Course materials for the teacher

Digitale Selbstverteidigung Klasse 9/10: Angriffe erkennen

6 lessons · approx. 90 minutes of teaching · 15 interactive tasks · As of: 23/11/2026

Fake-Profile, geklonte Stimmen, Betrug in Spielen, Datenschutz im Praktikum und Phishing, mit Praxistest zum Schluss.

How the course works

You lead the course at the board and decide yourself when to cover which lesson. The course does not expire. This course includes the phishing training: a great chance to practise what was learned on one's own device, in one's own inbox. Only for this does the class sign in via QR code in the first lesson; a first name is enough to take part. 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, which starts the phishing training: three simulated scam attempts by e-mail over the following weeks. Only students with parental consent (template: letter to parents) and a stored e-mail address can take part. The certificate confirms successful participation in this training and is only issued to participants.

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

Klassen 9 und 10 (etwa 14 bis 16 Jahre) · Scope: zwei Doppelstunden plus Praxistest in den Wochen danach · As of 03.10.2026

Angriffe erkennen: Fake-Profile und Social Engineering, Fake-Stimmen, Betrug in Spielen, Datenschutz im Praktikum und Phishing. Schließt mit dem Phishing-Praxistest ab, mit Einverständnis der Eltern. Fields of action of the guiding perspective “Living and learning in a digital world”: Verantwortungsvoll handeln und schützen, Digital kommunizieren, kooperieren, handeln, Informationen sammeln, verstehen, bewerten.

Area	Competence (reading guide for computer science and media education 2026/27 or 2016 curriculum)
Digitalität und Partizipation	Akteure und Interessen; Vertrauenswürdigkeit; Desinformation und Deepfakes Lessons: Fake-Profile, Deepfakes und Fake-Stimmen
Leitperspektive Medienbildung	Jugendmedienschutz, Informationelle Selbstbestimmung und Datenschutz, Kommunikation und Kooperation
Aufbaukurs Informatik, 3.1.4 Informationsgesellschaft und Datensicherheit	(6) Anfall personenbezogener Daten, Nutzen und Risiken

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.	**Fake Profiles, Catfishing and Social Engineering** Grade 9/10 · Digitalität und Partizipation How scammers pretend to be someone else and try to manipulate you.	Quiz, Word cloud, Quiz
2.	**Deepfakes and Fake Voices: Don't Trust Everything You See and Hear** Grade 9/10 · Digitalität und Partizipation How AI fakes deceptively real videos and voices, and how not to get fooled.	Quiz, Game: faktencheck
3.	**Gaming: Account Theft, Scams and How to Protect Yourself** Supplement · Praxis Betrug im Alltag Why your gaming account is valuable and how scammers try to steal it.	Word cloud, Quiz
4.	**Data Protection at Work: Why Secrets Are Worth Money Later** Supplement · Praxis Datenschutz (BP 2016, 3.1.4 (6)) The data protection game. Finding traces in a profile and building the bridge to working life.	Game: datenschutz, Game: orion, Quiz, Quiz
5.	**Recognising Phishing, Even When It Looks Like Your Favourite Game** Supplement · Praxis Phishing How to spot fake messages and links before you click on them.	Quiz, Game: phishing-duell, Quiz
6.	**Summary: Your Digital Toolkit** Supplement · Zusammenfassung Everything important at a glance and preparation for the practical phishing test.	Word cloud

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. Fake Profiles, Catfishing and Social Engineering

How scammers pretend to be someone else and try to manipulate you.



Not everyone is who they claim to be

You get a friend request from someone with a nice profile picture, mutual friends and similar interests. Everything looks genuine. But is it?

What is a fake profile?

A fake profile is an account created by someone pretending to be another person. It happens on **all** platforms:

- **Instagram**: copied profile pictures, made-up identities
- **Snapchat**: accounts pretending to be classmates
- **Discord**: strangers building trust on gaming servers
- **TikTok**: comments from fake accounts luring you to other platforms

Catfishing: when someone fakes a whole identity

Catfishing means that someone builds up a false identity over a longer period, often with stolen photos, invented stories and a lot of patience. The goal:

- Getting **personal information** out of you (address, school, daily routine)
- **Building trust**: and then demanding money or pictures
- **Manipulation**: getting you to do things you'd never normally do

> **Important**
>
> Catfishing is not a one-off. According to one study, one in three young people has already had to deal with fake profiles. The younger the target group, the more aggressive the offenders.

Social engineering: the art of manipulation

Social engineering is when someone uses psychological tricks to get you to do something or give something away. The most common levers:

Trick	Example
Time pressure	"Quick, your account is about to be blocked!"
Helpfulness	"Can you give me your password for a sec? I'm testing something."
Authority	"I'm the admin of this server, I need your details."
Curiosity	"Look, is that you in this video?" + link
Fear	"I've got screenshots of you. Pay up or I'll post them."

How to protect yourself

- **No stranger needs your password.** Nobody. No admin, no support, no friend
- **Cross-check**: do you really know the person? Ask via a different channel
- **Check pictures**: right-click → image search. Stolen profile pictures often turn up several times
- **No private pictures to strangers**: not even to "friends" you only know online
- **Block instead of arguing**: if something seems off to you, block straight away

> **Tip**
>
> A simple test: ask the person to write a specific word on a piece of paper during a video call and hold it up. Fake profiles reliably fail at this.

Quiz: Real or fake?

Someone writes to you on Instagram: "Hey, I'm new at your school and don't know anyone yet. Would you give me your number so we can meet up?"

Quiz question

What do you do?

Answer options
Send my number, sounds nice
Ask back: "Which class are you in?" and cross-check with classmates
Ignore it
Check the profile: how long has it existed? How many posts and followers does it have?

Word cloud

How can you tell that a profile might be fake?

Quiz question

A new profile messages you. What makes you suspicious?

Answer options
Few posts, but a huge number of followers
It wants to switch to another messenger quickly
It has a profile picture
It asks for personal details early on
All the photos look like they're from a catalogue

2. Deepfakes and Fake Voices: Don't Trust Everything You See and Hear

How AI fakes deceptively real videos and voices, and how not to get fooled.



When your eyes and ears deceive you

It used to be: a video or a voice message is proof. Not any more. Artificial intelligence can fake faces and voices so well that you can hardly see or hear the difference. This is called a **deepfake** (fake video/image) and **voice cloning** (cloned voice).

Where you come across this

- **Fake celebrity videos**: a star or streamer supposedly promotes a "free giveaway", but in reality it's an AI fake luring you to a scam site.
- **Cloned voices**: from a few seconds of a voice message, AI builds a copy of your voice. Then "your friend" calls and urgently asks for help.
- **"Mum, I've got a new phone"**: a message or call in a familiar voice asks for money or a password. An ancient trick, now much more convincing with AI.

Important

> A voice or a face is **no longer proof** of who is really writing or calling. Don't rely on it; rely on the way the message reached you.

How to recognise the trick

Not by how it looks, that keeps getting better. But by **how it plays out**:

- Suddenly it's **super urgent**.
- You're supposed to **keep it secret** ("don't tell anyone").
- It comes via an **unusual channel**.

How to protect yourself

- **Agree on a code word**: arrange a secret word with your family and friends for emergencies. Anyone who doesn't know it isn't the real person.
- **Call back**: on the number you already know, not the one from the message.
- **Don't believe something just because it looks real**: pictures, videos and voices can be faked.

Quiz question

You get a voice message. The voice sounds exactly like your best friend and urgently asks for your password. What do you do?

Answer options
Send the password, the voice is right after all
Call back on the number you know or ask in person
Get suspicious if it's "urgent" and meant to stay secret
Do what the voice says immediately

Learning game

Real or fake? Look at examples of pictures, videos and messages together and decide what's real and what isn't.

3. Gaming: Account Theft, Scams and How to Protect Yourself

Why your gaming account is valuable and how scammers try to steal it.



Your account is worth real money

You've put hundreds of hours into your game. Skins, ranks, items, maybe even rare cosmetics. What you might not know: on the black market, these accounts have a real cash value. A Fortnite account with rare skins goes for €50–500. A CS2 inventory with knife skins can be worth thousands.

And that's exactly why gaming accounts are a popular target.

The most common scams

1. "Free V-Bucks / Robux / coins"

You see a website or a YouTube video promising free in-game currency. You "just" have to enter your username and password. What really happens: your account is gone.

> **Important**
>
> There are **no** free V-Bucks, Robux or other in-game currency outside the official shops. Every site that promises this is a scam.

2. Trading scams

"I'll trade you my rare item for yours." The trade starts, but at the last moment the item is swapped or the trade is manipulated. Especially common in: Rocket League, CS2, Roblox.

3. Fake support

You get a message: "Your account has been reported for cheating. Click here to verify it, otherwise it will be banned." The link leads to a fake login page.

4. Phishing via Discord

"Hey, I still need one more for my team. Sign up on this tournament site!" The link looks like a real esports platform, but it's a copy that intercepts your password.

How attackers get into your account

Method	How it works
Phishing link	Fake login page that looks genuine
Guessing the password	Because you use the same one everywhere
Stealing a session token	Via manipulated browser extensions
Social engineering	"I'm a mod, I need your login"

How to protect yourself

- **Turn on two-factor authentication (2FA)**: on Steam, Epic, Riot, Blizzard, wherever possible
- **A unique password** for every gaming account
- **Never share login details on Discord, TeamSpeak or in chat**
- **Use official links**: don't search via Google, type the URL in yourself

- **Check browser extensions**: only install what you really need

> **Tip**
>
> Turn on 2FA. Now. Seriously. It takes two minutes and makes your account many times more secure. On Steam it's called "Steam Guard", on Epic "two-factor authentication", on Riot "authenticator app".

Puzzle: Spot the scam

You get this message on Discord from someone you know from a gaming server:

> "Hey, I've found a sponsor for our team! We all just need to register on this site: esport-turniere.net/anmelden. Be quick, places are limited!"

Word cloud

What are the warning signs?

Quiz question

A site promises you free in-game currency if you log in. What's true?

Answer options
It's always a scam
It sometimes works
Your account will be gone afterwards
The linked email address is at risk too

4. Data Protection at Work: Why Secrets Are Worth Money Later

The data protection game. Finding traces in a profile and building the bridge to working life.



From your profile to trade secrets

So far it's been about you in private. Now comes the part that will catch up with you later at work.

Anyone doing an internship, an apprenticeship or their first job suddenly has access to things that don't belong to them: customer data, prices, design plans, medical records, login details. Attackers hardly ever go after the technology for this, they go after **people**. And they start exactly where we just were: with the public profile.

> **Important**
>
> The method is always the same: first collect what's public. Then write a message that fits it exactly. If someone talks to you as if they know you, you check less.

How a real attack works

1. Someone finds out where you work; a photo in a company T-shirt is enough
2. They see who your boss is, when holiday season is, how the email addresses are built
3. Then an email arrives: "Quick favour, I'm on the train, need this urgently"
4. And because everything fits (name, tone, timing), someone just does it

This is called CEO fraud and costs German businesses huge sums every year. It all started with publicly visible information.

The data protection game

Your teacher is now unlocking the game. You'll see the public profile of a made-up person. Your task: find everything a stranger could make use of.

Learning game

Unlock it and project the QR code. The board shows who has found how much and

> **Addition**
>
> After the game, it's worth asking the class: which of these nine details are public for you yourselves? In my experience, it gets very quiet at that point.

And now into the office: Operation ORION

The profile was private. Now the same thing in a workplace. In "Operation ORION" you sneak through a perfectly normal office and look for the spots where an attacker would strike: the sticky note on the monitor, the open inbox, the USB stick from the trade fair stand, the meeting where people talk too loudly.

Learning game

About five minutes per round. Hold the phone sideways. On the board you

can see who

Important

Each finding on its own seems harmless. What's dangerous is the sum: a note plus an unlocked screen plus an overheard meeting add up to complete access.

What this means for later

- **What isn't yours, you don't share**: not even "just quickly" with your friends
- **No work stuff in private chats**: no screenshots, no photos of the screen
- **Login details are personal.** If you pass on your login, you're responsible for what's done with it
- **If in doubt, ask**: via a different channel, not by replying to the email

Quiz question

You're doing an internship. What can you post publicly?

Answer options
That you're doing an internship at a company
A photo of your screen with the customer list
The username you were given
That you enjoy the work
Screenshots from the internal chat

Quiz question

An email from "your boss": urgent, short, supposedly sent from a phone, asking for a bank transfer. What do you do?

Answer options
Do it right away, it's the boss after all
Ask by replying to the email
Check via a different channel, for example by calling

Have a colleague look over it with you

5. Recognising Phishing, Even When It Looks Like Your Favourite Game

How to spot fake messages and links before you click on them.



What is phishing?

Phishing is when someone pretends to be someone else to get your data. Usually by email, but also by text message, WhatsApp, Discord or even as a message inside a game.

The name comes from "fishing": the attacker casts out bait and waits until someone bites.

What phishing looks like in your everyday life

Example 1. The Steam trap:

> "Your Steam account has been suspended due to suspicious activity. Verify your identity within 24 hours: steamcommunlty.com/verify"

Can you see the mistake? It says "steamcommunlty" instead of "steamcommunity". One letter's difference, but you end up on a completely fake site.

Example 2. The Instagram message:

> "Hey, someone posted a video of you take a look: bit.ly/3xK9mP"

Shortened links hide where they really lead. And the message plays on curiosity and a little bit of panic.

Example 3. The Spotify email:

> "Your payment method has expired. Update your details so you don't lose your account."

Spotify really does send emails like this, but the real email links to spotify.com, not to spotify-account-update.com.

The 5-second check

Before you click on a link, pause for five seconds and check:

1. **Who's sending this?** Do I really know the person/company?
2. **Is there time pressure?** "Immediately", "within 24 hours", "now": that's almost always manipulation
3. **Where does the link lead?** Holding your finger on it (don't tap!) shows the real URL
4. **Does it make sense?** Would Steam/Instagram/Spotify contact me like this?
5. **Does it ask for login details?** Real services never ask for your password by message

> **Important**
>
> No legitimate service sends you a message with a link where you're supposed to enter your password. If you're unsure: open the app or website directly, not via the

> link.

What to do if you've clicked on it?

It's happened: you clicked on a phishing link and maybe even entered data. No reason to panic, but acting quickly is important:

1. **Change your password immediately**: for the affected service and everywhere you used the same password
2. **Turn on 2FA**: if you haven't already
3. **Tell someone**: parents, a teacher, the person responsible for IT. It's nothing to be ashamed of, it's a security incident
4. **Inform your bank**: if payment details are affected

> **Tip**
>
> You haven't done anything wrong if you report phishing. You've done something wrong if you keep quiet about it. Reporting helps you and others.

Quiz: Phishing or genuine?

Sort these messages. Phishing or genuine?

1. Email from Netflix: "Your subscription will be cancelled tomorrow. Click here to update your payment."
2. Text message from DHL: "Your parcel could not be delivered. Customs fee: €1.99. Pay here."
3. Email from your school: "The new club and activity dates are online. Check the school portal."
4. Discord DM: "Hey, is that you in the picture?? □ [link]"

Quiz question

Which of these messages are phishing?

Answer options



Netflix: subscription cancelled, update your payment
DHL text: pay a €1.99 customs fee via a link
School: new club dates in the school portal
Discord DM: “Is that you in the picture??” with a link

Learning game

Five messages, each one genuine or fake. After the game, go through the tell-tale signs on the board.

Quiz question

What's the most reliable way to recognise a phishing message?

Answer options
It puts you under time pressure
The sender address doesn't match the supposed sender
It's written in English
It asks for your password or payment details
It has a logo

6. Summary: Your Digital Toolkit

Everything important at a glance and preparation for the practical phishing test.



What you've learned in this course

You now have the knowledge to protect yourself much better online. Here are the most important points in summary:

Your data belongs to you.

- You decide who sees what
- Publicly posted data can be used for scams and manipulation
- Data protection is a right, not a luxury

Social media isn't your friend, it's a business model.

- The apps collect more data than you think
- Profile private, location off, check permissions
- Not everything you see online is real

Gaming involves real money and real dangers.

- Free in-game currency doesn't exist
- Turn on 2FA, use unique passwords
- No link from Discord or TeamSpeak is 100 % trustworthy

Your phone deserves protection.

- PIN/biometrics, updates, app permissions
- Open Wi-Fi = open book
- Delete old apps

One password, one account.

- Use a password manager
- Turn on two-factor authentication everywhere
- Never share passwords, not even with friends

Recognising phishing = thinking for five seconds.

- Who's sending this? Where does the link lead? Is there time pressure?
- If in doubt: don't click, go to the site directly instead
- Reporting isn't a weakness, it protects everyone

> **Important**
>
> Perfect security doesn't exist. But with what you know now, you're **much harder** to fool than before. And that's the point.

And now: the practical test

Over the next few days you'll receive **three simulated phishing emails** at your school email address. They look real, but they come from this course.

Your task: **Recognise them and don't click on them.**

You'll get your result afterwards as a personal report. And: there's no "failing". If you fall for an email, you learn from it. If you don't open any, you've passed the course.

> **Tip**



> Use the 5-second check. On every suspicious email. From now on. Not just on the test emails.

Final quiz: 10 questions, how many can you get?

1. How many passwords should you use in total?
2. What is 2FA?
3. What is catfishing?
4. Why is public Wi-Fi dangerous?
5. What do you do if you've clicked on a phishing link?
6. Can someone post a photo of you without asking you?
7. What does social engineering mean?
8. From what age are you criminally responsible in Germany?
9. What's the safest way to create a password?
10. What's the most important tip against phishing?

If you got at least 7 right, you're well prepared for the practical test.

Word cloud

What are you taking away from this course? One word is enough.