Course materials for the teacher

Digitale Selbstverteidigung Klasse 8: Deine Daten, deine Geräte

8 lessons · approx. 90 minutes of teaching · 18 interactive tasks · As of: 23/11/2026

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

How the course works

You lead the course at the board and decide yourself when to cover which lesson. The course does not expire. The class does not sign up: no names, no account, no signing in at the start of the lesson. You unlock interactive tasks one by one: a QR code appears on the board for each, the class answers on their phones, and “Reveal” shows the correct answer on the board and on every phone at the same time. The answer key to all quiz questions is in your cockpit; this open PDF deliberately leaves it out so it does not reach the class in advance. At the end you close the course. Nobody in the class registers; there are no names, accounts or e-mail addresses and therefore no individual certificates. This course has no phishing training, which is only part of the course “Digital self-defence”.

What you need: a projector or display with internet access, and the class with smartphones. Anyone without a phone joins in with their neighbour.

Link to the Baden-Württemberg curriculum

Klasse 8 (etwa 13 bis 14 Jahre) · Scope: zwei Doppelstunden, Lektionen einzeln einsetzbar · As of 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. Fields of action of the guiding perspective “Living and learning in a digital world”: Verantwortungsvoll handeln und schützen, Digital kommunizieren, kooperieren, handeln.

Area	Competence (reading guide for computer science and media education 2026/27 or 2016 curriculum)

Digitalität und Partizipation	Situationen der Datenerhebung; Interessen der Akteure; informationelle Selbstbestimmung Lessons: 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 Lessons: 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

This mapping is the provider's professional assessment, not an official approval. For grades 8 to 10, the 2016 curriculum applies until the computer science and media education curriculum takes effect (2027/28).

Overview of the lessons

Lesson		Interactive tasks
1.	**Introduction: What Does the Internet Know About You?** Grade 8 · Digitalität und Partizipation Why digital self-defence matters to you and what happens in this course.	Word cloud, Quiz
2.	**Social Media: What Your Apps Really Know About You** Grade 8 · Digitalität und Partizipation Instagram, TikTok, Snapchat: how platforms collect and use your data.	Word cloud, Quiz
3.	**Your Data, Your Rights: What the Law Says** Grade 8 · Digitalität und Partizipation What data protection has to do with you and what rights you have.	Quiz, Quiz
4.	**Where is my message right now? How the internet works** Grade 8 · Kommunikation und Sicherheit Nodes, routers, servers: which route a message takes, what client and server are, and why the storage location decides who can see your data.	Quiz, Quiz, Word cloud
5.	**Encryption: the padlock in the browser and the Caesar trick** Grade 8 · Kommunikation und Sicherheit Why WhatsApp and the padlock in the browser protect you, what end-to-end means, and how you can encrypt and crack messages yourself with the Caesar trick.	Quiz, Quiz, Word cloud

6.	**Passwords and Accounts: What Belongs to You and What You Never Share** Grade 8 · Kommunikation und Sicherheit Why every password has to be unique and what two-factor authentication does for you.	Game: passwort-knacker, Quiz
7.	**Securing Your Smartphone: PIN, Apps and Permissions** Grade 8 · Kommunikation und Sicherheit Why your phone is your most important device and how to protect it properly.	Game: berechtigungen, Quiz
8.	**Zusammenfassung: Deine Daten, deine Geräte** Supplement · Zusammenfassung Sicherung der Klasse-8-Reihe: Datenspuren, Rechte, Netz, Verschlüsselung, Passwörter, Smartphone.	Word cloud, Quiz

The following pages contain each lesson in full, with all quiz questions and answer options. You will find the marked solutions only in your Cockpit.

1. Introduction: What Does the Internet Know About You?

Why digital self-defence matters to you and what happens in this course.



Welcome to digital self-defence

Before we start, an honest question: how much does the internet actually know about you? Probably more than you think, and above all more than you've ever consciously put in.

Word cloud

What absolutely has to stay private for you?

What this course is about

Over the next few lessons it's not about technology, it's about you: how strangers get hold of your data, what they do with it, and how you stop that. We'll look at social media, gaming, your smartphone, your passwords, and right at the end you'll get a few fake emails without warning, to see whether it has sunk in.

Important

Anything you put on the internet can be found by strangers. Even if you think only your friends can see it.

Why this matters already

Imagine someone knows your full name, your school, your favourite game and the name of your pet. Sounds harmless? With this information, someone can:

- **Guess your password** (lots of people use their pet's name)
- Write you a **fake message** that matches your interests exactly
- **Pretend to be your friend** and fool other people

This isn't theory, it happens every day, thousands of times. And that's exactly why you're here.

Quiz question

Which of these pieces of information should you never post publicly?

Answer options
Your favourite song
Your mobile number
Your date of birth including the year
Your favourite film
Your address
The name of your school and your class

Tip

Rule of thumb: anything someone could use to find you, contact you or pretend to be you doesn't belong in a public profile.

2. Social Media: What Your Apps Really Know About You

Instagram, TikTok, Snapchat: how platforms collect and use your data.



Your profile is only the surface

You post a photo, like a reel, scroll through TikTok. Sounds harmless. But behind every swipe, the platforms collect data about you, far more than you think.

What Instagram, TikTok & co. store about you

What you do	What the app stores
Watch a reel	How long you watch, whether you swipe on or watch again
Post a photo	Location, time, device type, who sees it
Follow someone	Your social network, who knows whom
Type in the app	Even texts you **never sent** are partly recorded
Carry your phone with you	Movement profile from location data

Important

> TikTok, for example, says in its own privacy policy that it collects: device ID, IP address, keystrokes, browsing history within the app, biometric data (facial and voice features) and location. And that's only what they officially admit.

Why is this a problem?

1. You are the product. The apps are free because you pay with your data. The more they know about you, the more precisely they can target ads at you and the more money they make.

2. Data can be stolen. When a platform gets hacked, your data ends up on the dark web. That has already happened to TikTok, Facebook, Instagram and Snapchat, several times, with millions of accounts.

3. Your digital footprint stays. What you post today can still turn up in ten years' time, in a job application, a scholarship application or an argument.

What you can do

- **Set your profile to private**: possible on Instagram, TikTok and Snapchat
- **Turn off location**: most apps don't really need your location
- **Check permissions**: does TikTok really need access to your contacts?
- **Clean up old posts regularly**: what was funny two years ago doesn't have to be online forever

> **Tip**
>
> Go to your phone's settings now → Apps → Permissions. Look at which app is allowed to access what. You'll be surprised.

Puzzle: Data detective

Someone posts on Instagram:

- A selfie in front of their school (school name visible on the sign)

- A story saying "Finally 16! □" on 15 March
- Bio: "Gaming □ | Mainz | @max_gamer on Discord"

Word cloud

What information could a stranger piece together from this?

Quiz question

What does a social media app typically collect about you?

Answer options
Your location
How long you watch each video
Your address book, if you allow it
Only what you post yourself

3. Your Data, Your Rights: What the Law Says

What data protection has to do with you and what rights you have.



Data protection isn't boring, it protects you

If someone takes a photo of you and posts it without your okay, that's not just rude, in most cases it's **illegal**. The General Data Protection Regulation (GDPR) and, in Germany, the right to your own image (*Recht am eigenen Bild*) give you real rights.

Your most important rights

1. Right to information: you're allowed to know what data a service stores about you. On Instagram, TikTok and co. you can request a copy of your data, and you'll be amazed at everything in it.

2. Right to erasure: you can demand that your data is deleted. This also applies to photos and videos that other people have posted of you.

3. Right to your own image: nobody may publish photos or videos of you without your consent. That also applies at school, at parties and at your sports club.

4. Right to be forgotten: on request, search engines must remove links to outdated or irrelevant information about you.

What others are not allowed to do

Situation	Allowed?
A classmate posts a photo of you without asking	□
Someone forwards your private chat	□
An app passes your data on to ad networks without telling you	□
Your parents look at your phone (you're under 18)	□ Grey area, depends on age and context

> **Important**
>
> "I've got nothing to hide" isn't an argument. Data protection doesn't mean you're hiding something. It means that **you decide** who finds out what about you.

What you can do if your rights are violated

1. **Talk to the person directly**: "Please take the photo down."
2. **Report it to the platform**: all the big services have reporting functions
3. **Get your parents or a teacher involved**: especially if it's about bullying
4. **Make an official complaint**: to the data protection authority (in Germany, the one for your federal state; free of charge)

> **Tip**
>
> Take screenshots as evidence **before** you ask for it to be deleted. Once it's deleted, nothing can be proven any more.

Quiz: Your rights

Is that true? Discuss it as a class.

1. "If I'm under 16, social networks need my parents' consent."
2. "Anything I've posted on the internet can never be deleted."
3. "My teacher is allowed to film me in class without permission."
4. "If a friend knows my password and logs in, that isn't hacking."

Quiz question

Which statements are true?

Answer options
Under 16, social networks need parental consent.
Anything posted can never be deleted again.
My teacher may film me in class without permission.
If a friend logs in with my password, that isn't hacking.

Quiz question

What rights do you have towards a provider that has stored data about you?

Answer options
You can find out what's stored
You can demand deletion
You can have incorrect information corrected
You have to be an adult to do this

4. Where is my message right now? How the internet works

Nodes, routers, servers: which route a message takes, what client and server are, and why the storage location decides who can see your data.



Not a wire, a network

Many people imagine the internet as a cable: from your phone to your friend's phone. In reality it is a **meshed network** of millions of nodes: your phone, the Wi-Fi router, the provider, switching computers, undersea cables, data centres, another provider, a router, a phone.

Your message is split into small packets. Each packet hops from node to node, and each node only decides: "Where next?" If one route fails, the packets take another. That's why the network keeps working even when a cable breaks somewhere.

> **Important**
>
> On its way, your message passes **many strangers' computers** that you don't know. That's exactly why encryption isn't a gimmick: it's what stops others from reading along.

Client and server

Your phone **asks** ("Show me the video", "Send this message"), a big computer in a data centre **answers**. The one asking is called the **client**, the one answering the **server**. Every app, every website, every game works like this, even if it feels as if everything is "on your phone".

The flip side: the server sees everything you send it. Whoever runs the server has your data. It isn't the technology that decides about your privacy, it's **the operator**.

Where is your stuff?

Storage location	Example	Who can get at it?	When you delete it
Your device	Photos in your gallery	You, or whoever gets hold of your phone	Gone (except for backups)
Server on the school network	Files on the school server	You, teachers, school IT	According to the school's rules
The provider's server	Chat messages, posts	You, recipients, the provider	Your copy is gone, the others stay
Cloud	Online storage, backups	You, the provider, possibly authorities in the country where the server is	Often only permanently after a waiting period

When comparing, four things count: **availability** (can I get at it from anywhere?), **collaboration** (can others join in?), **security** (who can read along or steal it?) and **operator** (who owns the server, which country is it in, which rules apply there?).

Quiz question

What is true about the route a message takes on the internet?

Answer options
It is split into packets that travel across many nodes
If one route fails, the packets take another
There is a direct line from phone to phone

Technically, only the recipient can see the packets

Quiz question

You want to write a presentation together with three classmates. Which storage location fits best, and what do you pay attention to?

Answer options
Cloud or school server, because everyone can work on it at the same time
Check first who runs the service and where the server is
Only on my phone, that's the safest for working together
Doesn't matter where, as long as it's free

Word cloud

Which devices lie on the route between you and a friend when you chat? One word per answer.

Tip

If you want to know where a service keeps its servers: the privacy policy usually says so under "Hosting" or "Storage location". Germany or the EU means: European data protection rules (the GDPR) apply.

5. Encryption: the padlock in the browser and the Caesar trick

Why WhatsApp and the padlock in the browser protect you, what end-to-end means, and how you can encrypt and crack messages yourself with the Caesar trick.



Who is reading along?

Every message you send passes through dozens of strangers' computers: your Wi-Fi, the router in the café, the provider, servers somewhere in the world. Without encryption, any of them could read along, like with a postcard.

Encryption turns your text (the **plaintext**) into an unreadable **ciphertext**. Only someone with the matching **key** can make it readable again.

> **Important**
>
> Encoding is not encryption. **Anyone** who knows the rule can translate a QR code or Morse code back. Encryption also needs a **key** that only the right people have.

Two kinds you use every day

Transport encryption: the padlock in the browser (the "https"). Between your phone and the website nobody can read along, not even on open Wi-Fi. But: the operator of the website sees everything you enter there.

End-to-end encryption: WhatsApp, Signal, Threema. The message is encrypted on your phone and only decrypted again on the recipient's phone. Not even the provider can read it.

> **Tip**
>
> No padlock in the browser, or the browser warns you about the site? Then **never** enter a password or bank details there. No matter how real the site looks.

The Caesar trick

Julius Caesar already encrypted messages: every letter is shifted along the alphabet by a fixed number. The key is that number.

With key **3**, A becomes D, B becomes E, H becomes K:

```
Plaintext:  H E L L O
Ciphertext: K H O O R
```

Try it: encrypt your first name with key 3. At the end of the alphabet you carry on at the start, so X becomes A.

Quiz question

You intercept the ciphertext **VHFXUH. You know it's Caesar with key 3. What does it say?**

Answer options
SCHOOL
SECURE
SEARCH

SINGER

Why Caesar is useless today

There are only **25 possible keys**. An attacker simply tries them all. That's called **brute force**: not clever, but fast. A computer manages it in less than a second.

It's even faster with **frequency analysis**: in English, E is the most common letter. So the most common letter in the ciphertext is very likely the shifted E, and the key is already known.

> **Important**
>
> Exactly the same thing happens with **short passwords**: a computer tries every possibility. The more possible keys, the longer it takes. That's why long passwords and modern encryption with keys hundreds of digits long win.

Quiz question

What is true?

Answer options
With the padlock in the browser nobody on the Wi-Fi can read along, but the site operator can
With end-to-end encryption not even the provider can read the message
A QR code is secure encryption
Caesar is secure because hardly anyone knows it any more

Word cloud

Where do you come across encryption in everyday life? One word is enough.

6. Passwords and Accounts: What Belongs to You and What You Never Share

Why every password has to be unique and what two-factor authentication does for you.



Your password is your house key

Imagine you have one key that opens your front door, your locker, your bike lock and your gym locker. Sounds handy, until you lose it. Then everything is gone.

That's exactly what happens when you use the same password everywhere.

Why one password isn't enough

When a website gets hacked (and that happens all the time), the usernames and passwords end up on the dark web. Attackers then automatically try these combinations on hundreds of other sites. This is called **credential stuffing**.

So if you use the same password for Instagram, your email and your gaming account, and Instagram gets hacked, then **all three accounts** are at risk.

> **Important**
>
> The rule is simple: **One account, one password.** No password may be in use for two services at the same time.

What makes a secure password

Bad	Why	Better
JohnSmith2009	Name + year of birth = guessable	correct-horse-battery-staple
123456789	Most common password in the world	Combine random words
Summer2024!	Pattern used by millions	Use a password manager

A good password is:

- At least 12 characters long
- Not guessable (no name, date of birth, pet)
- Unique for every account

The easiest method: take four random words and join them: "Giraffe-Piano-Cloud-Seven". Long, memorable, secure.

Password manager: your digital key ring

A password manager stores all your passwords encrypted. You only need to remember **one** master password. The manager generates and fills in all the others automatically.

Free options: Bitwarden, KeePassXC, the keychain/password function from Apple/Google.

Two-factor authentication (2FA)

2FA means: even if someone knows your password, they also need a second factor, usually a code on your phone.

Where you should turn on 2FA right away:



1. Your email (it's the key to all your other accounts)
2. Your gaming accounts (Steam, Epic, Riot)
3. Social media (Instagram, TikTok, Snapchat)
4. Anything to do with money

What belongs to you and what you never share

✅ You can share	❌ You never share
Your gamertag	Your password
Your favourite film	Your birthday including the year
Your public profile	Your address
Screenshots (without sensitive data)	Your ID card / student ID
Your Discord server	Your email login

> **Tip**
>
> **Not even with your best friend.** Friendships change. Passwords you've shared can't be "taken back". And your friend could get hacked without meaning to, and then the attacker has your access too.

Puzzle: Password check

Which of these passwords are secure?

1. `Football2009` → ❌ (word + year of birth)
2. `kT9$mP2!xR4#` → ✅ (random, but hard to remember)
3. `Elephant-Ketchup-Drum-42` → ✅ (long, random, memorable)
4. `ILoveYou` → ❌ (in the top 20 most common passwords)
5. `qwerty` → ❌ (keyboard pattern)

> **Learning game**
>
> **Think up a password and see how long it holds out. Only the pattern is transmitted,**



Quiz question

What really makes a password strong?

Answer options
Length
An exclamation mark at the end
That it's only used for one single service
That you can remember it easily because it's your birthday
That it doesn't appear anywhere else

7. Securing Your Smartphone: PIN, Apps and Permissions

Why your phone is your most important device and how to protect it properly.



Your phone is the key to everything

Your smartphone isn't just a phone. It's your bank account, your inbox, your photo album, your satnav and your ID all in one. Whoever has access to your phone has access to your entire digital life.

Basic protection: lock and biometrics

Method	Security	Recommendation
No lock screen	None	Never
Swipe pattern	Very weak (smudges give the pattern away)	No
4-digit PIN	Weak (10,000 possibilities)	Minimum
6-digit PIN	Better (1 million possibilities)	Good
Fingerprint	Strong + fast	Recommended

Method	Security	Recommendation
Face ID / face recognition	Strong (on newer devices)	Recommended

> **Important**
>
> The **most common PINs** in Germany: 1234, 0000, 1111, 2580 (vertical line), year of birth. If yours is one of them: change it now.

App permissions: who's allowed to do what?

Every app asks for permissions. But not every app needs what it asks for:

- **Camera**: Instagram needs it, a torch app doesn't
- **Microphone**: a voice app needs it, a game doesn't
- **Contacts**: WhatsApp needs them, a weather service doesn't
- **Location**: Google Maps needs it, a calculator doesn't

Wi-Fi security: open networks are dangerous

Free Wi-Fi on the train, in a café or at the station sounds great. But on open networks, anyone can read what you're doing. This is called a **man-in-the-middle attack**: someone sits between you and the internet and reads along.

Rules for public Wi-Fi:

- No online banking, no logging in to important accounts
- Use a VPN (there are free versions)
- Turn off automatic Wi-Fi connection

> **Tip**
>
> Go to your Wi-Fi settings and delete all the networks you don't need any more. Otherwise your phone automatically connects to any network with the same name, and an attacker can easily fake a "Starbucks WiFi".

Updates: the most boring protection and the most important

Every update closes known security holes. If you put off updates, you're leaving a door open that attackers know exists.

- Install **operating system updates** straight away
- Run **app updates** regularly
- **Delete apps** you no longer use: fewer apps mean less attack surface

---

Quiz: How secure is your phone?

Check your device now:

1. Do you have a PIN or biometrics turned on? □ / □
2. Is your operating system up to date? □ / □
3. Do you have apps installed that you haven't used for months? □ / □
4. Does an app use permissions it doesn't need? □ / □

You get one point for every □ on 1–2 and every □ on 3–4. If you have all four points, you're in good shape.

Learning game

Six apps, six permissions. Let the class vote, then compare on the board.

Quiz question

Which permission is definitely suspicious for a torch app?

Answer options
Location
Contacts
Camera flash
Microphone

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.

> **Important**
>
> 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-Profile, geklonte Stimmen, Betrug in Spielen und Phishing, mit einem echten Praxistest am Ende.

Word cloud

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

Quiz question

Welche Aussage stimmt?

Answer options
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.