médiaTHEQUE MUNICIPALE de SAINT SYMPHORIEN Jean Vautrin

La sécurité sur Internet

Septembre 2018

La Passerelle Numérique

Publics		Niveau		Prérequis
Jeunes		Débutant		Utiliser Internet et posséder une adresse mail
Adultes	x	Moyen	x	
Tous		Confirmé	x	

Vous venez d'assister à un tour d'horizon des risques que vous êtes susceptibles de rencontrer lors de vos usages d'Internet. Nous vous avons montré comment déjouer les pièges, comment s'en prémunir et comment agir en cas de piratage avéré.
Dans cette fiche vous retrouverez les principaux points abordés, mais aussi des liens, des extensions, etc… pouvant vous aider à conserver un ordinateur sain.

Les bonnes pratiques

1 - Rappels de sécurité de l'ordinateur

Pour la protection de votre ordinateur, il est primordial d'être équipé d'un anti-virus et d'un firewall.
En ce qui concerne les ordinateurs récents (équipés de Windows 10), nous pouvons faire confiance à ceux intégrés au système d'exploitation.
Pour les systèmes plus anciens, ou ceux qui préfèrent, il existe des antivirus gratuits comme *Avast*, *Avira*, *AVG*, par exemple.

Il est aussi nécessaire de faire régulièrement du nettoyage sur le disque dur. Pour cela, il existe des logiciels spécialisés dans l'élimination des malwares, des cookies et autres fichiers indésirables qui prennent de la place et transmettent des informations à notre insu. En voici deux complémentaires, efficaces et gratuits, mais il en existe de nombreux autres : *CCleaner, Malwarbytes*.

2 - Des mots de passe sécuritaires

Utilisez un mot de passe différent pour chaque site… Il doit être long et suffisamment complexe (majuscule, minuscule, chiffre, caractères spéciaux… Impossible à deviner (ne jamais utiliser sa date de naissance, le prénom de vos enfants, le nom de votre animal de compagnie…)...Ne jamais communiquer votre mot de passe...N'enregistrez jamais vos mots de passe sur un ordinateur public et pensez à déconnecter vos sessions avant de partir… Si possible, utilisez un gestionnaire de mots de passe comme *Bitwarden, Keepass ou Lastpass.*

3 - Les sites marchands

Il est tout à fait possible de faire des achats sur Internet, sans mettre son compte bancaire et ses données personnelles en danger, tout au moins, pas plus qu'au distributeur de votre quartier.
Privilégiez toujours les sites connus, les magasins ayant pignon sur rue… Faites bien attention, au moment de la transaction, que le site soit sécurisé (**HTTPS**), surtout n'inscrivez jamais le numéro de votre Carte Bleue sur un site non sécurisé (HTTP).
Si toutefois, vous n'avez pas confiance, adresser-vous à votre établissement bancaire, qui peut vous faire bénéficier d'un service de Carte Bleue Virtuelle (un numéro généré par transaction...Donc impiratable).

4 - Les réseaux sociaux

Si possible utilisez la connexion par « double authentification »… Protégez vos publications en ciblant le public autorisé à les lire… Ne publier aucune information en mode public qui pourrait donner des indications sur vos absences de votre domicile… La liberté de parole ne donne pas le droit de tout dire et tout publier.

5 - Les mails

Pensez à vérifier l'adresse de l'expéditeur et celle du destinataire… Avant de cliquer sur un lien douteux, positionnez le curseur de votre souris sur ce lien (sans cliquer)… Ne communiquez jamais d'informations sensibles par messagerie ou téléphone (comme votre numéro de Carte Bleue)… Avant de transférer une alerte reçue par mail, vérifiez-en la véracité… Après avoir cliqué sur un lien, vérifiez l'adresse du site qui s'affiche dans votre navigateur… Si possible, utilisez des adresses mails différentes en fonction des destinataires (sites marchand, famille et amis, professionnelle…)

Que faire en cas de piratage

1 - En cas de virus, trojan, keylogger etc.

Faites des analyses avec votre antivirus, vos nettoyeurs de traces (CCleaner, Malwarebytes)… Eventuellement, faites appel à un professionnel afin de supprimer toutes les traces et tous les risques liés à cette attaque virale.

2 - Dans le cas d'un piratage de compte Internet

Changez immédiatement le mot de passe du site… Si vous avez été victime d'un « Keylogger », ce sont tous vos mots de passe de tous vos comptes qu'il faut changer… Penser à utiliser des mots de passe forts et différents sur chaque site… Il est peut-être temps de confier vos mots de passe à un logiciel dit coffre fort, plutôt qu'à Google...

3 - Dans le cas d'un piratage de comptes bancaire

Si les codes de votre Carte Bleue ont été volés, lors d'une transaction sur Internet par exemple, contactez immédiatement votre établissement bancaire. Ils vous expliqueront la procédure. En général, toutes les transactions faites à votre insu vous sont indemnisées.

4 - En cas de piratage d'un compte de réseaux sociaux

Changez le mot de passe… Utilisez la connexion par « double authentification »… Prévenez tous vos contacts sur ce réseau, car ils peuvent avoir reçu de votre part des messages bizarres...

5 - En cas de piratage d'adresse mail

Changez votre mot de passe, et éventuellement les mots de passe qui pourraient avoir été devinés par le pirate, à cause des mails que vous stockez dans votre boite mail… Voici un lien (https://assistance.orange.fr/ordinateurs-peripheriques/depanner/probleme-de-mail/probleme-pour-acceder-a-la-messagerie/messagerie-orange-suspicion-de-piratage-de-compte-mail_222914-765559#onglet1)

donnant toute la procédure à suivre pour récupérer votre adresse mail… Il est peut-être temps de vous créer des adresses mail différentes en fonction des utilisations...

Extensions de navigateur ou sites Internet pouvant vous aider

- **Signal Spam,** pour signaler les spams et autres pourriels (existe en site Internet et en extension)
- **Decodex,** extension permettant de classer les sites d'informations (code couleur)
- **Adblock,** extension pour stopper la publicité ciblée
- **Ghostery,** extension bloquant les mouchards, publicités et tracers
- **Avast online sécurité,** extension permettant de vérifier la réputation du site internet où vous naviguez
- Possibilité « **d'ouvrir une cession de navigation privée** » au sein de votre navigateur, afin de ne laisser qu'un minimum de traces
- **Hoaxkiller,** site internet permettant de savoir si le contenu du mail est une fausse information

A regarder ou à lire (pour aller plus loin)

- Vidéo Youtube, les bons conseils à ne suivre sous aucun prétexte, mais dit par Micode, s'est tout de suite plus limpide : https://www.youtube.com/watch?v=I5jZWXbFP5c&feature=youtu.be

- 4 vidéos pour expliquer comment et pourquoi les pirates agissent : https://www.hack-academy.fr/home

- Kit de sensibilisation de Cybermalveillance.gouv, à télécharger pour bien garder en mémoire :

https://www.cybermalveillance.gouv.fr/contenus-de-sensibilisation/

- Des vidéos en tout genre sur l'utilisation de votre ordinateur : https://www.youtube.com/channel/UCOfQqFN7BOWSjjqj9h-YUHA