Audit des paramètres de sécurité (1/2)

Clara

Inès

Gabriel

Yassir

Audit des paramètres de sécurité (2/2)

Clara

Capture 1

Paramètres TikTok

- Accès des applications non vérifié → Clara a autorisé TikTok à accéder à son micro et sa caméra en permanence.
- Compte en mode public → « Tout le monde peut voir tes vidéos et interagir avec toi. »

Capture 2

Messages privés sur WhatsApp

- Mot de passe noté dans un message → Clara écrit : « J'oublie toujours mon mot de passe Pinterest ! Je l'ai noté ici : *Clara12345.* »

Inès

Capture 1

- Mode Ghost désactivé sur Snap Map → « Inès est localisée en temps réel à la piscine municipale. »
- Wi-Fi public utilisé pour poster une story → « Connectée au Wi-Fi de la piscine municipale. »

Capture 2

- Connexion non sécurisée → BeReal n'a pas activé l'authentification à deux facteurs
- Mot de passe faible et prévisible → « Mot de passe : *Cookie2005.* »

Gabriel

Capture 1

Capture d'écran des paramètres de son compte Steam

- Mode de connexion automatique activé → « Se connecter automatiquement sans demander le mot de passe. »
- Mot de passe faible et prévisible → « Mot de passe : *Gamer123.* »
- Absence de 2FA → « Authentification à deux facteurs : Désactivée. »

Capture 2

- Application Discord avec accès aux contacts et au micro → « Cette application peut accéder à : Contacts, Microphone, Position. »

Yassir

Capture 1

Captures d'écran de son compte Switch Online

- Mot de passe trop simple et non changé depuis 2 ans.
- Compte public : tout le monde peut voir mon profil et mes scores.
- Pas de restriction parentale activée.

Capture 2

Captures d'écran de Google Maps

- Partage automatique de la position activée – dernier lieu visité : Salle d'escalade Vertical Limit.
- Historique des trajets accessibles : lieux récents : École Saint Louis, Lac de Mons, Maison.

Cartes conseils sécurité (1/4)

Écrire ses mots de passe en Leet Speak

✖

Transforme tes mots de passe en code secret !

Activer l'authentification à deux facteurs (2FA)

✖

Double protection, double sécurité !

Vérifier et restreindre les autorisations des applications

✖

Pourquoi cette appli veut-elle accéder à ton micro ?

Choisir un mot de passe long et unique

✖

123456 ?
Mauvaise idée !

Cartes conseils sécurité (2/4)

Le Leet Speak consiste à remplacer certaines lettres par des chiffres et symboles ressemblants. Par exemple, « *SkateLife2024* » devient « *$k@t3L1f3_2O24!* ».

L'authentification à deux facteurs ajoute une étape supplémentaire pour accéder à ton compte. En plus du mot de passe, un code unique est envoyé par SMS, email ou via une appli comme Itsme, Microsoft Authentificator.

Lorsque tu télécharges une appli, elle peut demander des autorisations inutiles. Vérifie dans les paramètres de ton téléphone et désactive les accès superflus.

Un bon mot de passe doit être :

- Long (12 caractères minimum) ;
- Unique (ne pas réutiliser le même sur plusieurs sites) ;
- Complexe (chiffres, majuscules, caractères spéciaux).

Cartes conseils sécurité (3/4)

Protéger ses comptes avec un gestionnaire de mots de passe

✖

Retenir 10 mots de passe différents ? Trop compliqué. Mais j'ai une astuce !

Désactiver la géolocalisation automatique

✖

Pourquoi toutes tes applis savent où tu es ?

Faire attention aux Wi-Fi publics

✖

McDo, aéroport, gare : des pièges pour hacker !

Paramétrer ses réseaux sociaux en privé

✖

Ton Insta, c'est pour tes potes ou pour le monde entier ?

Cartes conseils sécurité (4/4)

Un gestionnaire de mots de passe (comme Bitwarden, Dashlane ou 1Password) stocke et chiffre tes mots de passe. Tu ne retiens qu'un seul mot de passe maître.
Il génère des mots de passe ultra sécurisés pour chaque compte.

Certaines applis activent ta position en permanence même quand tu ne les utilises pas. Désactive la géolocalisation permanente dans les paramètres. Active-la uniquement quand tu en as besoin (ex. GPS, livraison).

Les Wi-Fi publics (cafés, bibliothèques, écoles) ne sont pas sécurisés. Un hacker peut intercepter tes mots de passe et messages. Utilise tes données mobiles ou un VPN pour sécuriser ta connexion. ET Jamais de connexion bancaire sur un Wi-Fi public !

Un compte public expose toutes tes photos et infos. Mets ton compte en privé pour contrôler qui te suit. Vérifie qui peut voir tes stories et tes anciens posts.