

Sicher starten im Netz

10 Lektionen · ca. 90 Minuten Unterricht · 21 Mitmach-Aufgaben · Stand: 01.11.2026

Handy, Klassenchat, erste eigene Accounts: wie du von Anfang an klug und sicher unterwegs bist, ohne dass dir jemand den Spaß verdirbt.

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

Klassen 5 und 6 (etwa 10 bis 12 Jahre) · Umfang: zwei Doppelstunden oder vier Einzelstunden, Lektionen einzeln einsetzbar · Stand 03.10.2026

Der Einstieg ins neue Fach Informatik und Medienbildung: folgt der Lesehilfe für die Klassen 5 und 6 in den Bereichen Digitalität und Partizipation, Information und Daten sowie Kommunikation und Sicherheit. Algorithmen und Digitales Arbeiten bleiben beim Fachunterricht. Handlungsfelder der Leitperspektive „Leben und Lernen in einer digitalisierten Welt“: Verantwortungsvoll handeln und schützen, Digital kommunizieren, kooperieren, handeln, Informationen sammeln, verstehen, bewerten, Medien und Mediengesellschaft analysieren.

Bereich	Kompetenz (Lesehilfe Informatik und Medienbildung 2026/27 bzw. Bildungsplan 2016)
Sicher starten im Netz · Seite 1 von 24 Kursbeschreibung: secureit.icu/kurse/schulkurs-sicher-starten	



Digitalität und Partizipation	Regeln für die schulische Mediennutzung; eigene Mediennutzung beschreiben und reflektieren; Werbung identifizieren und ihre Auswahl erklären; Nutzungs- und Rahmenbedingungen von Apps; Situationen der Datenerhebung und Interessen der Akteure Lektionen: Dein Tag mit dem Handy, Werbung, Zustimmung?, Wem erzählst du was?
Information und Daten	Informationen kriterienbasiert prüfen; Kriterien für Vertrauenswürdigkeit; grundlegende Funktionsweise einer indexbasierten Suche Lektionen: Stimmt das?
Kommunikation und Sicherheit	Kommunikation im digitalen Raum (Klassenchat, Regeln, Folgen); verletzendes Verhalten, Hilfsangebote und Meldemöglichkeiten; Schutz des eigenen Zugangs; Speicherorte und Weg einer Nachricht; Recht am eigenen Bild Lektionen: Der Klassenchat, Fremde im Netz, Dein Schloss, Wo ist mein Foto gespeichert?
Basiskurs Medienbildung Klasse 5 (geht in IuM auf)	3.1.3 Kommunikation und Kooperation (Regeln im Netz, private Daten, Cybermobbing), 3.1.4 Mediengesellschaft, 3.1.1 Information und Wissen

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.	Dein Tag mit dem Handy Klasse 5/6 · Digitalität und Partizipation Wie viel, wofür und warum: deine eigene Mediennutzung ehrlich anschauen, und was die Regeln in der Schule damit zu tun haben.	Wortwolke, Quiz
2.	Werbung: Warum das Spiel kostenlos ist Klasse 5/6 · Digitalität und Partizipation Werbung in Apps und Videos erkennen, In-App-Käufe durchschauen und verstehen, warum du genau diese Werbung siehst.	Quiz, Wortwolke
3.	Zustimmen? Was du beim Konto-Anlegen unterschreibst Klasse 5/6 · Digitalität und Partizipation Nutzungsbedingungen, Altersgrenzen und Berechtigungen: was hinter dem Knopf „Akzeptieren“ steckt und worauf du vor dem Tippen schaust.	Spiel: berechtigungen, Quiz
4.	Wem erzählst du was? Deine Daten im Netz Klasse 5/6 · Digitalität und Partizipation Welche Daten bei Apps und Spielen anfallen, wer sich dafür interessiert und warum du selbst entscheidest, was du preisgibst.	Spiel: datenschutz, Quiz



5.	Stimmt das? Informationen prüfen Klasse 5/6 · Information und Daten Woher kommt das, wer sagt das, kann das sein? Drei Fragen vor dem Glauben und Weiterleiten, und wie eine Suchmaschine entscheidet, was oben steht.	Spiel: faktencheck, Quiz
6.	Der Klassenchat Klasse 5/6 · Kommunikation und Sicherheit Regeln, die im Chat anders sind als auf dem Schulhof, was aus einem Witz werden kann, und wie ihr Streit im Chat wieder einfängt.	Wortwolke, Quiz
7.	Fremde im Netz: Wer schreibt dir da? Klasse 5/6 · Kommunikation und Sicherheit Warum Fremde online nett sind, welche Nachrichten ein Warnsignal sind, und wo du Hilfe bekommst, ohne Ärger zu kriegen.	Quiz
8.	Dein Schloss: Passwort und Gerätesperre Klasse 5/6 · Kommunikation und Sicherheit Warum dein Zugang schützenswert ist, wie ein gutes Passwort aussieht, das du dir merken kannst, und warum du es nie teilst, auch nicht mit der besten Freundin.	Spiel: passwort-knacker, Quiz
9.	Wo ist mein Foto gespeichert? Klasse 5/6 · Kommunikation und Sicherheit Gerät, Server, Cloud: wo deine Sachen wirklich liegen, welchen Weg eine Nachricht durchs Netz nimmt, und warum ein Foto von anderen deren Erlaubnis braucht.	Quiz, Wortwolke
10.	Zusammenfassung: Dein Start-Werkzeugkasten Ergänzung · Zusammenfassung Alles Wichtige auf einen Blick, ein Abschlussquiz und die Regeln, die ihr euch als Klasse mitnehmt.	Quiz, Quiz, Quiz, Wortwolke

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



1. Dein Tag mit dem Handy

Wie viel, wofür und warum: deine eigene Mediennutzung ehrlich anschauen, und was die Regeln in der Schule damit zu tun haben.

Mal ehrlich

Wann hast du heute zum ersten Mal aufs Handy geschaut? Und wann zuletzt? Die meisten unterschätzen das. Das Handy ist nicht böse, aber es ist **gebaut, um dich festzuhalten**: Benachrichtigungen, Autoplay, „noch ein Video“.

Wortwolke

Wofür nutzt du dein Handy am meisten? Ein Wort genügt.

Was dir gut tut und was nicht

Es gibt kein „richtiges“ Maß für alle. Aber es gibt Zeichen, dass es zu viel wird:

- Du bist **gereizt**, wenn du das Handy weglegen sollst
- Hausaufgaben dauern **doppelt so lang**, weil zwischendurch immer etwas aufploppt
- Du **schläfst schlechter**, weil das Handy neben dem Bett liegt
- Es gibt **Streit** zu Hause oder mit Freunden wegen des Handys

Wichtig

Du entscheidest, nicht die App. Wer merkt, dass die App entscheidet, hat schon den wichtigsten Schritt gemacht: hinschauen.

Warum die Schule Regeln hat

Handy aus im Unterricht, keine Fotos auf dem Schulhof, nichts aus dem Klassenzimmer posten: Das sind keine Schikanen. Sie schützen **alle** im Raum, auch dich. Wer im Unterricht abgelenkt ist, verpasst Stoff. Wer heimlich fotografiert wird, kann sich nicht wehren.



Quizfrage

Woran merkst du, dass das Handy zu viel Platz einnimmt?

Antwortmöglichkeiten

Ich werde gereizt, wenn ich es weglegen soll

Ich schlafe schlechter, weil es neben dem Bett liegt

Ich nutze es, um Freunde zu treffen

Ich schaue nach, wann der Bus kommt

Tipp

Drei Dinge, die sofort helfen: Benachrichtigungen für Spiele und Social Media aus. Handy nachts raus aus dem Zimmer. Eine feste handyfreie Stunde am Tag, zum Beispiel beim Essen.



2. Werbung: Warum das Spiel kostenlos ist

Werbung in Apps und Videos erkennen, In-App-Käufe durchschauen und verstehen, warum du genau diese Werbung siehst.

Nichts ist umsonst

Ein Spiel kostet nichts, ein Video kostet nichts, die App kostet nichts. Wie verdienen die dann Geld? Fast immer auf zwei Wegen:

1. **Werbung.** Jede Anzeige, die du siehst, bringt der App Geld. Je länger du bleibst, desto mehr.
2. **In-App-Käufe.** Erst ist alles kostenlos. Dann kommt die Truhe, der Skin, das Extra-Leben, „nur 2,99 €“. Viele kleine Beträge sind am Ende viel Geld.

Wichtig

Wenn du nichts bezahlst, bezahlst du mit deiner **Zeit** und deiner **Aufmerksamkeit**. Beides ist für die Anbieter bares Geld.

Werbung erkennen

Werbung versteckt sich gern. Achte auf:

- „**Anzeige**“, „**Gesponsert**“, „**Werbung**“, oft klein und grau
- Videos von Influencern, in denen ein Produkt „zufällig“ immer im Bild ist
- Belohnungen im Spiel, wenn du ein Werbevideo anschaust
- Gewinnspiele, die nur deine Daten wollen

Quizfrage

Welche davon ist Werbung?

Antwortmöglichkeiten

Ein Video, in dem ein Influencer ein Getränk zeigt und „Link in Bio“ sagt

Ein kleines graues „Gesponsert“ über einem Beitrag

„Schau dieses Video und bekomme 50 Münzen“



Warum siehst du genau diese Werbung?

Die App merkt sich, was du anschaust, wie lange, worauf du tippst. Daraus baut sie ein Bild von dir: „Mag Fußball, schaut Minecraft, 11 Jahre.“ Und zeigt dir dann genau die Werbung, die dazu passt. Das nennt man **personalisierte Werbung**. Deshalb sieht dein Freund andere Anzeigen als du.

Wortwolke

Wo ist dir zuletzt Werbung aufgefallen? Ein Wort.

Tipp

In-App-Käufe lassen sich im Handy sperren oder mit Passwort schützen. Frag zu Hause, ob das eingestellt ist. Das schützt vor dem „aus Versehen gekauft“.



3. Zustimmung? Was du beim Konto-Anlegen unterschreibst

Nutzungsbedingungen, Altersgrenzen und Berechtigungen: was hinter dem Knopf „Akzeptieren“ steckt und worauf du vor dem Tippen schaust.

Der Knopf, den alle drücken

„Ich habe die Nutzungsbedingungen gelesen und stimme zu.“ Hand aufs Herz: Hast du sie je gelesen? Fast niemand tut das. Aber mit diesem Tippen schließt du einen **Vertrag**. Deshalb lohnt es sich zu wissen, was ungefähr drinsteht.

Drei Dinge, die fast immer drinstehen

1. **Mindestalter.** Viele Dienste sind erst ab 13, manche ab 16, einige ab 18. Das ist kein Spaß: Es geht darum, welche Daten von Kindern gespeichert werden dürfen und welche Inhalte passen. Wer beim Alter schummelt, verliert diesen Schutz.
2. **Was mit deinen Daten passiert.** Welche Daten gesammelt werden, wie lange sie gespeichert bleiben, ob sie an Werbefirmen gehen.
3. **Was du der App erlaubst.** Zum Beispiel: Alles, was du hochlädst, darf die App weiterverwenden.

Wichtig

Zustimmen ist okay, wenn du weißt, **wem** du **was** erlaubst. Nicht okay ist, blind zu tippen, weil der Knopf so schön grün ist.

Berechtigungen: Was will die App von deinem Handy?

Nach der Installation fragt eine App oft: „Darf ich auf deine Kontakte zugreifen? Auf den Standort? Auf das Mikrofon?“ Überleg dabei kurz: **Braucht die App das für ihre Aufgabe?**

- Eine Karten-App braucht den Standort. Eine Taschenlampe nicht.
- Ein Messenger braucht vielleicht die Kamera. Ein Spiel braucht nicht dein Adressbuch.



Lernspiel

Die Klasse bewertet App-Berechtigungen am Handy: Was braucht die App wirklich? Danach gemeinsam auflösen.

Quizfrage

Warum haben Apps ein Mindestalter?

Antwortmöglichkeiten

Weil Daten von Kindern besonders geschützt sind

Weil manche Inhalte nicht für jedes Alter passen

Weil die App sonst zu langsam wird

Damit Erwachsene nicht gestört werden

Tipp

Bevor du ein Konto anlegst: Alter prüfen, zu Hause Bescheid sagen, Berechtigungen nur geben, wenn die App sie für ihre Aufgabe braucht. Später kannst du sie in den Einstellungen jederzeit wieder wegnehmen.



4. Wem erzählst du was? Deine Daten im Netz

Welche Daten bei Apps und Spielen anfallen, wer sich dafür interessiert und warum du selbst entscheidest, was du preisgibst.

Daten entstehen überall

Du musst nichts eintippen, damit Daten über dich entstehen. Es reicht, dass du das Handy benutzt:

- **Standort:** wo du bist, wann du wo warst
- **Kontakte:** mit wem du schreibst, wie oft
- **Nutzung:** welche Videos du schaust, wie lange, was du überspringst
- **Gerät:** welches Handy, welche Sprache, welche Uhrzeit

Dazu kommt, was du **selbst** postest: Fotos, dein Name, deine Schule, dein Hobby.

Lernspiel

Im Profil einer erfundenen Person die Stellen antippen, mit denen ein Fremder etwas anfangen kann. Danach an der Tafel besprechen, was die Klasse übersehen hat.

Wer will das wissen?

- **Werbefirmen:** um dir passende Werbung zu zeigen (siehe letzte Lektion)
- **Die App selbst:** um dich länger zu halten und mehr über dich zu lernen
- **Fremde:** wer weiß, wo du zur Schule gehst und wann du Training hast, kann dich finden
- **Betrüger:** je mehr sie über dich wissen, desto echter klingen ihre Nachrichten

Wichtig

Was einmal im Netz ist, bekommst du kaum zurück. Ein Screenshot reicht. Deshalb vorher fragen: **Würde ich das auch einem Fremden auf der Straße erzählen?**



Du entscheidest

Das nennt man **informationelle Selbstbestimmung**: ein langes Wort für einen einfachen Satz. **Deine Daten gehören dir**. Du darfst entscheiden, was du teilst, mit wem und wie lange. Niemand darf dich zwingen, dein Profil öffentlich zu machen oder deinen Standort zu teilen, auch Freunde nicht.

Quizfrage

Welche Angaben gehören nicht in ein öffentliches Profil?

Antwortmöglichkeiten

Der Name deiner Schule

Deine Adresse oder dein Wohnort mit Straße

Wann du immer allein nach Hause gehst

Dein Lieblingsspiel

Tipp

Profil auf **privat** stellen, Standort nur teilen, wenn es gerade nötig ist, und bei jedem Foto kurz schauen, was im Hintergrund zu sehen ist: Straßenschild, Schulgebäude, Namensschild.



5. Stimmt das? Informationen prüfen

Woher kommt das, wer sagt das, kann das sein? Drei Fragen vor dem Glauben und Weiterleiten, und wie eine Suchmaschine entscheidet, was oben steht.

Nicht alles, was gut aussieht, ist wahr

Im Netz kann **jeder** alles schreiben. Ein schickes Bild, viele Likes, ein Logo: nichts davon beweist, dass es stimmt. Deshalb gibt es drei Fragen, die du vor dem Glauben und vor dem Weiterleiten stellst.

Die drei Fragen

1. **Woher kommt das?** Gibt es eine Quelle? Eine Seite, einen Namen, ein Datum? Oder nur „ein Freund hat gesagt“?
2. **Wer sagt das und warum?** Will die Person informieren, verkaufen, Aufmerksamkeit oder Streit?
3. **Kann das überhaupt sein?** Klingt es zu gut, zu schlimm oder zu verrückt, ist es oft erfunden.

Wichtig

Wenn du eine der drei Fragen nicht beantworten kannst: **nicht weiterleiten**.
Lieber einmal zu wenig geteilt als einmal einen Quatsch verbreitet.

Lernspiel

Fünf Schlagzeilen, echt oder erfunden? Die Klasse stimmt am Handy ab, danach zeigt die Tafel die Begründung.

Wie eine Suchmaschine arbeitet

Eine Suchmaschine „weiß“ nichts. Sie hat vorher Milliarden Seiten eingesammelt und in einem riesigen **Register** (Index) abgelegt, wie das Stichwortverzeichnis in einem Buch. Tippst du etwas ein, schaut sie im Register nach, welche Seiten das Wort enthalten, und sortiert sie: nach Beliebtheit, nach Aktualität, danach, was andere angeklickt haben, und



manchmal nach bezahlter Werbung.

Das heißt: **Oben steht nicht automatisch das Richtige.** Oben steht, was die Maschine für passend hält, oder was jemand bezahlt hat.

Quizfrage

Warum steht ein Treffer in der Suchmaschine ganz oben?

Antwortmöglichkeiten

Weil viele Leute ihn anklicken oder verlinken

Weil jemand dafür bezahlt hat (Anzeige)

Weil die Suchmaschine geprüft hat, dass er stimmt

Weil er der neueste ist, immer

Tipp

Such dasselbe mit zwei verschiedenen Wörtern oder auf zwei Seiten. Stimmen die Antworten überein, ist das ein gutes Zeichen. Widersprechen sie sich, frag jemanden, der sich auskennt.



6. Der Klassenchat

Regeln, die im Chat anders sind als auf dem Schulhof, was aus einem Witz werden kann, und wie ihr Streit im Chat wieder einfängt.

Warum der Chat anders ist als der Schulhof

Auf dem Schulhof siehst du das Gesicht der anderen. Du merkst, ob ein Spruch ankommt oder verletzt. Im Chat fehlt das: **kein Gesicht, keine Stimme, keine Pause**. Dafür lesen alle mit, alles bleibt gespeichert, und ein Screenshot ist in zwei Sekunden gemacht.

Deshalb passiert im Chat schneller etwas, das keiner wollte: Ein Witz wird zur Beleidigung, eine Frage wird ignoriert, ein Bild wird weitergeleitet.

Wortwolke

Was nervt dich im Klassenchat am meisten? Ein Wort.

Regeln, die sich bewährt haben

- **Nachts Ruhe.** Keine Nachrichten nach einer festen Uhrzeit, egal wie wichtig.
- **Keine Bilder von anderen** ohne zu fragen. Nie.
- **Nichts, was du nicht laut vor der Klasse sagen würdest.**
- **Nicht alle müssen antworten.** Dreißig „ok“ sind dreißig Störungen.
- **Streit nicht im Chat austragen.** Im Chat eskaliert alles, im Gespräch nicht.

Wichtig

Schreib so, dass du es auch noch gut findest, wenn deine Oma oder deine Klassenlehrerin es liest. Weil beides passieren kann.

Wenn es schon schief läuft

Jemand wird beleidigt, ein peinliches Bild macht die Runde, einer wird aus der Gruppe gemobbt. Dann:



1. **Nicht mitmachen.** Auch kein Lach-Emoji. Mitlachen ist Mitmachen.
2. **Screenshot als Beweis,** nicht zum Weiterleiten.
3. **Sagen, dass es nicht okay ist,** am besten direkt und ruhig.
4. **Hilfe holen:** Eltern, Lehrkraft, Vertrauenslehrer. Das ist kein Petzen. Petzen ist, wenn man jemandem schaden will. Hilfe holen ist, wenn man jemanden schützen will.

Quizfrage

**Jemand postet im Klassenchat ein peinliches Foto von einem Mitschüler.
Was tust du?**

Antwortmöglichkeiten

- Nicht weiterleiten und nicht darauf reagieren
- Der Person sagen, dass das nicht okay ist
- Einer Lehrkraft oder den Eltern Bescheid sagen
- Ein Lach-Emoji schicken, war ja nur Spaß

Tipp

Macht in der Klasse drei Chat-Regeln aus, die alle unterschreiben. Drei reichen.
Hängt sie ins Klassenzimmer.



7. Fremde im Netz: Wer schreibt dir da?

Warum Fremde online nett sind, welche Nachrichten ein Warnsignal sind, und wo du Hilfe bekommst, ohne Ärger zu kriegen.

Jeder kann jeder sein

Im Spiel, in der App, im Chat: Du siehst einen Namen und ein Bild. Beides kann **frei erfunden** sein. Hinter „Lena, 12“ kann jeder sitzen. Die meisten Menschen im Netz sind okay. Aber die wenigen, die es nicht sind, sind genau deshalb so vorsichtig und so freundlich.

Warnsignale

Eine Nachricht ist ein Warnsignal, wenn jemand, den du nicht aus dem echten Leben kennst,

- dich **auffällig oft lobt** und sagt, du seist etwas Besonderes
- fragt, ob du **allein** bist oder ob deine Eltern mitlesen
- will, dass ihr in einen **anderen Chat** wechselt, wo niemand mitliest
- nach **Fotos** fragt, erst harmlos, dann weniger harmlos
- dir **Geschenke**, Spielwährung oder Skins anbietet
- sagt, das sei **euer Geheimnis**

Wichtig

Geheimnisse mit Fremden sind nie okay. Wer dich bittet, etwas vor deinen Eltern zu verstecken, meint es nicht gut mit dir. Ohne Ausnahme.

Was du tust

1. **Nicht antworten**, nicht diskutieren, nichts schicken.
2. **Blockieren und melden.** Jede App hat dafür einen Knopf.
3. **Erzählen.** Eltern, Lehrkraft, ein Erwachsener, dem du vertraust. Du bekommst keinen Ärger. Du hast nichts falsch gemacht, die andere Person hat es.

Und wenn du schon etwas geschickt hast, das du bereust: **Trotzdem erzählen.** Je



früher, desto besser lässt es sich stoppen. Niemand wird dich dafür bestrafen.

Quizfrage

Welche Nachricht von einem Online-Bekannten ist ein Warnsignal?

Antwortmöglichkeiten

„Sind deine Eltern gerade da? Lass uns woanders schreiben.“

„Das bleibt unser Geheimnis, okay?“

„Ich schenk dir Skins, schick mir dafür ein Foto.“

„GG, gut gespielt, bis morgen.“

Tipp

Hilfe, auch ohne Namen: **Nummer gegen Kummer 116 111** (kostenlos, anonym).
Online melden: **jugendschutz.net**. Und immer: ein Erwachsener, dem du vertraust.



8. Dein Schloss: Passwort und Gerätesperre

Warum dein Zugang schützenswert ist, wie ein gutes Passwort aussieht, das du dir merken kannst, und warum du es nie teilst, auch nicht mit der besten Freundin.

Warum überhaupt?

Dein Handy und deine Accounts sind wie dein Zimmer: Da sind deine Fotos, deine Chats, deine Spiele. Ohne Schloss kann jeder rein, der das Handy findet oder dein Passwort errät. Dann schreibt plötzlich „du“ Blödsinn in den Klassenchat, oder jemand kauft mit deinem Spiele-Account ein.

Die Gerätesperre

Das Erste und Einfachste: eine **Sperre** fürs Handy. PIN, Muster, Fingerabdruck oder Gesicht. Ohne Sperre ist alles andere egal. Und: **1234** oder dein Geburtsdatum sind keine Sperre, die errät jeder.

Ein gutes Passwort, das du dir merken kannst

Lang schlägt kompliziert. Der einfachste Trick: **vier Wörter, die nichts miteinander zu tun haben**, zum Beispiel KatzeBrotRegenGitarre. Das ist leicht zu merken und für einen Computer sehr schwer zu knacken. Zahlen oder Zeichen dazwischen machen es noch stärker.

Schlecht sind: dein Name, dein Haustier, dein Lieblingsverein, `password`, 123456 und alles, was auf deinem Profil steht.

Lernspiel

Die Klasse tippt Beispielpasswörter ein und sieht, wie lange ein Computer dafür bräuchte. Übertragen wird nur das Muster, nie das Passwort, das steht auch auf den Handys.

Wichtig

Ein Passwort, ein Account. Wer überall dasselbe nimmt, verliert bei einem Leck



alles auf einmal. Und: Passwörter **teilt man nicht**, auch nicht mit der besten Freundin. Freundschaften ändern sich, Passwörter bleiben.

Quizfrage

Welches Passwort ist am besten?

Antwortmöglichkeiten
Max2014
passwort123
WolkeTellerLampeFrosch
111111

Tipp

Frag zu Hause, ob ihr einen **Passwort-Manager** nutzt. Der merkt sich alle Passwörter, du nur eins. Und schalte, wo es geht, die **zweite Bestätigung** ein (Code aufs Handy): Dann nützt ein geklautes Passwort allein nichts.



9. Wo ist mein Foto gespeichert?

Gerät, Server, Cloud: wo deine Sachen wirklich liegen, welchen Weg eine Nachricht durchs Netz nimmt, und warum ein Foto von anderen deren Erlaubnis braucht.

Drei Orte

Wenn du ein Foto machst, liegt es zuerst **auf deinem Gerät**. Schickst du es in den Chat, liegt es zusätzlich **auf einem Server** des Anbieters, einem großen Computer in einem Rechenzentrum. Schaltest du die Sicherung ein, liegt es auch in der **Cloud**: wieder ein Server, nur dass du ihn wie einen Ordner benutzen kannst.

Ort	Vorteil	Nachteil
Dein Gerät	Nur du hast es	Handy weg, Foto weg
Server des Chats	Freunde bekommen es	Der Anbieter hat eine Kopie, auch wenn du es löschst
Cloud	Überall abrufbar, Sicherung	Liegt bei einer Firma, oft in einem anderen Land

Wichtig

„Gelöscht“ auf deinem Handy heißt nicht gelöscht auf dem Server. Was du verschickst, ist nicht mehr nur deins.

Der Weg einer Nachricht

Das Internet ist kein einzelner Draht, sondern ein **Netz aus vielen Knoten**: dein Handy, der WLAN-Router, der Anbieter, Server irgendwo auf der Welt, der Router deiner Freundin, ihr Handy. Deine Nachricht springt von Knoten zu Knoten, und fällt einer aus, nimmt sie einen anderen Weg. Das macht das Netz so robust. Und es heißt: Unterwegs kommt die Nachricht an vielen fremden Rechnern vorbei. Deshalb ist **Verschlüsselung** wichtig; die lernst du in den nächsten Klassen genauer kennen.

Dein Handy ist dabei der **Client** (der fragt), der Server ist der, der antwortet. Jede App, jede Webseite funktioniert so.



Quizfrage

Du löschst ein Foto aus dem Chat auf deinem Handy. Was stimmt?

Antwortmöglichkeiten

Auf dem Server des Anbieters kann es weiterhin liegen

Wer es schon bekommen hat, hat es weiterhin

Es ist überall weg

Der Anbieter wird sofort benachrichtigt und löscht es

Fotos von anderen

Jeder Mensch hat das **Recht am eigenen Bild**. Das heißt: Ein Foto, auf dem jemand erkennbar ist, darfst du nur weitergeben oder posten, wenn die Person **einverstanden** ist. Bei Mitschülern also: vorher fragen. Bei einem Nein: nicht posten. Auch nicht „nur im Klassenchat“.

Wortwolke

Wen müsstest du fragen, bevor du euer letztes Gruppenfoto postest? Ein Wort: alle, keinen, Lehrer, ...

Tipp

Vor dem Teilen eines Fotos drei Sekunden: Wer ist drauf? Habe ich gefragt? Was sieht man im Hintergrund?



10. Zusammenfassung: Dein Start-Werkzeugkasten

Alles Wichtige auf einen Blick, ein Abschlussquiz und die Regeln, die ihr euch als Klasse mitnehmt.

Was du jetzt kannst

Du entscheidest, nicht die App. Benachrichtigungen aus, Handy nachts raus, eine handyfreie Stunde.

Nichts ist umsonst. Werbung erkennen, In-App-Käufe sperren, wissen, warum du genau diese Werbung siehst.

Zustimmen mit Verstand. Mindestalter ernst nehmen, Berechtigungen nur, wenn die App sie braucht.

Deine Daten gehören dir. Profil privat, kein Schulname, keine Adresse, kein Tagesablauf.

Erst prüfen, dann glauben. Woher? Wer? Kann das sein? Oben in der Suche steht nicht automatisch das Richtige.

Im Chat wie auf dem Schulhof, nur vorsichtiger. Keine Bilder ohne Fragen, nichts, was du nicht laut sagen würdest, Streit nicht im Chat.

Fremde bleiben Fremde. Geheimnisse mit Fremden sind nie okay. Blockieren, melden, erzählen. Nummer gegen Kummer 116 111.

Dein Schloss. Gerätesperre, vier Wörter als Passwort, nie teilen.

Gelöscht ist nicht gelöscht. Was du verschickst, liegt auf Servern. Fotos von anderen nur mit Erlaubnis.

Wichtig

Du musst nicht alles perfekt machen. Wer diese Regeln kennt, ist schon viel sicherer als die meisten Erwachsenen.



Abschlussquiz

Quizfrage

Was machst du, wenn ein Online-Bekannter sagt: „Das bleibt unser Geheimnis“?

Antwortmöglichkeiten

Nicht antworten, blockieren, einem Erwachsenen erzählen

Mitmachen, ist ja nur ein Spiel

Erst mal abwarten, was er noch schreibt

Ein Foto schicken, damit er Ruhe gibt

Quizfrage

Welche drei Fragen stellst du vor dem Weiterleiten einer Nachricht?

Antwortmöglichkeiten

Woher kommt das?

Wer sagt das und warum?

Kann das überhaupt sein?

Wie viele Likes hat das?

Quizfrage

Was gehört zu einem guten Schutz deines Handys?

Antwortmöglichkeiten

Gerätesperre, die nicht 1234 ist

Ein langes Passwort aus mehreren Wörtern

Passwort nicht mit Freunden teilen

Dasselbe Passwort überall, damit du es nicht vergisst

Wortwolke

Welche Regel nimmst du aus diesem Kurs mit? Ein Wort.



Tipp

Lehrkraft: Die drei Chat-Regeln aus der Klassenchat-Lektion jetzt gemeinsam festlegen und aufhängen. Das ist das, was von diesem Kurs am längsten bleibt.

