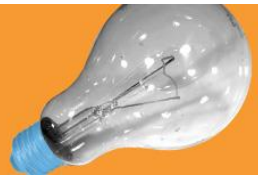
Conseils et astuces



# Prenez de bonnes habitudes avec ces conseils et astuces

## Gardez un système propre

- **Maintenez la sécurité de vos logiciels au goût du jour :** Avoir toujours la dernière version pour votre navigateur web, votre système d'exploitation et les logiciels de sécurité est la meilleure défense contre les virus, les logiciels malveillants et les autres menaces en ligne.
- **Automatisez les mises à jour de logiciels** : De nombreux programmes se connectent automatiquement pour se tenir à jour et se défendre contre des risques connus. Activez la mise à jour automatique si l'option est disponible.
- **Protégez tous les appareils qui se connectent à Internet** : Les ordinateurs, téléphones intelligents, les consoles de jeu, et autres appareils connectés à Internet ont également besoin de protection contre les virus et les logiciels malveillants.
- **Branchez & vérifiez** : Les clés USB et autres périphériques externes peuvent être infectés par des virus et des logiciels malveillants. Utilisez votre logiciel de sécurité pour les vérifier.

## Protégez vos informations personnelles

- **Sécurisez vos comptes** : Demandez une protection allant au-delà des mots de passe. Beaucoup de fournisseurs de compte offrent maintenant des moyens supplémentaires pour vérifier qui vous êtes avant de vous connecter ou d'utiliser un service en ligne.

- **Utilisez des mots de passe longs et complexes** : Combinez majuscules et minuscules avec des chiffres et des symboles pour créer un mot de passe plus sécurisé.

- **Compte unique, mot de passe unique** : des mots de passe différents pour chaque compte permettent de déjouer les cyber-criminels.

- **Conservez-le en sécurité** : Tout le monde peut oublier un mot de passe. Gardez une liste qui est stockée dans un endroit sûr, loin de votre ordinateur, ou dans un logiciel de stockage de mot de passe de confiance.

- **Devenez propriétaire de votre présence en ligne** : Lorsqu'ils sont disponibles, définissez les paramètres de confidentialité et de sécurité sur les sites Internet selon vos préférences, notamment en ce qui concerne le partage de l'information. Il est possible de limiter comment et avec qui vous partagez des informations personnelles et vos publications.

Des conseils supplémentaires sur la gestion des mots de passe sont disponibles sur le site de la CNIL : http://w.cecyf.fr/cnilmdp

## Connectez-vous avec précaution

- **Dans le doute, jetez-le** : Liens dans les courriers électroniques, tweets, et autres messages ou publicité en ligne sont détournés par les cyber-criminels pour compromettre votre ordinateur. Si un message vous semble suspect, même si vous connaissez l'émetteur qui s'affiche sur votre écran, il est préférable de le supprimer ou, le cas échéant, de marquer le message comme indésirable.

- **Soyez attentifs avec les points d'accès Wi-Fi** : Très souvent, la liaison entre votre ordinateur et un point d'accès Wi-Fi en libre-service n'est pas sécurisé. Limitez le type d'activité que vous entreprenez une fois connecté, protégez-vous des accès malveillants à votre machine (pare-feu) et utilisez un réseau privé virtuel (VPN) si votre entreprise ou votre fournisseur d'accès résidentiel le proposent.

- **Protégez votre argent** : Lorsque vous accédez à une banque ou des sites de commerce électronique, vérifiez que la sécurité est activée (utilisation d'une connexion sécurisée par le protocole TLS qui se caractérise par une adresse en https:// ou l'affichage d'un cadenas dans votre navigateur). Ne cliquez pas sur des liens reçus de sources inconnues et saisissez vous-même l'adresse de votre banque ou utilisez l'un de vos favoris.

## Soyez un internaute avisé

- **Tenez-vous au courant** : Restez à niveau sur les nouvelles façons de se protéger en ligne: Visitez régulièrement les sites Web de confiance pour recevoir une information à jour, suivez les comptes de réseaux sociaux et relayez les messages auprès de vos amis, de votre famille et de vos collègues ; encouragez-les à être des internautes avisés !

- **Réfléchissez avant d'agir** : Soyez attentifs dès qu'un message vous incite à agir immédiatement, vous offre quelque chose qui semble trop beau pour être vrai ou encore vous demande des informations à caractère personnel.

- **Faites des sauvegardes** : Protégez vos travaux de valeur, votre musique, vos photographies et toutes vos données numériques en faisant une copie numérique, de préférence sur des supports amovibles, stockés en sécurité

## Soyez aussi un citoyen numérique

- **Ce qui vous rend plus sûr, protège aussi les autres** : Vos comportements en ligne peuvent avoir un impact sur tous - à la maison, au travail et même dans le monde entier. Avoir de bonnes pratiques de sécurité en ligne bénéficie à l'ensemble de la communauté numérique.

- **Publiez sur les autres avec bienveillance, comme vous aimeriez qu'ils parlent de vous en ligne**.

- **Aidez les autorités à lutter contre la cybercriminalité** : Déposez plainte quand vous souffrez d'un préjudice et signalez les contenus illégaux sur les sites officiels et partenaires :

    - Site interministériel pour le signalement de contenus https://www.internet-signalement.gouv.fr
    - ou le portail de signalement de l'Association française des prestataires de l'Internet, http://www.pointdecontact.net/
    - et pour les courriers électroniques non sollicités : https://www.signal-spam.fr/

## Maîtrisez votre présence en ligne

- **Les données personnelles ont de la valeur, protégez-les** : Les informations personnelles qui vous concernent, telles que vos historiques d'achats ou de localisation, ont de la valeur. Soyez attentifs aux personnes à qui vous confiez ces informations et à la façon dont elles sont collectées par les applications et les sites Web.

- **Ayez conscience des informations qui sont partagées** : Configurez les règles de sécurité et de vie privée des services sur lesquels vous êtes inscrits et de vos téléphones ou tablettes. Il est parfaitement légitime de limiter comment et avez qui vous partagez de l'information.

- **Partagez avec précaution** : Réfléchissez avant de publier des informations sur vous-même ou autrui en ligne. Pensez à ce qu'un message peut révéler de personnel, à qui peut y accéder et comment le message pourra être perçu aujourd'hui et demain.