Sujet :	[Information] Règles de sécurité numérique
Date :	Fri, 04 Mar 2022 14:39:36 +0000
De :	MINISTERE DE L'EDUCATION NATIONALE, DE LA JEUNESSE ET DES SPORTS <information@education.gouv.fr>

Mesdames et Messieurs,

La cybersécurité est devenue un élément fondamental pour le bon fonctionnement de notre service public. La situation internationale actuelle nous oblige à renforcer cette exigence et requiert un niveau de vigilance accru de la part de tous.
Chacun d'entre nous, dans ses usages individuels quotidiens, professionnels comme personnels, a une responsabilité et est un acteur à part entière de la sécurité des systèmes d'information dans sa globalité.
Prenez quelques instants pour lire ces recommandations : ce sont des règles de bonne hygiène informatique, valables tout le temps, et que vous devez appliquer particulièrement dans le contexte que nous connaissons actuellement. Elles vous seront également utiles dans vos usages informatiques personnels.
Nous vous remercions, par avance, pour l'attention et la vigilance que vous porterez à ce sujet.

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 sur un message ou dans son téléphone.
Ayez autant de mots de passe différents que de comptes.

2. Méfiez-vous des messages inattendus

Ne les ouvrez pas, car ils peuvent vous piéger pour dérober des informations confidentielles ou contenir un virus dans une pièce jointe ou un lien.
Exemples :

- un message qui se prétend de source ministérielle mais comporte une adresse se terminant par « .fr » ou « .com » au lieu de « .gouv.fr » ou dont l'adresse de l'académie est légèrement erronée ;
- un message qui comporte des fautes de français ;
- un message qui vient d'un interlocuteur inhabituel ou non professionnel ;
- un message reçu d'un (ancien) contact mais qui vous écrit sans rapport avec l'objet du courriel.

Dans le doute, n'ouvrez pas le message, ne cliquez sur aucun lien, n'ouvrez aucune pièce jointe et ne répondez pas au message**.**

3. Appliquez les mises à jour de sécurité sur tous vos appareils (PC, tablettes, téléphones…), et ce, dès qu'elles vous sont proposées

Vous corrigez ainsi les failles de sécurité qui pourraient être utilisées par des personnes pour s'introduire dans vos appareils, pour y dérober des données ou vos mots de passe, voire pour détruire des données ou les saisir à votre insu.

4. Sauvegardez régulièrement vos données

Pour éviter toute perte de données, veillez à les sauvegarder régulièrement, soit en les enregistrant sur les serveurs bureautiques de votre réseau professionnel, soit dans le cadre d'un dispositif de sauvegarde des données stockées sur le poste de travail lui-même.

5. Séparez vos usages personnels et professionnels

Il faut séparer autant que possible vos usages afin que le piratage d'un accès personnel ne nuise pas au ministère, ou inversement.

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.

Ayez une utilisation responsable d'internet au travail.

N'utilisez pas de services de stockage en ligne personnel à des fins professionnelles.

Limitez au maximum l'utilisation de supports USB (risques de pertes, clés pouvant être piégées pour « aspirer » vos données une fois branchées sur votre matériel, etc.).

6. Évitez les réseaux Wifi publics ou inconnus

En mobilité, 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 un réseau privé virtuel – VPN – si vous en avez un).

7. Maîtrisez votre utilisation des réseaux sociaux

Les réseaux sociaux contiennent de nombreuses informations personnelles qui ne doivent pas tomber dans de mauvaises mains.

Sécurisez leur accès par un mot de passe solide et unique. Ayez autant de mots de passe différents que de comptes.

Définissez les autorisations sur vos informations et publications pour qu'elles ne soient pas inconsidérément publiques ou utilisées pour vous nuire.

Soyez prudent si vous évoquez votre travail car cela pourrait vous porter préjudice.

Faites attention à qui vous parlez, car les cybercriminels utilisent les réseaux sociaux pour commettre des escroqueries ou voler des informations personnelles ou professionnelles.

8. Déconnectez vos appareils en cas de comportement anormal, de préférence sans l'éteindre (débranchez le câble réseau, désactivez le Wifi)

Ces conseils ne sont pas exhaustifs mais ils constituent des règles minimales à respecter par tous.

Pour aller plus loin :

- Vous trouverez quelques conseils simples à mettre en œuvre, détaillés pour certains, dans les fiches ci-dessous :

  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.

Cordialement,

MINISTÈRE
DE L'ÉDUCATION
NATIONALE,
DE LA JEUNESSE
ET DES SPORTS
Liberté
Égalité
Fraternité