

Digitale Selbstverteidigung Klasse 8: Deine Daten, deine Geräte

8 Lektionen · ca. 90 Minuten Unterricht · 18 Mitmach-Aufgaben · Stand: 01.11.2026

Was das Netz über dich weiß, welche Rechte du hast, wie eine Nachricht reist und wie Passwort und Handy sicher werden.

So läuft der Kurs

Sie führen den Kurs an der Tafel und entscheiden selbst, wann Sie welche Lektion durchführen. Der Kurs läuft nicht ab. Die Klasse meldet sich nicht an: keine Namen, kein Konto, kein Eintragen zu Beginn der Stunde. Mitmach-Aufgaben schalten Sie einzeln frei: An der Tafel erscheint dazu ein QR-Code, die Klasse antwortet am Handy, und mit „Auflösen“ erscheint die richtige Antwort gleichzeitig an der Tafel und auf allen Handys. Den Lösungsschlüssel zu allen Quizfragen sehen Sie in Ihrem Cockpit; dieses offene PDF enthält ihn bewusst nicht, damit er nicht vorab bei der Klasse landet. Am Ende schließen Sie den Kurs ab. Niemand aus der Klasse registriert sich, es gibt weder Namen noch Konto noch E-Mail-Adresse und deshalb auch keine Einzelzertifikate. Dieser Kurs hat kein Phishing-Training, das gibt es nur im Kurs „Digitale Selbstverteidigung“.

Was Sie brauchen: Beamer oder Display mit Internetzugang, die Klasse mit Smartphones. Wer kein Handy dabei hat, macht mit der Sitznachbarin mit.

Bezug zum Bildungsplan Baden-Württemberg

Klasse 8 (etwa 13 bis 14 Jahre) · Umfang: zwei Doppelstunden, Lektionen einzeln einsetzbar · Stand 03.10.2026

Deine Daten, deine Geräte: Was das Netz über dich weiß, welche Rechte du hast, wie eine Nachricht reist, warum Verschlüsselung zählt und wie Passwort und Handy sicher werden. Entspricht dem Aufbaukurs Informatik (BP 2016, Klasse 7) und vertieft die Lesehilfe-Grundlagen. Handlungsfelder der Leitperspektive „Leben und Lernen in einer digitalisierten Welt“: Verantwortungsvoll handeln und schützen, Digital kommunizieren, kooperieren, handeln.



Bereich	Kompetenz (Lesehilfe Informatik und Medienbildung 2026/27 bzw. Bildungsplan 2016)
Digitalität und Partizipation	Situationen der Datenerhebung; Interessen der Akteure; informationelle Selbstbestimmung Lektionen: Was weiß das Internet über dich, Social Media, Deine Daten und deine Rechte
Kommunikation und Sicherheit	Weg einer Nachricht, Client-Server, Speicherorte; Verschlüsselung; Schutz des eigenen Zugangs Lektionen: Wie das Internet funktioniert, Verschlüsselung, Passwörter und Accounts, Dein Smartphone absichern
Aufbaukurs Informatik, 3.1.3 Rechner und Netze / 3.1.4 Informationsgesellschaft und Datensicherheit	Aufbau von Rechnernetzen; (1) Gründe für Verschlüsselung, (2) Caesar-Verfahren, (3) Brute Force, (4) Sicherheitsaspekte mobiler Geräte, (6) Anfall personenbezogener Daten
Leitperspektive Medienbildung	Informationelle Selbstbestimmung und Datenschutz, Informationstechnische Grundlagen

Die Zuordnung ist eine fachliche Einschätzung des Anbieters, keine amtliche Freigabe. Für die Klassen 8 bis 10 gilt bis zum Inkrafttreten des Bildungsplans Informatik und Medienbildung (2027/28) der Bildungsplan 2016.

Überblick über die Lektionen

Lektion	Mitmach-Aufgaben
1. Einstieg: Was weiß das Internet über dich? Klasse 8 · Digitalität und Partizipation Warum digitale Selbstverteidigung dich betrifft und was in diesem Kurs passiert.	Wortwolke, Quiz
2. Social Media: Was deine Apps wirklich über dich wissen Klasse 8 · Digitalität und Partizipation Instagram, TikTok, Snapchat: wie Plattformen deine Daten sammeln und nutzen.	Wortwolke, Quiz
3. Deine Daten, deine Rechte: Was das Gesetz sagt Klasse 8 · Digitalität und Partizipation Was Datenschutz mit dir zu tun hat und welche Rechte du hast.	Quiz, Quiz
4. Wo ist meine Nachricht gerade? Wie das Internet funktioniert Klasse 8 · Kommunikation und Sicherheit Knoten, Router, Server: welchen Weg eine Nachricht nimmt, was Client und Server sind, und warum der Speicherort entscheidet, wer deine Daten sehen kann.	Quiz, Quiz, Wortwolke



5.	Verschlüsselung: Das Schloss im Browser und der Caesar-Trick Klasse 8 · Kommunikation und Sicherheit Warum WhatsApp und das Schloss im Browser dich schützen, was Ende-zu-Ende bedeutet und wie du mit dem Caesar-Trick selbst verschlüsselst und knackst.	Quiz, Quiz, Wortwolke
6.	Passwörter und Accounts: Was gehört dir und was teilst du nie Klasse 8 · Kommunikation und Sicherheit Warum jedes Passwort einzigartig sein muss und was Zwei-Faktor-Authentifizierung bringt.	Spiel: passwortknacker, Quiz
7.	Dein Smartphone absichern: PIN, Apps und Berechtigungen Klasse 8 · Kommunikation und Sicherheit Warum dein Handy dein wichtigstes Gerät ist und wie du es richtig schützt.	Spiel: berechtigungen, Quiz
8.	Zusammenfassung: Deine Daten, deine Geräte Ergänzung · Zusammenfassung Sicherung der Klasse-8-Reihe: Datenspuren, Rechte, Netz, Verschlüsselung, Passwörter, Smartphone.	Wortwolke, Quiz

Auf den folgenden Seiten steht jede Lektion vollständig, mit allen Quizfragen und Antwortmöglichkeiten. Die markierten Lösungen finden Sie ausschließlich in Ihrem Cockpit.



1. Einstieg: Was weiß das Internet über dich?

Warum digitale Selbstverteidigung dich betrifft und was in diesem Kurs passiert.



Willkommen zur digitalen Selbstverteidigung

Bevor es losgeht, eine ehrliche Frage: Wie viel weiß das Internet eigentlich über dich? Vermutlich mehr, als du denkst und vor allem mehr, als du je bewusst hineingeschrieben hast.

Wortwolke

Was gehört für dich unbedingt privat?





Worum es in diesem Kurs geht

In den nächsten Stunden geht es nicht um Technik, sondern um dich: Wie Fremde an deine Daten kommen, was sie damit anfangen, und wie du das verhinderst. Wir schauen uns Social Media an, Gaming, dein Smartphone, deine Passwörter und ganz am Ende bekommst du unangekündigt ein paar gefälschte Mails, um zu sehen, ob es sitzt.

Wichtig

Alles, was du ins Internet stellst, kann von Fremden gefunden werden. Auch wenn du denkst, dass nur deine Freunde es sehen.

Warum das jetzt schon wichtig ist

Stell dir vor, jemand kennt deinen vollen Namen, deine Schule, dein Lieblingsspiel und den Namen deines Haustiers. Klingt harmlos? Mit diesen Infos kann jemand:

- Dein **Passwort erraten** (viele nutzen den Haustiernamen)
- Dir eine **gefälschte Nachricht** schreiben, die genau zu deinen Interessen passt
- Sich als **dein Freund ausgeben** und andere täuschen



Das ist keine Theorie, das passiert jeden Tag, tausendfach. Und genau deshalb bist du hier.

Quizfrage

Welche dieser Informationen solltest du niemals öffentlich posten?

Antwortmöglichkeiten

Dein Lieblingslied

Deine Handynummer

Dein Geburtsdatum mit Jahrgang

Dein Lieblingsfilm

Deine Adresse

Der Name deiner Schule und deine Klasse

Tipp

Faustregel: Alles, womit jemand dich finden, kontaktieren oder sich als du ausgeben könnte, gehört nicht ins öffentliche Profil.



2. Social Media: Was deine Apps wirklich über dich wissen

Instagram, TikTok, Snapchat: wie Plattformen deine Daten sammeln und nutzen.



Dein Profil ist nur die Oberfläche

Du postest ein Foto, likest ein Reel, scrollst durch TikTok. Klingt harmlos. Aber hinter jedem Wisch sammeln die Plattformen Daten über dich, viel mehr, als du denkst.





Was Instagram, TikTok & Co. über dich speichern

Was du tust	Was die App speichert
Ein Reel anschauen	Wie lange du schaust, ob du weiterwischst oder nochmal schaust
Ein Foto posten	Standort, Uhrzeit, Gerätetyp, wer es sieht
Jemandem folgen	Dein soziales Netzwerk, wer kennt wen
In der App tippen	Auch nicht abgeschickte Texte werden teilweise erfasst
Dein Handy dabeihaben	Bewegungsprofil über Standortdaten

Wichtig

TikTok zum Beispiel erfasst laut eigener Datenschutzerklärung: Geräte-ID, IP-Adresse, Tastatureingaben, Browserverlauf innerhalb der App, biometrische Daten (Gesichts- und Stimmerkmale) und Standort. Und das ist nur, was sie offiziell zugeben.

Warum ist das ein Problem?

1. Du bist das Produkt. Die Apps sind kostenlos, weil du mit deinen Daten bezahlst. Je mehr sie über dich wissen, desto gezielter können sie dir Werbung zeigen und desto



mehr Geld verdienen sie.

2. Daten können gestohlen werden. Wenn eine Plattform gehackt wird, landen deine Daten im Darknet. Das ist bei TikTok, Facebook, Instagram und Snapchat bereits passiert, mehrfach, mit Millionen von Accounts.

3. Dein digitaler Fußabdruck bleibt. Was du heute postest, kann in zehn Jahren noch auftauchen, bei einer Bewerbung, einem Stipendium oder einem Streit.

Was du tun kannst

- **Profil auf privat stellen:** bei Instagram, TikTok und Snapchat möglich
- **Standort deaktivieren:** die meisten Apps brauchen deinen Standort nicht wirklich
- **Berechtigungen prüfen:** braucht TikTok wirklich Zugriff auf deine Kontakte?
- **Regelmäßig alte Posts aufräumen:** was vor zwei Jahren lustig war, muss nicht für immer online sein

Tipp

Geh jetzt in die Einstellungen deines Handys → Apps → Berechtigungen. Schau dir an, welche App auf was zugreifen darf. Du wirst überrascht sein.

Rätsel: Daten-Detektiv

Jemand postet auf Instagram:

- Ein Selfie vor der Schule (Schulname auf dem Schild sichtbar)
- Story mit „Endlich 16! 🎉“ am 15. März
- Bio: „Gaming 🎮 | Mainz | @max_gamer auf Discord“

Wortwolke

Welche Informationen könnte ein Fremder daraus zusammensetzen?

Quizfrage



Was sammelt eine Social-Media-App typischerweise über dich?

Antwortmöglichkeiten

Deinen Standort

Wie lange du welches Video anschaust

Dein Adressbuch, wenn du es erlaubst

Nur das, was du selbst postest



3. Deine Daten, deine Rechte: Was das Gesetz sagt

Was Datenschutz mit dir zu tun hat und welche Rechte du hast.



Datenschutz ist nicht langweilig, er schützt dich

Wenn jemand ein Foto von dir macht und es ohne dein Okay postet, ist das nicht nur unhöflich, es ist in den meisten Fällen **illegal**. Die Datenschutz-Grundverordnung (DSGVO) und das Recht am eigenen Bild geben dir echte Rechte.





Deine wichtigsten Rechte

- 1. Recht auf Information:** Du darfst wissen, welche Daten ein Dienst über dich speichert. Bei Instagram, TikTok und Co. kannst du eine Kopie deiner Daten anfordern und wirst staunen, was da alles drin ist.
- 2. Recht auf Löschung:** Du kannst verlangen, dass deine Daten gelöscht werden. Das gilt auch für Fotos und Videos, die andere von dir gepostet haben.
- 3. Recht am eigenen Bild:** Niemand darf ohne deine Einwilligung Fotos oder Videos von dir veröffentlichen. Das gilt auch in der Schule, auf Partys und im Sportverein.
- 4. Recht auf Vergessenwerden:** Suchmaschinen müssen Links zu veralteten oder irrelevanten Informationen über dich auf Antrag entfernen.

Was andere nicht dürfen

Situation	Erlaubt?
Ein Mitschüler postet ein Foto von dir ohne zu fragen	☐
Jemand leitet deinen privaten Chat weiter	☐
Eine App gibt deine Daten an Werbenetzwerke weiter, ohne dich zu informieren	☐

Digitale Selbstverteidigung Klasse 8: Deine Daten, deine Geräte · Seite 12 von 31
Kursbeschreibung: secureit.icu/kurse/schulkurs-digitale-selbstverteidigung-8



Situation	Erlaubt?
Deine Eltern gucken auf dein Handy (du bist unter 18)	☐ Grauzone, hängt vom Alter und Kontext ab

Wichtig

„Ich hab doch nichts zu verbergen“ ist kein Argument. Datenschutz bedeutet nicht, dass du etwas versteckst. Es bedeutet, dass **du entscheidest**, wer was über dich erfährt.

Was du tun kannst, wenn deine Rechte verletzt werden

1. **Die Person direkt ansprechen:** „Bitte nimm das Foto runter.“
2. **Bei der Plattform melden:** Alle großen Dienste haben Melde-Funktionen
3. **Eltern oder Lehrkraft einschalten:** Besonders wenn es um Mobbing geht
4. **Offiziell beschweren:** Bei der Landesdatenschutzbehörde (kostenlos)

Tipp

Mach Screenshots als Beweis, **bevor** du die Löschung verlangst. Einmal gelöscht, lässt sich nichts mehr nachweisen.

Quiz: Deine Rechte

Stimmt das? Diskutiert in der Klasse.

1. „Wenn ich unter 16 bin, brauchen soziale Netzwerke die Zustimmung meiner Eltern.“
2. „Was ich einmal im Internet gepostet habe, kann ich nie wieder löschen.“
3. „Mein Lehrer darf mich im Unterricht ohne Erlaubnis filmen.“
4. „Wenn ein Freund mein Passwort kennt und sich einloggt, ist das kein Hacking.“

Quizfrage

Welche Aussagen stimmen?



Antwortmöglichkeiten

Unter 16 brauchen soziale Netzwerke die Zustimmung der Eltern.

Was einmal gepostet ist, lässt sich nie wieder löschen.

Die Lehrkraft darf mich im Unterricht ohne Erlaubnis filmen.

Loggt sich ein Freund mit meinem Passwort ein, ist das kein Hacking.

Quizfrage

Welche Rechte hast du gegenüber einem Anbieter, der Daten über dich gespeichert hat?

Antwortmöglichkeiten

Du darfst erfahren, was gespeichert ist

Du darfst Löschung verlangen

Du darfst falsche Angaben berichtigen lassen

Du musst dafür volljährig sein



4. Wo ist meine Nachricht gerade? Wie das Internet funktioniert

Knoten, Router, Server: welchen Weg eine Nachricht nimmt, was Client und Server sind, und warum der Speicherort entscheidet, wer deine Daten sehen kann.



Kein Draht, ein Netz

Viele stellen sich das Internet wie eine Leitung vor: von deinem Handy zum Handy deiner Freundin. In Wirklichkeit ist es ein **vermaschtes Netz** aus Millionen Knoten: dein Handy, der WLAN-Router, der Anbieter, Vermittlungsrechner, Unterseekabel, Rechenzentren, wieder ein Anbieter, ein Router, ein Handy.

Deine Nachricht wird in kleine Pakete zerlegt. Jedes Paket springt von Knoten zu Knoten, und jeder Knoten entscheidet nur: „Wohin als Nächstes?“ Fällt ein Weg aus, nehmen die Pakete einen anderen. Deshalb funktioniert das Netz auch, wenn irgendwo ein Kabel reißt.

Wichtig

Deine Nachricht kommt unterwegs an **vielen fremden Rechnern** vorbei, die du nicht kennst. Genau deshalb ist Verschlüsselung keine Spielerei, sondern das, was



Client und Server

Dein Handy **fragt** („Zeig mir das Video“, „Schick diese Nachricht“), ein großer Rechner im Rechenzentrum **antwortet**. Der Fragende heißt **Client**, der Antwortende **Server**. Jede App, jede Webseite, jedes Spiel funktioniert so, auch wenn es sich anfühlt, als wäre alles „auf deinem Handy“.

Das heißt umgekehrt: Der Server sieht alles, was du ihm schickst. Wer den Server betreibt, hat deine Daten. Nicht die Technik entscheidet über deinen Datenschutz, sondern **der Betreiber**.

Wo liegen deine Sachen?

Speicherort	Beispiel	Wer kommt dran?	Wenn du löschst
Dein Gerät	Fotos in der Galerie	Du, oder wer dein Handy in die Hand bekommt	Weg (bis auf Sicherungen)
Server im Schulnetz	Dateien auf dem Schulserver	Du, Lehrkräfte, Schul-IT	Nach Regeln der Schule
Server des Anbieters	Chat-Nachrichten, Posts	Du, Empfänger, der Anbieter	Deine Kopie weg, die anderen bleiben
Cloud	Online-Speicher, Backups	Du, der Anbieter, ggf. Behörden im Land des Servers	Oft erst nach Frist endgültig

Beim Vergleichen zählen vier Dinge: **Verfügbarkeit** (komme ich überall dran?), **Zusammenarbeit** (können andere mitmachen?), **Sicherheit** (wer kann mitlesen oder stehlen?) und **Betreiber** (wem gehört der Server, in welchem Land steht er, welche Regeln gelten dort?).

Quizfrage

Was stimmt über den Weg einer Nachricht im Internet?

Antwortmöglichkeiten

Sie wird in Pakete zerlegt, die über viele Knoten laufen



Fällt ein Weg aus, nehmen die Pakete einen anderen

Es gibt eine direkte Leitung von Handy zu Handy

Nur der Empfänger kann die Pakete technisch sehen

Quizfrage

Du willst ein Referat mit drei Mitschülern gemeinsam schreiben. Welcher Speicherort passt am besten, und worauf achtest du?

Antwortmöglichkeiten

Cloud oder Schulserver, weil alle gleichzeitig daran arbeiten können

Vorher schauen, wer den Dienst betreibt und wo der Server steht

Nur auf meinem Handy, das ist am sichersten für Zusammenarbeit

Egal wo, Hauptsache kostenlos

Wortwolke

Welche Geräte liegen auf dem Weg zwischen dir und einem Freund, wenn ihr chattet? Ein Wort pro Antwort.

Tipp

Wenn du wissen willst, wo ein Dienst seine Server stehen hat: In der Datenschutzerklärung steht es meistens unter „Hosting“ oder „Speicherort“. Deutschland oder EU heißt: europäische Datenschutzregeln gelten.



5. Verschlüsselung: Das Schloss im Browser und der Caesar-Trick

Warum WhatsApp und das Schloss im Browser dich schützen, was Ende-zu-Ende bedeutet und wie du mit dem Caesar-Trick selbst verschlüsselst und knackst.



Wer liest mit?

Jede Nachricht, die du verschickst, läuft über Dutzende fremde Rechner: dein WLAN, den Router im Café, den Anbieter, Server irgendwo auf der Welt. Ohne Verschlüsselung könnte jeder davon mitlesen, wie bei einer Postkarte.

Verschlüsselung macht aus deinem Text (dem **Klartext**) einen unlesbaren **Geheimtext**. Nur wer den passenden **Schlüssel** hat, kann ihn wieder lesbar machen.

Wichtig

Codierung ist nicht Verschlüsselung. Ein QR-Code oder Morsezeichen kann **jeder** zurückübersetzen, der die Regel kennt. Verschlüsselung braucht zusätzlich einen **Schlüssel**, den nur die Richtigen haben.



Zwei Arten, die du jeden Tag benutzt

Transportverschlüsselung: Das Schloss im Browser (das „https“). Zwischen deinem Handy und der Webseite kann niemand mitlesen, auch nicht im offenen WLAN. Aber: Der Betreiber der Seite sieht alles, was du dort eingibst.

Ende-zu-Ende-Verschlüsselung: WhatsApp, Signal, Threema. Die Nachricht wird auf deinem Handy verschlüsselt und erst auf dem Handy der Empfängerin wieder entschlüsselt. Nicht einmal der Anbieter kann sie lesen.

Tipp

Kein Schloss im Browser, oder der Browser warnt vor der Seite? Dann gib dort **nie** ein Passwort oder Bankdaten ein. Egal, wie echt die Seite aussieht.

Der Caesar-Trick

Schon Julius Caesar hat Nachrichten verschlüsselt: Jeder Buchstabe wird im Alphabet um eine feste Zahl weitergeschoben. Der Schlüssel ist diese Zahl.

Mit Schlüssel **3** wird aus A ein D, aus B ein E, aus H ein K:

Klartext: H A L L O

Geheimtext: K D O O R

Probier es: Verschlüsse deinen Vornamen mit Schlüssel 3. Hinten im Alphabet geht es vorn weiter, aus X wird A.

Quizfrage

Du fängst den Geheimtext **VLFKHU**** ab. Du weißt, dass es Caesar mit Schlüssel 3 ist. Was steht da?**

Antwortmöglichkeiten

SCHULE

SICHER

SUCHEN



Warum Caesar heute nichts mehr taugt

Es gibt nur **25 mögliche Schlüssel**. Ein Angreifer probiert einfach alle durch. Das nennt man **Brute Force**, rohe Gewalt: nicht schlau, aber schnell. Ein Computer schafft das in weniger als einer Sekunde.

Noch schneller geht es mit der **Häufigkeitsanalyse**: Im Deutschen ist das E der häufigste Buchstabe. Der häufigste Buchstabe im Geheimtext ist also sehr wahrscheinlich das verschobene E, und schon ist der Schlüssel bekannt.

Wichtig

Genau das passiert auch mit **kurzen Passwörtern**: Ein Rechner probiert alle Möglichkeiten durch. Je mehr mögliche Schlüssel, desto länger dauert es. Deshalb gewinnen lange Passwörter und moderne Verschlüsselung mit Schlüsseln, die aus Hunderten Stellen bestehen.

Quizfrage

Was stimmt?

Antwortmöglichkeiten

Beim Schloss im Browser kann im WLAN niemand mitlesen, der Seitenbetreiber aber schon

Bei Ende-zu-Ende-Verschlüsselung kann auch der Anbieter die Nachricht nicht lesen

Ein QR-Code ist eine sichere Verschlüsselung

Caesar ist sicher, weil ihn kaum noch jemand kennt

Wortwolke

Wo begegnet dir Verschlüsselung im Alltag? Ein Wort genügt.



6. Passwörter und Accounts: Was gehört dir und was teilst du nie

Warum jedes Passwort einzigartig sein muss und was Zwei-Faktor-Authentifizierung bringt.



Dein Passwort ist dein Hausschlüssel

Stell dir vor, du hast einen Schlüssel, der deine Haustür, dein Schließfach, dein Fahrradschloss und deinen Spind aufschließt. Klingt praktisch, bis du ihn verlierst. Dann ist alles weg.

Genau das passiert, wenn du überall dasselbe Passwort verwendest.





Warum ein Passwort nicht reicht

Wenn eine Webseite gehackt wird (und das passiert ständig), landen die Benutzernamen und Passwörter im Darknet. Angreifer probieren diese Kombinationen dann automatisch auf hunderten anderen Seiten aus. Das nennt sich **Credential Stuffing**.

Wenn du also dasselbe Passwort bei Instagram, deiner E-Mail und deinem Gaming-Account verwendest und Instagram gehackt wird, dann sind **alle drei Accounts** gefährdet.

Wichtig

Die Regel ist einfach: **Ein Account, ein Passwort**. Kein Passwort darf bei zwei Diensten gleichzeitig im Einsatz sein.

Was ein sicheres Passwort ausmacht

Schlecht	Warum	Besser
MaxMustermann2009	Name + Geburtsjahr = erratbar	Korrekt-Pferd-Batterie-Hefter



Schlecht	Warum	Besser
123456789	Häufigstes Passwort der Welt	Zufällige Wörter kombinieren
Sommer2024!	Muster, das Millionen nutzen	Passwort-Manager nutzen

Ein gutes Passwort ist:

- Mindestens 12 Zeichen lang
- Nicht erratbar (kein Name, Geburtsdatum, Haustier)
- Einzigartig für jeden Account

Die einfachste Methode: Nimm vier zufällige Wörter und verbinde sie: „Giraffe-Klavier-Wolke-Sieben“. Lang, einprägsam, sicher.

Passwort-Manager: Dein digitaler Schlüsselbund

Ein Passwort-Manager speichert alle deine Passwörter verschlüsselt. Du merkst dir nur noch **ein** Master-Passwort. Der Manager generiert und füllt alle anderen automatisch aus.

Kostenlose Optionen: Bitwarden, KeePassXC, die Schlüsselbund-Funktion von Apple/Google.

Zwei-Faktor-Authentifizierung (2FA)

2FA bedeutet: Selbst wenn jemand dein Passwort kennt, braucht er zusätzlich einen zweiten Faktor, meistens einen Code auf deinem Handy.

Wo du 2FA sofort einschalten solltest:

1. Deine E-Mail (die ist der Schlüssel zu allen anderen Accounts)
2. Deine Gaming-Accounts (Steam, Epic, Riot)
3. Social Media (Instagram, TikTok, Snapchat)
4. Alles, was mit Geld zu tun hat

Was gehört dir und was teilst du nie

☐ Darfst du teilen	☐ Teilst du nie
--	---



☐ Darfst du teilen	☐ Teilst du nie
Dein Gamertag	Dein Passwort
Dein Lieblingsfilm	Dein Geburtstag mit Jahrgang
Dein öffentliches Profil	Deine Adresse
Screenshots (ohne sensible Daten)	Dein Ausweis / Schülerschein
Dein Discord-Server	Dein E-Mail-Login

Tipp

Auch nicht mit deinem besten Freund. Freundschaften ändern sich. Passwörter, die du geteilt hast, kannst du nicht „zurücknehmen“. Und dein Freund kann unbeabsichtigt gehackt werden, dann hat der Angreifer auch deinen Zugang.

Rätsel: Passwort-Check

Welche dieser Passwörter sind sicher?

1. Fussball2009 → ☐ (Name + Geburtsjahr)
2. kT9\$mP2!xR4# → ☐ (zufällig, aber schwer zu merken)
3. Elefant-Ketchup-Trommel-42 → ☐ (lang, zufällig, merkbar)
4. IchLiebeDich → ☐ (unter den Top 20 der häufigsten Passwörter)
5. qwertz → ☐ (Tastaturmuster)

Lernspiel

Denkt euch ein Passwort aus und seht, wie lange es hält. Übertragen wird nur das Muster,

Quizfrage

Was macht ein Passwort wirklich stark?

Antwortmöglichkeiten

Länge

Ein Ausrufezeichen am Ende



Dass es nur für einen einzigen Dienst benutzt wird

Dass du es dir gut merken kannst, weil es dein Geburtstag ist

Dass es nirgends sonst vorkommt



7. Dein Smartphone absichern: PIN, Apps und Berechtigungen

Warum dein Handy dein wichtigstes Gerät ist und wie du es richtig schützt.



Dein Handy ist der Schlüssel zu allem

Dein Smartphone ist nicht nur ein Telefon. Es ist dein Bankkonto, dein Postfach, dein Fotoalbum, dein Navi und dein Ausweis in einem. Wer Zugriff auf dein Handy hat, hat Zugriff auf dein komplettes digitales Leben.





Grundschutz: Sperre und Biometrie

Methode	Sicherheit	Empfehlung
Kein Sperrbildschirm	Keine	Niemals
Wischmuster	Sehr schwach (Fettspuren verraten das Muster)	Nein
4-stellige PIN	Schwach (10.000 Möglichkeiten)	Minimum
6-stellige PIN	Besser (1 Million Möglichkeiten)	Gut
Fingerabdruck	Stark + schnell	Empfohlen
Face ID / Gesichtserkennung	Stark (bei neueren Geräten)	Empfohlen

Wichtig

Die **häufigsten PINs** in Deutschland: 1234, 0000, 1111, 2580 (senkrechte Linie), Geburtsjahr. Wenn deine dabei ist: sofort ändern.

App-Berechtigungen: Wer darf was?

Jede App fragt nach Berechtigungen. Aber nicht jede braucht, was sie verlangt:



- **Kamera:** braucht Instagram, eine Taschenlampen-App aber nicht
- **Mikrofon:** braucht eine Sprach-App, ein Spiel aber nicht
- **Kontakte:** braucht WhatsApp, ein Wetterdienst aber nicht
- **Standort:** braucht Google Maps, ein Taschenrechner aber nicht

WLAN-Sicherheit: Offene Netze sind gefährlich

Kostenloses WLAN in der Bahn, im Café oder am Bahnhof klingt super. Aber in offenen Netzen kann jeder mitlesen, was du tust. Das nennt sich **Man-in-the-Middle-Angriff**: Jemand sitzt zwischen dir und dem Internet und liest mit.

Regeln für öffentliches WLAN:

- Kein Online-Banking, kein Login in wichtige Accounts
- VPN nutzen (es gibt kostenlose Varianten)
- Automatische WLAN-Verbindung deaktivieren

Tipp

Geh in deine WLAN-Einstellungen und lösche alle Netzwerke, die du nicht mehr brauchst. Dein Handy verbindet sich sonst automatisch mit jedem gleichnamigen Netzwerk und ein Angreifer kann ein „Starbucks WiFi“ leicht fälschen.

Updates: Die langweiligste Schutzmaßnahme und die wichtigste

Jedes Update schließt bekannte Sicherheitslücken. Wenn du Updates aufschiebst, lässt du eine Tür offen, von der Angreifer wissen, dass sie existiert.

- **Betriebssystem-Updates** sofort installieren
- **App-Updates** regelmäßig durchführen
- **Apps löschen:** die du nicht mehr nutzt: weniger Apps bedeutet weniger Angriffsfläche

Quiz: Wie sicher ist dein Handy?



Prüfe jetzt auf deinem Gerät:

1. Hast du eine PIN oder Biometrie aktiv? ☐ / ☐
2. Ist dein Betriebssystem auf dem neuesten Stand? ☐ / ☐
3. Hast du Apps installiert, die du seit Monaten nicht benutzt hast? ☐ / ☐
4. Nutzt eine App Berechtigungen, die sie nicht braucht? ☐ / ☐

Für jedes ☐ bei 1–2 und jedes ☐ bei 3–4 gibt es einen Punkt. Wer alle vier Punkte hat, ist gut aufgestellt.

Lernspiel

Sechs Apps, sechs Berechtigungen. Abstimmen lassen, dann an der Tafel vergleichen.

Quizfrage

Welche Berechtigung ist bei einer Taschenlampen-App auf jeden Fall verdächtig?

Antwortmöglichkeiten
Standort
Kontakte
Kamera-Blitz
Mikrofon



8. Zusammenfassung: Deine Daten, deine Geräte

Sicherung der Klasse-8-Reihe: Datenspuren, Rechte, Netz, Verschlüsselung, Passwörter, Smartphone.



Fünf Dinge, die bleiben sollen

- **Dein Fußabdruck entsteht zur Hälfte durch andere.** Reden hilft mehr als Einstellungen allein.
- **Apps bekommen nur, was sie für ihre Aufgabe brauchen.** Eine Taschenlampe braucht kein Mikrofon.
- **Du hast Rechte.** Auskunft, Löschung, Beschwerde: drei Schritte, keine Anwältin nötig.
- **Eine Nachricht reist über viele Stationen.** Nur Ende-zu-Ende-Verschlüsselung hält sie unterwegs geheim.
- **Ein Passwort je Dienst, Sperre am Handy, zweiter Faktor an.** Kostet Sekunden, rettet Konten.

Wichtig

Sicherheit ist kein Zustand, sondern eine Gewohnheit: Sperre, eigenes Passwort, kurz nachdenken.



Wie es weitergeht

In Klasse 9 und 10 geht es um die Angreifer: Fake-Profil, geklonte Stimmen, Betrug in Spielen und Phishing, mit einem echten Praxistest am Ende.

Wortwolke

Was änderst du nach dieser Reihe als Erstes an deinem Handy?

Quizfrage

Welche Aussage stimmt?

Antwortmöglichkeiten

Wer ein starkes Passwort hat, kann es überall benutzen.

Bei Ende-zu-Ende-Verschlüsselung können nur Absender und Empfänger die Nachricht lesen.

Eine App darf alle Berechtigungen verlangen, die sie will, das ist normal.

Gelöschte Daten kann man bei Firmen nicht einfordern.

