MON MÉMO SÉCURITÉ INFORMATIQUE

5 réflexes essentiels pour naviguer en toute tranquillité sur Internet

Des Mots de Passe Forts et Sécurisés

- **Pas de données évidentes :** Évitez les prénoms, dates de naissance ou suites simples (123456).
- **L'astuce de la phrase :** Prenez la 1ère lettre de chaque mot d'une phrase facile à retenir. Ex : « Mon chat Mimile a 3 ans » → **McMa3a!**
- **Stockage :** Notez-les dans un petit cahier papier rangé chez vous, jamais sur un post-it collé à l'écran.

Méfiance face aux E-mails Suspects (Phishing)

- **Attention aux fausses urgences :** Menace de blocage de compte, amende ou colis bloqué.
- **Vérifiez l'expéditeur :** Si le mail prétend venir de votre banque mais se termine par `@gmail.com` ou une adresse bizarre, c'est un piège !

⚠ **REFLEXE : Ne cliquez JAMAIS sur les liens contenus dans un e-mail douteux. Allez directement sur le site officiel via votre navigateur habituel.**

Ignorer les Fausses Alertes "Virus Détecté !"

- Si un écran rouge ou sonore apparaît en disant que votre PC est bloqué ou infecté : **C'est une arnaque !**
- N'appelez **jamais** le numéro de téléphone affiché à l'écran.

💡 Que faire ? Fermez votre navigateur (croix en haut à droite) ou éteignez/redémarrez votre ordinateur.

Achats en Ligne sans Risque

- **Regardez la barre d'adresse :** Vérifiez la présence du **cadenas fermé** et du préfixe **`https://`**
- **Prix trop bas :** Un produit vendu 3 fois moins cher qu'ailleurs est souvent une arnaque.
- Validez toujours vos achats depuis votre téléphone portable (application bancaire).

Mises à Jour et Antivirus

- Acceptez les **mises à jour système** (Windows / Mac) : elles bouchent les failles de sécurité.
- Laissez votre antivirus actif (l'antivirus par défaut ***Windows Defender*** est parfait pour un usage quotidien).

📞 En cas de doute ou de piratage suspecté :

Contactez un proche ou un informatique de confiance. En cas de fraude avérée, faites opposition immédiatement auprès de votre banque.