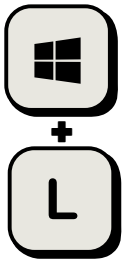
PAG
NOS MÉTIERS, VOTRE SÉRÉNITÉ

Accueil
Sécurité
Formation

Tout savoir sur les BONNES PRATIQUES EN INFORMATIQUE

Eteindre et verrouiller les outils informatiques

- **Éteindre les outils informatiques** à chaque fin de service pour économiser de l'énergie et prévenir les accès non autorisés.
- **Verrouiller son ordinateur dès que l'on quitte son poste**, même pour une courte absence. Utilisez le raccourci clavier Windows + L sur Windows pour verrouiller rapidement. *C'est comme fermer la porte de votre maison !*

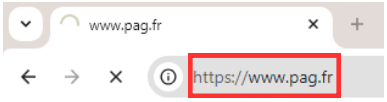


Effectuer les mises à jour

- **Faire les mises à jour proposées par l'ordinateur**, qu'il s'agisse du système d'exploitation ou des logiciels utilisés. Ces mises à jour corrigent souvent des vulnérabilités de sécurité. *Ne pas les ignorer !*
- **Respecter les consignes durant les mises à jour**, comme ne pas éteindre l'ordinateur ou le redémarrer si nécessaire.

Utiliser des sites web sécurisés

- **Utiliser des sites web sécurisés** : vérifiez que l'URL commence par "https://" et qu'il y a une icône de cadenas dans la barre d'adresse du navigateur.



- Évitez de fournir des informations sensibles sur des sites non sécurisés.

Vérifier les emails avec prudence

- **Vérifier l'adresse email de l'expéditeur avant d'ouvrir des pièces jointes ou de cliquer sur des liens.** Soyez particulièrement vigilant avec les expéditeurs inconnus ou suspects.
  Posez-vous la question : "Connaissez-vous cet expéditeur ?"
- **Méfiez-vous des emails contenant des pièces jointes inattendues ou des liens directs.**
- Préférez entrer une adresse du site web manuellement dans le navigateur.
- **Attention aux tentatives de phishing** : les emails qui demandent des informations personnelles ou financières sont souvent des pièges.
- **Méfiez-vous des adresses email avec des extensions suspectes.**

Exemples d'extensions suspectes :

.ru *(Russie)*
.cn *(Chine)*
.biz *(affaires, souvent utilisé dans le spam)*
.tk *(Tokelau, souvent utilisé pour des sites de phishing)*

Contrôler la sécurité de son adresse mail

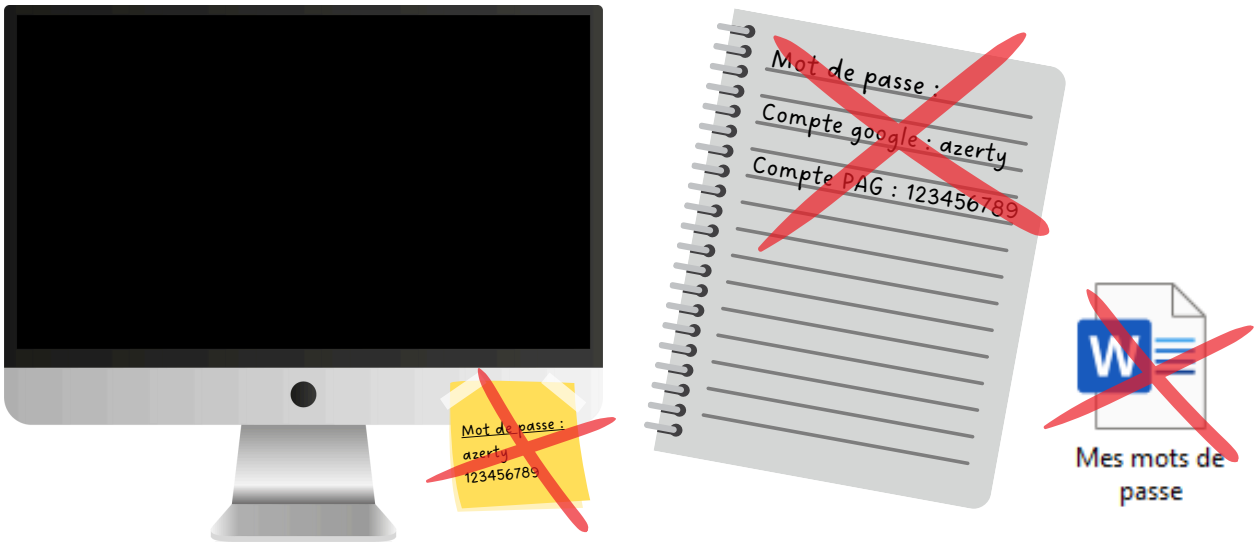
- **Contrôler régulièrement si son adresse email a été piratée** en utilisant le site web haveibeenpwned.com.
- **Tester la sécurité de ses mots de passe** et changer immédiatement ceux qui ont été compromis. Également sur haveibeenpwned.com dans la section Passwords.
  Faites de ce contrôle une habitude mensuelle, comme on vérifie la pression des pneus de sa voiture !

Créer et gérer des mots de passe forts

- **Utiliser des mots de passe forts** : une combinaison d'au moins 12 caractères comprenant des majuscules, des minuscules, des chiffres et des caractères spéciaux.

Exemple de mot de passe fort : MaCh@ts3cur1t3

- Renouveler régulièrement les mots de passe et ne pas réutiliser les mêmes mots de passe sur plusieurs comptes.
- **Ne pas laisser traîner les mots de passe sur son poste de travail**, ni sous forme de notes physiques ni dans des fichiers non sécurisés. Préférez l'utilisation d'un gestionnaire de mot de passe comme BitWarden.



Utilisation personnelle de l'ordinateur

- **Ne pas utiliser l'ordinateur professionnel à des fins personnelles** pour éviter l'introduction de malwares ou l'accès non autorisé à des informations sensibles. *C'est comme ne pas mélanger ses vêtements de travail avec ses tenues de sport.*

Formation et sensibilisation en continu

- Sensibiliser les collègues en partageant des informations pertinentes et en signalant les comportements à risque.
- Consulter les Ressources de l'ANSSI *(Agence Nationale de la Sécurité des Systèmes d'Information)* pour approfondir vos connaissances en cybersécurité et rester à jour sur les dernières menaces et bonnes pratiques, visitez le site de l'ANSSI *(ssi.gouv.fr)*.
  L'ANSSI propose des guides, des conseils de sécurité, et des actualités sur la cybersécurité. C'est une ressource précieuse pour toute personne souhaitant approfondir sa compréhension des enjeux de sécurité informatique et des meilleures pratiques.

Surveillance des activités suspectes

- Surveiller les activités suspectes sur son ordinateur et **signaler immédiatement tout comportement anormal au référent informatique**.

Lazar Popovic
Référent informatique pour le groupe
04 73 29 28 29
lazar.popovic@pag.fr