

secureIT · Course materials for the teacher

Digital Self-Defence for Students

13 lessons · approx. 90 minutes of teaching · 26 interactive tasks · As of: 09/10/2026

What you need to know about phishing, social media, gaming and your data so you can stay safe online.

How the course works

You lead the course on the board and decide yourself when to cover which lesson; the course does not expire. In the first lesson the class signs up via QR code; a first name is enough to take part. You release interactive tasks one at a time, the class answers on their phones, and with “Reveal” the correct answer appears on the board and on all phones at the same time. You can see the answer key for all quiz questions in your Cockpit; this public PDF deliberately does not contain it so that it does not reach the class in advance. At the end you complete the course and thereby start the phishing training: a phishing test scenario from secureIT with three simulated, professionally made scam attempts by email. Only students with parental consent (template: letter to parents) who provide an email address can take part. The certificate confirms successful participation in this training and is only issued to those who take part.

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

Grades 8 to 10 (about 13 to 16 years old) · Scope: two double lessons or four single lessons; lessons can be used individually · As of 03.10.2026

Fits into Informatik und Medienbildung (Computer Science and Media Education), cover and project lessons, and as a building block of the guiding perspective in German, social studies, economics/careers (WBS) and ethics. Fields of action of the guiding perspective “Living and learning in a digital world”: Acting responsibly and protecting,



Communicating, cooperating and acting digitally, Gathering, understanding and evaluating information.

Area	Competence (reading guide for computer science and media education 2026/27 or 2016 curriculum)
Communication and security	Explain personal reasons for protecting your own access; describe and apply measures to protect your own access Lessons: Passwords and Accounts, Securing Your Smartphone
Communication and security	Describe the internet as a meshed network and the path of a message; the client-server principle; compare storage locations (device, server, cloud) by availability, security and operator Lessons: Where is my message right now? How the internet works
Communication and security	Name reasons and everyday examples for encryption; describe transport and end-to-end encryption; carry out the Caesar cipher and assess its security Lessons: Encryption: the padlock in the browser and the Caesar trick
Digitality and participation	Name situations in which personal data is collected; explain the interests of those involved; reflect on your own media use in the light of informational self-determination Lessons: What Does the Internet Know About You, Social Media, Your Data, Your Rights
Digitality and participation	Identify signs of disinformation; engage with fake news and deepfakes Lessons: Fake Profiles and Social Engineering, Deepfakes and Fake Voices
Digitality and participation	Identify monetisation models of digital games; reflect on your own use Lessons: Gaming: Account Theft, Scams and In-Game Fraud
Media Education guiding perspective	Informational self-determination and data protection, protection of minors in the media, communication and cooperation, IT fundamentals
Advanced course in computer science, 3.1.3 Computers and networks / 3.1.4 Information society and data security	Structure of computer networks; (1) reasons for encryption, (2) the Caesar cipher, (3) brute-force attacks, (4) security aspects of mobile devices and protective measures, (6) where personal data arises, benefits and risks

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 5/6 · Digitality and participation 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 5/6 · Digitality and participation Instagram, TikTok, Snapchat: how platforms collect and use your data.	Quiz
3.	Your Data, Your Rights: What the Law Says Grade 5/6 · Digitality and participation What data protection has to do with you and what rights you have.	Quiz
4.	Data Protection at Work: Why Secrets Are Worth Money Later Supplement · Data protection in practice (2016 curriculum, 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.	Fake Profiles, Catfishing and Social Engineering Grade 7 · Digitality and participation How scammers pretend to be someone else and try to manipulate you.	Word cloud, Quiz
6.	Deepfakes and Fake Voices: Don't Trust Everything You See and Hear Grade 7 · Digitality and participation How AI fakes deceptively real videos and voices, and how not to get fooled.	Quiz, Game: faktencheck
7.	Gaming: Account Theft, Scams and How to Protect Yourself Supplement · Everyday scams in practice Why your gaming account is valuable and how scammers try to steal it.	Quiz
8.	Where is my message right now? How the internet works Grade 5/6 · Communication and security 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





9.	Encryption: the padlock in the browser and the Caesar trick <i>Grade 7 · Communication and security</i> 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
10.	Passwords and Accounts: What Belongs to You and What You Never Share <i>Grade 5/6 · Communication and security</i> Why every password has to be unique and what two-factor authentication does for you.	Game: passwort-knacker, Quiz
11.	Securing Your Smartphone: PIN, Apps and Permissions <i>Grade 5/6 · Communication and security</i> Why your phone is your most important device and how to protect it properly.	Game: berechtigungen, Quiz
12.	Recognising Phishing, Even When It Looks Like Your Favourite Game <i>Supplement · Phishing in practice</i> How to spot fake messages and links before you click on them.	Game: phishing-duell, Quiz
13.	Summary: Your Digital Toolkit <i>Supplement · Summary</i> 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. 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"

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	☐



Situation	Allowed?
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

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. 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. 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?"

What do you do?

- ☐ 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 |

6. 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.

7. 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!"

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

8. 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.

9. 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.



10. 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



Bad	Why	Better
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

11. 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
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



12. 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: steamcommunity.com/verify"

Can you see the mistake? It says "steamcommuntly" 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]"

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



13. 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.

