **3 Mal hintereinander falsches Passwort eingeben, Anzeige**
- **Sperr-Notruf** anrufen, **Bank benachrichtigen**
- Belege sammeln, auf Schadsoftware achten

3. Welche Möglichkeiten des mobilen Zahlens gibt es?

- **Vorteile:** schnell, mit allen Geräten möglich
- **Mobiles Zahlen: NFC (Nahfeldkommunikation)**
- Giro- oder Kreditkarte, Smartphone, Smart Watch mit NFC-Chip
- Apple: ApplePay, Android: PayPal, Bank App

*NFC
Apple: ApplePay
Android: PayPal,
Bank App*

4. Wie kann ich sicher mobil zahlen?

- **Updates, Zugriffsschutz, Ausgabenlimit**
- Sperren bei Verlust
- Sicherung: PIN, Fingerabdruck, Verwahrung
- mehrere Karten übereinander
- kein öffentliches WLAN
- Android: NFC deaktivieren

*Zwei-Faktor-Authentisierung
TAN
App-Freischtaltung*

F4 Online-Shopping

1. Wie kann ich bezahlen? (Wiederholung Level 1)

- **PayPal:** Eigenes Konto eröffnen
- **Klarna:** Rechnung, Lastschrift, Vorkasse, Sofortüberweisung, Ratenkauf
- **Paydirekt:** Überweisung Bankkonto mit TAN
- **Kreditkarte**

*PayPal, Klarna
https
TAN*

2. Was sind die Vor- und Nachteile von Online-Bezahldiensten?

(Wiederholung Level 1)

- Vorteil: Schnell, kostenlos, bequem
- Nachteil: weniger Kontrolle, Daten an Drittanbieter
- Achte auf Zwei-Faktor-Authentisierung

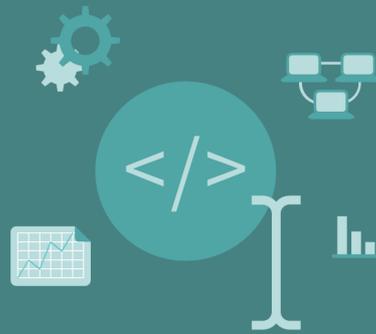
3. Was sind Fake Shops und wie schütze ich mich vor ihnen?

- Professionelle Website, Impressum
- Transparente Preise, **Zahlungsmethode**
- **Impressum:** Rechtsform, Kontaktdaten
- **Gütesiegel:** Trusted Shops, TÜV Süd Safer Shopping, Internet Privacy Standards, EHI
- **Bewertungen,** Kommentare
- Reihenfolge der Produkte (Filter)
- Abo-Pflicht
- SOS-Karte: Bundesamt für Sicherheit in der Informationstechnik

*TÜV Süd, Trusted Shop,
Internet Privacy
Standards, EHI
SOS-Karte*

4. Was muss ich im Betrugsfall tun?

- **Bank benachrichtigen**
- Belege aufbewahren, **Screenshots**
- Anzeige bei **Polizei**



Level 3

A | Geräte

A1 Router & (W)LAN

1. Was sind die Grundfunktionen des Routers? (Siehe Lernzentrale)

- Router: Schnittstelle Netz und Gerät
- WLAN, Frequenzbänder: **2,4 GHz, 5 GHz**
- Datenübertragung: **Mbit/s** (Megabit pro Sek)
- Anpassung: **IP Adresse in Browser**

*2,4 GHz, 5GHz, Mbit/s
Browser: IP Adresse:
192.168.0.1, fritz.box,
easy.box, speedport.id*

2. Was sind die Einstellungen, die ich vornehmen sollte?

- Sicherheitsmaßnahmen: **Verschlüsselung WPA** (Wi-Fi protected access): **WP2** oder **WP3** (Wörterbuch Attacken), Hybridmodus WP2/WP3
- **Netzwerkname** und **Passwort** ändern
- WP2: Schwachstelle WPS (Wi-Fi protected Setup), neue Geräte Knopfdruckverbindung
- WP3: Wi-Fi-Easy-Connect, QR-Code Verbindung, abhängig Gerätetreiber, Betriebssystem

*Verschlüsselung:
WP2, WPS
WP3, Wi-Fi-Easy-Connect
Hybrid WP2/WP3
WP3: minimum
Windows10,
macOS 10.15, Android
10, iOS 13
Heimnetzwerk*

3. Wie richte ich am Smartphone oder Tablet einen Hotspot ein?

- **Hotspot:** WLAN, mobile Daten Smartphone
- **Android-Einstellungen, Hotspot-Tethering** (USB/Bluetooth), WP2
- **iOS:** Einstellungen, Persönlicher Hotspot, alternativ Kabel, sicheres Passwort

*WLAN-Hotspot
Bluetooth-Tethering
WP2*

4. Wie richte ich ein Heimnetzwerk ein? (Siehe Lernzentrale)

- **Windows**
- **Mac**
- **Schneller Datenaustausch ohne USB-Stick oder externe Festplatte**

*Router = Schaltzentrale:
WLAN / Kabel
Drucker, VNC extra
Software*

A2 PC & Laptop, Smartphone & Tablet

1. Wie war das mit den Betriebssystemen?

- **Schnittstelle Betriebssystem**
- PC - Laptop: **Windows**
- MacBook - Apple Computer: **MacOS**
- Alternative: **Linux (open source)**, Ubuntu
- Smartphone - Tablet: **Android**
- iPhone - iPad: **iOS**
- Andere wenig genutzt

*Betriebssystem
Windows
MacOS (Operating Sytem)
Linux (open source),
Android
iOS*

2. Was gibt es über Linux zu wissen?

- Open-Source-Prinzip: Quellcode von allen einsehbar und veränderbar
- in **Finnland** von **Linus Torvalds** entwickelt
- **Android** beruht auf Linux
- Linux-Variante: Ubuntu
- Vorteile: sicherer, anpassbar, wenig Malware-Attacken
- Nachteile: mehr Einarbeitung, nicht alle Programme verfügbar, vor allem Games/ Unterhaltung, manche Linux Befehle nur in **Terminal** umsetzbar

*Open-Source
Terminal
Linus Torvalds
Linux-Distribution:
Ubuntu*

A3 Apps & Programme

1. Was gibt es grundsätzlich über Apps und Programme zu wissen?

- Erste Anlaufstelle: **Anbieter-Store**
- Alternative Programme: Vertrauenswürdigkeit, oft ohne Sicherheits-Updates
- **Bewertungen** lesen

*Microsoft Store
Play Store - App Store
Vertrauenswürdig*

2. Welche App-Berechtigungen sollte ich erteilen?

(Wiederholung Level 2)

- Kamera, Mikrophon, Standort, Adressbuch
- **Zugriffsrechte hinterfragen**

Berechtigungen: „Nur bei Nutzung der App“

3. Welche alternativen Apps und Programme gibt es?

(Wiederholung Level 2)

- **Open-Source-Software**
- Vorteile: **jeder macht mit**, Sicherheitslücken entdecken, Weiterentwicklung, Peer-Review
- Nachteile: ohne Support, wenig intuitiv

*Open-Source-Software
Peer-Review,
Libre Office, Gimp,
Mozilla Firefox*

4. Was ist Portable Software?

- Muss nicht installiert werden (USB-Stick)
- Vorteile: von **jedem Gerät** einsetzbar, klein, ohne Spuren, **ohne Administrator-Rechte**
- Nachteile: **Funktionen fehlen**, Viren

Portable Software

5. Was sind Custom ROMs und sollte ich sie nutzen?

- Betriebssystem tauschen, neu aufspielen
- Basis Android Open Source, allg. verfügbar
- Beliebte Beispiele: Lineage OS, Paranoid Android
- Kein Installationspaket, Kommandozentrale -Befehle nötig, nur Community-Support

*Custom ROM =
weiterentwickelte
Android-Version
Gerätegarantie erlischt*

A4 Smart Home

1. Was ist ein Smart Home? (Wiederholung Level 1)

- Video Smart Home: Länge 2:41
- Datenübertragung: **WLAN, Bluetooth, Funk**
- **Sprachassistenten**: Alexa, Siri, Google Pod
- Hub, Steuerungszentrale, Basisstation

*WLAN, Bluetooth, Funk
Steuerungszentrale,
Basisstation, Hub
Alexa, Siri, Google Pod*

2. Was macht ein Smart Home aus?

- Nutzen **WLAN** oder **Bluetooth**
- Andere **Funkstandards**: **ZigBee, Z-Wave**
- Datenschutz (Vorteil: lokale Steuerung)
- **Hub** in Cloud (Sprachassistent-Lautsprecher)
- App-Steuerung: Router ist Schnittstelle

*Internet of Things (IoT)
WLAN, Bluetooth, ZigBee,
Z-Wave
Hub
App-Steuerung*

3. Was sind die Vor- und Nachteile eines Smart Home?

- Vorteile: machen das Leben leichter und sicherer (Wasserstandsmelder, smarte Steckdose, Heizungs-Thermostat), **reibungslose Kommunikation** (gleicher Hersteller)
- Nachteile: Austausch sensibler Daten über Server, **Sicherheitslücken, Funkstandards** („MATTER“)

*WLAN, Bluetooth
Hub =
Steuerungszentrale,
Basisstation
Projekt „Matter“
einheitlicher
Funkstandard*

4. Wie halte ich mein Smart Home aktuell und sicher?

(Wiederholung Level 2)

- **Passwort und Sicherheitseinstellungen**
- Virenschutzprogramme installieren
- Eigenes Gastnetzwerk erstellen
- **Nur bekannte Hersteller (Deutschland sicher)**
- Möglichst **ohne Internetverbindung** nutzen
- Datenschutz: Welche Daten - wo gespeichert?
- **Verschlüsselte Kommunikation** zum Gerät

*Safety first
Sicherheitsupdates*

B | Internet

B1 Mobiles Internet

1. Was sind die Grundlagen des mobilen Internets

(Wiederholung Level 2)

- Kein WLAN, mobiles Internet, **Mobilfunk**
- Mobilfunkantenne, Funkzelle, Radius, Funklöcher

*Mobile Daten
Funkzelle,
Netzabdeckung*

2. Welche Mobilfunkanbieter gibt es?

- Telekom, Vodafone O2, Telefonica
- Vertrag oder Prepaid-Karte, Stadt oder Land

*Provider
Prepaid-Karte*

3. Wie gut ist der Empfang und was hat 5G damit zu tun?

- 2G (Edge), 3G (abgesch.), 4G-LTE (1Gbit/sek)
- **5G**: (bis 20 Gbit/sek), **niedrige Latenz**, IoT, autonomes Fahren, Augmented Reality, Kommunikationsstandart Industrieanlagen, **Network Slices** (Kapazitätenreservierung für z.B. Ampelsteuerung), Beam-Forming

LTE 1Gbit/sek, 5G bis 20 Gbit/sek, Augmented Reality, IoT, Network Slices (Silvester Effekt, shared medium), Beam-Forming (gezieltes Signal)

4. Wie viel Datenvolumen (ver)brauche ich? (Wiederholung Level 2)

- Nur Textnachrichten: ca. 3GB reicht
- Bilder und Videos: ca. 5GB reicht
- Musik hören, Videotelefonat: mind. 10GB

Datenvolumen

5. Wie kann ich unterwegs Daten sparen?

- Zu Hause WLAN nutzen, Einstellung: Verbrauchswarnung
- Qualität anpassen (Video, Musik), offline
- Downloads nutzen, Videoanrufe vermeiden

WLAN nutzen

B2 Web & Web 2.0

1. Was sind nochmal die Grundlagen des Web 2.0?

- **Web 2.0:** interaktiv, **user generated content**
- Website URL (Uniform Resource Locator)
- https: Hypertext Transfer Protokol (Secure)
- www: World Wide Web (auch ohne www)
- Domain, Top-Level-Domain (.de, .org)

*user generated content
www.sicher-im-netz.de
URL, http, https, www,
Top-Level-Domain
Domain*

2. Was ist ein Content-Management-System?

- **CMS** (Content-Management-Systeme),
Verwaltung von Inhalten, Oberfläche
- Backend: Zugriff-Login, HTML Kenntnisse

*CMS, Backend, HTML
Templates - Design
Vorlagen,*

3. Welche Anbieter gibt es und wie unterscheiden sie sich?

(Siehe Lernzentrale)

- Open-Source (Quellcode öffentl.)
- **proprietär (herstelleregebunden)**
- Wordpress (Design-Vorlagen)
- WIX, Squarespace (Kosten)

*Open-Source, proprietär
Wordpress, WIX,
Squarespace
drag and drop*

4. Wie kann ich ein CMS für mich nutzen?

- **Web Content Management:** Website,
Mehrsprachigkeit, Volltextsuche
- Blog Publishing / News: logische
Verknüpfungen (Kommentare), planbar
- Social Publishing / Communities:
Kommunikation

*Web Content
Management
Blog -, Social-Publishing
Communities,
Online Foren
modulare Systeme*

5. Was ist das Web 3.0?

- Video Web 3.0: Länge 2:23
- **Große Datenmengen**, Metadaten

*Metadaten
semantisches Web*

B3 Browser

1. Für welchen Browser sollte ich mich entscheiden?

(Wiederholung Level 1 - Zusatz: Cache löschen)

- Vor- und Nachteile von Browsern:
 - Schnelligkeit, Sicherheit, vertrauenswürdig
- **Google Chrome, Mozilla Firefox, Microsoft Edge (nicht Explorer), Safari (Apple)**
- Browser auf Mobilgeräten: Apps
- Browser: **surfen**, Suchverlauf speichern

*Google Chrome
Mozilla Firefox
Microsoft Edge
Safari
Cache regelmäßig löschen*

2. Welche Möglichkeiten des anonymen Surfens gibt es?

- Video Anonymes Surfen: Länge 3:00
- **Proxyserver, VPN** (Virtual Private Network)

*anonymer Proxyserver,
Stellvertreterserver, VPN*

3. Was ist das Darknet?

- Widerstandsaktionen, Drogen-, Waffengeschäfte
- Nicht illegal, strafrechtl. relevante Inhalte
- Kleiner Teil des Internets: nicht in Suchmaschine, verschiedene Netzwerke, TOR-Netzwerk ist das größte
- Nicht herkömmlich auffindbar, spezielle Suchmaschine, TOR-Browser
- Verbindungen manuell herstellen, Peer-to-Peer-Overlay-Netzwerk, komplizierte URL, sicherer: Zugang nur beteiligte Personen

*TOR Netzwerk
TOR (the onion router) .onion
Peer-to-Peer-Overlay-Netzwerk*

4. Sollte ich Tor benutzen? Was muss ich bei der Nutzung beachten?

- Allgemein nutzbar, auch **Zugang Darknet**
- TOR-Browser Bundle installieren, IP Adresse verschlüsselt, „sicherer“, Besen-Symbol
- Vorteil: **anonym**, Zugriff **.onion** Seiten
- Nachteil: langsame Surfgeschwindigkeit

TOR: mehrere Weiterleitungen, IP Adresse verschlüsselt, „neue Identität“

B4 Cookies

1. Was sind Cookies und weshalb existieren sie?

- Kleine Textdateien mit Informationen zu Surfverhalten
- Frage zu Cookies vom Gesetzgeber vorgeschrieben
- Einstellungen zu Cookies anpassen

Cookies

2. Welche Cookies gibt es?

- Notwendige Cookies: Website-Darstellung, z.B. Warenkorb
- Funktionale Cookies: Website-Bedienung, z.B. Formulare
- Leistungscookies: Fehlermeldung, Ladezeit
- **Evercookies**: Surfverhalten, schwer löscher
- Social-Plug-Ins: Website mit Social-Media-Button, zukünft. Schutz: 2-Klick-Verfahren

*Evercookies
2-Klick-Verfahren*

3. Wie vermeide ich Tracking durch Cookies?

- **Anti-Tracking Plug-Ins und Add-Ons nutzen**
- Cache leeren, Sicherheitseinstellungen prüfen
- Zustimmung: Nur technisch-nötige Cookies
- Inkognito-Modus, Anonym-Modus: keine Cookies, aber auch z.B. keine Warenkorbspeicherung

*Cookies löschen
Anti-Tracking
Plug-Ins, Add-Ons
Inkognito-Modus*

4. Welche Anti-Tracking-Software gibt es für den Browser?

(Siehe Lernzentrale) (Wiederholung Level 2)

- **Anti-Tracking Plug-Ins** (eigenständiges Zusatzprogramm) und **Add-Ons** (Erweiterung zu bestehendem Programm)
- Ghostery, uBlock Origin

*Ghostery
uBlock Origin*

B5 Suchmaschine

1. Wie funktioniert eine Suchmaschine?

- Suchmaschine greift auf vorher erstellten Index zu, Index: spezielle Bots (Crawler) durchsuchen Web, speichern Schlagwörter, nicht jede Suchmaschine hat eigenen Index

*Index
Bots, Crawler*

2. Was sind SERPs?

- **Search Engine Result Page**, Ergebnisseite Suchmaschine: Website, Bilder, Video, Ads
- einzigartig: Standort, Verlauf, Profil, Gerät

SERP (Search Engine Result Page)

3. Wie kommen eigentlich die Rankings bei den Suchergebnissen zustande?

- Anzeige (Ad) ganz oben, bezahlte Werbung
- Suchbegriff: Abgleich Datenbank, Klickzahl
- Vorhandene Verlinkung (Algorithmen), Aktualität
- **Standort, Sprache, Top-Level-Domain**

*Ad
Algorithmen
IP Adresse
Top-Level-Domain*

4. Für welche Suchmaschine entscheide ich mich?

(Siehe Lernzentrale) (Wiederholung Level 1)

- Unterschiede in Datenschutz, soziales Engagement oder genaue Suchergebnisse
- Unterschiede Suchmaschinen: **Google, Bing (Microsoft), DuckDuckGo, Ecosia (sozial)**
- Adresszeile Browser = Suchmaschine in Einstellungen festlegen

*Google
Bing
DuckDuckGo
Ecosia*

5. Wie kann ich die Suche durch Operatoren verbessern?

(Wiederholung Level 2)

- **Genauere Ergebnisse: AND, OR, Minus (ohne Leerzeichen)**, Anführungszeichen, **site**

*Suchoperatoren: And,
OR= | Pipe Operator, site*

C | Kommunikation

C1 E-Mail

1. Wie stelle ich meine Privatsphäre sicher?

- **E-Mail-Provider** auf DSGVO prüfen, Serverstandort
- Datensparsamkeit, nur auf Weg verschlüsselt
- Investiere in sicheren Provider (**ohne Werbung/Tracking**): **Posteo**, mailbox.org

Posteo, Mailbox.org

2. Sollte ich E-Mails verschlüsseln?

- Verschlüsselte Messenger (WhatsApp, Signal)
- E-Mail **Punkt-zu-Punkt-Verschlüsselung** (Transportverschlüsselung): Transport-Layer (Secur Sockets Layer), auf Server Klartext
- **Ende-zu Ende-Verschlüsselung**: auch auf Server verschlüsselt, nur Sender/Empfänger haben Schlüssel und sehen Klartext

*Klartext
Transport-Layer, Secur
Sockets Layer
Ende-zu-Ende-
Verschlüsselung*

3. Wie kann ich meine E-Mails Ende-zu-Ende verschlüsseln?

- **PGP (Pretty Good Privacy, ziemlich gute Privatsphäre)**: basiert auf Ende-zu-Ende-Verschlüsselung, Plug-In, Server Standort, Datensparsamkeit, **GnUPG** (open source)
- Privater (nur Sender) und öffentlicher Schlüssel (wird geteilt)
- Einrichtung: Sender und Empfänger Plug-In installieren, jeder privaten Schlüssel
- GPG für Apple, Windows oder Thunderbird (Siehe Lerninhalt)

*PGP (Pretty Good
Privacy)
GnUPG (open-source)
Sender, Empfänger,
privater Schlüssel,
öffentlicher Schlüssel*

C2 Messenger & SMS

1. Messenger & SMS (Siehe Lernzentrale)

- **SMS** (short message service), **160 Zeichen**, **Zwei-Faktor-Authentisierung**, über Telefonnetz
- **Messenger:** App, WhatsApp, Signal, Telegram, mobile Daten oder WLAN
- **DSGVO, AGB, Datenschutz**
- **WhatsApp:** Ende-zu-Ende-Verschlüsselung, Geräte und Verbindungsdaten, Achtung bei Kommunikation zu Unternehmen
- **Signal:** Ende-zu-Ende-Verschlüsselung, kein Daten sammeln
- **Threema:** Downloadgebühr, Ende-zu-Ende-Verschlüsselung, **anonym (ohne Telefonnummer)**, **europäischer Server**
- **Telegram:** Ende-zu-Ende-Verschlüsselung deaktiviert, geheimer Chat, Datenspeicherung
- Updates/Backup wichtig, **in Browser abmelden**

*SMS
Messenger: App
installiert, beide Apps,
online
DSGVO, AGB,
Datenschutz
WhatsApp, Signal,
Threema, Telegram
Ende-zu-Ende-
Verschlüsselung,
anonym
Update, Backup*

2. Welche erweiterten Messenger-Funktionen gibt es?

(Wiederholung Level 2)

- WhatsApp-Broadcast: ähnlich Gruppe, Mitglieder müssen Nummer speichern, Antwort an Sender
- Telegram-Kanal: öffentl. oder privat, **privat nur mit Einladung**, Threema / Signal ohne

*WhatsApp Broadcast
Telegram-Kanal*

3. Wie kann ich meine(n) Messenger im Browser oder auf mehreren Geräten parallel nutzen? (Siehe Lernzentrale)

- Signal
- Threema
- WhatsApp
- Telegram

*gekoppelte Geräte,
QR-Code
Browser (abmelden nach
Nutzung), App*

C3 Videokonferenzen

1. Welche Anbieter gibt es? (Wiederholung Level 1)

- Videoanruf: **Kamera, Mikrofon, Internet**
- Anbieter: **Skype, Zoom, Messenger** (WhatsApp, Signal, Telegram), **Skypen** = Videoanruf

*Skype - skypen
Zoom
Messenger*

2. Wie wähle ich einen Anbieter aus?

(Siehe Lernzentrale) (Wiederholung Level 1)

- Vor- und Nachteile: Skype, Zoom, Messenger
- **Funktionen: Chatten, Bildschirm teilen, Daten senden, Aufzeichnung, Tastaturkürzel**
- **Datenschutz, AGB, Nutzungsbedingungen**
- **Kostenlos, nur Anmeldung nötig**

Tastaturkürzel (ohne Maus)

3. Wie gestalte ich einen sicheren Videonruf? (Wiederholung Level 1)

- Datenschutz, Ende-zu-Ende-Verschlüsselung
- keine Weitergabe an Drittanbieter
- Sicheres Passwort, Zugriffsrechte, Updates
- **Einladung: E-Mail, Messenger**

Passwort, Ende-zu-Ende-Verschlüsselung

4. Wie teile ich Inhalte während des Videoanrufs?

(Wiederholung Level 2)

- Ganzen **Bildschirm** teilen / **Fenster**
- Chat-Fenster nutzen, Büroklammer / Plus

Teilen, Freigeben, Chat

5. Wie bereite ich eine Videokonferenz gut vor?

- Kamera, Mikrofon an, Stabile Internet-Verbindung
- Ruhiger Ort, Mit Program vertraut machen
- Break Out Rooms: **Virtuelle Räume**, um die **Gruppe zu teilen**, Skype hat das nicht

Break Out Rooms = Virtuelle Räume

C4 Soziale Netzwerke

1. Welche sozialen Netzwerke gibt es?

(Siehe Lernzentrale) (Wiederholung Level 2)

- Austausch: **posten, adden, liken**
- **Facebook**
- **Instagram**
- **Snapchat**
- **Twitter**
- **TikTok**
- **YouTube**
- **Twitch**
- Vor allem Europa, Nordamerika, China:
SinaWeibo, Q-Zone, TencentQQ, WeChat;
russisch VK

*Soziale Netzwerke:
Facebook, Instagram,
Snapchat, Twitter,
TikTok, YouTube
Posten, Adden, Liken
Accounts, Follower,
Gamer
Livestream, Plattform*

2. Welche Sicherheitsaspekte muss ich beachten?

(Wiederholung Level 2)

- **Keine Anfragen von Unbekannten**
- **Datensparsamkeit**, private Inhalte überdenken
- **Persönlichkeitsrechte (Kinder), Urheber-, Verwertungsrecht** (Bearbeitung)
- Keine Fotos/Videos von Kinder, **Jugendschutz**
- Auf **Social Login** verzichten, **Zugriffsrechte**

*Datensparsamkeit
Urheberrechte,
Verwertungsrecht,
Persönlichkeitsrechte
Finanzieller Vorteil
Social Login*

3. Kann ich Inhalte einfach so in sozialen Netzwerken teilen?

- Video Soziale Netzwerke: Länge 2:18

70 Jahre nach Tod Autor

4. Wo finde ich lizenzfreie Inhalte (Musik, Töne, Videos, Fotos)?

- Bilder: Unsplash, Pixabay, Pixelio
- Musik: Jamendo, Sound Bible, Audiyou
- Töne: geraueschesammler.de

*Open Content
Creative Common*

C5 Belästigungen & Fake News

1. Welche Belästigungen gibt es? (Wiederholung Level 1)

- Video Belästigungen: Dauer 3:10 Minuten
- Hate Speech, Cyber-Mobbing, Grooming, Stalking

*Hate Speech
Cyber = Internet*

2. Wie kann ich mich vor Belästigungen und Beleidigungen schützen?

- **Ernst nehmen, keine Provokation, Beweise, Beitrag melden (NetzDG: rechtswidrige Inhalte 24 Std. Löschung)**
- **Nicht alles mit allen teilen, Datensparsamkeit**
- Sicherheitssoftware und Firewall aktuell halten

*Netzwerkdurchsetzungsgesetz (NetzDG)
Cyber-Mobbing-Grooming-Stalking, Blockieren
Firewall*

3. Welche Angebote gibt es für Betroffene? (Wiederholung Level 1)

- Hate Aid, Weißer Ring, Polizei, Vertrauensperson

Hate Aid, Weißer Ring

4. Wie erkenne ich Fake News? (Wiederholung Level 1)

- **Autor:in**, Impressum, Überschrift prüfen
- Verifizierter Account mit Häkchen, Followerzahl
- Faktenfinder (Tagesschau, Mimikama, Hoaxmap)

*Quellen prüfen
Follower
Verifizierte Accounts*

5. Was mache ich, wenn ich Fake News erkannt habe?

(Wiederholung Level 1)

- Beitrag, Bild, News melden
- Person einschränken, blockieren, melden
- Cybermobbing: Polizei

D | Datenwelt

D1 Datenschutz

1. Welche Datenschutzrechte habe ich im Netz?

- Europ. Datenschutzgrundverordnung **DSGVO**
- Recht auf Selbstbestimmung und Sicherheit
- Datensicherheit: nur Daten, die nötig sind
- Daten-, Sicherheitsmaßnahmen, Schutz vor Hacker
- Recht auf Auskunft und Beschwerde
- Leak (Datenleck), kein ungefragtes Foto/ Video
- Foto erlaubt: **Person der Zeitgeschichte**

*DSGVO, informationelle Selbstbestimmung
Datensicherheit:
Kontakt-, Login-, Kommunikations-, technische Daten , Leak, Upskirting, Downblousing*

2. Welche Mythen rund um den Datenschutz gibt es?

- **1978 Bundesdatenschutzgesetz (BDSG)**
- Einwilligung, wenn nicht per Gesetz erlaubt
- Kunsturhebergesetz, Bsp. **Demonstrationen**

Bundesdatenschutzgesetz (BDSG) 1978

3. Was kann ich für den Schutz meiner Daten tun?

- Lese die **Datenschutzerklärung**:
Sicherheitsmaßnahmen,
Datenschutzbeauftragte(r), -behörde
Bundesland, Server-Standort
- **App-Berechtigungen** anpassen
- Login-Daten nicht speichern
- Apps löschen, die man nicht braucht

4. Was mache ich, wenn gegen den Datenschutz verstoßen wurde?

- Datenschutzbeauftragte:r/-behörde kontaktieren
- Beweise sichern

Beweise sichern

D2 Datensparsamkeit

1. Was bedeutet Datensparsamkeit? (Wiederholung Level 1)

- Verantwortungsbewusster Umgang mit persönlichen Daten
- **So wenig Daten wie möglich** bei Onlineanbietern speichern

2. Was sind Tipps für mehr Datensparsamkeit? (Wiederholung Level 1)

- Nur das Nötigste angeben, Pflichtfelder *
- Diskret sein, keine persönlichen Fotos
- Anonym bleiben (**Pseudonyme**, Spitzname)
- Verschiedene E-Mail-Adressen nutzen
- Alle Anbieter dürfen nur die Daten abfragen und speichern, die für die Nutzung notwendig sind
- Datenzugriff in Einstellungen kontrollieren

3. Wie kann ich meine Daten endgültig löschen? (Wiederholung Level 2)

- Konto kündigen, Hilfe durch justdeleteme.me
- **Anbieter** direkt kontaktieren, Kundenservice
- Kontakt **Datenschutzbeauftragte(r)** des Unternehmens oder **Datenschutzbehörde** Bundeslandes (eventuell Gebühren)

4. Wie erkenne ich, ob ein Online-Unternehmen Datensparsamkeit ernst nimmt? (Wiederholung Level 2)

- **Zweck** der Datenerhebung
- **Transparenz, Datenweitergabe**, wann werden Daten gelöscht
- Auflistung deiner Rechte, **Datenspeicherung**

D3 Logins und Passwörter

1. Was ist ein starkes Passwort?

- Einmalig, lang, komplex, kreativ
- Klein- und Großbuchstaben, Zahlen, Sonderzeichen

*iKGa#951_W
Identity Leak Checker:
haveibeenpwned*

2. Wie bilde und merke ich mir ein starkes Passwort?

(Wiederholung Level 1)

- Merksatzmethode (erster oder letzter Buchstabe) + App-Verlängerung
- „**Passwort vergessen**“ nutzen

Merksatzmethode

3. Was können Passwortmanager? (Wiederholung Level 2)

- **Passwörter nicht im Browser speichern**
- App- oder Plug-In-Passwortmanager, **Datenschutzerklärung lesen**
- Vorteil: nur 1 Masterpasswort (kein Zettel)
- Nachteil: Cloud, **Serverstandort** (Europa)

*Masterpasswort merken
Passwortmanager:
Enpass, LastPass,
NordPass*

4. Was ist die Zwei-Faktor-Authentisierung? (Wiederholung Level 1)

- **Zwei Komponenten** zum Login
- Per: **SMS, Anruf, Authenticator-App, Gesichtserkennung, Fingerabdrucksensor**

*Zwei-Faktor-Authentisierung
Authenticator-App*

5. Was sind U2F-Sticks und wie funktionieren sie?

(Wiederholung Level 2)

- Universal Second Factor: Passwort + USB-Stick
- Alle im Handel Zertifikat Standard „FIDO“
- Account einrichten: Datenschutz/Sicherheit/Login
- Tipps: Ersatz-Stick einrichten, Smartphone-Sticks über NFC oder Bluetooth

*U2F-Sticks
2 Faktoren Login:
Passwort + USB-Stick*

D4 Backups

1. Wie bin ich vor Datenverlust geschützt?

- **Datenverlust:** USB-Stick bricht, Wasser-, Feuerschäden, Löschen, Hackerangriff, Verlust
- Backup externer Datenträger oder Cloud

*BackUp:
Externer Speicher/
Datenträger, Cloud*

2. Welche Synchronisierungsoptionen gibt es?

- **Vollsicherung:** neues Voll-Backup, altes löschen
- **Inkrementell:** nur Dateien, die verändert wurden
- **Differenzielle Datensicherung:** inkrementell + Sicherheitskopie alte Version der Daten

*Vollsicherung
inkrementelle oder
differenzielle
Datensicherung*

3. Welche Programme zur Sicherung gibt es? (Siehe Lernzentrale)

- GoodSync, PureSync, SyncToy, AcronisCyberProtect, NovaBackup
- Windows/MacOS/Android/iOS: eigene Systeme

*Schlüssel=Passwort
Quell-und Zielordner
Synchronisation
Schattenkopie*

4. Was sind die Vorteile von Verschlüsselung? (Wiederholung Level 2)

- Schutz bei Hacking oder Diebstahl
- Kinder-, Jugendschutz, Schadsoftwareschutz

Schlüssel=Passwort

5. Wie verschlüssele ich meine Dateien am besten?

(Wiederholung Level 2)

- Verschlüsselungssoftware: SteganoSafe, Gpg4Win, ArchiCrypt, VeraCrypt, TruPax
- **Festplatte:** Passwort, **Gehäuse:** mit Schloß
- Finger-, Gesichtserkennung

*Software
Festplatte
Gehäuse*

D5 Clouds

1. Welche Potentiale bietet Cloud Computing?

- Betriebssicherheit, Störungsfreiheit: sehr gute Sicherheitskonfiguration
- Riesige Speicher: z.B. Musikspeicher Spotify, Deezer
- Cloud-Gaming: Computerspiele sind rechenhungrig, geringe Anforderung an eigenes System

*Cloud, Server
Synchronisierung*

2. Welchen Cloud-Anbieter sollte ich nutzen? (Wiederholung Level 2)

- Viele Anbieter: Dropbox und OneDrive (Microsoft), Hidrive (Strato), MagentaCloud (Telekom), OwnCloud
- Preise
- **Datenschutzerklärung**, Datensparsamkeit
- Sicherheitsmaßnahmen, Verschlüsselung
- **Zwei-Faktor-Authentisierung**
- Verschlüsselungstechnologie: **Tresor**
- **In Cloud keine persönlichen Daten hochladen**

3. Wie verschlüssele ich meine Daten in der Cloud?

- Verschlüsselung nach dem Upload: **Tresor** (Microsoft OneDrive, Dropbox): bei Öffnung Tresor erhält man Code
- Verschlüsselung vor dem Upload: Magenta Cloud: Datei auf Festplatte mit z.B. BoxCryptor, Cryptomator verschlüsselt, lässt sich nur mit Zusatzprogramm wieder öffnen
- Wenn die Daten in der Cloud sind, sind sie auf dem Computer/Server von jemand anderem.

***Tresor**
BoxCryptor, Cryptomator*

E | Gefahrenschutz

E1 Updates

1. Kleine Erinnerung: Wo finde ich Updates? (Siehe Lernzentrale)

- Software immer auf. neuestem Stand halten: Fehlerbehebung, **Sicherheitslücke schließen**, Neue Funktionen, Systemabstürze vermeiden
- **iOS, Android, Windows, MacOS**

Betriebssystem

2. Welche Updates sollte ich wie schnell installieren?

(Wiederholung Level 2)

- **Sofort:** Sicherheitsupdates, Bug-Fixes, Patches
- Funktions-Updates: größer, Aussehen, Funktionen
- **Major-Updates:** umfassend

*Bug-Fixes, Patches
Major-Updates > Backup*

3. Wie ist eine Versionsnummer aufgeschlüsselt? (Wiederholung Level 2)

- 4(**Major**).3(**Minor**).56(**Patch-Level**)-384(Build-Nummer), **je weiter rechts, desto kleiner Änderung**, bei Major oder Minor folgen Nullen

*Versionsnummer
4.3.56-384
jede Version erhöht Zahl*

4. Wie kann ich Updates im Changelog nachvollziehen?

(Siehe Lernzentrale)

- Changelog (Änderungsprotokoll)
- iOS
- Android
- Windows
- MacOS
- Sideloadung Apps, nicht in Stores, Website

*Changelog
App Store
Sideloadung Apps*

E2 Schadsoftware

1. Welche Schadsoftware gibt es?

- Malware (Schadsoftware): **E-Mail-Anhänge, Links, Downloads**
- Computervirus: Systemzugriff, verändert Daten
- Computerwürmer: verbreiten sich selbst, kapern Programme, z.B. verschicken E-Mails
- Trojaner: Vortäuschung Nutzen, Datenspionage
- **Backdoor/Trapdoor**: erlaubt Dritten Zugang
- **Ransomware**: Erpresser sperren Systemzugang
- Spyware: spioniert, verkauft Informationen
- Scareware: Angst durch Systemwarnung
- **Adware**: harmlos, unerwünschte Werbung

*Malware
Trojaner, Wurm
Ransomware
Backdoor/Trapdoor
Spyware
Scareware
Adware (Werbung)*

2. Wie kann ich mich und andere vor Malware schützen?

- Keine verdächtigen Links / Anhänge öffnen
- Betriebssystem / Programme aktuell halten
- Nicht ohne Sicherheitssoftware surfen:
- Windows Defender, Firewall, Bordmittel
- Nur sichere Software installieren
- Nicht auf verlockende Angebot eingehen

*Sicherheitssoftware:
Firewall, Bordmittel
X tippen, Alt F4*

3. Was muss ich tun, wenn doch etwas passiert ist?

- Virenalarm: **Löschen / Quarantäne Lösung**
- Wenn nichts hilft: Betriebssystem neu installieren
- In abgesichertem/sicherem Modus Virensan
- **Vom Netz trennen**, Hilfesuche anderes Gerät
- Online-Hilfe
- Formatieren und neu aufsetzen
- Hilfe beim Spezialisten suchen

*Quarantäne Lösung,
abgesicherter/sicherer
Modus und Virensan,
Verbraucherzentralen,
Bundesamt für Sicherheit
in der
Informationstechnik (BSI)*

E3 Social Engineering

1. Was ist Social Engineering? (Wiederholung Level 1)

- Oberbegriff Betrug und Täuschung
- Beispiele: Einzeltrick, Anruf Bankmitarbeiter, E-Mail Anhang

*Social Engineering =
Soziale Manipulation*

2. Was ist Phishing? (Wiederholung Level 1)

- Passwort + Fishing
- **Vorsicht: Login-Daten werden abgefragt, Banking Login, Zugangsdaten**
- Über Telefonanruf: **Vishing**

*Phishing
Vishing*

3. Wie erkenne ich Phishing? (Wiederholung Level 1)

- **E-Mail Adresse, Betreff, Anhang, Erscheinungsbild, Ansprache, Links, Fehler**
- Verlockendes Angebot, kein Konto, keine Bestellung, Frage nach Zugangsdaten

4. Wie gehe ich mit Phishing um? (Wiederholung Level 2)

- Spam Filter, Spam-E-Mails löschen
- Phishing-E-Mails löschen
- **E-Mail-Format von HTML auf nur Text ändern**
- Internetrecherche, Person anrufen und nachfragen

*Spam-Filter
E-Mail-Format :Text
ändern*

5. Was, wenn doch etwas passiert ist? (Wiederholung Level 1)

- Andere informieren
- **Passwort ändern**, Bank-Login 3x falsch
- **Anbieter informieren**, Anzeige erstatten

E4 Doxxing

1. Was ist Doxxing? (Wiederholung Level 1)

- **Negativ:** Persönliche, nicht veröffentlichte Daten und Dokumente werden im Internet veröffentlicht
- Folgen: E-Mail-Flut, Angriff Privatwohnung
- **Positiv:** Veröffentlichung von Misstände und Skandalen

Doxxing

2. Wie schütze ich mich vor Doxxing? (Wiederholung Level 1)

- **Datensparsamkeit**
- Social Media Einstellungen
- Sicherheitsvorkehrungen: **Zwei-Faktor-Authentisierung, Updates**
- Datenbroker:innen, Datenschnüffler:innen: gegen Bezahlung gezielt nach Daten suchen und zusammentragen

Datenbroker:innen

3. Was kann ich tun, wenn ich gedoxxed wurde? (Wiederholung Level 1)

- **Nur personenbezogenen Daten, die nicht frei zugänglich sind**
- Doxxing ist strafbar
- Andere informieren
- Beitrag melden
- Beweise sammeln
- Anzeige erstatten

E5 Identitätsdiebstahl

1. Was ist Identitätsdiebstahl? (Wiederholung Level 1)

- Jemand gibt sich online für jemand anderen aus
- Meistens **Geldbetrug** oder Online-Bestellungen, kostenpflichtige Abos
- Identity Leak Checker

*Identitätsdiebstahl
Identity Leak Checker
Datenlecks*

2. Wie vermeide ich Identitätsdiebstahl? (Wiederholung Level 1)

- **Datensparsamkeit**
- **Privatsphäre-Einstellungen**
- **Auf Phishing-Versuche achten**

Datensparsamkeit

3. Was muss ich tun, wenn doch etwas passiert ist?

(Wiederholung Level 1)

- Konto und Karten sperren (**Bank** Login 3x falsch eingeben)
- Anzeige **Polizei**
- **Passwörter ändern**
- Mahnung, Vollstreckungsbescheid oder Inkasso- Briefe sofort beantworten (Widerspruchsfrist)
- **Schufa** Meldung

E6 Scam

1. Was ist Scam? (Wiederholung Level 1)

- Video Scam: Dauer 2:29 Minuten
- Betrug: **Vorschussbetrug, Romance Scam** (vorgaukeln von **Gefühlen, Vertrauen** aufbauen)

*Scam
Romance Scam*

2. Wie erkenne ich Scamming? (Wiederholung Level 1)

- **Geldforderung**
- **Bauchgefühl**, „zu gut, um wahr zu sein“
- Anzeichen einer Fälschung, Umwege von Überweisung, Fehler
- Kommunikation über **andere Plattformen**
- **Persönliches Treffen abgelehnt**
- **Suche im Netz**

Geldforderung

3. Was muss ich tun, wenn ich Opfer von Scamming wurde?

(Wiederholung Level 1)

- Nicht auf Forderungen eingehen und kein Geld überweisen
- Beweise sichern, Rückbuchung
- Anzeige bei Polizei
- Kontakt abbrechen

F | Technologiealltag

F1 Fitnessstracker & eHealth

1. Was steckt alles in eHealth? (Wiederholung Level 1)

- Video eHealth: Dauer 2:32 Minuten
- Wearables (**Kalorien, Schritte, Puls**), Krankenkassen-Apps

*eHealth
Wearables*

2. Welche Sicherheitsaspekte gibt es zu beachten?

(Wiederholung Level 1)

- **Datensparsamkeit**, wo werden Daten geteilt?
- **Updates und Virenschutz**
- **Einwilligungen** überdenken, Server Standort

3. Wie sieht eHealth im Gesundheitswesen aus? (Wiederholung Level 1)

- Elektronische Patientenakte (ePA)
- Elektronische Rezept, **E-Rezept**
- **Digitale Gesundheitsanwendung** DiGAs
- Medizintechnik, **Arztbesuch Videocall**
- Telematikinfrastruktur zur Sicherheit
- Termine: Doctolib, Doctena
- Krankenkassen-App: Boni, Impfnachweis, Übungen, digitale Sprechstunde

*ePA
E-Rezept
DiGAs
Telematikinfrastruktur*

4. Was ist digital detox? (Wiederholung Level 1)

- Digitales Fasten
- Zeit am Bildschirm reduzieren, Wecker stellen, Flugmodus nutzen
- Benachrichtigungen ausschalten
- Bildschirmzeit beobachten, Zeiten oder Orte festlegen

digital detox

F2 Digitaler Personalausweis

1. Was genau ist der digitale Personalausweis? (Wiederholung Level 1)

- Video Personalausweis: Dauer 2:34 Minuten
- eID: analoger Personalausweis (Symbol), Kartenlesegerät oder **AusweisApp2**, **6stellige Pin**
- Onlinezugangsgesetz: Ämter, Post, Rentenversicherung

*E-Government
eID, Smart-e-ID
Onlinezugangsgesetz
2017*

2. Welche Möglichkeiten bietet er? (Wiederholung Level 1)

- Bafög
- **Rentenkonto** bei Deutscher Rentenversicherung
- **Punkttestand beim Kraftfahrt-Bundesamt**
- Bürgerämter Dienste auf Anfrage
- Service Deutsche Post und Deutsche Bahn
- Chip prüft staatliche Berechtigung zur Abfrage

Postiden-Verfahren

3. Was muss ich beachten? (Wiederholung Level 1)

- Verbindung nach Nutzung trennen
- **Updates** und Virenschutz
- **Verlust** sofort melden (**Polizei, Bürgeramt**)
- Nutzung ist sicher

F3 Online-Banking

1. Wie bleibe ich beim Online-Banking geschützt?

(Wiederholung Level 2)

- **Sichere Passwörter**
- **Phishing:** Banken fragen nie per E-Mail ab
- Kontoauszüge prüfen
- Sichere Website (**https, Schlosssymbol**)
- Datensparsamkeit
- Auf Website Kleinigkeiten achten
- **Verschlüsseltes WLAN, WPA2,WPA3**
- **Zahlungslimit** bei Bank

*Sichere Passwörter
Phishing
NFC Hülle*

2. Und wenn doch etwas passiert ist? (Wiederholung Level 1)

- Bankverbindung sperren, **3 Mal hintereinander falsches Passwort, Anzeige**
- **Sperr-Notruf** anrufen, **Bank benachrichtigen**
- Belege sammeln, auf Schadsoftware achten

3. Welche Möglichkeiten des mobilen Zahlens gibt es?

(Wiederholung Level 2)

- **Vorteile:** schnell, mit allen Geräten möglich
- **Mobiles Zahlen: NFC (Nahfeldkommunikation)**
- Giro- oder Kreditkarte, Smartphone, Smart Watch mit NFC-Chip
- Apple: ApplePay, Android: PayPal, Bank-App

*NFC
Apple: ApplePay
Android: PayPal,
Bank-App*

4. Wie kann ich sicher mobil zahlen? (Wiederholung Level 2)

- **Updates, Zugriffsschutz, Ausgabenlimit**
- Sperren bei Verlust, NFC deaktivieren
- Sicherung: PIN, Fingerabdruck, Verwahrung
- mehrere Karten übereinander
- kein öffentliches WLAN
- Android: NFC deaktivieren

*Zwei-Faktor-Authentisierung
TAN
App-Freischaltung*

F4 Online-Shopping

1. Welche Zahlungsmöglichkeiten beim Online-Shopping gibt es?

(Wiederholung Level 1)

- **PayPal:** Eigenes Konto eröffnen, Zahlung an Shops oder Freunde
- **Klarna: Rechnung,** Lastschrift, Vorkasse, Sofortüberweisung, Ratenkauf
- **Paydirekt:** Überweisung Bankkonto mit TAN
- **Kreditkarte**

*PayPal, Klarna
https
TAN*

2. Was sind die Vor- und Nachteile von Online-Bezahldiensten?

(Wiederholung Level 1)

- Vorteil: Schnell, kostenlos, bequem
- Nachteil: weniger Kontrolle, Daten an Drittanbieter
- Achte auf Zwei-Faktor-Authentisierung

3. Was sind Fake Shops und wie schütze ich mich vor ihnen?

(Wiederholung Level 2)

- Professionelle Website, Impressum
- Transparente Preise, **Zahlungsmethode**
- **Impressum:** Rechtsform, Kontaktdaten
- **Gütesiegel:** Trusted Shops, TÜV Süd Safer Shopping, Internet Privacy Standards, EHI,
- **Bewertungen,** Kommentare
- Reihenfolge der Produkte (Filter)
- Abo-Pflicht
- SOS-Karte: Bundesamt für Sicherheit in der Informationstechnik

*TÜV Süd, Trusted Shop,
Internet Privacy
Standards, EHI
SOS-Karte*

3. Was muss ich im Betrugsfall tun? (Wiederholung Level 2)

- **Bank benachrichtigen**
- Belege aufbewahren, **Screenshots**
- Anzeige bei **Polizei**

Glossar

Account	Digitales Nutzerkonto einer Person, welches weitere Onlinedienstleistungen ermöglicht. Ein Account wird mithilfe eines Nutzernamens/einer E-Mail-Adresse/einer ID und eines individuellen Passworts erstellt. Beispiele hierfür sind Accounts für Onlineshops oder auch Streaming-Services.
Adden	„Hinzufügen“. Adden bezieht sich zumeist auf soziale Netzwerke wie zum Beispiel Facebook, zu denen man Freunde hinzufügt oder selbst hinzugefügt wird.
Add-on	Kleine Erweiterung zum Browserprogramm, um bestimmte Funktionalitäten hinzuzufügen. Beispielsweise ist ein Ad-Blocker ein Add-on, welches Werbung auf Websites blockiert.
Algorithmic Bias	Algorithmische Voreingenommenheit. Eine KI mit Algorithmic Bias entsteht durch den Einsatz ungeeigneter, einförmiger Trainingsdaten.
Algorithmus	Eine eindeutige Folge von Handlungen zur Lösung eines Problems. Ein Algorithmus kann in einem Computerprogramm enthalten sein, er kann aber auch als Reihe von Befehlen in menschlicher Sprache formuliert werden. Auch eine Diagrammdarstellung ist möglich.
Algorithmus	Eine Reihe von Anweisungen, denen Schritt für Schritt gefolgt wird. Die Anweisungen sind so eindeutig, dass sie von einer Maschine gelesen werden können, um bestimmte Probleme zu lösen oder Vorgänge auszuführen. Algorithmen werden in sozialen Netzwerken angewendet, diese entscheiden automatisiert, was Nutzer:innen angezeigt wird und was nicht.
Anonymer Modus/ Inkognito-Modus	Wird auch privates Surfen genannt und ist eine Browsereinstellung, die ein gewisses Maß an Privatsphäre ermöglicht, indem Internetverläufe, Cookies, Downloads oder Anmeldedaten nicht gespeichert werden.

Anti-Tracking-Software	Programme (Tools), die das Protokollieren oder Verfolgen von Nutzerverhalten verhindern. Sie können leicht im Browser installiert werden. Beispielsweise gehören dazu auch Werbeblocker.
Antivirenprogramm	Überprüft neue Dateien (zum Beispiel Anhänge von E-Mails) und den gesamten Computer auf Schadsoftware. Dazu vergleicht es in erster Linie die Daten auf dem Rechner mit den „Fingerabdrücken“ bekannter Schadprogramme.
App	Steht für „Applikation“ und ist eine Anwendungssoftware. Der Begriff App wird oft im Zusammenhang mit Anwendungen für Smartphones oder Tablets verwendet.
App Store/Store	Digitale Vertriebsplattform für Apps. Die Apps können aus dem Store (Geschäft) auf das Endgerät heruntergeladen werden. Die bekanntesten App Stores sind Apple Store, Google Play Store und Microsoft Store.
Apple-ID	Die Apple-ID sind die Zugangsdaten, mit denen man sich bei allen Leistungen von Apple anmeldet, zum Beispiel im Apple Store, FaceTime oder Apple Music.
Assistenzsysteme	Diese Geräte können Sprache analysieren und auf gesprochene Anweisungen reagieren.
Augmented Reality	„Erweiterte Realität“. Hierbei wird die reale Welt um virtuelle Elemente erweitert. Ein Beispiel dafür ist das Spiel „Pokémon Go“.
Authentifizierung	Ein vorgelegter Identitätsnachweis einer Person wird überprüft (das Vorlegen des Nachweises nennt sich Authentisierung). Erst nach erfolgreicher Authentifizierung erfolgt die Autorisierung.
Authentisierung	Eine Person legt einen Nachweis über ihre Identität vor, um dies von einem System überprüfen zu lassen, unter anderem durch Passwort-Eingabe, Chipkarte oder Biometrie. Die Authentisierung von Daten erfolgt zum Beispiel durch kryptografische Signaturen.
Autorisierung	Für eine bereits erfolgreich authentifizierte Person werden die ihr auf einem System eingeräumten Rechte freigeschaltet.
Avatar	Ist ein „Virtueller Stellvertreter“. Meist eine Grafik oder eine Animation, die im Internet – beispielsweise in Chatrooms – zur Darstellung einer Person genutzt wird.

Backup	Sicherung der Daten zum Schutz vor Datenverlust. Es werden dabei Kopien von vorhandenen Datenbeständen erstellt.
Bandbreite	Beschreibt den Frequenzbereich, in welchem Daten übertragen werden. Je größer die Bandbreite ist, desto schneller können die Daten übertragen werden.
Beam Forming/ Beams	Intelligente Antennentechnik in 5G-Netzen. Beim „Beam Forming“ richten spezielle Antennen ihr Signal, die „Beams“, gezielt auf einen Empfänger, anstatt es ziellos abzustrahlen.
Betriebssystem	Das Betriebssystem verwaltet das Zusammenspiel der einzelnen Teile eines Computers oder Handys. Für Nutzer:innen bedeutet das vor allem eine erleichterte Bedienung. Die bekanntesten Betriebssysteme sind Windows, MacOS, Linux, Android oder iOS.
Bilder-Rückwärts-suche	Durch die Google-Bildersuche kannst du den Ursprung eines Bildes herausfinden. Dafür gibt es mehrere Möglichkeiten: <ul style="list-style-type: none"> · Google-Bildersuche durch Hineinziehen eines Bildes · Google-Bildersuche mit einem hochgeladenen Bild · Google-Bildersuche mit einer Bild-URL · Google-Bildersuche mit einem hochgeladenen Bild auf dem Smartphone
Blog	Eine Art elektronisches „Tagebuch“ im Internet, das ständig aktualisiert wird. Die Verbreitung sowie die Themenfelder sind sehr weitreichend. Beispielsweise gibt es Modeblogs, Kochblogs oder IT-Blogs. Die Blogs sind auch untereinander gut vernetzt und lassen sich daher über Suchmaschinen leicht finden.
Bluetooth	Industriestandard für die drahtlose Datenübertragung zwischen Geräten über eine kurze Distanz per Funktechnik.
Bordmittel	Bezeichnung für alle eigenen Mittel, die zur Verfügung stehen und eingesetzt werden können.
Botnetz	Verbund von Systemen, die von einem fernsteuerbaren Schadprogramm (Bot) befallen sind.
Boxcryptor/ Cryptomator	Programme, die dazu dienen, verschiedene Cloud-Speicher zu synchronisieren sowie die Dateien und Ordner, beispielsweise bei OneDrive oder Dropbox, zu verschlüsseln bzw. zu sichern.

Broadcast	„Übertragung“. Im Zusammenhang mit Nachrichtendiensten wie zum Beispiel WhatsApp kann eine Person eine Gruppe erstellen und somit Nachrichten an alle Leute in der Gruppe schicken, allerdings können die Gruppenmitglieder sich nicht gegenseitig in der Gruppe sehen und nur der Hauptperson direkt antworten.
Browser	Spezielles Programm, um im Internet zu surfen. „To browse“ bedeutet so viel wie „blättern“ oder „durchstöbern“.
Bug Fixes	Bei Bug Fixes oder Bugfixing wird ein Fehler in einem Programm ausgebessert oder behoben. Hierbei werden auch neuere Versionen oder Updates veröffentlicht, die zum größten Teil nur dazu dienen, die vorkommenden Fehler zu beseitigen.
Byte	Bezeichnet eine Maßeinheit oder Dateneinheit der Digitaltechnik und der Informatik. Diese Maßeinheit wird zum Beispiel oft genutzt, um anzugeben, wie groß eine Datei ist. So wie 1 Meter aus 100 Zentimetern besteht, besteht 1 Byte aus 8 Bit. Die weiteren Einheiten sind dann: 1024 Byte = 1 Kilobyte 1024 Kilobyte = 1 Megabyte 1024 Megabyte = 1 Gigabyte 1024 Gigabyte = 1 Terabyte
Cache	Bezeichnet einen Zwischen- oder Pufferspeicher, der Daten schneller zur Bearbeitung bereitstellt, zum Beispiel ein lokales Verzeichnis für beim Surfen im Internet besuchte Seiten, die so nicht neuerlich geladen werden müssen.
Changelog	„Änderungsprotokoll“. Dient zur Dokumentation von Veränderungen an einem Projekt, einer Website oder einer Software.
Chat/Chatten	Über bestimmte Programme oder auf bestimmten Internetseiten ist mit dem Chat eine schnelle, direkte Kommunikation in Echtzeit möglich. Die Kommunikation kann unter anderem aus Bildern, Texten oder auch aufgenommenen Audionachrichten (Sprachnachrichten) bestehen. Das Programm bzw. Dialogfeld ist der Chat, während das Austauschen der Nachrichten als chatten, zu Deutsch plaudern, sich unterhalten, bezeichnet wird.

Chatbot	Ein Programm, das anstatt eines Menschen im Chat antwortet. Chatbots werden im Kundenservice eingesetzt.
CHIP (das Magazin)	Ein Magazin, das sich rund um Technik, Computer, neue Programmedazugehörigen News sowie Testberichte dreht.
Chipkarte	Meist eine Plastikkarte, die einen Chip mit verschiedenen Funktionen enthält. Der Chip kann als Speichermedium dienen, das dann beschrieben oder ausgelesen wird (zum Beispiel bei Telefon- oder Zahlungskarten), oder auch selbst Daten verarbeiten.
Click & Collect/ Pick-up	Beschreibt den Vorgang, etwas im Internet zu bestellen, es jedoch vor Ort oder an einem ausgewählten Ort abzuholen, statt es nach Hause geliefert zu bekommen.
Cloud/ Cloud-Server	Cloud Computing kann als „Rechenleistung aus der Wolke“ verstanden werden. Die Wolke (Cloud) ist dabei ein bildlicher Ausdruck für Rechenzentren, die mit dem Internet verbunden sind. Dabei wird nicht mehr auf die Rechenleistung oder den Speicher der eigenen Geräte zurückgegriffen, sondern die Rechenleistung eines Cloud-Anbieters genutzt. Hierbei können Daten wie zum Beispiel Bilder zusätzlich in der Cloud statt nur auf dem Handy gespeichert werden.
Cluster	Gruppe oder Bündel.
Code	Eine Menge von Zeichen, die für eine andere Menge von Zeichen steht; Sprache.
Cookie	Zeichenfolge, die mit einer Website vom Server geladen werden kann und bei einer erneuten Anfrage an den Server mitgesendet wird. Sinn ist unter anderem, Besucher:innen wiederzuerkennen, sodass es beispielsweise nicht erforderlich ist, die Daten der Nutzer:innen neu einzugeben.
CSS	Cascading Style Sheets. Mit Formatvorlagen in dieser Sprache können Webseiten farblich, typografisch usw. gestaltet werden. Es handelt sich nicht um eine Programmiersprache in engerem Sinn.
Cursor	„Mauszeiger“. Markiert die aktuelle Position auf dem Bildschirm und zeigt, wo als Nächstes eine neue Eingabe erscheint. Beim Schreibprogramm Word wird der Cursor als blinkender Strich angezeigt. Der Cursor wird fast immer mit der Maus bedient.

Custom-ROM	Alternatives Betriebssystem für Android (zum Beispiel das Betriebssystem von Samsung). ROM steht für „Read-Only Memory“ (Nur-Lese-Speicher), also nur die vorhandenen Daten werden abgerufen. Bei Custom-ROMs können die Daten jedoch verändert werden.
Cyber-grooming	Bezeichnet die Kontaktaufnahme von Erwachsenen zu Kindern und Jugendlichen über das Internet mit dem Ziel, sexuelle Handlungen oder Kontakte anzubahnen.
Cyber-mobbing	Steht für verschiedene Formen der Diffamierung, Belästigung, Bedrängung und Nötigung anderer Menschen oder Firmen über das Internet. Das Opfer wird durch aggressive oder beleidigende Texte, kompromittierende Fotos oder Videos angegriffen oder der Lächerlichkeit ausgesetzt.
Cyber-stalking	Bezeichnet das Nachstellen, Verfolgen und auch Überwachen einer Person mit digitalen Hilfsmitteln (auch Digital Stalking oder Onlinestalking). Dies geschieht insbesondere in Beziehungen, beispielsweise überwacht ein Partner seinen aktuellen Partner oder Ex-Partner.
Darknet	„Anonymes Netz“. Versteckter Teil des Internets, der nicht über herkömmliche Browser zugänglich ist. Man benötigt eine bestimmte Software, um anonym zu bleiben. In diesem Teil des Netzes bewegen sich beispielsweise Menschen, die etwas zu verbergen haben, (in ihrem Land) verbotene Sachverhalte einsehen wollen oder geheime Informationen austauschen.
Data Science	Die „Datenwissenschaft“ beschäftigt sich mit der Gewinnung von Wissen aus Rohdaten.
Datenleak	„Datenleck“. Bei einem Datenleak geraten Daten in falsche Hände. Cyberkriminelle können über eine kompromittierte Website an diese Daten kommen oder über eine Panne, bei der ein Unternehmen die sensiblen Daten ungeschützt aufbewahrt. Teilweise werden die sensiblen Daten dann auch veröffentlicht.
Desktop	Bezeichnet einerseits das Gehäuse/den Bildschirm des Computers, der auf einem Tisch steht, andererseits versteht man darunter auch die grafische Oberfläche des Betriebssystems, die auf dem Bildschirm dargestellt wird.

Digital Detox	„Digitale Entgiftung“. Bezeichnet die psychisch-mentale Entgiftung eines Menschen, indem digitale Geräte und Medien für einen gewissen Zeitraum deutlich weniger oder gar nicht verwendet werden, um der realen Welt mehr Aufmerksamkeit zu schenken.
digitale Assistenten	Diese Geräte können Sprache analysieren und auf gesprochene Anweisungen reagieren.
DoS-/ DDoS-Angriffe	„Denial of Service“(DoS)-Angriffe richten sich gegen die Verfügbarkeit von Diensten, Websites, einzelnen Systemen oder ganzen Netzen. Wird ein solcher Angriff mittels mehrerer Systeme parallel ausgeführt, spricht man von einem verteilten DoS- oder „Distributed Denial of Service“(DDoS)-Angriff. DDoS-Angriffe erfolgen häufig durch eine sehr große Anzahl von Computern oder Servern.
Download	Datenübertragung (Herunterladen) von einem fremden Rechner auf den eigenen Rechner, zum Beispiel die aktuelle Version des eigenen Browsers aus dem Internet oder eine neue App aus dem App Store.
Download-rate	Geschwindigkeit, mit der Daten empfangen werden können. Das beeinflusst also auch, wie schnell sich Websites öffnen, Videos laden oder Spiele spielen lassen.
Doxxing	Täter:innen sammeln personenbezogene Daten, die sie bündeln und öffentlich verfügbar machen.
Data Science	Die „Datenwissenschaft“ beschäftigt sich mit der Gewinnung von Wissen aus Rohdaten.
Echokammer-Effekt	Beschreibt das Phänomen, dass viele Menschen dazu neigen, sich zum größten Teil mit Gleichgesinnten zu umgeben, um die eigene Meinung zu verschiedenen Themen bestätigt zu bekommen. Es findet kaum noch Reflexion statt und Meinungen können sich radikalieren.
E-Mail	„Electronic Mail“ (elektronischer Brief). Damit können schriftliche Nachrichten und digitale Daten an einen ausgewählten Empfänger schnell und bequem versendet werden.
Ende-zu-Ende-Ver-schlüsselung	Verschlüsselung von Daten, die ausschließlich von den Kommunikationspartnern und nicht von Dritten entschlüsselt bzw. gelesen werden können.

Endgerät	Elektronisches Gerät, das physisch (durch einen Steckverbinder) oder nicht physisch (zum Beispiel per Funk) über einen Netzanschluss an ein Daten- oder Telekommunikationsnetzwerk angeschlossen ist. Dazu gehören beispielsweise Computer, Laptops, Smartphones, Tablets oder Telefonanlagen
externe Festplatte	Auf einer Festplatte werden alle Daten gespeichert, egal ob Dokumente, Fotos oder Videos. Normalerweise sind Festplatten fest verbaut, aber es gibt auch externe Festplatten. Diese lassen sich beispielsweise per Kabel mit dem Computer verbinden, damit dort Daten gespeichert werden können.
Fake News	„Falschmeldungen“. Werden teils irrtümlich, teils bewusst im Internet verbreitet, insbesondere in den sozialen Medien.
Fake Shops	„Gefälschte Onlineshops“, hinter denen sich Betrüger:innen verbergen. Nach Erhalt der Bezahlung wird keine Ware ausgeliefert.
Features	Steht für das Wort „Eigenschaft“. Verschiedene Apps können Features haben, zum Beispiel einen neuen Button für Sprachaufnahmen.
Feed	Ein Feed (etwa „füttern“, „einspeisen“) ist eine Art strukturierter Fluss von Neuigkeiten. Auf einer Nachrichtenwebsite sieht man die Headlines (Schlagzeilen) als Erstes, oft kann man jedoch auch nach unten scrollen. Die hier folgenden Nachrichten bilden den Feed. Auch in sozialen Netzwerken findet man oft einen Feed, meist ist dieser chronologisch oder benutzerdefiniert geordnet. Einen Feed musst du abonnieren.
Filterblase	Beschreibt einen Effekt aus den Medienwissenschaften. Weil Websites oder soziale Netzwerke versuchen, algorithmisch vorauszusagen, welche Informationen Benutzer:innen auffinden möchten, werden vermehrt Inhalte gezeigt, die der eigenen Meinung entsprechen. So werden Leser:innen nicht mehr mit Informationen konfrontiert, die den bisherigen Ansichten widersprechen. Auf diese Weise können die eigenen Auffassungen auch nicht mehr überprüft und eventuell relativiert werden.
Finder	Suchleiste auf einer Website oder in einem Programm

Firewall	Besteht aus Hard- und Software, die den Datenfluss zwischen dem internen und externen Netzwerk kontrolliert. Alle Daten, die das Netz verlassen oder hinein wollen, können überprüft werden
Firmware-Update	Updates, das heißt Aktualisierungen, die nicht nur einzelne Programme mit Verbesserungen versorgen, sondern das Software-Grundgerüst eines Geräts verbessern. Dies betrifft neben PCs oder Smartphones auch Fernseher und Drucker.
Flatrate	„Pauschale“ oder „Pauschaltarif“. Eine Flatrate kann bei verschiedenen Anbietern erworben werden. Hierbei bezahlt man einen im Voraus festgelegten Betrag und hat im Gegenzug ein bestimmtes Datenkontingent zu Verfügung. Ein Beispiel wären Telefonanbieter, die eine gewisse Anzahl an Freiminuten für Auslandstelefonate zur Verfügung stellen.
Flugmodus	Einstellung eines Endgeräts, zum Beispiel eines Mobiltelefons oder Tablets, bei dem die drahtlosen Verbindungen und Kommunikationsmöglichkeiten deaktiviert werden. Andere Funktionen werden jedoch nicht beeinflusst. Der Flugmodus ist beispielsweise immer in einem Flugzeug zu aktivieren.
Follower	Als Follower kann man sich selbst bezeichnen oder diejenigen Personen, die einer anderen Person auf sozialen Plattformen folgen. Wenn du auf einer sozialen Plattform, beispielsweise bei Instagram, ein Profil siehst, welches Bilder postet, die dir gefallen, kannst du diesem Profil bzw. dieser Person folgen (abonnieren) und zum Follower werden. Oder umgekehrt: Die Nutzer:innen, die dir folgen, sind dann deine Follower.
Formatierung	Das Zurücksetzen eines Datenträger - zum Beispiel einer Festplatte - in den Zustand, in dem er zum ersten Mal verwendet wurde. Dadurch lässt sich Schadsoftware bereinigen oder auch die Leistung verbessern. Oft beinhaltet das, dass die Daten (Fotos, Videos, Internetverläufe, usw.) eines Computers gelöscht werden.
Fritz!Box	Produktbezeichnung für eine Routerreihe. Die Router eignen sich für verschiedene Internetanschlüsse wie zum Beispiel DSL, Kabel, Glasfaser oder LTE.

FTP	„File Transfer Protocol“. Übertragungsprotokoll, welches alle möglichen Dateien zwischen Computern im Internet oder anderen Netzwerken übermittelt. Es können aber auch Dateien aus dem Internet auf den eigenen Computer heruntergeladen werden.
Funkzelle	Räumlich begrenzter Bereich, in dem Signale von Endgeräten ankommen und teils entschlüsselt werden.
Gesichts-entsperrung	Nur wenn das Gerät dein Gesicht erkennt, wird es entsperrt und benutzbar.
Go	Ein sehr komplexes Brettspiel für zwei Personen. Ähnlich wie beim Schach wird mit schwarzen und weißen Steinen gespielt.
GPS	„Global Positioning System“. Es handelt sich um ein globales Navigationssatellitensystem, mit welchem Positionen bestimmt werden können. Dient als Hilfsmittel zur exakteren Navigation oder Ortsbestimmung.
Hardware	Umfasst alle physisch greifbaren Teile, die einen Computer funktionsfähig machen. Hierzu gehören unter anderem das Gehäuse, der Prozessor, die Hauptplatine, der Monitor, die Tastatur, die Grafikkarte oder die Festplatte.
Hashtag (#)	Schlagwörter oder Wortketten, welche mit einer Raute (#) davor gekennzeichnet werden. Der hochgeladene Beitrag wird automatisch mit dem genutzten Hashtag verknüpft und kann, wie auch andere Beiträge, die diesen Hashtag genutzt haben, unter dem Hashtag gefunden werden. Hierzu kann man den Hashtag selbst anklicken oder ihn in einer Suchleiste eingeben.
Hoax	Bedeutet „Gerücht“, „Scherz“, „Schwindel“. Bezeichnet eine Falschmeldung, die über E-Mail, Messenger-Programme, SMS oder MMS verbreitet wird
Homepage	Erste Seite, die als Startseite für eine Website fungiert. Von der Homepage aus können alle anderen Teile bzw. Inhalte der Website aufgerufen werden. Manchmal wird auch die gesamte Website, zum Beispiel eines Unternehmens, als Homepage bezeichnet.

Homescreen	Wird meist in Bezug auf Smartphones verwendet und meint den Bildschirm, der zu sehen ist, wenn das Handy angeschaltet oder entsperrt wird. Hier finden sich auch verschiedene Apps oder eine Zeitanzeige. Je nach individueller Anpassung der Nutzer:innen unterscheidet sich das Aussehen des Homescreens.
HTML	„Hypertext Markup Language“. Auszeichnungssprache im Internet. Mittels HTML werden die Strukturen und der Aufbau von Websites festgelegt, zum Beispiel wie die Schrift aussieht oder wo genau ein Textblock positioniert ist. Es handelt sich nicht um eine Programmiersprache in engerem Sinn.
http	„Hypertext Transfer Protocol“. Bezeichnet ein Übertragungsprotokoll für Websites.
https	„Hypertext Transfer Protocol over SSL“. Bezeichnet ein Protokoll zur verschlüsselten Übertragung von Websites.
IDE	Integrated Development Environment. Deutsch: „integrierte Entwicklungsumgebung“. Diese Programme erleichtern das Programmieren z. B. durch farbliche Hervorhebung von Wörtern, automatische Fehlererkennung, Formatierung, Kompilierung u. v. m.
IMAP	„Internet Message Access Protocol“. Protokoll für den Zugriff auf E-Mail-Programme wie zum Beispiel Microsoft Outlook. Anhand des Protokolls können E-Mails empfangen und versendet, Ordner angelegt oder bestimmte E-Mails und/oder Anhänge im Postfach gesucht werden. IMAP benötigt dauerhafte Verbindung zu einem Server.
Input Layer	Eingabeschicht(en)
Instagram	Soziales Netzwerk zum Teilen von Fotos und Videos.
Internetfernsehen	Übertragung von Programmen über das Internet. Allerdings gehören abrufbare Programme wie in einer Mediathek nicht dazu, auch wenn sie sich auf derselben Plattform befinden.
IoT	„Internet of Things“ („Internet der Dinge“). System von Maschinen, Anlagen und Geräten, die über das Internet miteinander verbunden sind. Unter anderem wird IoT auch als Sammelbegriff für globale Technologie verwendet. Diese ermöglicht es, physische und virtuelle Objekte miteinander zu verbinden und zu teilen.

IP-Adresse	Adresse, unter der ein Rechner innerhalb eines Netzwerks nach dem Internetprotokoll (IP) identifiziert wird. Eine IP-Adresse ist eine Zeichenreihe und besteht aus vier Teilen, die durch Punkte getrennt sind, zum Beispiel 194.95.179.205.
Junk/Junk-Mail	„Abfall-Mail“. Als Junk-Mails werden Massenmails bezeichnet, die einem Empfänger ungewollt zugestellt werden und meistens Werbeangebote enthalten.
KI	„Künstliche Intelligenz“. Maschinen erlernen menschenähnliches intelligentes Verhalten. Der Computer lernt hierbei aus Erfahrungen und Daten, um Aufgaben immer besser auszuführen.
Kipppunkt	Punkt, an dem eine Entwicklung abbricht, die Richtung wechselt oder stark beschleunigt wird. Das Wort wird häufig in Zusammenhang mit dem Klimawandel gebraucht. Manche Kipppunkte haben Wirkungen, die sich nicht mehr umkehren lassen.
Komprimieren	Die Anzahl der Bits die für die Darstellung von Dateien benötigt werden, werden reduziert. Durch die Komprimierung (Verdichtung) einer Datei wird Speicher gespart und Übertragungen können beschleunigt werden. Wird beispielsweise ein Bild komprimiert, so ist die Auflösung bzw. Qualität des Bildes nicht mehr so gut wie zuvor.
Konfigurieren	Ein Programm und/oder Hardwarebestandteile eines Systems werden neu angepasst, konfiguriert. Auch das vorhandene System selbst kann hierbei angepasst und erneuert werden.
Kryptowährungen	Digitale Währungen mit einem abgesicherten Zahlungssystem, jedoch unabhängig und ohne Aufsicht oder Mitwirkung von Banken und Behörden. Kryptowährungen werden zunehmend zu Zahlungsalternativen unter Privatpersonen. Das wohl bekannteste Beispiel für eine Kryptowährung ist Bitcoin.
LAN	„Local Area Network“ (lokales oder örtliches Netzwerk). So wird beispielsweise das hausinterne Netz eines Unternehmens genannt.
Latenz	Reaktionszeit zwischen einem Ereignis und der eigentlichen eintretenden Reaktion. In der digitalen Welt ist das die Länge, also sozusagen der Weg, welchen die Daten zurücklegen.

Lesezeichen	Lesezeichen, Bookmarks oder auch Favoriten sind Links oder Websites, die in einer Art Sammlung vom Nutzer:innen in ihrem Browser abgespeichert werden können. Durch das gesetzte Lesezeichen können die Websites schnell und einfach wiedergefunden und direkt geöffnet werden. Meist muss man zum Setzen des Lesezeichens nur in der Adresszeile auf den kleinen Stern rechts klicken.
Likes	In den meisten sozialen Netzwerken können die Beiträge mit einem Like (vom Englischen „to like“ für „mögen/gefallen“) markiert werden, um zu zeigen, dass einem etwas gefällt oder man es unterstützt. Dafür gibt es meist einen kleinen Button unter dem Beitrag, zum Beispiel in Form eines Daumens nach oben (Facebook, YouTube) oder auch eines Herzens (Instagram).
Link/Hyperlink	Querverweis mit der Adresse einer Website oder zu einem anderen elektronischen Dokument.
Livestream	Beinhaltet in Echtzeit und über das Internet übertragene Audio- und/oder Videodaten. Beispielsweise kann man Fußballspiele im Internet über einen Livestream sehen statt auf dem Fernseher. Aber auch in sozialen Netzwerken gibt es Livestreams. Hierbei gehen zum Beispiel bekannte Persönlichkeiten live (über eine Funktion des sozialen Netzwerks) und unterhalten sich mit Fans, die unter anderem während des Livestreams Fragen stellen können, welche dann in Echtzeit beantwortet werden.
Login	„Einloggen“. Anmeldevorgang für die Nutzung eines PC, von auf dem PC installierten Programmen oder von Onlinediensten, wie zum Beispiel Nutzerkonten für Onlineshops.
LTE	„Long Term Evolution“ („Langzeitevolution“). Bezeichnung für den Mobilfunkstandard der dritten Generation (3G), mit dem die Datenrate, Kapazität und Intelligenz des Netzes verbessert wurden. Er wird seit 2019 immer mehr durch 5G abgelöst.

Mail-Client/ E-Mail- Programm	Programm, mit dem E-Mails gelesen, geschrieben, versendet und empfangen werden. E-Mail-Programme werden oft kostenlos angeboten. Die dafür benötigte Software kann man auf den Computer laden und auch als Symbol auf dem Bildschirm anzeigen lassen. Mail-Clients sind zum Beispiel Microsoft Outlook oder Thunderbird von Mozilla. Im Gegensatz dazu steht die Webmail, die über den Browser, sozusagen im Internet selbst, verwaltet wird. Hierzu gehören zum Beispiel Gmail, GMX oder Web.de.
Mailen	Bezeichnet den Vorgang, bei dem E-Mails hin und her geschickt werden oder bei dem man selbst eine E-Mail an eine Person verschickt. Man mails jemandem also eine Information.
Major-Update	Hauptaktualisierung einer Software. Hierbei gibt es umfangreiche Neuerungen, die auf das Endgerät geladen werden. Beispielsweise muss beim Handy hin und wieder ein Major-Update ausgeführt werden, damit es auf dem neuesten Stand bleibt.
Malware	Zusammensetzung aus dem englischen „malicious“ (böartig) und „ware“ (von Software). Schädliches Programm oder auch Schadsoftware. Diese Programme wurden entwickelt, um schädigende und unerwünschte Funktionen auf dem Endgerät auszuführen.
Marketing	Ausrichtung von Unternehmen auf die Bedürfnisse, die der Markt entwickelt. Hierbei ist eine der wichtigsten und größten Herausforderungen, Marktveränderungen und Bedürfnisverschiebungen so schnell wie möglich zu erkennen, um rechtzeitig Wettbewerbsvorteile aufzubauen.
Mediathek	Die Mediathek ähnelt einer Online-Bibliothek für Videos. Es handelt sich um ein Onlineportal, in welchem Fernsehsender einzelne Programme oder Inhalte als Livestream oder Video zur Verfügung stellen. Die Inhalte können bei bestehender Internetverbindung über den Internetbrowser auf dem PC oder auch über Apps auf dem Handy abgerufen werden.
Messenger (Instant Messenger)	Instant Messaging bedeutet „sofortige Nachrichtenübermittlung“. Ein Messenger ist ein Service für Onlinechats und das Versenden kurzer Nachrichten. Dabei ist vorab keine Verabredung nötig – die Anwesenheit von Gesprächspartner:innen wird automatisch signalisiert.

Meta/ Facebook	Facebook, jetzt Meta genannt, ist eines der bekanntesten sozialen Netzwerke der Welt. Hier erstellen Personen ein virtuelles Profil und können sich mit anderen Nutzer:innen vernetzen, chatten, Gruppen beitreten oder Beiträge veröffentlichen (posten).
Mining	Bedeutet so viel wie Datensammlung. Es handelt sich hierbei um eine systematische Anwendung von computergestützten Methoden. Diese sind dafür da, Trends und Muster zu erkennen und Zusammenhänge zu schaffen.
Mobiles Disen-rollment	Ermöglicht dem Handy oder Tablet im Internet zu surfen, ohne dabei im WLAN zu sein. Hierbei gelangt man über das Mobilfunknetz ins Internet und ist nicht an einen Standort gebunden. Das Handy schaltet meist von allein von WLAN zu Mobile Daten, wenn die Verbindung zum WLAN unterbrochen ist. Aber: Man hat nur eine begrenzte Menge an Daten zur Verfügung, je nach abgeschlossenem Tarif. Ist die laut Vertrag vereinbarte Menge aufgebraucht, wird das Internet deutlich langsamer.
Mobiles Internet	Beschreibt die Internetnutzung auf Endgeräten, unabhängig davon, ob eine (W)LAN-Verbindung besteht oder ein anderes mobiles Netz genutzt wird.
Mobiles Netz	Das mobile Netz ist eine Verbindung zum Internet, die auch ohne Router und (W)LAN möglich ist. Mithilfe von Funkmasten lässt sich in Deutschland fast überall lückenlos mit einem Handy oder Tablet auf das mobile Netz zugreifen.
Modder	Hobby-Programmierer, die zum Beispiel ein Computerspiel oder ein Programm modifizieren, also verändern. Der Prozess des Veränderns wird Modding genannt.
MOOC	Massive Open Online Course. Deutsch: „riesiger offener Onlinekurs“. Lern- bzw. Bildungsangebot im Web mit sehr hoher möglicher Teilnehmerzahl.
NAS	„Network Attached Storage“. Speicher, der mit dem Netzwerk verbunden ist. Sobald das Netzwerk eingerichtet ist, erscheint das Laufwerk auf dem Computer und kann genauso genutzt werden wie eine vorher eingebaute Festplatte oder Laufwerke, die direkt am Rechner angeschlossen sind.
Network Slices	Eigenschaft von 5G-Netzen. Hierbei wird beispielsweise das WLAN zu Hause manuell unterteilt bzw. in Scheiben geteilt.

Netzwerkkarte	Schnittstelle zum Austausch von Daten zwischen einem Computer und einem lokalen Netzwerk
Netzwerkname	Auch SSID („Service Set Identifier“). Der Netzwerkname ist eine Zeichenfolge, die ein drahtloses lokales Netzwerk (WLAN) benennt. Dieser kann von den Nutzer:innen angepasst werden.
Neuronale Netze	Biologie: Geflecht aus verbundenen Neuronen, die Teil eines Nervensystems sind. Informatik: Von biologischen Nervensystemen inspirierte Art der Informationsverarbeitung.
News-Feed	Bezeichnet die strukturierte Vermittlung bzw. Darstellung von neuen Nachrichten, Informationen und Blogbeiträgen (oft chronologisch oder benutzerdefiniert) auf einer Website oder einer App.
Newsletter	Elektronischer, regelmäßig erscheinender „Rundbrief“. Dieser wird üblicherweise von Vereinen, Verbänden, Shops und Unternehmen herausgegeben, um ihre Mitglieder, Kunden oder Mitarbeiter über Neuigkeiten zu informieren und die Reichweite zu erhöhen.
NFC	„Near Field Communication“ („Nahfeldkommunikation“). Internationaler Übertragungsstandard für drahtlose Verbindungen über kurze Distanzen und ermöglicht unter anderem das kontaktlose Bezahlen. Durch die NFC ist es möglich, auf sehr kurze Distanz kleine Datenmengen zu übertragen. Dazu zählen Zugangs- und Bezahl-daten oder Datenpakete, die beispielsweise Passwörter oder andere Codes enthalten.
Nutzer-generiert/ User Generated	Bezieht sich auf die Inhalte auf digitalen Plattformen, die von anderen Nutzer:innen erstellt und zur Verfügung gestellt wurden. Dazu gehören unter anderem Kommentare, Artikel, Bilder oder auch Videos, welche die eigene Meinung widerspiegeln.
Online-banking	Bankgeschäfte (zum Beispiel Überweisungen), die über das Internet erledigt werden.
Online-shopping	Einkauf von Produkten und Diensten über das Internet.

Open Source/ Open-Source- Plattformen	„Offene Quelle“. Der Programmcode von Open-Source-Software ist öffentlich einsehbar und kann – mit entsprechenden Kenntnissen – verändert werden.
Open-Source- Prinzip	Der Begriff „Open Source“ („offene Quelle“) lässt sich auf Open-Source-Software zurückführen. Hierbei handelt es sich um einen Code, der für alle zugänglich ist. Man darf die Programme selbst bearbeiten und an die eigenen Bedürfnisse anpassen, sofern die nötigen Programmierkenntnisse vorhanden sind, und das meist kostenlos. Beispiele hierfür sind Firefox, GIMP oder Open Office.
Output Layer	Ausgabeschicht(en)
Passwort- manager	Programm, beispielsweise als Bestandteil eines Internetbrowsers, das bei der Verwaltung von Passwörtern hilft und diese archiviert. Es unterstützt dabei, für jeden Dienst ein separates Passwort zu nutzen.
Patch	„Flicken“. Softwarepaket, mit dem Softwarehersteller Sicherheitslücken in ihren Programmen schließen oder andere Verbesserungen integrieren.
Patch- Management	Bezeichnet Prozesse und Verfahren, die helfen, verfügbare Patches für die IT-Umgebung möglichst rasch erhalten, verwalten und einspielen zu können.
Persönlich- keitsrecht	Persönlichkeitsrechte umfassen zahlreiche staatliche Regelungen zum Schutz vor Eingriffen in die Privatsphäre von Menschen. Dazu zählen vor allem Rechte zum Schutz persönlicher Daten wie zum Beispiel E-Mail-Adressen, Wohnschriften oder Passwörter. Persönlichkeitsrechte beruhen auf dem Schutz der freien Entfaltung der Persönlichkeit (Art. 2 des Grundgesetzes).
PGP	„Pretty Good Privacy“ („ziemlich gute Privatsphäre“). Programm zum Verschlüsseln und zur Signatur (Unterschreiben) von Daten. Es gibt entweder einen „öffentlichen Schlüssel“, mit dem jeder die Daten für die Empfänger:innen verschlüsseln bzw. öffnen und deren Signaturen prüfen kann, oder es gibt einen „privaten Schlüssel“. Den „privaten Schlüssel“ besitzen nur Empfänger:innen oder er ist passwortgeschützt. Somit wird sichergestellt, dass nur sie Zugriff auf die Daten bekommen.

Phishing	Zusammensetzung aus „Password“ und „Fishing“, zu Deutsch „nach Passwörtern angeln“. Beim Phishing wird zum Beispiel mittels gefälschter E-Mails und/oder Websites versucht, Zugangsdaten für einen Dienst oder eine Website zu erlangen.
Pipe-Operator	Folgendes Symbol: . Hierfür werden bei Windows die Tasten „Alt Gr + “ (das Symbol links neben „y“) oder „alt + strg + “ verwendet und bei iOS 2alt + 7“.
Plattform	Eine digitale Plattform stellt eine Schnittstelle zwischen Unternehmen und Kunden, Partnern und Mitarbeitern oder auch Nutzer:innen dar. Auf dieser Plattform kann interagiert werden; je mehr Nutzer:innen die Plattform verwenden, umso nützlicher ist sie.
Plug-in	Optionale Zusatzsoftware oder Softwaremodul, das in ein Computerprogramm eingebunden werden kann, um dessen Funktionalität zu erweitern.
Podcast	Sammlungen einzelner Audio- und Videobeiträge, die über das Internet verfügbar sind. Meist sind diese Beiträge unterteilt in einzelne Episoden, die sich auf verschiedene Themenbereiche beziehen. Zum Beispiel kann eine Person einen Podcast produzieren und ihn „Geschäftswelt“ nennen. Der Podcast wird dann verschiedene Episoden (Audiodateien) zum Thema „Geschäftswelt“ enthalten, die sich die Nutzer:innen anhören können. Wenn der Podcast gefällt, kann er auch abonniert werden.
POP3	Das „Post Office Protocol“ (POP) ist ein Kommunikationsprotokoll, über welches ein Client E-Mails abrufen kann.
Pop-up-Fenster	Erscheint meist „plötzlich“ auf dem Bildschirm. In diesen Pop-up-Fenstern werden zusätzliche Inhalte angezeigt oder andere Interaktionen angeboten.
Portable Software	Anwendungssoftware, die beispielsweise auf einem USB-Stick oder einem ähnlichen Träger gespeichert ist. Die Software muss beim Verwenden des USB-Sticks nicht auf dem Hauptgerät installiert werden, kann eigenständig auf dem USB-Stick funktionieren und Daten sowie Einstellungen speichern.

Posten	Bezieht sich auf alles, was man selbst auf einer Onlineplattform hochlädt („abschickt“). Dazu gehören zum Beispiel Kommentare, Bilder, Videos oder auch Blogs.
Powerline-Adapter	Powerline sorgt dafür, dass eine Datenübertragung über elektrische Leitungen in einem bestimmten Netz ermöglicht wird. Der Adapter wird mit einer Steckdose und über ein LAN-Kabel mit dem Router verbunden. Das digitale Eingangssignal wird in ein analoges Signal umgewandelt und über das Stromnetz zu den anderen Steckdosen in der Wohnung geleitet. Dort wird es dann wieder in ein digitales Signal umgewandelt.
Prepaid-Karte	Ein festgelegtes Guthaben wird auf die Prepaid-Karte („Guthabekarte“) geladen, um zu telefonieren, SMS zu schreiben und im Internet surfen zu können. Alternative zu vertragsgebundenen Handy-Flatrates, bei denen die Kunden einen monatlichen Festpreis bezahlen.
Provider	Allgemein handelt es sich hierbei um einen „Anbieter“, der dem Verbrauchenden beispielsweise einen Telefon-, Internet- oder Mobilfunkanschluss zur Verfügung stellt. Diese nennt man daher Internet- oder Mobilfunk-Provider. Hierzu gehören zum Beispiel T-Online oder Vodafone.
Proxyserver	Arbeitet als ein Vermittler innerhalb eines Netzwerks, der zwischen Nutzer:innen und Netzwerk (zum Beispiel einer Website) eingesetzt wird. Ein Proxyserver kann beispielsweise die Kommunikation zwischen Nutzer:innen und Netzwerk sichern, beschleunigen oder verschleiern.
Prozessor	Schaltkreis auf einem Chip, der andere Schaltungen steuert und dabei einen Algorithmus vorantreibt. Jeder Computer und jedes Smartphone besitzt Prozessoren.
Push-Benachrichtigung	Benachrichtigungen von Apps, die auf dem Handybildschirm (meist Sperrbildschirm) oder in der Benachrichtigungsleiste erscheinen. WhatsApp vermerkt dadurch beispielsweise den Eingang einer neuen Nachricht.
Quellcode	In einer speziellen Programmiersprache geschriebener und für Menschen lesbarer Text. Dieser Text gibt Computern exakte Vorgaben und Regeln, die dann in Maschinensprache übersetzt werden und daraufhin die Grundlage für Websites oder Programme bilden.

QR-Code	Ein aus Punkten zusammengesetztes Quadrat, das elektronisch lesbar ist und von Geräten wie dem Smartphone oder dem Tablet eingescannt werden kann. Bei den dabei übermittelten Daten handelt es sich meist um Webadressen, Werbetexte oder SMS. QR-Codes spielen vor allem in der Marketingwelt eine Rolle.
Ranking	Rangordnung bzw. Reihenfolge von vergleichbaren Objekten, Situationen etc.
Ransomware	Schadprogramme, die den Zugriff auf Daten und Systeme einschränken oder verhindern und diese Ressourcen nur gegen Zahlung eines Lösegeldes (englisch „ransom“) wieder freigeben.
Repeater	Element eines Netzwerks, das Signale empfängt, aufbereitet und dann verstärkt. Beispielsweise kann so das W-LAN-Signal verstärkt werden und ist in einer größeren Reichweite verfügbar.
Roaming	Wechsel eines mobilen Geräts (meist das Smartphone) vom Mobilfunknetz des eigenen Anbieters in das Netzwerk eines anderen Betreibers. Dies kann national wie auch international stattfinden. Bei der Nutzung von internationalen Netzen können Roaminggebühren anfallen.
Router	Verbindet das Heimnetzwerk und das Internet. Der Router bildet den Knotenpunkt für die Kommunikation der internetfähigen Geräte und verbindet neben dem Computer auch den smarten Fernseher und teilweise die intelligente Haustechnik mit dem Internet.
RSS-Feed	RSS steht für „Really Simple Syndication“ („sehr einfache Verbreitung“) und beschreibt Dateiformate für Inhalte auf verschiedenen Websites. Beispielsweise zeigen sie die Änderungen, in diesem Fall Neuigkeiten, auf einer News-Seite an. Jedoch wird hier nur die Struktur der Inhalte beachtet, nicht aber das Layout oder sonstige Zusätze. Einen RSS-Feed musst du abonnieren.
Scam	Bedeutet wörtlich übersetzt „Betrug“, in der Kriminologie auch „Vorschussbetrug“, weil es meistens darum geht, dass die Opfer in Vorkasse gehen und den Betrügern Geld senden sollen.

Schadprogramme	Auch Schadfunktion, Schadsoftware oder Malware. Schadprogramme bezeichnen Software, die entwickelt wurde, um unerwünschte und schädliche Funktionen auszuführen.
Screenshot	Eine Art „Foto“ oder Abbild dessen, was auf dem Bildschirm zu sehen ist, das heißt eine Bildaufnahme des Bildschirms. So können beispielsweise Fehlermeldungen auf dem Bildschirm gescreenshotet werden, um sich damit an den Support zu wenden oder sie vor Ort als Foto vorzuzeigen.
Selfie	Foto in der Art eines Selbstporträts, das man fast immer mit dem Handy von sich selbst, meist nur seinem Gesicht, mithilfe der Innenkamera am Handy macht.
SEO	SEO steht für Search Engine Optimization (Suchmaschinenoptimierung). Mithilfe relevanter Begriffe, die im Backend einer Website hinterlegt werden, können die Suchmaschinen die Seite schließlich leichter finden und bei den Suchergebnissen anbieten.
SERPs	„Search Engine Result Pages“ („Suchergebnisseiten“). Hierbei handelt es sich um die Websites, die angezeigt werden, nachdem ein Schlagwort in Suchmaschinen wie Google oder Yahoo eingegeben wurde.
Server	Typischerweise bezeichnet Server einen Rechner, der seine Ressourcen anderen Rechnern zugänglich macht. Auf diesem Server laufen wiederum Serverprogramme wie z. B. Web- oder E-Mail-Server. Das Wort hat also einen doppelten Sinn: Hardware und Software.
Shared Medium	Damit ist eine schwächere Verbindungsqualität bei vielen Personen an einem Ort gemeint. Jeder Sendemast hat nur eine begrenzte Kapazität, die sich alle gleichzeitig auf das Netz zugreifende Nutzer:innen teilen. Das bedeutet: Je mehr Geräte in derselben Funkzelle sind, desto langsamer wird die Verbindung für jeden einzelnen.
Sicherheitsvoreinstellungen	Einstellungen bezüglich der eigenen Sicherheit, der des Gerätes, Programms oder des Angebots, die meist von den Herstellern vor der Benutzung festgelegt wurden, jedoch von den Nutzer:innen verändert werden können.

Signatur	Eine digitale Signatur (Unterschrift) besteht aus Daten in elektronischer Form. Die Signatur wird an andere elektronische Daten angehängt, um die Verfasser von Informationen klar zu identifizieren und zu belegen, dass die Daten nach dem Signieren nicht mehr verändert wurden. Zum Beispiel können Dokumente oder Programme signiert werden.
SIM-Karte	Chipkarte, die für den Betrieb des Mobiltelefons nötig ist und auf welcher persönliche Daten und eine Identifikationsnummer des Besitzers gespeichert sind.
Smart Home	Verbindet die verschiedenen Systeme im Eigenheim. Hierbei sollen die Wohn- und Lebensqualität sowie die Sicherheit erhöht werden. Dies geschieht, indem die Haushaltsgeräte beispielsweise mit einer App verbunden sind. Mit der App kann man dann zum Beispiel Jalousien schließen oder Licht ausschalten. Alle Geräte können technisch vernetzt werden.
Smartphone	Mobiltelefon mit Touchscreen („Berührungsbildschirm“) und umfangreichen computerähnlichen Funktionen und Verbindungsmöglichkeiten, auf dem sich, neben dem Telefonieren und Nachrichten versenden, zusätzliche Funktion wie GPS (Ortungsdienst) und Apps befinden.
Smartwatches	„Kluge Uhren“. Zeigen nicht nur die Zeit, sondern können zum Telefonieren und Versenden von Nachrichten genutzt werden.
SMTP	„Simple Mail Transfer Protocol“. Übertragungsprotokoll, welches zum Versenden von E-Mails verwendet wird. Verwalten oder abrufen kann man die E-Mails hiermit nicht.
Social Engineering	„Soziale Manipulation“. Bei Cyberangriffen durch Social Engineering versuchen Kriminelle ihre Opfer dazu zu verleiten, eigenständig Daten preiszugeben, Schutzmaßnahmen zu umgehen oder selbstständig Schadprogramme auf ihren Systemen zu installieren.
Social Login	Beim Social Login werden bereits vorhandene Konten für die Anmeldung bei einem anderen Anbieter in einem geschützten Bereich verwendet. Beispielsweise kann man sich mit seinem Google Account auch bei einer anderen App oder Website anmelden und muss nicht extra ein neues Nutzerkonto erstellen. Hierauf sollte man aus Datenschutzgründen wenn möglich verzichten.

Social Media	<p>Plattformen (oft Apps), die es den Nutzer:innen ermöglichen, sich im Internet miteinander zu vernetzen und zu kommunizieren. Hierbei geht es auch um das Teilen bzw. #das Veröffentlichen von medialen Inhalten wie Bildern oder Videos. Da alle Nutzer:innen ein eigenes Benutzerkonto haben, können sie mit diesem die geteilten Medien von anderen bewerten oder andere Nutzer:innen, deren Inhalte gefallen, abonnieren. Zu den beliebtesten Social-Media-Apps zählen momentan Instagram und TikTok.</p>
Software	<p>Software ist ein Sammelbegriff für Betriebssysteme, Anwendungs- und Dienstprogramme. Software kann zum einen für einen reibungslosen Ablauf der Computer sorgen, gleichzeitig auch Funktionen erfüllen, wie ein Routenplaner, ein Programm zum Schreiben oder ein Browser. Der Gegensatz zur Software ist die Hardware, die materiell existiert.</p>
Software-systeme	<p>Software, die aus mehreren Teilen besteht. Programme können etwa zahlreiche Unterprogramme, Erweiterungen, Hilfedateien für Anwender u. v. m. enthalten.</p>
Soziale Netzwerke	<p>Onlineplattformen, welche die Möglichkeit zum Informationsaustausch und Beziehungsaufbau bieten. Hierdurch entsteht eine Online-Community, die digital miteinander kommuniziert. Soziale Netzwerke sind zum Beispiel Instagram (hauptsächlicher Austausch von Bildern), TikTok (hauptsächlicher Austausch von Videos) oder Facebook (Mischung aus Schrift, Bild und Video).</p>
Spam/Junk	<p>„Müll“. Unerwünschte Nachrichten, die massenhaft und ungezielt per E-Mail oder über andere Kommunikationsdienste versendet werden.</p>
Spamfilter	<p>Fängt automatisch unerwünschte oder störende E-Mails, wie Werbung oder Gewinnspiele, ab und sortiert sie in einen extra Ordner (Spam- oder Junk-Ordner).</p>
Speedport-Router	<p>„Speedport“ ist die Bezeichnung, für alle Router-Modelle der Telekom. Er ist wie der normale Router verantwortlich für WLAN etc.</p>
Sprach-Assistenz-systeme	<p>Diese Geräte können Sprache analysieren und auf gesprochene Anweisungen reagieren.</p>

SQL	Structured Query Language. Mit Befehlen in dieser Sprache können Datenbanken aufgebaut, bearbeitet und ausgelesen werden.
SSL-Zertifikat	SSL steht für „Secure Socket Layer“. Ein SSL-Zertifikat ist ein kleiner Datensatz, den der Anbieter einer Website nur erhält, wenn er gewisse Sicherheitsstandards einhält. Hierbei gilt ein bestimmtes Verschlüsselungsprotokoll für Datenübertragungen im Internet bzw. zur Verschlüsselung der Verbindung zwischen Server und der verbundenen Person.
Startbildschirm	Grafische Oberfläche, die nach dem Einschalten eines PC auf dem Bildschirm angezeigt wird. Hier befinden sich auch verschiedene Symbole, die durch Klicken ein anderes Programm öffnen.
Streaming	Bezeichnet das Abspielen von Video- und Audioinformationen, ohne sie dauerhaft auf dem Gerät zu speichern. Das Streaming (Fließen, Strömen) wird durch eine spezielle Software (Plug-ins oder Wiedergabeprogramme) ermöglicht, die in der Regel kostenlos angeboten werden. Durch Streaming gelangen Videobilder und -töne live auf den Bildschirm des Endgeräts. Beim Streamen kannst du Musik, Filme und Podcasts direkt im Browser wiedergeben. Die Übertragung und Wiedergabe der Mediendatei erfolgen gleichzeitig.
Suchmaschine	Ermöglicht die Recherche von Inhalten, die im Internet oder auf einem Computer gespeichert sind. Beispiele für Suchmaschinen sind Google oder Bing.
Surfen	Sich im Internet frei bewegen und verschiedene Websites aufsuchen.
TAN	„Transaktionsnummer“. Fungiert als einmaliges Kennwort, welches aus sechs Zahlen besteht und beim Online-Banking verwendet wird.
Taskleiste	Bereich am unteren Rand des Bildschirms, in welchem die Programme angezeigt werden, die gerade geöffnet sind oder häufig genutzt werden.
Third-Party	Steht meist für Drittanbieter. Beispielsweise wird ein Produkt nicht über die markeneigene Website angeboten, sondern über dritte, also „fremde“ Websites, die das Produkt ebenfalls im Sortiment haben.

TikTok	Soziales Netzwerk zum Teilen kurzer Videoclips.
Timeline	Zeitachse. Darstellung der Abfolge von verschiedenen Ereignissen. In sozialen Netzwerken ist eine Timeline entweder chronologisch angeordnet oder es wird angezeigt, was das soziale Netzwerk meint, dass individuelle Nutzer:innen es sehen wollen bzw. sich dafür interessieren
Top-Level-Domain	„Domäne oberster Ebene“. Endung einer Internetadresse, zum Beispiel „.de“ oder „.eu“, bzw. eines Anbieters, zum Beispiel „.com“, „.org“ oder „.net“.
Tor Browser	Mit dem Tor Browser kann man anonym im Internet surfen, ohne dass Daten dabei gespeichert werden. Hierbei werden die verschiedenen Daten mehrfach verschlüsselt.
Touch-Display/ Touchscreen	Bildschirm, der bei Berührung reagiert, das heißt per Handberührung gesteuert wird.
Tracking	Das Verhalten der Nutzer:innen wird protokolliert, um unter anderem herauszufinden, über welche Websites die Nutzer:innen auf die eigene Website gekommen sind, wie lange sich die Besucher:innen auf der Website aufgehalten haben, welche Seiten aufgerufen wurden und welche IP-Adresse die Nutzer:innen haben.
Treiber	Bezeichnet ein Computerprogramm oder Softwaremodul. Ein Treiber kann dann die Steuerung von weiteren angeschlossenen Geräten übernehmen.
Trojaner	Schadsoftware, die als nützliches oder wichtiges Programm getarnt wird, um Zugang zum System zu bekommen. Sind Trojaner einmal installiert, können sie im Hintergrund Schaden am System anrichten und Daten ausspionieren. Beispielsweise kann so der Laptop einer Person ausspioniert werden.
Tutorial	Gebrauchsanleitung bzw. Erklärung eines gewissen Vorgangs oder einer Funktion. Am bekanntesten sind YouTube-Tutorials. Auf der Videoplattform YouTube laden Nutzer:innen Videos hoch, in denen die verschiedensten Dinge erklärt werden. Man kann Erklärungen zu nahezu allem finden. Beispielsweise gibt es Videos zum Reifenwechsel, aber auch zum Umtopfen von Pflanzen oder Origami.

Tweet	Kurze Mitteilung von nicht mehr als 140 Zeichen. Wird zum Beispiel auf Twitter genutzt.
U2F-Sticks	U2F steht für „Universal Second Factor“ und bedeutet so viel wie „universelle zweistufige Authentifizierung“. Ein U2F-Stick dient dem Nachweis der Zugriffsberechtigung, neben einem Zugangskennwort, zum Beispiel für webbasierte Dienste. U2F-Sticks schützen zum Beispiel auch vor Cyberangriffen.
Update	Neue Version bzw. Ergänzung einer Software, die Programmängel korrigiert oder Programmverbesserungen enthält. Updates werden in der Regel in elektronischer Form zum Herunterladen aus dem Internet zur Verfügung gestellt.
Upload	Daten werden von einem Computer oder Smartphone auf ein anderes Endgerät oder ins Internet „hochgeladen“ (übertragen). Veröffentlicht man zum Beispiel ein Foto im Internet, so wird dieses hochgeladen.
Uploadrate	Definiert die Geschwindigkeit, mit welcher Daten „hochgeladen“ werden können. Sie wird vom Provider (Anbieter) zur Verfügung gestellt.
URL	„Uniform Resource Locator“. Gibt eine Adresse im Internet an. Sie besteht aus dem Protokoll (zum Beispiel „http//“), dem Rechnernamen (zum Beispiel „www.bund.de“) und gegebenenfalls auch aus der Angabe des Ports (zum Beispiel „80“) und des Pfades (zum Beispiel „/startseite.html“).
USB-Stick	Mobiles Speichermedium, das über den USB-Anschluss mit einem anderen Gerät, z.B. einen PC, verbunden wird.
User	Bezeichnung der Onlinenutzer:innen.
Vault	Separater, gesicherter Raum in der digitalen Welt. In diesem können vertrauliche oder sensible Daten gespeichert werden, um sie dort vor Diebstahl /Schadprogrammen zu schützen.
Ver-schlüsselung	Durch einen Schlüssel (Code) werden Daten in eine nicht lesbare Form umgewandelt, um sie vor Dritten zu schützen. So wird eine sichere digitale Kommunikation ermöglicht.
Versions-nummer (bei Updates)	Hilft dabei, die verschiedenen Versionen oder Stufen eines Programms zu unterscheiden, und dient der Verwaltung.

Videocall	Videotelefonate. Hierbei handelt es sich um einen Anruf (vom Smartphone, Laptop oder PC), wobei sich beide Parteien auf dem Bildschirm des jeweils anderen sehen können.
Video-konferenz	Ähnlich wie der Videocall geht eine Videokonferenz von einem Smartphone, Laptop oder PC aus. Hierbei sind jedoch mehr als nur zwei Parteien involviert, zum Beispiel drei bis zehn Parteien. Der Anrufer kann die anderen Teilnehmer:innen auf dem Bildschirm sehen.
Virtual Reality	„Virtuelle Realität“. In diese rein digitale Welt kann man mittels spezieller Brillen eintauchen. Virtual Reality wird zum Spielen, aber auch in der Ausbildung genutzt.
VPN	„Virtual Private Network“ („virtuelles privates Netzwerk“). Es verschlüsselt die Datenkommunikation zwischen zwei Endpunkten – zum Beispiel zwischen einem Endgerät und einem anderen. Auf diese Weise kann die Kommunikation nicht von Dritten beeinflusst werden.
Wearables	Kleine Computer, die man „tragen“ kann: Zum Beispiel Fitnessarmbänder, die die Schritte zählen und die Herzfrequenz messen. Aber auch digitale Armbanduhren, mit denen man Nachrichten empfangen und telefonieren kann, gehören dazu.
Web 2.0	Wird auch als „Mitmach-Internet“ bezeichnet. Das Web 2.0 verändert die Nutzung des Internets und entwickelt sie weiter. Es geht nun nicht mehr ausschließlich darum, die Inhalte des Internets bzw. von verschiedenen Anbietern im Internet zu konsumieren, sondern zu interagieren und selbst Inhalte zu erstellen. Beispielsweise kann man Artikel/Blogs kommentieren oder auch selbst schreiben und veröffentlichen.
WLAN	„Wireless Local Area Network“ („drahtloses lokales Netzwerk“). Ermöglicht die kabelfreie Kommunikation zwischen mehreren lokalen Computern. WLAN wird häufig genutzt, um unterwegs mit dem Computer oder Smartphone ins Internet zu gehen.
Wörterbuch-Attacken	Methode, bei der in einen passwortgeschützten Computer oder Server eingebrochen wird. Hierbei wird jedes Wort in einer speziell vorgefertigten Liste systematisch als Passwort durchprobiert.

WPA	„Wi-Fi Protected Access“ („geschützter Zugang“). Sicherheitsstandard für Computer mit einer Wi-Fi-Verbindung. Hierdurch werden auch Sicherheitslücken und Schwachstellen beseitigt.
WPS	„Wi-Fi Protected Setup“. Standard, der den Anmeldevorgang von Endgeräten in einem verschlüsselten WLAN vereinfacht (zum Beispiel Handy oder Laptop).
ZigBee	Programm, welches regelt, wie die Geräte im Eigenheim miteinander kommunizieren. Produkte auf kurzer Distanz können so auch miteinander verbunden werden.
Z-Wave	Internationaler drahtloser Funkstandard, der vom Unternehmen Sigma Designs und der Z-Wave Alliance für ein Smart Home entwickelt wurde. Hierbei werden Produkte von unterschiedlichen Herstellern (zum Beispiel Waschmaschine, Jalousien) miteinander verbunden und gesteuert.
Zwei-Faktor-Authentifizierung	Bezeichnet die Kombination von zwei Faktoren aus den drei Bereichen Wissen (zum Beispiel Passwort), Besitz (zum Beispiel Chipkarte) und Biometrie (zum Beispiel Fingerabdruck).
2G/4G/5G	Das G steht für die Generation des Mobilfunks. 5G ist seit 2019 der Mobilfunkstandard, der an Verbreitung gewinnt. Dieser Standard sorgt für höhere Datenraten, verbesserte Kapazität und ein intelligentes Netz.

Video-Anleitungen zum
DsiN-Digitalführerschein hier:



In Kooperation mit dem:



Ein Projekt von:



Gefördert vom:

