Sécurité numérique, les bons gestes

publié le 04/04/2024 - mis à jour le 11/11/2025

Descriptif :

Chacun d'entre nous, dans ses usages quotidiens, professionnels comme personnels, a une responsabilité dans la sécurité numérique.
Cet article vous présente quelques règles simples à mettre en oeuvre et un mémo d'aide à afficher.

Sommaire :

Chacun d'entre nous, dans ses usages quotidiens, professionnels comme personnels, a une responsabilité dans la sécurité numérique.
Voici quelques règles simples à mettre en œuvre.

● Utilisez des mots de passe robustes.

- Un mot de passe robuste doit comporter au moins 12 signes mélangeant des majuscules, des minuscules, des chiffres et des caractères spéciaux.
- Il ne doit pas être noté sur un papier, ni stocké de manière non sécurisée (fichier texte, navigateur…).
- Ayez autant de mots de passe différents que de comptes.
- Privilégiez des mots de passe différents sur chaque service en ligne afin d'éviter les piratages en cascade.
- N'enregistrez pas vos mots de passe dans un ordinateur partagé et pensez à vous déconnecter en partant. Sinon vos mots de passe et vos sessions seront aussi partagés.
- Activez les authentifications renforcées quand c'est possible.
- Les mots de passe se renouvellent au minimum tous les trois ans.

● Méfiez-vous des messages inattendus sur votre messagerie.

- Certains messages peuvent venir d'un interlocuteur inhabituel.
- Au moindre doute, ne les ouvrez pas, ne cliquez sur aucun lien et n'ouvrez aucune pièce jointe : ces messages peuvent vous piéger pour dérober des informations confidentielles ou installer un virus.
- En plaçant la souris sur le lien, sans cliquer, vous pourrez voir vers quel site vous seriez dirigé.
- En cas de doute, vous pouvez vérifier un document ou un courriel en le déposant sur le service en ligne « Je Clique ou Pas » de l'ANSSI : https://jecliqueoupas.cyber.gouv.fr

● Protégez vos données professionnelles.

- Pour éviter toute perte de données, veillez à utiliser exclusivement les lecteurs réseaux (serveurs bureautiques) qui bénéficient de sauvegardes automatisées quand c'est possible.

- Faites des sauvegardes régulières des données importantes sur support externe.

● Séparez vos usages personnels et professionnels.

- Ne mélangez pas votre messagerie professionnelle et personnelle et utilisez des mots de passe différents.
- Ne vous envoyez pas de message d'une messagerie professionnelle à une messagerie personnelle et inversement.
- N'utilisez pas de services de stockage en ligne personnel à des fins professionnelles.
- Ne branchez pas de support USB dont l'origine n'est pas parfaitement fiable (une clé peut être piégée pour « aspirer » vos données une fois branchée sur votre matériel).

● Utilisez un anti-virus à jour et ne le désactivez jamais

- Un anti-virus permet de détecter une grande partie des menaces, s'il est bien à jour.
- Ne désactivez jamais un anti-virus ; les logiciels malveillants invitent à le désactiver pour pouvoir s'installer.

● Appliquez les mises à jour de sécurité sur tous vos appareils.

- Que ce soient des PC, des tablettes ou des smartphones,…) installez les mises à jour dès qu'elles vous sont proposées. Vous corrigez ainsi les failles de sécurité qui pourraient être utilisées par des personnes malveillantes pour dérober vos données ou vos mots de passe, voire pour détruire vos données.

● N'installez aucun logiciel dont l'origine n'est pas garantie.

- Un logiciel ou un module additionnel (plug-in) téléchargé depuis un site non-officiel peut contenir des virus et installer des logiciels malveillants comme des dérobeurs de mots de passe (stealers).
- La plupart des cas d'usurpation d'identité actuels sont causés par des vols de mots de passe réalisés par ce type de logiciel.

● Évitez les réseaux Wifi publics ou inconnus.

- Privilégiez la connexion à un réseau Wifi connu ou le partage de connexion avec votre téléphone.
- Évitez les réseaux Wifi publics ou inconnus qui sont souvent mal sécurisés et peuvent être contrôlés ou usurpés par des personnes malveillantes.
- Si vous n'avez d'autre choix que d'utiliser un Wifi public, veillez à ne jamais y réaliser d'opérations sensibles.

Pour aller plus loin :

Vous trouverez quelques conseils simples à mettre en œuvre détaillés dans les ressources suivantes :

- PIX.fr propose des modules sur la sécurité des données et des usages numériques : https://pix.fr
- M@gistère dispose d'un module de sensibilisation : SensCyber Agir pour contribuer à ma sécurité numérique et celle de mon organisation : https://magistere.education.fr/dgesco/course/view.php?id=2646

Cybermalveillance.gouv.fr publie de nombreuses ressources :

- Dix mesures essentielles pour assurer une sécurité numérique
- Des bonnes pratiques pour les mots de passe
- Des bonnes pratiques sur les réseaux sociaux
- La sécurité des usages pro/perso

Enfin, un MOOC conçu et mis à disposition par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) permet de se former aux risques cyber et aux réflexes à avoir au quotidien et en cas de crise.
Il est disponible à l'adresse suivante :

secnumacademie.gouv.fr

Si, malgré votre vigilance, vous constatiez la moindre anomalie, ou même en cas de doute, signalez-le à votre assistance informatique de proximité.

Vous trouverez enfin une affichette téléchargeable sur les « 7 conseils pour lutter contre le piratage informatique » dans la page dédiée du site ministériel :