SÉCURITÉ HORS LIGNE & EN LIGNE

🔒 1. Sécurité hors ligne

📄 Papiers personnels

- Détruire les documents avant de les jeter
- Ranger les papiers importants au même endroit
- Garder une copie sur une clé USB à la maison
- Ancien ordinateur :
    - Fonctionnel → remise à zéro
    - Non fonctionnel → détruire le disque dur

Message clé : La sécurité commence dans la vraie vie.

📱 Téléphone / tablette

- Toujours mettre un code, Face ID ou empreinte
- Garder son code secret
- En cas de perte/vol : faire bloquer rapidement

Message clé : Un téléphone sans code, c'est une maison sans serrure.

🔑 Mots de passe

- Pas de Post-it visible
- Carnet rangé chez soi = OK
- Ne jamais utiliser le même mot de passe partout
- Un gestionnaire de mots de passe peut aider

Message clé : Mieux vaut un mot de passe noté que le même partout.

💾 Clés USB

- Ne jamais brancher une clé trouvée
- Utiliser uniquement ses propres clés

Message clé : Une clé USB inconnue, ça ne se branche jamais.

📞 Arnaques téléphoniques

- Le numéro affiché peut être falsifié

- Les arnaqueurs imitent : banque, impôts, opérateur, proche
- Objectif : obtenir des infos ou un paiement
- En cas de doute : raccrocher et rappeler soi-même

Message clé : On ne donne jamais d'informations au téléphone.

🛡️ 2. Antivirus, sauvegardes, mises à jour

🖥️ Antivirus

- Utile, mais ne protège pas des arnaques
- Un seul antivirus à la fois
- Windows inclut un antivirus gratuit efficace

Message clé : L'antivirus protège l'ordinateur, pas les décisions.

💽 Sauvegardes

- Sauvegarder : photos, documents, contacts
- Solutions : clé USB, disque dur externe, cloud
- Règle simple :
    - 1 sauvegarde automatique
    - 1 sauvegarde déconnectée

Message clé : Ce n'est pas "si" on perd ses données, mais "quand".

🔄 Mises à jour

- Concerne : ordinateur, téléphone, tablette, applications
- Elles corrigent des failles de sécurité
- Ne pas les retarder

Message clé : Une mise à jour, c'est une protection.

🌐 3. Sécurité en ligne

🕵️ Arnaques en ligne

- Faux sites (banque, impôts, colis)
- QR codes frauduleux
- Faux supports techniques
- Messages d'urgence

- Arnaques sentimentales
- Téléchargements piégés

Message clé : Une arnaque fonctionne quand on agit trop vite.

🌍 Navigation sécurisée

- Prudence sur le Wi-Fi public
- Navigation privée sur ordinateur partagé
- Ne jamais cliquer sur un lien reçu par mail
- Vérifier l'adresse du site
- Télécharger depuis les stores officiels

Message clé : Avant de cliquer, on vérifie toujours.

💳 Paiement en ligne & banque

- Taper soi-même l'adresse de la banque
- Ne jamais cliquer sur un lien reçu
- Codes SMS : ne jamais les donner
- Ne jamais valider un virement demandé par téléphone
- Vérifier ses comptes régulièrement

Message clé : Un code bancaire ne se partage jamais.

🤖 4. IA & nouveaux risques

🧠 Faux contenus

Images truquées, vidéos modifiées, faux articles

- Réflexe : Vérifier la source

🎙️ Voix clonées

Une voix peut être imitée

- Réflexe : Raccrocher et rappeler soi-même

👤 Faux profils / usurpation

Photos générées, comptes piratés

- Réflexe : Vérifier en appelant la vraie personne

📰 Désinformation

Faux avis, faux témoignages, rumeurs amplifiées

- Réflexe : Ne pas partager sans être sûr

💬 Arnaques automatisées

Mails et SMS très bien écrits

- Réflexe : Se méfier des messages trop parfaits

🔐 Bons réflexes face à l'IA

- Vérifier la source
- Se méfier des contenus trop parfaits
- Ne jamais agir dans l'urgence
- Confirmer par un autre moyen

Message clé : Avant de croire, on vérifie. Avant d'agir, on respire.

⭐ Conclusion

Vos 5 réflexes de sécurité

1. Vérifier avant de cliquer
2. Ne jamais agir dans l'urgence
3. Appeler soi-même en cas de doute
4. Protéger ses appareils (code, mises à jour, sauvegardes)
5. Garder en tête que tout peut être imité