MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER
*Liberté
Égalité
Fraternité*

Gendarmerie nationale

LA LETTRE CYBER *en région Grand Est*

avril 2023

La thématique du mois
10 mesures pour assurer sa sécurité numérique

La sécurité numérique, c'est quoi ?

La sécurité numérique désigne l'ensemble des stratégies, méthodes, solutions et outils pour protéger la confidentialité, l'intégrité et la disponibilité des données et des ressources numériques.

1 Protégez vos accès avec des mots de passe solides :

Utilisez des mots de passe suffisamment longs et complexes (10 à 12 caractères avec lettres majuscules, minuscules, chiffres et caractères spéciaux) différents sur tous les équipements et les services auxquels vous accédez. Il est souhaitable de les changer tous les 6 mois. Vous pouvez utiliser un coffre-fort de mot de passe (Lockpass par exemple) et activer la double authentification pour renforcer votre sécurité.

2 Sauvegardez vos données régulièrement :

La **sauvegarde** sera souvent le seul moyen de retrouver vos données après une attaque, un piratage ou alors en cas de vol ou de perte de votre appareil. Effectuez cette sauvegarde en double exemplaire, dont un support sera déconnecté du réseau et protégé après la sauvegarde.

3 Appliquez les mises à jour de sécurité sur vos appareils :

Lorsque vous effectuez ces mises à jours proposées par les éditeurs, vous corrigez ainsi les failles de sécurité connues et utilisées par les pirates pour pénétrer dans votre système.

4 Utilisez un antivirus :

Un antivirus vous protégera d'une grande majorité d'attaques et de virus connus. Il existe de nombreuses solutions gratuites ou payantes suivants vos usages et les niveaux de protection recherchés.

5 N'installez que des applications officielles :

Cela limitera les risques d'installation d'une application piégée pour pirater vos équipement. Eviter les sites de téléchargements, streaming illégaux...

6 Méfiez-vous des messages inattendus :

En cas de réception d'un E-mail, SMS ou Chat inattendu ou alarmiste, demandez toujours une confirmation par un autre moyen (connu et légitime)

7 Vérifiez les sites sur lesquels vous faites des achats :

La facilité des achats en lignes offre l'accès à de nombreux sites douteux ou malveillants. Avant de faire un achat, vérifiez que vous n'êtes pas sur une copie frauduleuse d'un site Officiel. Vérifiez la crédibilité de l'offre et les avis des consommateurs.

8 Maîtrisez vos réseaux sociaux :

Les réseaux sociaux sont de formidables outils de communication. Ils contiennent souvent des informations personnelles. Sécurisez l'accès à vos réseaux avec des mots de passe solides et uniques. Définissez les autorisations de publication (publiques ou privées). Ne relayez pas de fake news.

9 Séparez vos usages personnels et professionnels :

Avec l'accroissement des usages numériques, la frontière entre le personnel et le professionnel est souvent délicate. Ces utilisations peuvent parfois s'imbriquer. Séparez vos usages afin que le piratage d'un accès personnel ne puisse pas nuire à votre activité professionnelle.

10 Le nomadisme :

En utilisation nomade de vos outils numériques, privilégiez votre abonnement 4G ou 5G aux réseaux Wifi publics. Ils sont souvent mal sécurisés et peuvent être contrôlés ou usurpés afin de capturer vos informations personnelles ou confidentielles. Si vous n'avez pas d'autre choix, Évitez les opérations sensibles et utilisez un VPN

+ D'INFOS

internet-signalement.gouv.fr
Portail officiel de signalement des contenus illicites de l'Internet

PHAROS
PLATEFORME D'HARMONISATION, D'ANALYSE, DE RECOUPEMENT ET D'ORIENTATION DES SIGNALEMENTS

Région de gendarmerie du Grand Est

LA LETTRE CYBER en région Grand Est

Directeur de la publication : GCA S. OTTAVI
Responsable éditorial : COL A. SCHWEITZER
Rédacteurs : COL A. SCHWEITZER – MDC M. KNOBLOCH
MAJ (ER) WOLFERT

Si vous souhaitez recevoir cette lettre, envoyez un mail à :
arnaud.schweitzer@gendarmerie.interieur.gouv.fr
mathieu.knobloch@gendarmerie.interieur.gouv.fr

Suivez l'actualité de la gendarmerie :