Supports de cours pour l’enseignant

Digitale Selbstverteidigung Klasse 9/10: Angriffe erkennen

6 leçons · env. 90 minutes de cours · 15 activités interactives · Version du 23/11/2026

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

Déroulement du cours

Vous menez le cours au tableau et décidez vous-même quand aborder quelle leçon. Le cours n'expire pas. Ce cours comprend l'entraînement anti-hameçonnage : une belle occasion de mettre en pratique ce qui a été appris sur son propre appareil, dans sa propre boîte mail. C'est uniquement pour cela que la classe s'inscrit via un code QR lors de la première heure ; le prénom suffit pour participer. 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, ce qui lance l'entraînement anti-hameçonnage : trois tentatives d'escroquerie simulées par e-mail au cours des semaines suivantes. Seuls les élèves ayant l'accord des parents (modèle : lettre aux parents) et une adresse e-mail enregistrée peuvent participer. Le certificat atteste la participation réussie à cet entraînement et n'est délivré qu'aux participants.

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

Klassen 9 und 10 (etwa 14 bis 16 Jahre) · Durée : zwei Doppelstunden plus Praxistest in den Wochen danach · Version du 03.10.2026

Angriffe erkennen: Fake-Profile und Social Engineering, Fake-Stimmen, Betrug in Spielen, Datenschutz im Praktikum und Phishing. Schließt mit dem Phishing-Praxistest ab, mit Einverständnis der Eltern. Champs d’action de la perspective directrice « Vivre et apprendre dans un monde numérique » : Verantwortungsvoll handeln und schützen,

Digital kommunizieren, kooperieren, handeln, Informationen sammeln, verstehen, bewerten.

Domaine	Compétence (guide de lecture Informatique et éducation aux médias 2026/27 ou programme 2016)
Digitalität und Partizipation	Akteure und Interessen; Vertrauenswürdigkeit; Desinformation und Deepfakes Leçons : Fake-Profile, Deepfakes und Fake-Stimmen
Leitperspektive Medienbildung	Jugendmedienschutz, Informationelle Selbstbestimmung und Datenschutz, Kommunikation und Kooperation
Aufbaukurs Informatik, 3.1.4 Informationsgesellschaft und Datensicherheit	(6) Anfall personenbezogener Daten, Nutzen und Risiken

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.	**Faux profils, catfishing et ingénierie sociale** Niveau 9/10 · Digitalität und Partizipation Comment des escrocs se font passer pour d’autres et cherchent à te manipuler.	Quiz, Nuage de mots, Quiz
2.	**Deepfakes et fausses voix : ne crois pas tout ce que tu vois et entends** Niveau 9/10 · Digitalität und Partizipation Comment l’IA fabrique des vidéos et des voix plus vraies que nature, et comment ne pas te faire avoir.	Quiz, Jeu : faktencheck
3.	**Gaming : vol de compte, arnaques et comment te protéger** Complément · Praxis Betrug im Alltag Pourquoi ton compte de jeu a de la valeur et comment les escrocs essaient de le voler.	Nuage de mots, Quiz
4.	**La protection des données au travail : pourquoi les secrets vaudront de l’argent plus tard** Complément · Praxis Datenschutz (BP 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.	**Reconnaître le phishing, même quand il ressemble à ton jeu préféré** Complément · Praxis Phishing Comment repérer les faux messages et les faux liens avant de cliquer dessus.	Quiz, Jeu : phishing-duell, Quiz
6.	**Résumé : ta boîte à outils numérique** Complément · Zusammenfassung 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 possibles. Les solutions marquées se trouvent uniquement dans votre Cockpit.

1. 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 ? »

Question de quiz

Que fais-tu ?

Réponses possibles
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

2. 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

- **Fausses 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.

3. 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 ! »

Nuage de mots

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

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 débloque 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 faufilez 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. 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 : steamcommunlty.com/verify »

Tu vois l’erreur ? C’est écrit « steamcommunlty » 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] »

Question de quiz

Lesquels de ces messages sont du phishing ?

Réponses possibles
Netflix : abonnement résilié, mettre à jour le paiement
SMS DHL : payer 1,99 € de frais de douane via un lien

École : nouveaux horaires des clubs sur le portail
Message Discord : « C’est toi sur la photo ?? » avec un 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

6. 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.**