Materiales del curso para el docente

Digitale Selbstverteidigung Klasse 8: Deine Daten, deine Geräte

8 lecciones · aprox. 90 minutos de clase · 18 actividades interactivas · Versión: 23/11/2026

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

Cómo funciona el curso

Usted dirige el curso en la pizarra y decide cuándo tratar cada lección. El curso no caduca. La clase no se registra: sin nombres, sin cuenta, sin apuntarse al empezar la clase. Las actividades se activan una a una: en la pizarra aparece un código QR, la clase responde desde el móvil y con «Resolver» aparece la respuesta correcta a la vez en la pizarra y en todos los móviles. Las soluciones de todas las preguntas están en su panel; este PDF abierto no las incluye a propósito para que no lleguen antes a la clase. Al final cierra el curso. Nadie de la clase se registra: no hay nombres, cuentas ni correos y por tanto tampoco certificados individuales. Este curso no incluye entrenamiento contra el phishing, que solo forma parte del curso «Autodefensa digital».

Qué necesita: un proyector o una pantalla con acceso a internet y la clase con smartphones. Quien no tenga móvil participa con su compañero de al lado.

Relación con el plan de estudios de Baden-Württemberg

Klasse 8 (etwa 13 bis 14 Jahre) · Duración: zwei Doppelstunden, Lektionen einzeln einsetzbar · Versión de 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. Ámbitos de acción de la perspectiva rectora «Vivir y aprender en un mundo digitalizado»: Verantwortungsvoll handeln und schützen, Digital kommunizieren, kooperieren, handeln.

Ámbito	Competencia (guía de lectura de Informática y Educación Mediática 2026/27 o plan de estudios 2016)

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

Esta correspondencia es una valoración profesional del proveedor, no una aprobación oficial. Para los cursos 8.º a 10.º rige el plan de estudios de 2016 hasta la entrada en vigor del plan de Informática y Educación Mediática (2027/28).

Resumen de las lecciones

Lección		Actividades interactivas
1.	**Introducción: ¿qué sabe internet de ti?** Curso 8 · Digitalität und Partizipation Por qué la autodefensa digital te afecta y qué pasa en este curso.	Nube de palabras, Quiz
2.	**Redes sociales: lo que tus apps saben de verdad sobre ti** Curso 8 · Digitalität und Partizipation Instagram, TikTok, Snapchat: cómo recopilan y usan tus datos las plataformas.	Nube de palabras, Quiz
3.	**Tus datos, tus derechos: lo que dice la ley** Curso 8 · Digitalität und Partizipation Qué tiene que ver la protección de datos contigo y qué derechos tienes.	Quiz, Quiz
4.	**¿Dónde está ahora mi mensaje? Cómo funciona internet** Curso 8 · Kommunikation und Sicherheit Nodos, routers, servidores: qué camino sigue un mensaje, qué son un cliente y un servidor, y por qué el lugar de almacenamiento decide quién puede ver tus datos.	Quiz, Quiz, Nube de palabras
5.	**Cifrado: el candado del navegador y el truco de César** Curso 8 · Kommunikation und Sicherheit Por qué WhatsApp y el candado del navegador te protegen, qué significa «de extremo a extremo» y cómo cifrar y descifrar tú mismo con el truco de César.	Quiz, Quiz, Nube de palabras

6.	**Contraseñas y cuentas: lo que es tuyo y lo que nunca compartes** Curso 8 · Kommunikation und Sicherheit Por qué cada contraseña tiene que ser única y qué aporta la autenticación de dos factores.	Juego: passwort-knacker, Quiz
7.	**Proteger tu smartphone: PIN, apps y permisos** Curso 8 · Kommunikation und Sicherheit Por qué tu móvil es tu dispositivo más importante y cómo protegerlo bien.	Juego: berechtigungen, Quiz
8.	**Zusammenfassung: Deine Daten, deine Geräte** Complemento · Zusammenfassung Sicherung der Klasse-8-Reihe: Datenspuren, Rechte, Netz, Verschlüsselung, Passwörter, Smartphone.	Nube de palabras, Quiz

En las páginas siguientes aparece cada lección completa, con todas las preguntas y opciones de respuesta. Las soluciones marcadas solo están en su Cockpit.

1. Introducción: ¿qué sabe internet de ti?

Por qué la autodefensa digital te afecta y qué pasa en este curso.



Bienvenido a la autodefensa digital

Antes de empezar, una pregunta sincera: ¿cuánto sabe internet de ti en realidad? Probablemente más de lo que crees y, sobre todo, más de lo que nunca has puesto ahí conscientemente.

Nube de palabras

¿Qué tiene que quedar privado sí o sí para ti?

De qué trata este curso

En las próximas sesiones no se trata de tecnología, sino de ti: cómo consiguen desconocidos tus datos, qué hacen con ellos y cómo lo evitas. Vamos a ver las redes sociales, los videojuegos, tu smartphone, tus contraseñas y, al final del todo, recibirás sin aviso algunos correos falsos, para ver si lo has aprendido.

Importante

Todo lo que subes a internet lo pueden encontrar desconocidos. Aunque creas que solo lo ven tus amigos.

Por qué esto ya es importante ahora

Imagina que alguien conoce tu nombre completo, tu centro escolar, tu juego favorito y el nombre de tu mascota. ¿Parece inofensivo? Con esa información, alguien puede:

- **Adivinar tu contraseña** (mucha gente usa el nombre de su mascota)
- Escribirte un **mensaje falso** que encaja exactamente con tus intereses
- **Hacerse pasar por tu amigo** y engañar a otras personas

No es teoría, pasa todos los días, miles de veces. Y justo por eso estás aquí.

Pregunta de quiz

¿Cuáles de estos datos no deberías publicar nunca en abierto?

Opciones de respuesta
Tu canción favorita
Tu número de móvil
Tu fecha de nacimiento con el año
Tu película favorita
Tu dirección
El nombre de tu centro escolar y tu clase

Consejo

Regla práctica: todo lo que permita a alguien encontrarte, contactarte o hacerse pasar por ti no debe estar en un perfil público.

2. Redes sociales: lo que tus apps saben de verdad sobre ti

Instagram, TikTok, Snapchat: cómo recopilan y usan tus datos las plataformas.



Tu perfil es solo la superficie

Publicas una foto, das like a un reel, haces scroll en TikTok. Parece inofensivo. Pero detrás de cada deslizamiento, las plataformas recopilan datos sobre ti, muchos más de los que crees.

Lo que Instagram, TikTok y compañía guardan sobre ti

Lo que haces	Lo que guarda la app
Ver un reel	Cuánto tiempo lo ves, si pasas al siguiente o lo vuelves a ver
Publicar una foto	Ubicación, hora, tipo de dispositivo, quién la ve
Seguir a alguien	Tu red social, quién conoce a quién
Escribir en la app	Incluso los textos **que no envías** se registran en parte
Llevar el móvil encima	Perfil de movimientos a partir de los datos de ubicación

> **Importante**
>
> TikTok, por ejemplo, recoge según su propia política de privacidad: ID del dispositivo, dirección IP, pulsaciones de teclado, historial de navegación dentro de la app, datos biométricos (rasgos de la cara y de la voz) y ubicación. Y eso es solo lo que reconocen oficialmente.

¿Por qué es un problema?

1. El producto eres tú. Las apps son gratis porque pagas con tus datos. Cuanto más saben de ti, más dirigida es la publicidad que te pueden mostrar y más dinero ganan.

2. Los datos se pueden robar. Cuando hackean una plataforma, tus datos acaban en la dark web. Eso ya ha pasado con TikTok, Facebook, Instagram y Snapchat, varias veces, con millones de cuentas.

3. Tu huella digital se queda. Lo que publicas hoy puede aparecer dentro de diez años, en una solicitud de empleo, de una beca o en una discusión.

Lo que puedes hacer

- **Poner tu perfil en privado**: se puede en Instagram, TikTok y Snapchat
- **Desactivar la ubicación**: la mayoría de las apps no necesitan de verdad tu ubicación
- **Revisar los permisos**: ¿de verdad necesita TikTok acceder a tus contactos?
- **Limpiar las publicaciones antiguas con regularidad**: lo que tenía gracia hace dos años no tiene por qué estar en internet para siempre

> **Consejo**
>
> Ve ahora a los ajustes de tu móvil → Aplicaciones → Permisos. Mira qué app puede acceder a qué. Te vas a sorprender.

Acertijo: detective de datos

Alguien publica en Instagram:

- Un selfi delante del instituto (el nombre del centro se ve en el cartel)
- Una historia con «¡Por fin 16! □» el 15 de marzo
- Bio: «Gaming □ | Maguncia | @max_gamer en Discord»

Nube de palabras

¿Qué información podría juntar un desconocido a partir de esto?

Pregunta de quiz

¿Qué recopila normalmente una app de redes sociales sobre ti?

Opciones de respuesta
Tu ubicación
Cuánto tiempo ves cada vídeo
Tu agenda de contactos, si lo permites
Solo lo que publicas tú

3. Tus datos, tus derechos: lo que dice la ley

Qué tiene que ver la protección de datos contigo y qué derechos tienes.



La protección de datos no es aburrida, te protege

Si alguien te hace una foto y la publica sin tu permiso, no solo es de mala educación: en la mayoría de los casos es **ilegal**. El Reglamento General de Protección de Datos (RGPD) y el derecho a la propia imagen (en Alemania, *Recht am eigenen Bild*) te dan derechos de verdad.

Tus derechos más importantes

1. Derecho de acceso: puedes saber qué datos guarda un servicio sobre ti. En Instagram, TikTok y compañía puedes pedir una copia de tus datos, y te sorprenderá todo lo que hay.

2. Derecho de supresión: puedes exigir que se borren tus datos. Eso vale también para fotos y vídeos tuyos que hayan publicado otras personas.

3. Derecho a la propia imagen: nadie puede publicar fotos o vídeos tuyos sin tu consentimiento. Eso vale también en el centro, en las fiestas y en el club deportivo.

4. Derecho al olvido: los buscadores tienen que retirar, si lo pides, los enlaces a información tuya desfasada o irrelevante.

Lo que los demás no pueden hacer

Situación	¿Está permitido?
Un compañero publica una foto tuya sin preguntar	□
Alguien reenvía tu chat privado	□
Una app pasa tus datos a redes publicitarias sin informarte	□
Tus padres miran tu móvil (eres menor de 18)	□ Zona gris, depende de la edad y del contexto

> **Importante**
>
> «No tengo nada que esconder» no es un argumento. Protección de datos no significa que escondas algo. Significa que **decides tú** quién sabe qué de ti.

Lo que puedes hacer si se vulneran tus derechos

1. **Hablar directamente con la persona**: «Por favor, quita la foto».
2. **Denunciarlo en la plataforma**: todos los grandes servicios tienen funciones para denunciar
3. **Implicar a tus padres o a un docente**: sobre todo si se trata de acoso
4. **Presentar una reclamación oficial**: ante la autoridad de protección de datos (en Alemania, la de tu estado federado; es gratis)

> **Consejo**
>
> Haz capturas de pantalla como prueba **antes** de pedir que lo borren. Una vez borrado, ya no se puede demostrar nada.

Cuestionario: tus derechos

¿Es verdad? Debatidlo en clase.

1. «Si tengo menos de 16 años, las redes sociales necesitan el consentimiento de mis padres».
2. «Lo que he publicado una vez en internet no lo puedo borrar nunca».
3. «Mi profesor puede grabarme en clase sin permiso».
4. «Si un amigo conoce mi contraseña e inicia sesión, eso no es hackear».

Pregunta de quiz

¿Qué afirmaciones son ciertas?

Opciones de respuesta
Con menos de 16 años, las redes sociales necesitan el consentimiento de los padres.
Lo que se ha publicado no se puede borrar nunca.
Mi profesor puede grabarme en clase sin permiso.
Si un amigo inicia sesión con mi contraseña, eso no es hackear.

Pregunta de quiz

¿Qué derechos tienes frente a un proveedor que ha guardado datos sobre ti?

Opciones de respuesta
Puedes saber qué está guardado
Puedes exigir que se borre
Puedes hacer que se corrijan datos erróneos
Tienes que ser mayor de edad para ello

4. ¿Dónde está ahora mi mensaje? Cómo funciona internet

Nodos, routers, servidores: qué camino sigue un mensaje, qué son un cliente y un servidor, y por qué el lugar de almacenamiento decide quién puede ver tus datos.



No es un cable, es una red

Mucha gente se imagina internet como un cable: de tu móvil al móvil de tu amiga. En realidad es una **red mallada** de millones de nodos: tu móvil, el router wifi, el proveedor, ordenadores de conmutación, cables submarinos, centros de datos, otro proveedor, un router, un móvil.

Tu mensaje se divide en pequeños paquetes. Cada paquete salta de nodo en nodo, y cada nodo solo decide: «¿Adónde ahora?». Si un camino falla, los paquetes toman otro. Por eso la red sigue funcionando aunque se rompa un cable en algún sitio.

> **Importante**
>
> Por el camino, tu mensaje pasa por **muchos ordenadores ajenos** que no conoces. Justo por eso el cifrado no es un capricho, sino lo que impide que otros lo lean.

Cliente y servidor

Tu móvil **pregunta** («Enséñame el vídeo», «Envía este mensaje») y un gran ordenador en un centro de datos **responde**. El que pregunta se llama **cliente**; el que responde, **servidor**. Cada app, cada página web, cada juego funciona así, aunque parezca que todo está «en tu móvil».

Y al revés: el servidor ve todo lo que le envías. Quien gestiona el servidor tiene tus datos. No es la técnica la que decide sobre la protección de tus datos, sino **el operador**.

¿Dónde están tus cosas?

Lugar de almacenamiento	Ejemplo	¿Quién puede acceder?	Cuando lo borras
Tu dispositivo	Fotos en la galería	Tú, o quien tenga tu móvil en la mano	Desaparece (salvo las copias de seguridad)
Servidor de la red del centro	Archivos en el servidor del centro	Tú, el profesorado, el servicio informático del centro	Según las normas del centro
Servidor del proveedor	Mensajes de chat, publicaciones	Tú, los destinatarios, el proveedor	Tu copia desaparece, las de los demás se quedan
Nube	Almacenamiento en línea, copias de seguridad	Tú, el proveedor y, en su caso, las autoridades del país del servidor	A menudo solo de forma definitiva tras un plazo

Al comparar cuentan cuatro cosas: **disponibilidad** (¿puedo acceder desde cualquier sitio?), **colaboración** (¿pueden participar otros?), **seguridad** (¿quién puede leerlo o robarlo?) y **operador** (¿de quién es el servidor, en qué país está, qué normas rigen allí?).

Pregunta de quiz

¿Qué es cierto sobre el camino de un mensaje en internet?

Opciones de respuesta

Se divide en paquetes que pasan por muchos nodos
Si un camino falla, los paquetes toman otro
Hay una línea directa de móvil a móvil
Técnicamente, solo el destinatario puede ver los paquetes

Pregunta de quiz

Quieres hacer un trabajo con tres compañeros de clase. ¿Qué lugar de almacenamiento encaja mejor y en qué te fijas?

Opciones de respuesta
La nube o el servidor del centro, porque todos pueden trabajar a la vez
Mirar antes quién gestiona el servicio y dónde está el servidor
Solo en mi móvil, es lo más seguro para trabajar juntos
Da igual dónde, lo importante es que sea gratis

Nube de palabras

¿Qué dispositivos hay en el camino entre tú y un amigo cuando chateáis? Una palabra por respuesta.

Consejo

Si quieres saber dónde tiene sus servidores un servicio: la política de privacidad suele indicarlo en «Alojamiento» o «Lugar de almacenamiento». Alemania o la UE significa: se aplican las normas europeas de protección de datos (el RGPD).

5. Cifrado: el candado del navegador y el truco de César

Por qué WhatsApp y el candado del navegador te protegen, qué significa «de extremo a extremo» y cómo cifrar y descifrar tú mismo con el truco de César.



¿Quién lo está leyendo?

Cada mensaje que envías pasa por decenas de ordenadores ajenos: tu wifi, el router de la cafetería, el proveedor, servidores en cualquier parte del mundo. Sin cifrado, cualquiera de ellos podría leerlo, como una postal.

El **cifrado** convierte tu texto (el **texto en claro**) en un **texto cifrado** ilegible. Solo quien tiene la **clave** correcta puede volver a hacerlo legible.

> **Importante**
>
> Codificar no es cifrar. Un código QR o el morse los puede traducir **cualquiera** que conozca la regla. El cifrado necesita además una **clave** que solo tienen las personas adecuadas.

Dos tipos que usas cada día

Cifrado del transporte: el candado del navegador (el «https»). Entre tu móvil y la página web nadie puede leer nada, ni siquiera en una wifi abierta. Pero: el operador de la página ve todo lo que escribes en ella.

Cifrado de extremo a extremo: WhatsApp, Signal, Threema. El mensaje se cifra en tu móvil y solo se descifra en el móvil de la destinataria. Ni siquiera el proveedor puede leerlo.

> **Consejo**
>
> ¿No hay candado en el navegador o el navegador te advierte sobre la página? Entonces **nunca** escribas ahí una contraseña ni datos bancarios. Da igual lo auténtica que parezca la página.

El truco de César

Julio César ya cifraba mensajes: cada letra se desplaza en el alfabeto un número fijo de posiciones. La clave es ese número.

Con la clave **3**, la A se convierte en D, la B en E, la H en K:

```
Texto en claro: H O L A
Texto cifrado:  K R O D
```

Pruébalo: cifra tu nombre con la clave 3 (usa el alfabeto de 26 letras, sin la Ñ). Al final del alfabeto se vuelve a empezar: la X se convierte en A.

Pregunta de quiz

Interceptas el texto cifrado **VHJXUR. Sabes que es César con la clave 3. ¿Qué pone?**

Opciones de respuesta
SEMANA
SEGURO
SALIDA

SILLAS

Por qué César ya no sirve hoy

Solo hay **25 claves posibles**. Un atacante simplemente las prueba todas. Eso se llama **fuerza bruta**: no es listo, pero es rápido. Un ordenador lo consigue en menos de un segundo.

Aún más rápido es el **análisis de frecuencias**: en español, la E es la letra más frecuente. Así que la letra más frecuente del texto cifrado es muy probablemente la E desplazada, y ya se conoce la clave.

> **Importante**
>
> Exactamente lo mismo pasa con las **contraseñas cortas**: un ordenador prueba todas las posibilidades. Cuantas más claves posibles, más tarda. Por eso ganan las contraseñas largas y el cifrado moderno, con claves de cientos de cifras.

Pregunta de quiz

¿Qué es cierto?

Opciones de respuesta
Con el candado del navegador nadie puede leer nada en la wifi, pero el operador de la página sí
Con el cifrado de extremo a extremo ni siquiera el proveedor puede leer el mensaje
Un código QR es un cifrado seguro
César es seguro porque ya casi nadie lo conoce

Nube de palabras

¿Dónde te encuentras el cifrado en el día a día? Basta una palabra.

6. Contraseñas y cuentas: lo que es tuyo y lo que nunca compartes

Por qué cada contraseña tiene que ser única y qué aporta la autenticación de dos factores.



Tu contraseña es la llave de tu casa

Imagina que tienes una sola llave que abre la puerta de tu casa, tu taquilla, el candado de la bici y el vestuario. Parece práctico, hasta que la pierdes. Entonces lo pierdes todo.

Eso es justo lo que pasa cuando usas la misma contraseña en todas partes.

Por qué no basta con una contraseña

Cuando hackean una web (y pasa constantemente), los nombres de usuario y las contraseñas acaban en la dark web. Los atacantes prueban entonces esas combinaciones automáticamente en cientos de webs. Esto se llama **credential stuffing** (relleno de credenciales).

Así que si usas la misma contraseña en Instagram, en tu correo y en tu cuenta de juegos, y hackean Instagram, **las tres cuentas** están en peligro.

> **Importante**
>
> La regla es sencilla: **Una cuenta, una contraseña.** Ninguna contraseña puede usarse en dos servicios a la vez.

Qué hace segura una contraseña

Mala	Por qué	Mejor
JuanPerez2009	Nombre + año de nacimiento = adivinable	Correcto-Caballo-Batería-Grapa
123456789	La contraseña más común del mundo	Combinar palabras al azar
Verano2024!	Patrón que usan millones de personas	Usar un gestor de contraseñas

Una buena contraseña:

- Tiene al menos 12 caracteres
- No se puede adivinar (ni nombre, ni fecha de nacimiento, ni mascota)
- Es única para cada cuenta

El método más sencillo: coge cuatro palabras al azar y únelas: «Jirafa-Piano-Nube-Siete». Larga, fácil de recordar, segura.

Gestor de contraseñas: tu llavero digital

Un gestor de contraseñas guarda todas tus contraseñas cifradas. Solo tienes que recordar **una** contraseña maestra. El gestor genera y rellena todas las demás automáticamente.

Opciones gratuitas: Bitwarden, KeePassXC, la función de llavero de Apple/Google.

Autenticación de dos factores (2FA)

2FA significa: aunque alguien conozca tu contraseña, necesita además un segundo factor, normalmente un código en tu móvil.

Dónde deberías activar la 2FA ya mismo:

1. Tu correo electrónico (es la llave de todas tus demás cuentas)
2. Tus cuentas de juegos (Steam, Epic, Riot)
3. Redes sociales (Instagram, TikTok, Snapchat)
4. Todo lo que tenga que ver con dinero

Lo que es tuyo y lo que nunca compartes

✅ **Puedes compartir**	❌ **Nunca compartes**
Tu nombre de jugador	Tu contraseña
Tu película favorita	Tu cumpleaños con el año
Tu perfil público	Tu dirección
Capturas de pantalla (sin datos sensibles)	Tu DNI / carné de estudiante
Tu servidor de Discord	Tus datos de acceso al correo

> **Consejo**
>
> **Tampoco con tu mejor amigo.** Las amistades cambian. Las contraseñas que has compartido no se pueden «recuperar». Y a tu amigo pueden hackearlo sin que se dé cuenta, y entonces el atacante también tiene tu acceso.

Acertijo: revisión de contraseñas

¿Cuáles de estas contraseñas son seguras?

1. `Futbol2009` → ❌ (palabra + año de nacimiento)
2. `kT9$mP2!xR4#` → ❌ (aleatoria, pero difícil de recordar)
3. `Elefante-Ketchup-Tambor-42` → ✅ (larga, aleatoria, fácil de recordar)
4. `TeQuiero` → ❌ (entre las 20 contraseñas más comunes)
5. `qwerty` → ❌ (patrón de teclado)

> **Juego didáctico**
>
> **Inventad una contraseña y mirad cuánto aguanta. Solo se transmite el patrón,**

Pregunta de quiz

¿Qué hace realmente fuerte una contraseña?

Opciones de respuesta
La longitud
Un signo de exclamación al final
Que solo se use para un único servicio
Que la puedas recordar bien porque es tu cumpleaños
Que no aparezca en ningún otro sitio

7. Proteger tu smartphone: PIN, apps y permisos

Por qué tu móvil es tu dispositivo más importante y cómo protegerlo bien.



Tu móvil es la llave de todo

Tu smartphone no es solo un teléfono. Es tu cuenta bancaria, tu correo, tu álbum de fotos, tu GPS y tu documento de identidad, todo en uno. Quien tiene acceso a tu móvil tiene acceso a toda tu vida digital.

Protección básica: bloqueo y biometría

Método	Seguridad	Recomendación
Sin pantalla de bloqueo	Ninguna	Nunca
Patrón	Muy débil (las marcas de grasa delatan el patrón)	No
PIN de 4 cifras	Débil (10.000 posibilidades)	Mínimo
PIN de 6 cifras	Mejor (1 millón de posibilidades)	Bien
Huella dactilar	Fuerte + rápido	Recomendado
Face ID / reconocimiento facial	Fuerte (en dispositivos recientes)	Recomendado

> **Importante**
>
> Los **PIN más habituales** en Alemania: 1234, 0000, 1111, 2580 (línea vertical), el año de nacimiento. Si el tuyo está entre ellos: cámbialo ya.

Permisos de las apps: ¿quién puede hacer qué?

Cada app pide permisos. Pero no todas necesitan lo que piden:

- **Cámara**: Instagram la necesita, una app de linterna no
- **Micrófono**: una app de voz lo necesita, un juego no
- **Contactos**: WhatsApp los necesita, una app del tiempo no
- **Ubicación**: Google Maps la necesita, una calculadora no

Seguridad wifi: las redes abiertas son peligrosas

El wifi gratis en el tren, en una cafetería o en la estación suena genial. Pero en las redes abiertas cualquiera puede ver lo que haces. Esto se llama **ataque de intermediario** (man-in-the-middle): alguien se pone entre tú e internet y lo lee todo.

Normas para el wifi público:

- Nada de banca online ni de iniciar sesión en cuentas importantes
- Usar una VPN (hay versiones gratuitas)
- Desactivar la conexión wifi automática

> **Consejo**
>
> Ve a los ajustes de wifi y borra todas las redes que ya no necesites. Si no, tu móvil se conecta automáticamente a cualquier red con el mismo nombre, y un atacante puede falsificar fácilmente un «Starbucks WiFi».

Actualizaciones: la protección más aburrida y la más

importante

Cada actualización cierra agujeros de seguridad conocidos. Si aplazas las actualizaciones, dejas abierta una puerta que los atacantes saben que existe.

- Instalar enseguida las **actualizaciones del sistema operativo**
- Hacer con regularidad las **actualizaciones de las apps**
- **Borrar las apps** que ya no usas: menos apps significa menos superficie de ataque

---

Cuestionario: ¿qué tan seguro es tu móvil?

Compruébalo ahora en tu dispositivo:

1. ¿Tienes activado un PIN o la biometría? □ / □
2. ¿Está tu sistema operativo actualizado? □ / □
3. ¿Tienes instaladas apps que no usas desde hace meses? □ / □
4. ¿Alguna app usa permisos que no necesita? □ / □

Cada □ en la 1–2 y cada □ en la 3–4 suma un punto. Quien tiene los cuatro puntos está bien protegido.

Juego didáctico

Seis apps, seis permisos. Que vote la clase y luego comparar en la pizarra.

Pregunta de quiz

¿Qué permiso es sospechoso sin duda en una app de linterna?

Opciones de respuesta
Ubicación
Contactos
Flash de la cámara
Micrófono

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.

> **Importante**
>
> 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.

Nube de palabras

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

Pregunta de quiz

Welche Aussage stimmt?

Opciones de respuesta
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.