Consignes sécurité numérique : conseils, règles et ressources

Chacun d'entre nous, dans ses usages quotidiens, professionnels comme personnels, a une responsabilité dans la sécurité numérique. Des règles simples, de bonne hygiène informatique, facilement applicables, sont rappelées dans le présent message.

1. Utilisez des mots de passe solides

Un mot de passe doit comporter 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.
Les mots de passe se renouvellent au minimum tous les trois ans.

2. Méfiez-vous des messages inattendus

Au moindre doute sur un message, ne l'ouvrez pas, ne cliquez sur aucun lien et n'ouvrez aucune pièce jointe : il peut vous piéger pour dérober des informations confidentielles ou installer un virus.

En cas de doute, il est possible de 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

3. 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.

4. Appliquez les mises à jour de sécurité sur tous vos appareils (PC, tablettes, téléphones…) 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.

5. Protégez vos données professionnelles

Pour éviter toute perte de données, veillez à utiliser exclusivement les lecteurs réseaux (serveurs bureautiques) qui bénéficient de sauvegardes automatisées.

6. 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).

7. 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 (ou utilisez le réseau privé virtuel – VPN – fournit par votre organisation[2]).

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 :

  https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/10-mesures-essentielles-assurer-securite-numerique

  https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/mots-de-passe

  https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/reseaux-sociaux

https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/securite-usages-pro-perso

- Un MOOC conçu et mis à disposition par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) permet de se former au risque cyber et aux réflexes à avoir au quotidien et en cas de crise. Il est disponible à l'adresse suivante secnumacademie.gouv.fr.
- Vous pouvez aussi consulter le site : cybermalveillance.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 : **https://www.education.gouv.fr/securite-des-espaces-numeriques-de-travail-ent-mesures-et-conseils-414030**

N'hésitez pas à diffuser et à apposer en bonne place cette affichette des bonnes pratiques numériques.