Supports de cours pour l’enseignant

Digitale Selbstverteidigung Klasse 8: Deine Daten, deine Geräte

8 leçons · env. 90 minutes de cours · 18 activités interactives · Version du 23/11/2026

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

Déroulement du cours

Vous menez le cours au tableau et décidez vous-même quand aborder quelle leçon. Le cours n'expire pas. La classe ne s'inscrit pas : pas de noms, pas de compte, aucune inscription en début de séance. Vous déverrouillez les activités une à une : un code QR s'affiche alors au tableau, la classe répond sur son téléphone, et « Révéler » affiche la bonne réponse en même temps au tableau et sur tous les téléphones. Le corrigé de toutes les questions se trouve dans votre cockpit ; ce PDF ouvert ne le contient volontairement pas, pour qu'il n'arrive pas en avance à la classe. À la fin, vous clôturez le cours. Personne dans la classe ne s'inscrit : ni nom, ni compte, ni adresse e-mail, donc pas de certificats individuels. Ce cours ne comporte pas d'entraînement anti-hameçonnage, réservé au cours « Autodéfense numérique ».

Ce dont vous avez besoin : un vidéoprojecteur ou un écran avec accès à Internet, et la classe avec des smartphones. Les élèves sans téléphone participent avec leur voisin.

Lien avec le programme scolaire du Bade-Wurtemberg

Klasse 8 (etwa 13 bis 14 Jahre) · Durée : zwei Doppelstunden, Lektionen einzeln einsetzbar · Version du 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. Champs d’action de la perspective directrice « Vivre et apprendre dans un monde numérique » : Verantwortungsvoll handeln und schützen, Digital kommunizieren, kooperieren, handeln.

Domaine	Compétence (guide de lecture Informatique et éducation aux médias 2026/27 ou programme 2016)
Digitalität und Partizipation	Situationen der Datenerhebung; Interessen der Akteure; informationelle Selbstbestimmung Leçons : 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 Leçons : 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

Cette correspondance est une appréciation professionnelle du prestataire, et non une validation officielle. Pour les classes de 8e à 10e année, le programme 2016 s’applique jusqu’à l’entrée en vigueur du programme Informatique et éducation aux médias (2027/28).

Aperçu des leçons

Leçon		Activités interactives
1.	**Introduction : que sait Internet sur toi ?** Niveau 8 · Digitalität und Partizipation Pourquoi l’autodéfense numérique te concerne et ce qui se passe dans ce cours.	Nuage de mots, Quiz
2.	**Réseaux sociaux : ce que tes applis savent vraiment sur toi** Niveau 8 · Digitalität und Partizipation Instagram, TikTok, Snapchat : comment les plateformes collectent et utilisent tes données.	Nuage de mots, Quiz
3.	**Tes données, tes droits : ce que dit la loi** Niveau 8 · Digitalität und Partizipation Ce que la protection des données a à voir avec toi et quels droits tu as.	Quiz, Quiz
4.	**Où est mon message en ce moment ? Comment fonctionne Internet** Niveau 8 · Kommunikation und Sicherheit Nœuds, routeurs, serveurs : le chemin que prend un message, ce que sont un client et un serveur, et pourquoi le lieu de stockage décide de qui peut voir tes données.	Quiz, Quiz, Nuage de mots

5.	**Le chiffrement : le cadenas du navigateur et l’astuce de César** Niveau 8 · Kommunikation und Sicherheit Pourquoi WhatsApp et le cadenas du navigateur te protègent, ce que veut dire « de bout en bout », et comment chiffrer et casser toi-même un message avec l’astuce de César.	Quiz, Quiz, Nuage de mots
6.	**Mots de passe et comptes : ce qui t’appartient et ce que tu ne partages jamais** Niveau 8 · Kommunikation und Sicherheit Pourquoi chaque mot de passe doit être unique et ce qu’apporte l’authentification à deux facteurs.	Jeu : passwort-knacker, Quiz
7.	**Sécuriser ton smartphone : code PIN, applis et autorisations** Niveau 8 · Kommunikation und Sicherheit Pourquoi ton téléphone est ton appareil le plus important et comment bien le protéger.	Jeu : berechtigungen, Quiz
8.	**Zusammenfassung: Deine Daten, deine Geräte** Complément · Zusammenfassung Sicherung der Klasse-8-Reihe: Datenspuren, Rechte, Netz, Verschlüsselung, Passwörter, Smartphone.	Nuage de mots, Quiz

Les pages suivantes présentent chaque leçon en entier, avec toutes les questions de quiz et les réponses possibles. Les solutions marquées se trouvent uniquement dans votre Cockpit.

1. Introduction : que sait Internet sur toi ?

Pourquoi l’autodéfense numérique te concerne et ce qui se passe dans ce cours.



Bienvenue dans l’autodéfense numérique

Avant de commencer, une question honnête : que sait Internet sur toi, au juste ? Sans doute plus que tu ne le penses, et surtout plus que ce que tu y as jamais mis consciemment.

Nuage de mots

Qu’est-ce qui doit absolument rester privé pour toi ?

De quoi parle ce cours

Pendant les prochaines séances, il ne s’agit pas de technique, mais de toi : comment des inconnus obtiennent tes données, ce qu’ils en font et comment tu l’empêches. Nous allons regarder les réseaux sociaux, le gaming, ton smartphone, tes mots de passe, et tout à la fin tu recevras sans prévenir quelques faux e-mails, pour voir si c’est bien acquis.

Important

Tout ce que tu mets sur Internet peut être trouvé par des inconnus. Même si tu penses que seuls tes amis le voient.

Pourquoi c’est déjà important maintenant

Imagine que quelqu’un connaisse ton nom complet, ton école, ton jeu préféré et le nom de ton animal. Ça a l’air anodin ? Avec ces infos, quelqu’un peut :

- **Deviner ton mot de passe** (beaucoup utilisent le nom de leur animal)
- T’écrire un **faux message** qui correspond exactement à tes centres d’intérêt
- **Se faire passer pour ton ami** et tromper d’autres personnes

Ce n’est pas de la théorie, ça arrive tous les jours, des milliers de fois. Et c’est justement pour ça que tu es là.

Question de quiz

Lesquelles de ces informations ne devrais-tu jamais publier publiquement ?

Réponses possibles
Ta chanson préférée
Ton numéro de portable
Ta date de naissance avec l’année
Ton film préféré
Ton adresse
Le nom de ton école et ta classe

Astuce

Règle d’or : tout ce qui permettrait à quelqu’un de te trouver, de te contacter ou de se faire passer pour toi n’a rien à faire dans un profil public.

2. Réseaux sociaux : ce que tes applis savent vraiment sur toi

Instagram, TikTok, Snapchat : comment les plateformes collectent et utilisent tes données.



Ton profil n’est que la surface

Tu publies une photo, tu likes un reel, tu fais défiler TikTok. Ça a l’air anodin. Mais derrière chaque glissement de doigt, les plateformes collectent des données sur toi, bien plus que tu ne le penses.

Ce qu’Instagram, TikTok & cie enregistrent sur toi

Ce que tu fais	Ce que l’appli enregistre
Regarder un reel	Combien de temps tu regardes, si tu passes ou si tu regardes encore
Publier une photo	Lieu, heure, type d’appareil, qui la voit
Suivre quelqu’un	Ton réseau social, qui connaît qui
Taper dans l’appli	Même les textes **jamais envoyés** sont en partie enregistrés
Avoir ton téléphone sur toi	Profil de déplacements grâce aux données de localisation

> **Important**
>
> TikTok, par exemple, indique dans sa propre politique de confidentialité qu'il collecte : identifiant de l'appareil, adresse IP, frappes au clavier, historique de navigation dans l'appli, données biométriques (traits du visage et de la voix) et localisation. Et ce n'est que ce qu'ils admettent officiellement.

Pourquoi est-ce un problème ?

1. Le produit, c'est toi. Les applis sont gratuites parce que tu paies avec tes données. Plus elles en savent sur toi, plus elles peuvent te montrer de la publicité ciblée et plus elles gagnent d'argent.

2. Les données peuvent être volées. Quand une plateforme est piratée, tes données atterrissent sur le dark web. C'est déjà arrivé à TikTok, Facebook, Instagram et Snapchat, plusieurs fois, avec des millions de comptes.

3. Ton empreinte numérique reste. Ce que tu publies aujourd'hui peut encore ressortir dans dix ans, lors d'une candidature, d'une demande de bourse ou d'une dispute.

Ce que tu peux faire

- **Mettre ton profil en privé** : possible sur Instagram, TikTok et Snapchat
- **Désactiver la localisation** : la plupart des applis n'ont pas vraiment besoin de ta position
- **Vérifier les autorisations** : TikTok a-t-il vraiment besoin d'accéder à tes contacts ?
- **Faire régulièrement le tri dans tes anciennes publications** : ce qui était drôle il y a deux ans n'a pas besoin de rester en ligne pour toujours

> **Astuce**
>
> Va maintenant dans les réglages de ton téléphone → Applications → Autorisations. Regarde quelle appli a le droit d'accéder à quoi. Tu vas être surpris.

Énigme : détective des données

Quelqu’un publie sur Instagram :

- Un selfie devant l’école (nom de l’école visible sur le panneau)
- Une story « Enfin 16 ans ! □ » le 15 mars
- Bio : « Gaming □ | Mayence | @max_gamer sur Discord »

Nuage de mots

Quelles informations un inconnu pourrait-il en déduire ?

Question de quiz

Que collecte typiquement une appli de réseau social sur toi ?

Réponses possibles
Ta position
Combien de temps tu regardes chaque vidéo
Ton carnet d’adresses, si tu l’autorises
Seulement ce que tu publies toi-même

3. Tes données, tes droits : ce que dit la loi

Ce que la protection des données a à voir avec toi et quels droits tu as.



La protection des données n’est pas ennuyeuse, elle te protège

Si quelqu’un te prend en photo et la publie sans ton accord, ce n’est pas seulement impoli, c’est dans la plupart des cas **illégal**. Le Règlement général sur la protection des données (RGPD) et le droit à l’image (en Allemagne : *Recht am eigenen Bild*) te donnent de vrais droits.

Tes droits les plus importants

1. Droit d’accès : tu as le droit de savoir quelles données un service enregistre sur toi. Sur Instagram, TikTok et compagnie, tu peux demander une copie de tes données, et tu seras étonné de tout ce qu’il y a dedans.

2. Droit à l’effacement : tu peux exiger que tes données soient effacées. Ça vaut aussi pour les photos et vidéos de toi que d’autres ont publiées.

3. Droit à l’image : personne ne peut publier de photos ou de vidéos de toi sans ton

consentement. Ça vaut aussi à l’école, dans les fêtes et au club de sport.

4. Droit à l’oubli : sur demande, les moteurs de recherche doivent retirer les liens vers des informations obsolètes ou non pertinentes à ton sujet.

Ce que les autres n’ont pas le droit de faire

Situation	Autorisé ?
Un camarade publie une photo de toi sans demander	
Quelqu’un transfère ta conversation privée	
Une appli transmet tes données à des régies publicitaires sans t’en informer	
Tes parents regardent ton téléphone (tu as moins de 18 ans)	Zone grise, ça dépend de l’âge et du contexte

> **Important**
>
> « Je n’ai rien à cacher » n’est pas un argument. La protection des données ne veut pas dire que tu caches quelque chose. Elle veut dire que **c’est toi qui décides** qui apprend quoi sur toi.

Ce que tu peux faire si tes droits ne sont pas respectés

1. **Parler directement à la personne** : « Retire la photo, s’il te plaît. »
2. **Signaler à la plateforme** : tous les grands services ont des fonctions de signalement
3. **Impliquer tes parents ou un enseignant** : surtout s’il s’agit de harcèlement
4. **Déposer une plainte officielle** : auprès de l’autorité de protection des données (en Allemagne, celle de ton Land ; gratuit)

> **Astuce**
>
> Fais des captures d’écran comme preuve **avant** de demander l’effacement. Une fois effacé, plus rien ne peut être prouvé.

Quiz : tes droits

Vrai ou faux ? Discutez-en en classe.

1. « Si j’ai moins de 16 ans, les réseaux sociaux ont besoin de l’accord de mes parents. »
2. « Ce que j’ai publié une fois sur Internet, je ne pourrai jamais l’effacer. »
3. « Mon professeur a le droit de me filmer en cours sans autorisation. »
4. « Si un ami connaît mon mot de passe et se connecte, ce n’est pas du piratage. »

Question de quiz

Quelles affirmations sont vraies ?

Réponses possibles
Avant 16 ans, les réseaux sociaux ont besoin de l’accord des parents.
Ce qui a été publié ne peut plus jamais être effacé.
Mon professeur peut me filmer en cours sans autorisation.
Si un ami se connecte avec mon mot de passe, ce n’est pas du piratage.

Question de quiz

Quels droits as-tu face à un fournisseur qui a enregistré des données sur toi ?

Réponses possibles
Tu as le droit de savoir ce qui est enregistré
Tu as le droit d’exiger l’effacement
Tu as le droit de faire corriger des informations fausses
Tu dois être majeur pour ça

4. Où est mon message en ce moment ? Comment fonctionne Internet

Nœuds, routeurs, serveurs : le chemin que prend un message, ce que sont un client et un serveur, et pourquoi le lieu de stockage décide de qui peut voir tes données.



Pas un fil, un réseau

Beaucoup imaginent Internet comme un câble : de ton téléphone à celui de ton amie. En réalité, c’est un **réseau maillé** de millions de nœuds : ton téléphone, le routeur Wi-Fi, le fournisseur d’accès, des ordinateurs de routage, des câbles sous-marins, des centres de données, un autre fournisseur, un routeur, un téléphone.

Ton message est découpé en petits paquets. Chaque paquet saute de nœud en nœud, et chaque nœud décide seulement : « Où ensuite ? » Si un chemin tombe en panne, les paquets en prennent un autre. C’est pour ça que le réseau fonctionne même quand un câble se rompt quelque part.

> **Important**
>
> En route, ton message passe par **beaucoup d’ordinateurs inconnus**. C’est justement pour ça que le chiffrement n’est pas un gadget : c’est ce qui empêche les

> autres de lire.

Client et serveur

Ton téléphone **demande** (« Montre-moi la vidéo », « Envoie ce message »), un gros ordinateur dans un centre de données **répond**. Celui qui demande s'appelle le **client**, celui qui répond le **serveur**. Chaque appli, chaque site web, chaque jeu fonctionne comme ça, même si on a l'impression que tout est « sur ton téléphone ».

Ça veut dire aussi : le serveur voit tout ce que tu lui envoies. Celui qui exploite le serveur a tes données. Ce n'est pas la technique qui décide de la protection de tes données, c'est **l'exploitant**.

Où sont tes affaires ?

Lieu de stockage	Exemple	Qui peut y accéder ?	Quand tu supprimes
Ton appareil	Photos dans la galerie	Toi, ou celui qui a ton téléphone en main	Effacé (sauf les sauvegardes)
Serveur du réseau de l'école	Fichiers sur le serveur de l'école	Toi, les enseignants, l'informatique de l'école	Selon les règles de l'école
Serveur du fournisseur	Messages de chat, publications	Toi, les destinataires, le fournisseur	Ta copie disparaît, celles des autres restent
Cloud	Stockage en ligne, sauvegardes	Toi, le fournisseur, éventuellement les autorités du pays du serveur	Souvent définitivement seulement après un délai

Pour comparer, quatre choses comptent : la **disponibilité** (est-ce que j'y ai accès partout ?), la **collaboration** (est-ce que d'autres peuvent participer ?), la **sécurité** (qui peut lire ou voler ?) et l'**exploitant** (à qui appartient le serveur, dans quel pays se trouve-t-il, quelles règles s'y appliquent ?).

Question de quiz

Qu'est-ce qui est vrai sur le chemin d'un message sur Internet ?

Réponses possibles
Il est découpé en paquets qui passent par de nombreux nœuds
Si un chemin tombe en panne, les paquets en prennent un autre
Il existe une ligne directe de téléphone à téléphone
Techniquement, seul le destinataire peut voir les paquets

Question de quiz

Tu veux préparer un exposé avec trois camarades. Quel lieu de stockage convient le mieux, et à quoi fais-tu attention ?

Réponses possibles
Le cloud ou le serveur de l’école, parce que tout le monde peut y travailler en même temps
Regarder d’abord qui exploite le service et où se trouve le serveur
Seulement sur mon téléphone, c’est le plus sûr pour travailler ensemble
Peu importe où, du moment que c’est gratuit

Nuage de mots

Quels appareils se trouvent sur le chemin entre toi et un ami quand vous chattez ? Un mot par réponse.

Astuce

Si tu veux savoir où un service a ses serveurs : la politique de confidentialité l’indique le plus souvent sous « Hébergement » ou « Lieu de stockage ». Allemagne ou UE, ça veut dire : les règles européennes de protection des données (le RGPD) s’appliquent.

5. Le chiffrement : le cadenas du navigateur et l’astuce de César

Pourquoi WhatsApp et le cadenas du navigateur te protègent, ce que veut dire « de bout en bout », et comment chiffrer et casser toi-même un message avec l’astuce de César.



Qui lit en même temps ?

Chaque message que tu envoies passe par des dizaines d’ordinateurs inconnus : ton Wi-Fi, le routeur du café, le fournisseur, des serveurs quelque part dans le monde. Sans chiffrement, chacun d’eux pourrait le lire, comme une carte postale.

Le **chiffrement** transforme ton texte (le **texte en clair**) en un **texte chiffré** illisible. Seul celui qui a la bonne **clé** peut le rendre de nouveau lisible.

> **Important**
>
> Coder, ce n’est pas chiffrer. Un QR code ou du morse, **n’importe qui** peut le retraduire s’il connaît la règle. Le chiffrement a en plus besoin d’une **clé** que seules les bonnes personnes possèdent.

Deux sortes que tu utilises tous les jours

Chiffrement du transport : le cadenas dans le navigateur (le « https »). Entre ton téléphone et le site, personne ne peut lire, même pas sur un Wi-Fi ouvert. Mais : l'exploitant du site voit tout ce que tu y saisis.

Chiffrement de bout en bout : WhatsApp, Signal, Threema. Le message est chiffré sur ton téléphone et n'est déchiffré que sur le téléphone de la destinataire. Même le fournisseur ne peut pas le lire.

> **Astuce**
>
> Pas de cadenas dans le navigateur, ou le navigateur te met en garde contre le site ? Alors n'y saisis **jamais** de mot de passe ni de coordonnées bancaires. Peu importe à quel point le site a l'air vrai.

L'astuce de César

Jules César chiffrait déjà ses messages : chaque lettre est décalée dans l'alphabet d'un nombre fixe. La clé, c'est ce nombre.

Avec la clé **3**, A devient D, B devient E, S devient V :

```
Texte en clair : S A L U T
Texte chiffré  : V D O X W
```

Essaie : chiffre ton prénom avec la clé 3. Arrivé au bout de l'alphabet, on recommence au début : X devient A.

Question de quiz

Tu interceptes le texte chiffré **VHFUHW. Tu sais que c'est César avec la clé 3. Qu'est-ce qui est écrit ?**

Réponses possibles
SOLEIL
SECRET
SIGNAL

SALADE

Pourquoi César ne vaut plus rien aujourd’hui

Il n’y a que **25 clés possibles**. Un attaquant les essaie toutes, tout simplement. On appelle ça la **force brute** : pas malin, mais rapide. Un ordinateur y arrive en moins d’une seconde.

C’est encore plus rapide avec l’**analyse de fréquence** : en français, le E est la lettre la plus fréquente. La lettre la plus fréquente du texte chiffré est donc très probablement le E décalé, et la clé est trouvée.

> **Important**
>
> C’est exactement ce qui arrive aussi avec les **mots de passe courts** : un ordinateur essaie toutes les possibilités. Plus il y a de clés possibles, plus ça prend de temps. C’est pour ça que les mots de passe longs et le chiffrement moderne, avec des clés de plusieurs centaines de chiffres, l’emportent.

Question de quiz

Qu’est-ce qui est vrai ?

Réponses possibles
Avec le cadenas du navigateur, personne ne peut lire sur le Wi-Fi, mais l’exploitant du site, lui, le peut
Avec le chiffrement de bout en bout, même le fournisseur ne peut pas lire le message
Un QR code est un chiffrement sûr
César est sûr parce que presque plus personne ne le connaît

Nuage de mots

Où rencontres-tu le chiffrement au quotidien ? Un mot suffit.

6. Mots de passe et comptes : ce qui t’appartient et ce que tu ne partages jamais

Pourquoi chaque mot de passe doit être unique et ce qu’apporte l’authentification à deux facteurs.



Ton mot de passe, c’est la clé de ta maison

Imagine que tu as une seule clé qui ouvre ta porte d’entrée, ton casier, ton antivol de vélo et ton vestiaire. Pratique, jusqu’au jour où tu la perds. Et là, tout est perdu.

C’est exactement ce qui se passe quand tu utilises le même mot de passe partout.

Pourquoi un seul mot de passe ne suffit pas

Quand un site est piraté (et ça arrive tout le temps), les noms d’utilisateur et les mots de passe atterrissent sur le dark web. Les attaquants essaient alors automatiquement ces combinaisons sur des centaines d’autres sites. On appelle ça le **credential stuffing** (bourrage d’identifiants).

Donc si tu utilises le même mot de passe pour Instagram, ton e-mail et ton compte de jeu, et qu’Instagram est piraté, **les trois comptes** sont en danger.

> **Important**
>
> La règle est simple : **Un compte, un mot de passe.** Aucun mot de passe ne doit servir pour deux services en même temps.

Ce qui fait un mot de passe sûr

Mauvais	Pourquoi	Mieux
JeanDupont2009	Nom + année de naissance = devinable	Correct-Cheval-Pile-Agrafe
123456789	Mot de passe le plus courant au monde	Combiner des mots au hasard
Ete2024!	Modèle utilisé par des millions de gens	Utiliser un gestionnaire de mots de passe

Un bon mot de passe :

- Fait au moins 12 caractères
- N’est pas devinable (pas de nom, de date de naissance, d’animal)
- Est unique pour chaque compte

La méthode la plus simple : prends quatre mots au hasard et relie-les : « Girafe-Piano-Nuage-Sept ». Long, facile à retenir, sûr.

Le gestionnaire de mots de passe : ton trousseau numérique

Un gestionnaire de mots de passe enregistre tous tes mots de passe de façon chiffrée. Tu n’as plus à retenir qu’**un seul** mot de passe principal. Le gestionnaire génère et remplit tous les autres automatiquement.

Options gratuites : Bitwarden, KeePassXC, la fonction trousseau d’Apple/Google.

L’authentification à deux facteurs (2FA)

La 2FA, ça veut dire : même si quelqu’un connaît ton mot de passe, il lui faut en plus un

deuxième facteur, le plus souvent un code sur ton téléphone.

Où tu devrais activer la 2FA tout de suite :

1. Ton e-mail (c’est la clé de tous tes autres comptes)
2. Tes comptes de jeu (Steam, Epic, Riot)
3. Les réseaux sociaux (Instagram, TikTok, Snapchat)
4. Tout ce qui touche à l’argent

Ce qui t’appartient et ce que tu ne partages jamais

✅ Tu peux partager	❌ Tu ne partages jamais
Ton pseudo de joueur	Ton mot de passe
Ton film préféré	Ta date d’anniversaire avec l’année
Ton profil public	Ton adresse
Des captures d’écran (sans données sensibles)	Ta pièce d’identité / ta carte d’élève
Ton serveur Discord	Tes identifiants e-mail

> **Astuce**
>
> **Même pas avec ton meilleur ami.** Les amitiés changent. Les mots de passe que tu as partagés, tu ne peux pas les « reprendre ». Et ton ami peut se faire pirater sans le vouloir : l’attaquant a alors aussi ton accès.

Énigme : contrôle des mots de passe

Lesquels de ces mots de passe sont sûrs ?

1. `Football2009` → ❌ (mot + année de naissance)
2. `kT9$mP2!xR4#` → ✅ (aléatoire, mais difficile à retenir)
3. `Elephant-Ketchup-Tambour-42` → ✅ (long, aléatoire, facile à retenir)
4. `JeTaime` → ❌ (parmi les 20 mots de passe les plus courants)
5. `azerty` → ❌ (suite de touches du clavier)

Jeu pédagogique

Inventez un mot de passe et voyez combien de temps il tient. Seul le modèle est transmis,

Question de quiz

Qu’est-ce qui rend vraiment un mot de passe solide ?

Réponses possibles
La longueur
Un point d’exclamation à la fin
Qu’il ne serve que pour un seul service
Que tu puisses bien le retenir parce que c’est ta date d’anniversaire
Qu’il n’apparaisse nulle part ailleurs

7. Sécuriser ton smartphone : code PIN, applis et autorisations

Pourquoi ton téléphone est ton appareil le plus important et comment bien le protéger.



Ton téléphone est la clé de tout

Ton smartphone n’est pas qu’un téléphone. C’est ton compte bancaire, ta boîte mail, ton album photo, ton GPS et ta pièce d’identité en un. Celui qui a accès à ton téléphone a accès à toute ta vie numérique.

Protection de base : verrouillage et biométrie

Méthode	Sécurité	Recommandation
Pas d’écran de verrouillage	Aucune	Jamais
Schéma	Très faible (les traces de doigts trahissent le schéma)	Non
Code PIN à 4 chiffres	Faible (10 000 possibilités)	Minimum
Code PIN à 6 chiffres	Mieux (1 million de possibilités)	Bien
Empreinte digitale	Solide + rapide	Recommandé

Méthode	Sécurité	Recommandation
Face ID / reconnaissance faciale	Solide (sur les appareils récents)	Recommandé

> **Important**
>
> Les **codes PIN les plus fréquents** en Allemagne : 1234, 0000, 1111, 2580 (ligne verticale), l'année de naissance. Si le tien en fait partie : change-le tout de suite.

Autorisations des applis : qui a le droit de faire quoi ?

Chaque appli demande des autorisations. Mais toutes n'ont pas besoin de ce qu'elles réclament :

- **Appareil photo** : Instagram en a besoin, une appli lampe de poche non
- **Micro** : une appli vocale en a besoin, un jeu non
- **Contacts** : WhatsApp en a besoin, un service météo non
- **Position** : Google Maps en a besoin, une calculatrice non

Sécurité du Wi-Fi : les réseaux ouverts sont dangereux

Le Wi-Fi gratuit dans le train, au café ou à la gare, ça a l'air super. Mais sur un réseau ouvert, n'importe qui peut voir ce que tu fais. On appelle ça une **attaque de l'homme du milieu** (man-in-the-middle) : quelqu'un se place entre toi et Internet et lit tout.

Règles pour le Wi-Fi public :

- Pas de banque en ligne, pas de connexion à des comptes importants
- Utiliser un VPN (il existe des versions gratuites)
- Désactiver la connexion Wi-Fi automatique

> **Astuce**
>
> Va dans tes réglages Wi-Fi et supprime tous les réseaux dont tu n'as plus besoin. Sinon, ton téléphone se connecte automatiquement à tout réseau portant le même nom, et un attaquant peut facilement imiter un « Starbucks WiFi ».

Les mises à jour : la protection la plus ennuyeuse et la plus importante

Chaque mise à jour corrige des failles de sécurité connues. Si tu repousses les mises à jour, tu laisses ouverte une porte dont les attaquants connaissent l'existence.

- Installer tout de suite les **mises à jour du système**
- Faire régulièrement les **mises à jour des applis**
- **Supprimer les applis** que tu n'utilises plus : moins d'applis, c'est moins de surface d'attaque

---

Quiz : ton téléphone est-il bien protégé ?

Vérifie maintenant sur ton appareil :

1. As-tu un code PIN ou la biométrie activés ? □ / □
2. Ton système d'exploitation est-il à jour ? □ / □
3. As-tu installé des applis que tu n'as pas utilisées depuis des mois ? □ / □
4. Une appli utilise-t-elle des autorisations dont elle n'a pas besoin ? □ / □

Chaque □ aux questions 1–2 et chaque □ aux questions 3–4 rapporte un point. Avec les quatre points, tu es bien équipé.

Jeu pédagogique

Six applis, six autorisations. Faire voter la classe, puis comparer au tableau.

Question de quiz

Quelle autorisation est forcément suspecte pour une appli lampe de poche ?

Réponses possibles
Position
Contacts

Flash de l’appareil photo
Micro

8. Zusammenfassung: Deine Daten, deine Geräte

Sicherung der Klasse-8-Reihe: Datenspuren, Rechte, Netz, Verschlüsselung, Passwörter, Smartphone.



Fünf Dinge, die bleiben sollen

- **Dein Fußabdruck entsteht zur Hälfte durch andere.** Reden hilft mehr als Einstellungen allein.
- **Apps bekommen nur, was sie für ihre Aufgabe brauchen.** Eine Taschenlampe braucht kein Mikrofon.
- **Du hast Rechte.** Auskunft, Löschung, Beschwerde: drei Schritte, keine Anwältin nötig.
- **Eine Nachricht reist über viele Stationen.** Nur Ende-zu-Ende-Verschlüsselung hält sie unterwegs geheim.
- **Ein Passwort je Dienst, Sperre am Handy, zweiter Faktor an.** Kostet Sekunden, rettet Konten.

> **Important**
>
> Sicherheit ist kein Zustand, sondern eine Gewohnheit: Sperre, eigenes Passwort, kurz nachdenken.

Wie es weitergeht

In Klasse 9 und 10 geht es um die Angreifer: Fake-Profile, geklonte Stimmen, Betrug in Spielen und Phishing, mit einem echten Praxistest am Ende.

Nuage de mots

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

Question de quiz

Welche Aussage stimmt?

Réponses possibles
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.