POLICE NATIONALE

CONSEILS CYBER

Sous-direction de la lutte contre la cybercriminalité

SOUS DIRECTION DE LA LUTTE CONTRE LA CYBERCRIMINALITÉ
POLICE NATIONALE

COMMENT PROTÉGER MON IDENTITÉ NUMÉRIQUE ?

Votre **identité numérique** est une extension de ce que vous êtes dans la vie réelle. Prenez-en soin et veillez à garantir une cohérence entre ce que vous êtes dans la vie réelle et sur Internet.

- **Vérifiez**, une fois par trimestre environ, vos **paramètres de confidentialité** sur les différentes plateformes sociales. Vous connaitrez ainsi le type d'informations que vous partagez en mode «public».

- Veillez particulièrement à protéger vos données à caractère personnel et **ne communiquez jamais vos coordonnées bancaires** par exemple.
  Certaines personnes malveillantes pourraient se servir de ces informations pour usurper votre identité et faire des achats sur des sites marchands avec votre compte bancaire.

- La discrétion est de rigueur, faites attention et à **ne pas vous géolocaliser**. En partageant vos données de localisation, vous fournissez également des informations à caractère personnel.

- Faites régulièrement une recherche de contenu sur un moteur de recherche du type Google, Bing, Qwant... avec vos nom et prénom et/ou adresse mail. Vous aurez alors la capacité de **vérifier quels types d'informations sont disponibles sur Internet** vous concernant.

- Utilisez des **mots de passe forts** (10 caractères au minimum, des majuscules, minuscules, chiffres et caractères spéciaux) et pensez à les changer régulièrement.

- Soyez vigilant, **tous les sites que vous consultez sont potentiellement à risque** pour vos données à caractère personnel, particulièrement les réseaux sociaux, les sites de rencontres, sites de jeux en ligne, ... en raison du caractère et du nombre de données demandées lors des inscriptions.

- Gardez à l'esprit que **vous pouvez ne fournir que les informations à caractère obligatoire** (qui comporte en général un *). Le reste est optionnel et donc non necessaire.

COMMENT ME PROTÉGER DES ATTAQUES INFORMATIQUES ?

Aujourd'hui tout appareil connecté peut potentiellement se faire pirater. Gardez à l'esprit que vos tablettes, smartphones, imprimantes ou tv connectés, sont tout aussi vulnérables que vos ordinateurs, et par conséquent doivent aussi faire l'objet d'un suivi accru en terme de sécurité.

- Sécurisez votre usage d'Internet en protégeant votre ordinateur des attaques et en **filtrant les accès non autorisés** et autres menaces.

- Effectuez les **mises à jour logiciels** dès qu'elles sont disponibles et depuis les plateformes officielles.

- Mettez en place un **logiciel anti-virus**, ainsi qu'un **pare-feu**. Soyez vigilants face aux **pièces jointes** que vous recevez par message électronique et prenez le temps d'**analyser** si celles-ci sont légitimes, ou non, **avant de cliquer dessus**. Il en est de même pour les liens que vous recevez par courrier électronique. Posez-vous la question de savoir si l'expéditeur du message est un tiers de confiance et si vous pouvez cliquer sur le lien en toute sécurité.

- Apprenez à **identifier les extensions des fichiers douteux**. Une pièce jointe se terminant par .scr, .cab ou .exe par exemple, à toutes les chances d'être corrompue.

- Pensez à activer **la double authentification** lorsque vous le pouvez. A chaque connection, une vérification sera effectuée sur le numéro de téléphone que vous avez renseigné.

- En déplacement ou en télétravail, installez un **filtre de confidentialité** sur les écrans et prévoyez des mécanismes de protection contre le vol par exemple.

- Attention également à l'utilisation des **Wifi publics**. Prenez le temps d'activer un **VPN (virtual private network)** afin de chiffrer votre connexion et d'empêcher que quelqu'un ne puisse intercepter votre flux d'activité.

ENTREPRISE, VOUS PENSEZ ÊTRE VICTIME D'UNE ATTAQUE INFORMATIQUE

Quels sont les signes d'un **système compromis** ?

- Impossibilité de se connecter à la machine
- Services ouverts non autorisés
- Fichier(s) disparu(s)
- Modifications du coffre-fort de mots de passe
- Système de fichiers endommagé
- Création ou destruction de nouveaux comptes
- Connexions ou activités inhabituelles
- Création de fichiers
- Ralentissement du système.

Dans ce cas, **déconnectez la machine du réseau** mais **maintenez-la sous tension** et ne la redémarrez pas.

Après avoir effectué ces démarches, repartez sur des bases saines :

- Ré-installez le système d'exploitation à partir d'une version saine.
- Supprimez tous les services inutiles.
- Appliquez tous les correctifs de sécurité préconisés.
- Restaurez les données d'après une copie de sauvegarde non compromise.
- Changez tous les mots de passe.

Contactez le service de police ou la brigade de gendarmerie la plus proche de chez vous pour **déposer plainte**.

Le saviez-vous ?

Vous pouvez également consulter le site Internet **www.cybermalveillance.gouv.fr**, dispositif d'assistance aux victimes d'actes de cybermalveillance.