www.ordicoupdepouce.fr
ordicoupdepouce@gmx.fr
06 66 97 15 22

FICHE n°4

Au quotidien,

utilisez votre ordi en toute sécurité

Bonjour à toutes et à tous, après le mail sur les arnaques (que vous avez lu bien-sûr !), je continue à vous sensibiliser à la sécurité.
Ne lâchons rien car des problèmes liés à la sécurité informatique arrivent encore trop fréquemment. En tant qu'utilisateur, vous devez y être attentif ! Pour cela, je vais vous donner quelques conseils importants. Pour que cela ne vous paraisse pas trop rébarbatif, je vais essayer d'être synthétique.

Florence, le 19/05/22

Tout d'abord, il faut impérativement que vous soyez en mesure de vérifier la **mise à jour de votre système d'Exploitation Windows**.
Cette mise à jour comporte des évolutions techniques mais aussi des corrections de bugs et de sécurité.
A ce jour, pour un Windows 10 Famille, c'est la version 21H2 19044.1706. Vous voyez cela dans Paramètres/Système/A propos de (tout en bas).
Il en est de même pour **vos logiciels, vous devez accepter leur mise à jour**.

Très important aussi, il vous faut un **anti-virus** (celui intégré à Windows 10 est très bien : ).
Votre anti-virus doit être **impérativement à jour** car chaque jour de nouveaux virus sont créés.

Pour le reste, la sécurité repose sur vos épaules, ne jouez pas les curieux !

- Concernant la Messagerie, si vous avez un doute, vérifiez très précisément l'adresse de messagerie de l'expéditeur et l'adresse des liens inclus dans vos mails (sans cliquer dessus bien-sûr) et n'ouvrez pas les pièces jointes.

- Concernant la navigation Internet, n'allez pas sur n'importe quel site, méfiez-vous ! Si une fenêtre suspicieuse apparait vous proposant tout type de démarches (commerciale, informatique...), éteignez votre ordinateur, tout simplement et ne retournez pas sur le site en question.

Si vous n'êtes pas à l'origine d'une commande, d'une demande quelconque, d'un remboursement, d'un changement d'identifiant ou mot de passe... Ne faites rien, ne suivez pas les instructions, même si cela provient d'un organisme administratif très connu. Ne donner jamais vos informations personnelles que ce soit par mail ou sur internet car elles peuvent ensuite être utiliser à des fins d'usurpation d'identité.

Vous êtes en sécurité lorsque vous êtes connecté à un organisme à l'aide de votre identifiant et mot de passe. Vous êtes alors reconnu en tant que "client" et l'organisme assure la sécurité sur son site. **Encore faut-il avoir des mots de passe suffisamment compliqués**. Il ne faut pas que vos mots de passe soient des mots ou des syllabes de la langue française ou votre prénom et votre date de naissance, il faut impérativement (là-aussi) que ce soit une suite de lettres, chiffres et symboles mélangés. On parle de "phrase de passe", cela permet de retenir ses mots de passe même s'ils sont longs et compliqués.

Pour finir, je vous rappelle l'importance de la sauvegarde de vos données (cf Fiche n°1) car s'il arrive quoique ce soit, vous récupérerez toujours les données sauvegardées.
Prenez aussi le temps de regarder les vidéos-capsules de François Charron (cf Fiche Arnaques), très bien faites, dans lesquelles il expose toutes les pratiques actuelles.

En termes de sécurité, tout ceci est également valable pour vos téléphones et tablettes bien que d'autres notions se rajoutent sur les appareils mobiles : localisation, réseau mobile, partage de connexion, bluetooth, verrouillage, stockage...

Je vous souhaite à toutes et à tous un agréable "début d'été". Je vous retrouve en juillet pour la fiche n°5.
Vous pouvez accéder aux fiches sur https://www.ordicoupdepouce.fr/ **(Rubrique "Conseils") où que vous soyez pendant vos vacances.**
Et merci de transmettre mes coordonnées à vos amis aux 4 coins de la France.