JMD85'info	**Quelques conseils...**	**Android / Windows** *Fiche 2*

1 – Mots de passe

Utilisant de plus en plus d'outils numériques (par choix et/ou par obligation), nous créons régulièrement des comptes avec identifiant/mot de passe et notre liste de codes ne fait que s'agrandir au fil du temps. Il devient alors difficile, voir impossible de les mémoriser tous. Du coup, de nombreux utilisateurs choisissent le même mot de passe pour plusieurs services (parfois le même pour tous), ce qu'il ne faut pas faire.

Vous devez les choisir uniques (c*haque mot de passe ne doit être utilisé qu'une seule fois*) et solides.

Consignes à respecter :

- Varier les mots de passe selon les services et choisissez les assez longs (8 à 12 caractères),
- Eviter les informations personnelles (date de naissance, nom, prénom, code postal...),
- Ne pas utiliser une chaîne séquentielle du clavier comme azerty ni de nombres qui se suivent comme 123456,
- Intégrer des caractères spéciaux, des chiffres, des lettres, en majuscule et en minuscule,
- Ne pas enregistrer vos mots de passe dans le navigateur Internet (Edge, Chrome, Firefox...),
- Supprimer de votre boîte mail les messages de confirmation des comptes que vous venez de créer,
- Changez de mot de passe régulièrement pour les sites sensibles (banque, e-mails).

Conseils pour les construire :

- La méthode de la phrase : Choisir une courte phrase qui sera votre mot de passe, par exemple : «J'aime la Norvège »,
- La méthode phonétique : « J'ai acheté 8 cd pour 100 € cet après-midi » deviendra "ght8CDs%E7am »,
- La méthode des premières lettres de chaque mot d'une phrase : « *Mon mot de passe est un secret bien gardé depuis 25 ans !* » qui donne, par exemple, « Mmdpeusbgd25a! ».

Vous pouvez utiliser :

- L'outil proposé par la Cnil pour générer des mots de passe à la fois solides et faciles à retenir (*https://www.cnil.fr/fr/generer-un-mot-de-passe-solide*).
- Un gestionnaire de mots de passe comme **Bitwarden**.

Vous pouvez tester vos mots de passe :

- Vous pouvez utiliser **Password Checker**, le vérificateur de mot de passe de la société Internxt, entreprise européenne qui propose une solution de stockage en ligne avec une bonne protection des données et de la vie privée.

2 – Smartphone/tablette/ordinateur

Sur votre ordinateur :

- Mettre un **mot de passe au démarrage** de votre ordinateur pour accéder à votre session même si vous êtes le seul utilisateur. Cela créé une première protection pour vos données,
- Installer un **antivirus** pour vous protéger des logiciels espions, malwares, ransomwares... Les pirates utilisent ces programmes pour récupérer sur les ordinateurs toutes sortes de données personnelles (coordonnées bancaires, mots de passe, adresses e-mail...) et les utiliser à des fins malveillantes ou pour prendre le contrôle de l'ordinateur à distance.
  - Windows Defender, intégré à Windows 10 et 11, est un antivirus gratuit et performant.
- **Sauvegarder les fichiers** (documents, photos, vidéos...) stockés sur votre ordinateur sur un disque dur externe ou sur un NAS (disque réseau avec possibilité d'accès depuis l'extérieur). Cela vous permettra de les retrouver en cas de panne de disque dur, de virus... En fonction de ce que vous avez dessus, il peut être important de sauvegarder aussi le contenu de votre smartphone.

Sur votre smartphone (ou tablette), via le système d'exploitation et les applis, Google et Apple collectent un maximum d'informations sur vous. Quelques réglages s'imposent donc pour limiter cette collecte et protéger vos données personnelles :

- Créer un code pour verrouiller votre smartphone,
  - Glissement : ouverture du téléphone par un simple glissement de doigt --> Pas de sécurité
  - Modèle (schéma) : dessin à l'écran joignant plusieurs points --> Sécurité faible à moyenne
  - Code PIN : code à quatre chiffres --> Sécurité moyenne à élevée
  - Mot de passe --> Sécurité moyenne à élevée
  - Empreinte digitale (sur certains smartphone moyen et haut de gamme) --> Sécurité élevé
- Installer des applis à partir du Playstore (Android) ou App Store (iOs),
- Limiter les applis qui ont accès à votre localisation,
- Localiser votre mobile à distance et effacer les données si vous l'avez perdu
  - pour Android : **tutoriel en ligne**
  - pour iOs : Connectez-vous avec vos identifiants Apple puis, avec un navigateur Web, allez sur www.icloud.com. Repérez l'appareil à effacer puis cliquez sur « Effacer l'iPhone ».

3 – Navigation internet / Moteur de recherche / Messagerie

La navigation sur internet devient vite désagréable avec les fenêtres de publicité (pop-up) qui se superposent à la page web. Pour limiter ce problème, vous pouvez installer un bloqueur de pop-up comme **uBlock Origin**. Cette extension existe pour les principaux navigateurs (Edge, Chrome, Firefox...).

Google est le moteur de recherche le plus utilisé au monde. Lorsque nous l'utilisons pour rechercher des informations, nous laissons des traces (*l'historique de recherche en dit long sur nos centres d'intérêt*) et devenons des clients (*les premiers liens qui s'affichent sont souvent des publicités*). On peut laisser Google pour des moteurs de recherche alternatifs qui protègent mieux notre vie privée. C'est le cas de l'américain **DuckDuckGo,** du français **Qwant** ou du Hollandais **Startpage**.

Pour être moins pisté, vous pouvez aussi utiliser la navigation privée. Ce mode de navigation n'enregistre pas votre historique de navigation ainsi que vos mots de passe. Vous pouvez aussi refuser les cookies qui ne sont pas indispensables à la navigation, interdire la géolocalisation, activer l'option « Ne pas me suivre »...

Pour bien gérer vos **méls** (ou mails), il est conseillé de créer plusieurs adresses méls :

- un compte de messagerie pour tous les méls persos et/ou importants (administration, travail, famille, amis...),
- un autre compte de messagerie pour les sites où vous vous inscrivez (jeux, achats...) et les réseaux sociaux (vous pouvez aussi vous créer une messagerie que pour les réseaux sociaux).

4 – Réseaux sociaux

Toutes les informations personnelles, messages, photos publiées sur les réseaux sociaux finissent par vous échapper. Ensuite, il est difficile de faire disparaître un contenu d'Internet.
Quelques Conseils :

- En dire le moins possible sur soi,
- Utiliser un pseudonyme pour cacher son identité,
- Sur Facebook, Twitter, Instagram...vérifier les paramètres de confidentialité de votre compte,
- Ne pas se connecter à des services tiers avec ses identifiants Facebook ou Twitter.

Sur **Cybermalveillance.gouv.fr**,vous trouverez « *10 bonnes pratiques à adopter pour votre sécurité sur les réseaux sociaux* ».

Vous pouvez aussi utiliser des réseaux sociaux plus respectueux de la vie privée comme **Signal** (équivalent de WhatsApp) ou ceux du **Fediverse** comme **Mastodon**, une alternative libre à Twitter, décentralisée et opensource. Pour en savoir plus sur le Fediverse, consultez cet article : *Le Fediverse expliqué : l'avenir des réseaux sociaux sera-t-il décentralisé ?*