

secureIT · Supports de cours pour l'enseignant

Autodéfense numérique pour les élèves

13 leçons · env. 90 minutes de cours · 26 activités interactives · Version du 09/10/2026

Ce que tu dois savoir sur le phishing, les réseaux sociaux, le gaming et tes données pour être en sécurité en ligne.

Déroulement du cours

Vous animez le cours au tableau et décidez vous-même quand traiter chaque leçon ; le cours n'expire pas. Lors de la première séance, la classe s'inscrit elle-même par QR code ; le prénom suffit pour participer. Vous débloquez les activités interactives une par une, la classe répond sur téléphone, et avec « Révéler » la bonne réponse s'affiche en même temps au tableau et sur tous les téléphones. Le corrigé de toutes les questions de quiz se trouve dans votre Cockpit ; ce PDF public ne le contient volontairement pas, afin qu'il ne parvienne pas à la classe à l'avance. À la fin, vous clôturez le cours et lancez ainsi l'entraînement au phishing : un scénario de test de phishing de secureIT avec trois tentatives d'escroquerie par e-mail simulées et réalisées de manière professionnelle. Seuls les élèves ayant l'accord de leurs parents (modèle : lettre aux parents) et ayant indiqué une adresse e-mail peuvent participer. Le certificat atteste la participation réussie à cet entraînement et n'est délivré qu'en cas de participation.

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

De la 8e à la 10e année (environ 13 à 16 ans) · Durée : deux heures doubles ou quatre heures simples, leçons utilisables séparément · Version du 03.10.2026

S'intègre en Informatik und Medienbildung (informatique et éducation aux médias),



dans les heures de remplacement et de projet, et comme élément de la perspective directrice en allemand, en éducation civique, en économie et orientation professionnelle (WBS) et en éthique. Champs d'action de la perspective directrice « Vivre et apprendre dans un monde numérique » : Agir de manière responsable et se protéger, Communiquer, coopérer et agir avec le numérique, Collecter, comprendre et évaluer des informations.

Domaine	Compétence (guide de lecture Informatique et éducation aux médias 2026/27 ou programme 2016)
Communication et sécurité	Expliquer les raisons personnelles de protéger son propre accès ; décrire et appliquer des mesures pour le protéger Leçons : Mots de passe et comptes, Sécuriser ton smartphone
Communication et sécurité	Décrire Internet comme réseau maillé et le trajet d'un message ; principe client-serveur ; comparer les lieux de stockage (appareil, serveur, cloud) selon la disponibilité, la sécurité et l'exploitant Leçons : Où est mon message en ce moment ? Comment fonctionne Internet
Communication et sécurité	Citer des raisons et des exemples concrets de chiffrement ; décrire le chiffrement de transport et de bout en bout ; appliquer le chiffre de César et évaluer sa sécurité Leçons : Le chiffrement : le cadenas du navigateur et l'astuce de César
Numérique et participation	Citer des situations où des données personnelles sont collectées ; expliquer les intérêts des acteurs ; analyser son propre usage des médias au regard de l'autodétermination informationnelle Leçons : Que sait Internet sur toi, Réseaux sociaux, Tes données, tes droits
Numérique et participation	Repérer les indices de désinformation ; se confronter aux fake news et aux deepfakes Leçons : Faux profils et ingénierie sociale, Deepfakes et fausses voix
Numérique et participation	Identifier les modèles de monétisation des jeux numériques ; analyser son propre usage Leçons : Gaming : vol de compte, arnaques et fraude en jeu
Perspective directrice Éducation aux médias	Autodétermination informationnelle et protection des données, protection des mineurs dans les médias, communication et coopération, bases de l'informatique

**Cours
d'approfondissement
en informatique,
3.1.3 Ordinateurs et
réseaux / 3.1.4
Société de
l'information et
sécurité des données**

Structure des réseaux informatiques ; (1) raisons du chiffrement, (2) chiffre de César, (3) attaques par force brute, (4) aspects de sécurité des appareils mobiles et mesures de protection, (6) production de données personnelles, avantages et risques

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 5/6 · Numérique et participation 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 5/6 · Numérique et participation Instagram, TikTok, Snapchat : comment les plateformes collectent et utilisent tes données.	Quiz
3.	Tes données, tes droits : ce que dit la loi Niveau 5/6 · Numérique et participation Ce que la protection des données a à voir avec toi et quels droits tu as.	Quiz
4.	La protection des données au travail : pourquoi les secrets vaudront de l'argent plus tard Complément · Pratique de la protection des données (programme de 2016, 3.1.4 (6)) Le jeu de la protection des données. Trouver des traces dans un profil et faire le lien avec la vie professionnelle.	Jeu : datenschutz, Jeu : orion, Quiz, Quiz
5.	Faux profils, catfishing et ingénierie sociale Niveau 7 · Numérique et participation Comment des escrocs se font passer pour d'autres et cherchent à te manipuler.	Nuage de mots, Quiz





6.	Deepfakes et fausses voix : ne crois pas tout ce que tu vois et entends Niveau 7 · Numérique et participation Comment l'IA fabrique des vidéos et des voix plus vraies que nature, et comment ne pas te faire avoir.	Quiz, Jeu : faktencheck
7.	Gaming : vol de compte, arnaques et comment te protéger Complément · Pratique : arnaques du quotidien Pourquoi ton compte de jeu a de la valeur et comment les escrocs essaient de le voler.	Quiz
8.	Où est mon message en ce moment ? Comment fonctionne Internet Niveau 5/6 · Communication et sécurité 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
9.	Le chiffrement : le cadenas du navigateur et l'astuce de César Niveau 7 · Communication et sécurité 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
10.	Mots de passe et comptes : ce qui t'appartient et ce que tu ne partages jamais Niveau 5/6 · Communication et sécurité Pourquoi chaque mot de passe doit être unique et ce qu'apporte l'authentification à deux facteurs.	Jeu : passwort-knacker, Quiz
11.	Sécuriser ton smartphone : code PIN, applis et autorisations Niveau 5/6 · Communication et sécurité Pourquoi ton téléphone est ton appareil le plus important et comment bien le protéger.	Jeu : berechtigungen, Quiz
12.	Reconnaître le phishing, même quand il ressemble à ton jeu préféré Complément · Pratique : phishing Comment repérer les faux messages et les faux liens avant de cliquer dessus.	Jeu : phishing-duell, Quiz
13.	Résumé : ta boîte à outils numérique Complément · Synthèse Tout l'essentiel en un coup d'œil et la préparation au test de phishing pratique.	Nuage de mots

Les pages suivantes présentent chaque leçon en entier, avec toutes les questions de quiz et les réponses





secureIT

Daten und User schützen. Mit Sicherheit.

possibles. Les solutions marquées se trouvent uniquement dans votre Cockpit.



secureIT

Daten und User schützen. Mit Sicherheit.

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 »

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	☐



Situation	Autorisé ?
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

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. La protection des données au travail : pourquoi les secrets vaudront de l'argent plus tard

Le jeu de la protection des données. Trouver des traces dans un profil et faire le lien avec la vie professionnelle.

De ton profil au secret d'entreprise

Jusqu'ici, il s'agissait de toi dans ta vie privée. Voici maintenant la partie qui te rattrapera plus tard au travail.

Celui qui fait un stage, un apprentissage ou occupe son premier emploi a soudain accès à des choses qui ne lui appartiennent pas : données clients, prix, plans de construction, dossiers médicaux, identifiants. Pour y arriver, les attaquants ne s'en prennent presque jamais à la technique, ils s'en prennent aux **personnes**. Et ils commencent exactement là où nous étions à l'instant : au profil public.

Important

La méthode est toujours la même : d'abord rassembler ce qui est public. Ensuite écrire un message qui colle parfaitement. Quand on s'adresse à toi comme si on te connaissait, tu vérifies moins.

Comment se déroule une vraie attaque

1. Quelqu'un découvre où tu travailles ; une photo avec le t-shirt de l'entreprise suffit
2. Il voit qui est ton chef, quand ce sont les vacances, comment sont construites les adresses e-mail
3. Puis arrive un e-mail : « Petit service, je suis dans le train, j'en ai besoin d'urgence »





4. Et comme tout colle (le nom, le ton, le moment), quelqu'un le fait tout simplement

On appelle ça la fraude au président, et elle coûte chaque année des sommes énormes aux entreprises allemandes. Tout a commencé avec des informations visibles publiquement.

Le jeu de la protection des données

Ton enseignant débloquent maintenant le jeu. Vous voyez le profil public d'une personne inventée. Votre mission : trouver tout ce qu'un inconnu pourrait exploiter.

Jeu pédagogique

Débloquer le jeu, projeter le QR code. Le tableau affiche en direct qui a trouvé combien

Complément

Après le jeu, ça vaut la peine de demander à la classe : lesquelles de ces neuf informations sont publiques chez vous-mêmes ? D'expérience, la salle devient alors très silencieuse.

Et maintenant, au bureau : Opération ORION

Le profil était privé. Maintenant, la même chose sur un lieu de travail. Dans « Opération ORION », vous vous faufillez dans un bureau tout à fait ordinaire et cherchez les endroits où un attaquant pourrait frapper : le post-it sur l'écran, la boîte mail ouverte, la clé USB du stand du salon, la réunion où l'on parle trop fort.

Jeu pédagogique

Environ cinq minutes par partie. Tenir le téléphone à l'horizontale. Au





tableau, vous voyez qui

Important

Chaque indice, pris seul, semble anodin. Ce qui est dangereux, c'est la somme : un post-it plus un écran non verrouillé plus une réunion entendue par hasard donnent un accès complet.

Ce que ça veut dire pour plus tard

- **Ce qui n'est pas à toi, tu ne le partages pas** : même pas « vite fait » entre amis
- **Pas de trucs du boulot dans les chats privés** : pas de captures d'écran, pas de photos de l'écran
- **Les identifiants sont personnels**. Celui qui transmet son accès est responsable de ce qui en est fait
- **En cas de doute, demander** : par un autre canal, pas en répondant à l'e-mail

Question de quiz

Tu fais un stage. Qu'as-tu le droit de publier publiquement ?

Réponses possibles

- Que tu fais un stage dans une entreprise
- Une photo de ton écran avec la liste des clients
- L'identifiant que tu as reçu
- Que le travail te plaît
- Des captures d'écran du chat interne

Question de quiz





Un e-mail de « ton chef » : urgent, court, soi-disant envoyé depuis son téléphone, demandant un virement. Que fais-tu ?

Réponses possibles

Le faire tout de suite, c'est le chef

Demander en répondant à l'e-mail

Vérifier par un autre moyen, par exemple en appelant

Faire relire par une ou un collègue



5. Faux profils, catfishing et ingénierie sociale

Comment des escrocs se font passer pour d'autres et cherchent à te manipuler.

Tout le monde n'est pas celui qu'il prétend être

Tu reçois une demande d'ami de quelqu'un avec une jolie photo de profil, des amis en commun et des centres d'intérêt similaires. Tout a l'air vrai. Mais est-ce vraiment le cas ?

Qu'est-ce qu'un faux profil ?

Un faux profil est un compte créé par quelqu'un qui se fait passer pour une autre personne. Ça arrive sur **toutes** les plateformes :

- **Instagram** : photos de profil copiées, identités inventées
- **Snapchat** : comptes qui se font passer pour des camarades de classe
- **Discord** : inconnus qui gagnent la confiance sur des serveurs de jeu
- **TikTok** : commentaires de faux comptes qui attirent vers d'autres plateformes

Le catfishing : quand quelqu'un falsifie toute une identité

Le catfishing, c'est quand quelqu'un construit une fausse identité sur une longue période, souvent avec des photos volées, des histoires inventées et beaucoup de patience. Le but :

- Obtenir des **infos personnelles** (adresse, école, emploi du temps)
- **Gagner la confiance** : pour ensuite exiger de l'argent ou des images
- **Manipuler** : te pousser à faire des choses que tu ne ferais jamais autrement

Important

Le catfishing n'est pas un cas isolé. Selon une étude, un jeune sur trois a déjà eu





affaire à de faux profils. Plus le groupe visé est jeune, plus les auteurs sont agressifs.

L'ingénierie sociale : l'art de la manipulation

On parle d'ingénierie sociale quand quelqu'un utilise des astuces psychologiques pour te pousser à faire ou à révéler quelque chose. Les leviers les plus fréquents :

Astuce	Exemple
Pression du temps	« Vite, ton compte va être bloqué ! »
Serviabilité	« Tu peux me donner ton mot de passe deux secondes ? Je teste un truc. »
Autorité	« Je suis admin de ce serveur, j'ai besoin de tes données. »
Curiosité	« Regarde, c'est toi sur cette vidéo ? » + lien
Peur	« J'ai des captures d'écran de toi. Paie ou je les publie. »

Comment te protéger

- **Aucun inconnu n'a besoin de ton mot de passe.** Personne. Ni un admin, ni le support, ni un ami
- **Faire une contre-vérification** : connais-tu vraiment la personne ? Renseigne-toi par un autre canal
- **Vérifier les images** : clic droit → recherche d'image. Les photos de profil volées apparaissent souvent plusieurs fois
- **Pas d'images privées à des inconnus** : même pas à des « amis » que tu ne connais qu'en ligne
- **Bloquer au lieu de discuter** : si quelque chose te paraît bizarre, bloque tout de suite

Astuce





Un test simple : demande à la personne d'écrire un mot précis sur une feuille pendant un appel vidéo et de la montrer. Les faux profils échouent à coup sûr.

Quiz : vrai ou faux ?

Quelqu'un t'écrit sur Instagram : « Salut, je suis nouveau dans ton école et je ne connais encore personne. Tu veux bien me donner ton numéro pour qu'on se voie ? »

Que fais-tu ?

- ☐ Envoyer mon numéro, il a l'air sympa
- ☒ Demander : « Tu es dans quelle classe ? » et vérifier auprès de camarades
- ☐ Ignorer
- ☒ Vérifier le profil : depuis quand existe-t-il ? Combien de publications et d'abonnés a-t-il ?

Nuage de mots

À quoi vois-tu qu'un profil pourrait être faux ?

Question de quiz

Un nouveau profil t'écrit. Qu'est-ce qui te rend méfiant ?

Réponses possibles

- Peu de publications, mais énormément d'abonnés
- Il veut passer rapidement sur une autre messagerie
- Il a une photo de profil
- Il demande très tôt des détails personnels
- Toutes les photos ont l'air de sortir d'un catalogue





6. Deepfakes et fausses voix : ne crois pas tout ce que tu vois et entends

Comment l'IA fabrique des vidéos et des voix plus vraies que nature, et comment ne pas te faire avoir.

Quand tes yeux et tes oreilles te trompent

Avant, une vidéo ou un message vocal, c'était une preuve. Plus aujourd'hui.

L'intelligence artificielle peut imiter les visages et les voix si bien qu'on ne voit ou n'entend presque plus la différence. On appelle ça un **deepfake** (vidéo/image truquée) et le **clonage de voix** (voix clonée).

Où tu croises ça

- **Fausse vidéos de stars** : une star ou un streamer fait soi-disant la promo d'un « concours gratuit », mais en réalité c'est un faux créé par IA qui t'attire vers un site d'arnaque.
- **Voix clonées** : à partir de quelques secondes d'un message vocal, l'IA fabrique une copie de ta voix. Puis « ton ami » appelle et demande de l'aide en urgence.
- « **Maman, j'ai un nouveau téléphone** » : un message ou un appel avec une voix familière demande de l'argent ou un mot de passe. Une très vieille ruse, bien plus convaincante aujourd'hui avec l'IA.

Important

Une voix ou un visage n'est **plus une preuve** de qui écrit ou appelle vraiment. Ne te fie pas à ça, mais au chemin par lequel le message est arrivé.





Comment repérer la ruse

Pas à l'apparence, elle s'améliore sans cesse. Mais au **déroulement** :

- Tout à coup, c'est **super urgent**.
- Tu dois **garder le secret** (« ne le dis à personne »).
- Ça arrive par un **canal inhabituel**.

Comment te protéger

- **Convenir d'un mot de code** : choisis avec ta famille et tes amis un mot secret pour les urgences. Celui qui ne le connaît pas n'est pas la vraie personne.
- **Rappeler** : au numéro que tu connais déjà, pas à celui du message.
- **Ne rien croire juste parce que ça a l'air vrai** : les images, les vidéos et les voix peuvent être truquées.

Question de quiz

Tu reçois un message vocal. La voix ressemble exactement à celle de ton meilleur ami et te demande d'urgence ton mot de passe. Que fais-tu ?

Réponses possibles

Envoyer le mot de passe, c'est bien sa voix

Rappeler au numéro connu ou demander en personne

Devenir méfiant si c'est « urgent » et que ça doit rester secret

Faire tout de suite ce que dit la voix

Jeu pédagogique

Vrai ou truqué ? Regardez ensemble des exemples d'images, de vidéos et de messages et décidez ce qui est vrai et ce qui ne l'est pas.





7. Gaming : vol de compte, arnaques et comment te protéger

Pourquoi ton compte de jeu a de la valeur et comment les escrocs essaient de le voler.

Ton compte vaut de l'argent

Tu as investi des centaines d'heures dans ton jeu. Skins, rangs, objets, peut-être même des cosmétiques rares. Ce que tu ne sais peut-être pas : sur le marché noir, ces comptes ont une vraie valeur en argent. Un compte Fortnite avec des skins rares se vend entre 50 et 500 €. Un inventaire CS2 avec des skins de couteau peut valoir des milliers d'euros.

Et c'est justement pour ça que les comptes de jeu sont une cible prisée.

Les arnaques les plus fréquentes

1. « V-Bucks / Robux / pièces gratuits »

Tu vois un site ou une vidéo YouTube qui promet de la monnaie de jeu gratuite. Tu dois « juste » saisir ton nom d'utilisateur et ton mot de passe. Ce qui se passe vraiment : ton compte a disparu.

Important

Il n'existe **aucun** V-Bucks, Robux ou autre monnaie de jeu gratuite en dehors des boutiques officielles. Tout site qui promet ça est une arnaque.

2. Arnaques à l'échange

« Je t'échange mon objet rare contre le tien. » L'échange commence, mais au dernier moment l'objet est remplacé ou l'échange est manipulé. Particulièrement répandu dans



: Rocket League, CS2, Roblox.

3. Faux support

Tu reçois un message : « Ton compte a été signalé pour triche. Clique ici pour le vérifier, sinon il sera bloqué. » Le lien mène à une fausse page de connexion.

4. Phishing via Discord

« Salut, il me manque encore quelqu'un pour mon équipe. Inscris-toi sur ce site de tournoi ! » Le lien ressemble à une vraie plateforme d'e-sport, mais c'est une copie qui intercepte ton mot de passe.

Comment les attaquants accèdent à ton compte

Méthode	Comment ça marche
Lien de phishing	Fausse page de connexion qui a l'air vraie
Deviner le mot de passe	Parce que tu utilises le même partout
Voler un jeton de session	Via des extensions de navigateur manipulées
Ingénierie sociale	« Je suis modo, j'ai besoin de tes identifiants »

Comment te protéger

- **Activer l'authentification à deux facteurs (2FA)** : sur Steam, Epic, Riot, Blizzard, partout où c'est possible
- **Un mot de passe unique** pour chaque compte de jeu
- **Ne jamais partager tes identifiants sur Discord, TeamSpeak ou dans un chat**
- **Utiliser les liens officiels** : ne pas chercher via Google, mais taper l'adresse toi-même
- **Vérifier les extensions de navigateur** : n'installer que ce dont tu as vraiment besoin



Astuce

Active la 2FA. Maintenant. Sérieusement. Ça prend deux minutes et rend ton compte bien plus sûr. Sur Steam, ça s'appelle « Steam Guard », sur Epic « authentification à deux facteurs », sur Riot « application d'authentification ».

Énigme : repère l'arnaque

Tu reçois ce message sur Discord de quelqu'un que tu connais d'un serveur de jeu :

« Hé, j'ai trouvé un sponsor pour notre équipe ! On doit juste tous s'inscrire sur ce site : esport-turniere.net/anmelden. Fais vite, les places sont limitées ! »

Quels sont les signaux d'alarme ?

Question de quiz

Un site te promet de la monnaie de jeu gratuite si tu te connectes. Qu'est-ce qui est vrai ?

Réponses possibles

C'est toujours une arnaque

Ça marche parfois

Ton compte aura disparu ensuite

L'adresse e-mail associée est aussi en danger





8. 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.



9. 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.





10. 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

11. 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
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 **mise 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



12. Reconnaître le phishing, même quand il ressemble à ton jeu préféré

Comment repérer les faux messages et les faux liens avant de cliquer dessus.

Qu'est-ce que le phishing ?

Le phishing, c'est quand quelqu'un se fait passer pour quelqu'un d'autre pour obtenir tes données. Le plus souvent par e-mail, mais aussi par SMS, WhatsApp, Discord ou même par un message dans un jeu.

Le nom vient de « fishing » (la pêche, en anglais) : l'attaquant lance un appât et attend que quelqu'un morde.

À quoi ressemble le phishing dans ton quotidien

Exemple 1. Le piège Steam :

« Ton compte Steam a été suspendu en raison d'une activité suspecte. Vérifie ton identité dans les 24 heures : steamcommunity.com/verify »

Tu vois l'erreur ? C'est écrit « steamcommuntly » au lieu de « steamcommunity ». Une seule lettre de différence, mais tu atterris sur un site complètement faux.

Exemple 2. Le message Instagram :

« Hé, quelqu'un a posté une vidéo de toi 📺 regarde : bit.ly/3xK9mP »

Les liens raccourcis cachent où ils mènent vraiment. Et le message joue sur la curiosité

et une petite panique.

Exemple 3. L'e-mail de Spotify :

« Votre moyen de paiement a expiré. Mettez à jour vos informations pour ne pas perdre votre compte. »

Spotify envoie vraiment ce genre d'e-mails, mais le vrai e-mail renvoie vers spotify.com, pas vers spotify-account-update.com.

Le contrôle en 5 secondes

Avant de cliquer sur un lien, arrête-toi cinq secondes et vérifie :

1. **Qui envoie ça ?** Est-ce que je connais vraiment la personne/l'entreprise ?
2. **Y a-t-il de la pression ?** « Immédiatement », « dans les 24 heures », « maintenant » : c'est presque toujours de la manipulation
3. **Où mène le lien ?** Laisser le doigt appuyé dessus (sans taper !) affiche la vraie adresse
4. **Est-ce logique ?** Steam/Instagram/Spotify me contacterait-il comme ça ?
5. **Demande-t-on mes identifiants ?** Les vrais services ne demandent jamais ton mot de passe par message

Important

Aucun service sérieux ne t'envoie un message avec un lien où tu dois saisir ton mot de passe. Si tu as un doute : ouvre l'appli ou le site directement, pas par le lien.

Que faire si tu as cliqué ?

C'est arrivé : tu as cliqué sur un lien de phishing et tu as peut-être même saisi des

données. Pas de panique, mais il faut agir vite :

1. **Changer ton mot de passe tout de suite** : pour le service concerné et partout où tu as utilisé le même mot de passe
2. **Activer la 2FA** : si ce n'est pas déjà fait
3. **Prévenir quelqu'un** : parents, enseignant, responsable informatique. Ce n'est pas une honte, c'est un incident de sécurité
4. **Prévenir la banque** : si des données de paiement sont concernées

Astuce

Tu n'as rien fait de mal si tu signales du phishing. Tu fais une erreur si tu le caches. Signaler aide, toi et les autres.

Quiz : phishing ou authentique ?

Classe ces messages. Phishing ou authentique ?

1. E-mail de Netflix : « Ton abonnement sera résilié demain. Clique ici pour mettre à jour ton paiement. »
2. SMS de DHL : « Votre colis n'a pas pu être livré. Frais de douane : 1,99 €. Payez ici. »
3. E-mail de ton école : « Les nouveaux horaires des clubs et ateliers sont en ligne. Regarde sur le portail de l'école. »
4. Message privé Discord : « Hé, c'est toi sur la photo ?? [\[lien\]](#) »

Jeu pédagogique

Cinq messages, à chaque fois authentique ou faux. Après le jeu, passer en revue les indices au tableau.



Question de quiz

À quoi reconnais-tu le plus sûrement un message de phishing ?

Réponses possibles
Il te met sous pression
L'adresse de l'expéditeur ne correspond pas à l'expéditeur supposé
Il est écrit en français
Il demande ton mot de passe ou tes données de paiement
Il a un logo

13. Résumé : ta boîte à outils numérique

Tout l'essentiel en un coup d'œil et la préparation au test de phishing pratique.

Ce que tu as appris dans ce cours

Tu as maintenant les connaissances pour te protéger bien mieux en ligne. Voici les points les plus importants en résumé :

Tes données t'appartiennent.

- C'est toi qui décides qui voit quoi
- Les données publiées publiquement peuvent servir à des arnaques et à de la manipulation
- La protection des données est un droit, pas un luxe

Les réseaux sociaux ne sont pas tes amis, ce sont un modèle économique.

- Les applis collectent plus de données que tu ne le penses
- Profil en privé, localisation désactivée, autorisations vérifiées
- Tout ce que tu vois en ligne n'est pas vrai

Dans le gaming, il y a de l'argent réel et des dangers réels.

- La monnaie de jeu gratuite n'existe pas
- Activer la 2FA, utiliser des mots de passe uniques
- Aucun lien venant de Discord ou TeamSpeak n'est fiable à 100 %

Ton téléphone mérite d'être protégé.

- Code PIN/biométrie, mises à jour, autorisations des applis
- Wi-Fi ouvert = livre ouvert
- Supprimer les vieilles applis

Un mot de passe, un compte.



- Utiliser un gestionnaire de mots de passe
- Activer l'authentification à deux facteurs partout
- Ne jamais partager tes mots de passe, même pas avec tes amis

Reconnaître le phishing = réfléchir cinq secondes.

- Qui envoie ça ? Où mène le lien ? Y a-t-il de la pression ?
- En cas de doute : ne pas cliquer, mais aller directement sur le site
- Signaler n'est pas une faiblesse, ça protège tout le monde

Important

La sécurité parfaite n'existe pas. Mais avec ce que tu sais maintenant, tu es **bien plus difficile** à tromper qu'avant. Et c'est tout l'intérêt.

Et maintenant : le test pratique

Dans les prochains jours, tu vas recevoir **trois e-mails de phishing simulés** sur ton adresse e-mail scolaire. Ils ont l'air vrais, mais ils viennent de ce cours.

Ta mission : **Les reconnaître et ne pas cliquer dessus.**

Tu recevras ensuite ton résultat sous forme de rapport personnel. Et : on ne peut pas « échouer ». Celui qui se fait avoir par un e-mail en tire une leçon. Celui qui n'en ouvre aucun a réussi le cours.

Astuce

Applique le contrôle en 5 secondes. À chaque e-mail suspect. À partir de maintenant. Pas seulement pour les e-mails de test.



Quiz final : 10 questions, combien en réussis-tu ?

1. Combien de mots de passe devrais-tu utiliser au total ?
2. Qu'est-ce que la 2FA ?
3. Qu'est-ce que le catfishing ?
4. Pourquoi le Wi-Fi public est-il dangereux ?
5. Que fais-tu si tu as cliqué sur un lien de phishing ?
6. Quelqu'un a-t-il le droit de publier une photo de toi sans te demander ?
7. Que signifie l'ingénierie sociale ?
8. À partir de quel âge es-tu pénalement responsable en Allemagne ?
9. Quelle est la façon la plus sûre de créer un mot de passe ?
10. Quel est le conseil le plus important contre le phishing ?

Avec au moins 7 bonnes réponses, tu es bien préparé pour le test pratique.

Nuage de mots

Que retiens-tu de ce cours ? Un mot suffit.