Le guide de SurVie sur Internet

Utiliser Internet de façon sécurisée dans le monde contemporain

Cyberini

Michel Kartner

Le Guide de Survie sur Internet

Utiliser Internet de façon sécurisée dans le monde contemporain

Issu du site web Cyberini.com

E-mail :admin@cyberini.com

Table des matières

Introduction

Internet est devenu très rapidement un outil indispensable dans notre quotidien. Plus de la moitié de la population mondiale est connectée à Internet. En France, le taux de pénétration d'Internet est de **90%** (en augmentation chaque année).

Internet est également accessible depuis de plus en plus de périphériques : 93% des Français ont un mobile, 71% un smartphone, 81% un ordinateur et 41% une tablette*.

Ce monde connecté à tous instants depuis tous les périphériques a créé proportionnellement plus de problèmes de sécurité :

- 91% des sondés estiment que la **sécurité et la protection des données sont très importantes**.
- 42% suppriment les cookies du navigateur pour **protéger leur vie privée**.
- 36% utilisent un outil de blocage de publicités.

* : Source *Hootsuite We are social*.

Internet va trop vite, du moins plus vite qu'on ne l'imagine. Chaque mois, chaque jour, chaque minute, des quantités astronomiques de données sont traitées, analysées, scrutées. Durant la même période, de nouvelles **menaces** voient le jour, de nouveaux **piratages** se produisent et touchent **tout le monde**. Personne n'est à l'abri, ni les entreprises, ni les particuliers. Internet ne peut pas simplement pas être considéré comme un endroit sûr et sans risques.

Mais alors comment profiter de ce formidable outil en évitant les dangers ? Et après tout, est-ce vraiment possible ?

Ce guide de survie à destination des particuliers désireux d'apprendre comment mieux se protéger en ligne vise à fournir des pistes à ces questions, en démêlant le vrai du faux et en assistant le lecteur de façon pédagogique et pragmatique.

Nous verrons ensemble, point par point, les grandes lignes de conduite à suivre, les bons outils à installer, et comment faire pour « survivre sur Internet ».

Excellente lecture.

Michel de *Cyberini*.

1 Les fondamentaux

Dans cette première partie, le but est de mettre à plat les fondamentaux de la sécurité sur Internet en partant des outils et périphériques utilisés pour s'y connecter.

Internet n'est accessible qu'à partir d'un *équipement connecté*. Cela signifie que l'équipement doit être doté d'un moyen d'interagir avec d'autres ordinateurs à travers le réseau. Les ordinateurs sont naturellement connectés au réseau à travers une **box Internet**, mais une connexion réseau physique par câble n'est pas obligatoire. En effet, la technologie sans-fil Wi-Fi permet à des équipements plus « portable » de communiquer eux aussi sur Internet. Les smartphones, mais aussi les montres connectées et tous les autres objets dotés d'un moyen de communication sans-fil sont également connectés ou connectables à Internet.

De ce fait, les réseaux 3G, 4G ou même 5G des téléphones mobiles peuvent aussi être utilisés pour se connecter au réseau Internet.

Dans la plupart des cas, chacun des équipements cités est autorisé à accéder au réseau qu'à partir du moment où un abonnement à un service a été contracté.

Du point de vue des cybermenaces, cela signifie que tous les périphériques connectés sont susceptibles de faire face à des dangers. Et à ce propos, **même les périphériques non connectés peuvent être malmenés**, notamment avec l'insertion manuelle de clés USB contenant des programmes malveillants.

Seulement, les menaces ne s'adaptent pas toutes automatiquement au périphérique utilisé. Cela signifie qu'un « virus » visant un système *Windows*, ne fonctionnera pas (ou pas toujours) sur un système *Mac* ni même sur un smartphone ou une montre connectée. Cela vient du fait que les « virus » sont des programmes informatiques créés par des individus malveillants pour un ou des systèmes spécifiques.

Le système quel qu'il soit, n'est pas capable de différencier un programme malveillant d'un programme sain, car tout ce qu'il sait faire est justement d'exécuter ce que le programme lui demande. Si le programme lui demande de supprimer tous les fichiers, il le fait. Et dire à *Windows* de supprimer des fichiers ne se fait pas forcément de la même manière que de le dire à *Mac* ou à un autre objet connecté. Les langages de programmation sont en ce sens semblables aux langues parlées. Il faut que l'émetteur et le récepteur se

comprennent.

Avec les langues internationales comme l'anglais, on arrive parfois à se comprendre entre individus d'origines différentes. Cela fonctionne de la même manière en informatique. Certains langages de programmation peuvent être compris par différents systèmes/équipements. On les appelle des langages « portables ».

1.1 Points importants à retenir

- Il faut souvent un équipement **connecté à Internet** pour risquer d'attraper un « virus » (mais l'accès physique n'est pas à négliger pour autant).
- Les programmes malveillants ne sont qu'une suite d'instructions que le système exécute mécaniquement sans se soucier des conséquences.
- Les programmes malveillants visent **tous les systèmes**, et parfois plusieurs systèmes différents en même temps.

2 Sécuriser ses adresses e-mail

Ce point est **très important**.

L'adresse e-mail, c'est comme un portefeuille. Elle contient beaucoup de données sensibles dont personne n'a intérêt à toucher sans autorisation. En effet, avez-vous déjà envoyé votre CV par e-mail ? Avez-vous reçu un contrat d'assurance ? Qu'en est-il avec vos messages professionnels ? L'adresse e-mail contient toutes ces données confidentielles **en un seul endroit**.

Pire encore, **elle permet de trouver bien d'autres informations confidentielles** via la « cascade d'informations ». C'est-à-dire qu'une donnée permet potentiellement d'en trouver plusieurs autres, qui elles-mêmes permettent d'en trouver d'autres et ainsi de suite.

L'adresse e-mail est d'autant plus importante qu'elle est connectée (et permet même de donner l'accès) **à tous vos autres comptes** sur lesquels vous êtes inscrit(e).

Il ne faut absolument plus voir l'adresse e-mail comme une donnée permettant d'écrire de simples mails mais bien comme un portefeuille contenant votre identité numérique.

De ce fait, il y a plusieurs points importants à comprendre pour sécuriser nos adresses e-mail.

Tout d'abord, il convient de **bien séparer les e-mails par activités** : une adresse pour l'activité professionnelle, une adresse pour les amis, une autre pour les paiements en ligne, etc.

Ensuite, il convient d'activer un maximum de précautions pour **empêcher le piratage** de chaque adresse : mécanisme d'authentification en deux étapes (demandant une autorisation supplémentaire en cas de connexion valide), question de secours (avec réponse non évidente pour autrui, etc…). Ces précautions doivent être mises en place via votre compte directement. Les procédures varient donc selon les prestataires, mais voici comment faire avec gmail et comment faire avec outlook.

Il convient également d'activer (et d'observer régulièrement) l'historique de connexion. Voici comment faire avec gmail et voici comment faire avec outlook.

Enfin, il convient de garder en tête les bonnes pratiques pour éviter de se faire avoir :

- Faire attention à l'hameçonnage par e-mail.
- Faire attention aux pièces jointes douteuses.

- Faire attention au lien sur lequel on clique (observer l'adresse dans le navigateur et/ou au passage du curseur dessus).
- Faire attention à son mot de passe (voir plus loin dans le guide)

2.1 Points importants à retenir

- L'adresse e-mail **contient beaucoup de données personnelles**.
- Il convient de créer **plusieurs adresses e-mail différentes** (une par activité/domaine), avec des mots de passe différents.
- Il convient de mettre en place **un maximum de sécurité** technique autour des adresses e-mail, mais aussi de toujours **rester vigilant(e)**.

3 Comment protéger son réseau

Le système et le réseau fonctionnent ensemble en permanence. Cela permet non seulement la connexion initiale à Internet mais en plus de faire les mises à jour, de télécharger des fichiers et programmes, et de naviguer sur le web.

Sans connexion réseau il n'y a pas d'accès à Internet. Et sans accès à Internet il n'y a pas de communications avec l'extérieur. Mais justement, il faut se connecter au réseau pour profiter d'Internet.

Techniquement parlant, les ondes radio (Wi-Fi), les signaux lumineux (fibre) ou analogique/numérique (ADSL) permettent de faire transiter des données de systèmes en systèmes à travers le monde entier. Et parmi ces données, nous retrouvons évidemment nos logiciels malveillants !

Suivant la façon dont sont transmises les données, elles arrivent habituellement sur un système par une porte d'entrée spécifique que l'on appelle techniquement un « **port réseau** ». Les ports réseau sont donc les points d'entrée depuis l'extérieur, comme une porte d'une maison qui permet à des individus d'entrer. Chaque port à un numéro spécifique (de 1 à 65535), et cela permet de

proposer différents services. Un peu comme dans un hôtel, où il y a une porte pour chaque chambre, et même une porte pour le local vélo, une porte pour le bureau de l'agent de sécurité etc…

En tant qu'utilisateur du système, vous n'avez pas à vous soucier de cela. C'est l'affaire des systèmes (et des programmeurs). Mais concernant les programmes malveillants, cela signifie qu'il faut surveiller ces ports pour détecter des intrus. Ce rôle est donné au **pare-feu**. Il est souvent **intégré de base avec le système d'exploitation** et ne nécessite pas d'installation additionnelle, mais plutôt des mises à jour constantes et une bonne configuration.

Le réseau dans son sens le plus large représente une interconnexion d'ordinateurs à travers le monde. Mais concrètement, ce sont plusieurs sous-réseaux qui communiquent entre eux. Le sous-réseau que vous utilisez probablement actuellement est aussi appelé le « **réseau local** » dont votre box Internet est le point central.

Tous vos équipements informatiques sont connectés à la même box à travers un câble ou avec le réseau sans-fil Wi-Fi.

Note : pour ne pas compliquer les explications, on va considérer que le flux des données entre Internet et vos équipements est direct. Mais techniquement, c'est la box Internet qui reçoit d'abord les données et qui les redirige vers l'équipement concerné.

Au sein même du réseau local, les ordinateurs lui appartenant peuvent non seulement communiquer entre eux mais aussi lire/écouter des informations qui ne les concernent pas forcément (un peu comme une discussion entre plusieurs personnes dans une même pièce). Et si un espion se trouve dans la discussion, il peut causer des gros problèmes.

Avec un réseau tout câblé, il « suffit » de savoir quels ordinateurs sont branchés et de faire confiance aux personnes qui les utilisent. Mais avec le réseau sans fil, c'est plus complexe car n'importe qui se trouvant suffisamment proche du point d'accès (de la box Internet) peut s'y connecter et rejoindre le réseau local. C'est pour cela que le réseau local est protégé par **un mot de passe Wi-Fi**.

Si ce mot de passe est compromis et trouvé par un pirate, il peut se faufiler dans le réseau local et potentiellement « écouter le trafic ».

Le réseau doit donc être protégé à la fois contre les menaces extérieures (blocages de ports et pare-feu) et à la fois contre les menaces intérieures (mot de passe Wi-Fi et autres mesures de protection techniques).

3.1 Points importants à retenir

- N'importe quelle donnée (dont des **programmes malveillants**) peut arriver dans notre ordinateur depuis n'importe où dans le monde, via Internet.
- Le pare-feu permet d'éviter des intrusions externes vers des ports réseau spécifiques du système.
- Le mot de passe du réseau sans fil local est très précieux pour éviter des intrusions dans le réseau local.

4 Créer de bons mots de passe

Le mot de passe est le point central de la sécurité sur Internet. Il s'agit de la clé de la maison ou de la clé de la voiture qu'il ne faut pas perdre ni donner à qui que ce soit sans connaissance de cause.

Le mot de passe est même plus précieux (ou plus sensible devrais-je dire) que la clé de la maison. La maison possède un gros avantage qui la rend bien plus sécurisée qu'un ordinateur : elle n'est pas accessible depuis le monde entier en une seconde. Votre ordinateur, vos comptes, et de manière générale tout ce qui est lié à Internet est techniquement **accessible depuis n'importe où dans le monde**.

Pour bien comprendre l'ampleur du problème, il faut savoir que le mot de passe d'un compte (e-mail par exemple) ouvre la porte à beaucoup de données personnelles. Nous en avons parlé précédemment : avez-vous déjà reçu un contrat d'assurance par e-mail ? avez-vous envoyé des e-mails à des proches, des collègues, voire à votre patron ? Eh bien ces données sont ainsi accessibles **en une seconde par n'importe qui dans le monde** si votre mot de passe est faillible.

Un mot de passe faillible est un mot de passe découvert par une tierce personne. Et il existe plusieurs façons de le découvrir :

- Soit en le **devinant** tout simplement
- Soit en le **dérobant** (via un logiciel malveillant installé au préalable)
- Soit en le **récupérant** (suite à un piratage d'un site contenant vos informations de compte par exemple)
- Soit en **passant outre** (en permettant d'accéder au compte sans avoir à le fournir)
- Sans compter que la **perte** du mot de passe peut condamner l'accès à vos données personnelles dans le cas où vous ne pouvez pas récupérer votre compte.

S'en suivent des dommages collatéraux potentiels : avec les données du compte, d'autres comptes peuvent être récupérés (la fameuse cascade d'informations).

Pour rendre nos mots de passe robustes, il y a cependant un problème : **notre mémoire**…

Pour lutter contre les diverses façons de découvrir un mot

de passe, il faut en effet qu'il soit d'abord difficile à deviner. Cela implique qu'il doit être le plus unique possible, et le plus compliqué possible, sans pour autant être impossible à retenir. De ce fait, plusieurs moyens mnémotechniques ont été inventés, comme la création d'une phrase qui nous dit quelque chose, puis en prenant chaque première lettre de chaque mot (et en incluant la ponctuation).

Les mots de passe doivent également être différents pour chaque compte (et surtout pour les comptes sensibles comme les comptes e-mail, les comptes bancaires, les comptes sur les réseaux sociaux, etc..). Cela permet de lutter contre diverses récupérations de mots de passe.

Enfin, il est essentiel de bien gérer les sauvegardes et nos données personnelles de façon à se préparer à faire face à un piratage, plutôt que d'espérer qu'il ne se produise jamais.

4.1 Points importants à retenir

- Les mots de passe sont **le point central** de la sécurité sur Internet.
- Les mots de passe donnent accès à énormément d'informations personnelles, à n'importe qui dans le monde, en très peu de temps.
- Les bonnes pratiques doivent complémenter les bons mots de passe.

5 Chiffrer et sauvegarder les données

Chiffrer et sauvegarder les données sont deux points qui se complètent et qui prennent le problème dans le sens inverse de la démarche *classique* (éviter les menaces) : il s'agit de se **préparer au pire** au lieu d'essayer de l'éviter. Autrement dit, « mieux vaut prévenir que guérir ».

Le chiffrement des données permet d'éviter que des tiers non autorisés y aient accès. Et cela que ce soit pour sauvegarder des données dans le Cloud ou sur une clé USB par exemple. Des outils existent comme VeraCrypt ou Bitlocker permettant d'automatiser et/ou de faciliter le chiffrement des données.

Les sauvegardes peuvent elles aussi être automatisées à l'aide de divers outils. Mais pour que les sauvegardes soient vraiment sûres, il faudrait qu'elles soient non seulement **répliquées sur différents périphériques**, mais aussi **chiffrées** pour éviter leur lecture par un tiers non autorisé.

Je vous recommande donc de cumuler chiffrement et sauvegardes, notamment à l'aide de l'outil BoxCryptor.

5.1 Points importants à retenir

- Chiffrer des données, c'est garantir que seules les personnes autorisées à lire le contenu peuvent les déchiffrer.
- Sauvegarder les données permet de les récupérer facilement en cas de piratage, de perte ou de suppression.
- Chiffrer et sauvegarder les données en même temps est tout à fait possible, et **recommandé**.

6 L'historique de navigation

Le navigateur web enregistre un historique de navigation pour permettre à l'internaute de retrouver facilement les liens visités.

Cela peut évidemment poser problème lors de la visite de certains sites indésirables ou qui ne regardent personne d'autre.

Heureusement, la plupart des navigateurs web permettent d'entrer dans un mode dit « de navigation privée ». Pour ce faire, vous pouvez appuyer sur les touches suivantes sous *Mozilla Firefox* :

`CTRL + MAJ + P` (ou `POMME + MAJ + P` sous *Mac*)

Sous *Google Chrome*, c'est presque le même raccourci clavier :

`CTRL + MAJ + N` (ou `POMME + MAJ + N` sous *Mac*)

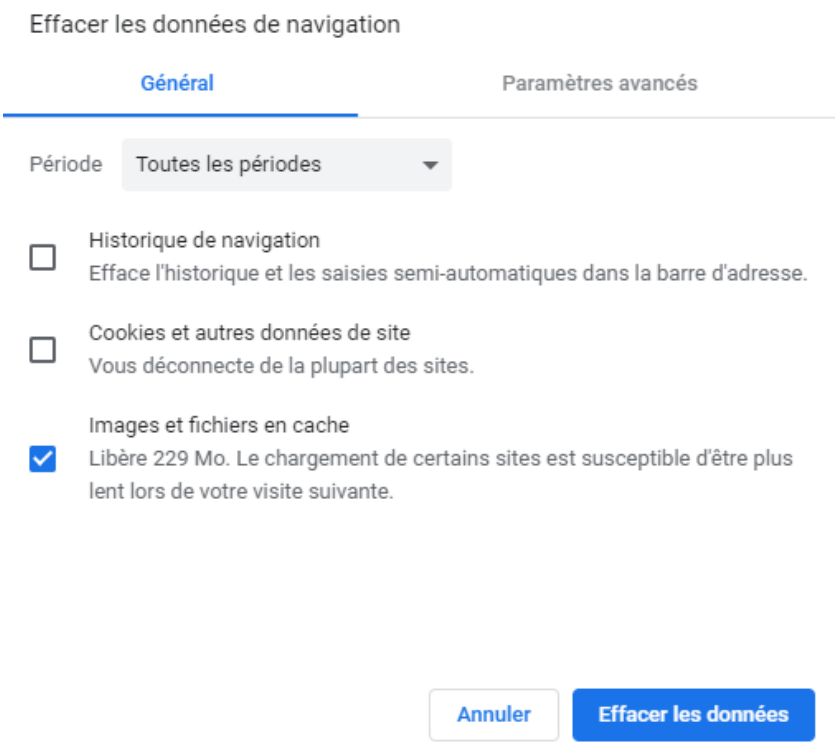
Vous pouvez également supprimer votre ancien historique (et vos traces de manière générale) via le navigateur. Pour entrer dans les options de suppressions sous Firefox, vous pouvez directement entrer le texte suivant dans la barre d'adresse :

`about:preferences#privacy`

Vous y trouverez ensuite le bouton « Effacer les données… » avec la fenêtre de suppression :

Sous Chrome, même principe, en tapant dans la barre d'adresse le texte suivant :

`chrome://settings/clearBrowserData`



6.1 Points importants à retenir

- Le mode de navigation privée permet de surfer sur Internet sans garder l'historique (et sans pistage).
- Il est possible de nettoyer les traces du passé via le navigateur (cookies, cache et historique).
- Mais cela ne supprime aucunement les données envoyées sur des sites web. On va en parler.

7 Le point sur les cookies

Les cookies sont des petits fichiers qui enregistrent localement (sur l'ordinateur) des petites informations concernant votre visite sur les sites web.

Par exemple, ils peuvent retenir vos articles dans votre panier sur un site commerçant. Ils peuvent également retenir votre pseudonyme ou votre « session » pour rendre votre navigation plus ergonomique.

Ils peuvent aussi **servir à vous pister**, par exemple lorsqu'un site donné (disons *Google*) stocke des cookies au sujet de vos pages visitées afin de pouvoir ensuite vous afficher de la publicité ciblée. Techniquement, cela fonctionnerait uniquement si vous visitez le site *Google*. Cela dit, nombreux sont les webmasters qui ajoutent volontairement des scripts de *Google* dans leurs pages web. Le but est légitime (quoique parfois controversé) : ajouter de la publicité pour être rémunéré ou obtenir des statistiques d'audience. Et le fait de retrouver les scripts de *Google* dans énormément de pages web lui donne un certain avantage et surtout beaucoup de données à brasser.

La « loi cookies » et le « RGPD » permettent de redonner le pouvoir aux internautes, mais vous pouvez aussi lutter

techniquement contre l'utilisation intempestive des cookies, notamment en utilisant des fenêtres de navigation en mode privé.

Plus d'informations sur le fonctionnement des Cookies et comment le supprimer.

7.1 Points importants à retenir

- Les fichiers cookies ne sont pas initialement utilisés pour pister les internautes.
- Les cookies « tiers », c'est-à-dire intégré dans d'autres sites permettent de pister les internautes.
- La suppression des cookies est facile via le navigateur, et le mode de navigation privée permet d'éviter leur utilisation au-delà de la session courante.

8 La protection contre les publicités

Nous allons intégrer dans cette partie les publicités et les traçages.

La publicité sur Internet amène un débat de taille : faut-il un web **sans publicités** (au risque de se retrouver avec un web payant), ou faut-il **autoriser** les publicités et prendre le risque d'être pisté et de voir nos données personnelles exploitées ?

Le web sans publicités est difficile à concevoir car il existe dorénavant des « bloqueurs de bloqueurs de publicités ». C'est-à-dire des outils forçant la désactivation d'un bloqueur de publicités pour afficher le contenu des pages web.

Mais il est aussi difficile de concevoir un web où l'on ne contrôle plus nos données. Et les publicités ne sont pas toutes bienveillantes. Certaines se servent de la crédulité des internautes pour tenter de les pirater.

Par défaut, il est recommandé d'installer un bloqueur de publicité comme Adblock Plus. Des extensions de navigateurs comme Disconnect.me et Privacy Badger existent également pour renforcer la lutte contre le pistage.

Vous pouvez faire le test en ligne pour observer avant/après ce que les sites web peuvent savoir de vous ici : Ce que l'on sait sur vous.

8.1 Points importants à retenir

- La publicité n'est pas toujours malveillante, mais son lien avec le pistage de données et ses côtés malicieux la rende plutôt nuisible.
- Des bloqueurs de bloqueurs de publicités existent vous demandant de désactiver votre bloqueur de publicités.
- Des extensions antipublicités peuvent vous aider à éviter des désagréments liés aux publicités.

9 L'anonymat sur Internet

Sujet à la mode et indispensable lorsqu'on parle de sécurité et de données personnelles sur Internet, l'anonymat est important à comprendre.

L'anonymat est un sujet transversal à tous les autres points qui permet de protéger nos données et notre activité en ligne.

Mais est-il vraiment nécessaire ?

La réponse dépend de chacun. Ou plus concrètement, elle dépend des activités de chacun. Dire que l'on n'a rien à cacher c'est comme laisser une caméra de surveillance dans sa chambre sous prétexte qu'on ne fait rien de mal et que personne ne s'intéressera aux vidéos filmées.

Le problème, c'est que bien des menaces **dont nous n'avons pas conscience existent**. L'anonymat est donc premièrement un moyen de protection **proactif**. Est-ce qu'une donnée à un moment « t » ne sera pas très utile à un pirate à un moment « t+1 » ?

L'anonymat permet également de contourner divers blocages injustifiés comme la **censure**. L'anonymat peut aussi être nécessaire à certaines activités qui relèvent du

secret professionnel. Mais plus simplement, l'anonymat peut permettre au particulier qui n'a pourtant « rien à se cacher » de se sentir **plus serein sur Internet**.

Seulement, il y a « anonymat » et « anonymat ». Être anonyme sur Internet envers quoi ou qui ? Ce concept d'anonymat relatif est important à saisir. Par exemple, si vous visitez un site web à l'aide d'un outil VPN, celui-ci n'aura pas conscience de votre véritable adresse IP. Mais un logiciel espion enregistrera toutes vos frappes au clavier en attendant !

Il existe plusieurs façons d'anonymiser sa connexion, entre les serveurs proxy, les logiciels VPN et le réseau Tor. Toutes ces façons ne se valent pas, je vous recommande de lire l'article complet à ce sujet : Comment devenir anonyme sur Internet.

9.1 Points importants à retenir

- L'anonymat n'est pas utile uniquement si l'on estime avoir « rien à cacher ».
- L'anonymat est « relatif » : il dépend de plusieurs facteurs et on devient plutôt anonyme envers un site ou une personne donné(e).
- Il existe plusieurs façons de devenir anonyme, mais les logiciels VPN sont recommandés.

10 Se protéger sur les réseaux sociaux

Depuis plusieurs années déjà, les réseaux sociaux ont totalement changé le paysage d'Internet. Ils ont bien entendu permis de retrouver des proches, ils ont changé notre mode de communication en ligne, ils ont permis à chacun de pouvoir s'exprimer librement, etc…

Mais ils ont aussi créé des problèmes. Et surtout des problèmes de vie privée. Voici donc certains conseils à mettre en place sur les réseaux sociaux :

- N'utilisez pas votre vrai nom si vous n'en avez pas envie. Certes Facebook impose un véritable nom, mais vous pouvez changer le prénom ou le nom de famille si vous désirez garder un minimum d'anonymat.
- Faites bien attention à ce que vous publiez. Tout d'abord en vérifiant la confidentialité associée aux publications, mais tout particulièrement en vous demandant toujours si vous afficheriez dans la rue ce que vous écrivez (et cela indépendamment du niveau de confidentialité choisi).
- Protégez bien votre compte (en choisissant un bon

mot de passe) et en évitant de donner des pistes aux pirates. Vous pouvez également activer l'authentification à double facteur et la mise en place des alertes de connexion.

- Attention à toutes les rumeurs, fake news et autres contacts piratés qui pourraient vous amener à cliquer ici et là et à télécharger un programme malveillant.

Voir d'autres conseils et comment les mettre concrètement en place.

10.1 Points importants à retenir

- Les réseaux sociaux ont apporté beaucoup de points positifs, mais posent désormais des problèmes de vie privée.
- Mieux vaut ne pas publier du tout quelque chose de sensible.
- Rester attentif(ve) en permanence pour ne pas tomber dans les pièges.

11 Y a-t-il un système plus sécurisé qu'un autre ?

Au-delà d'Internet, la sécurité informatique repose aussi sur le système et sur un ensemble de domaines (techniques ou non à protéger).

Le système, que l'on devrait appeler le « système d'exploitation » est un ensemble de programmes informatiques qui ont pour charge de faire le pont entre l'utilisateur et la machine. Les programmes permettent notamment de gérer l'ajout de périphériques tels qu'une souris ou un clavier. Ils permettent également de gérer plusieurs mécanismes indispensables à la bonne exécution des diverses fonctions de l'ordinateur. Et ils permettent aussi à d'autres programmes de s'exécuter correctement. Ce point est très important. C'est celui qui permet par exemple l'installation d'un navigateur web pour visiter des pages web ou l'installation d'un jeu vidéo.

Mais c'est aussi cela qui permet la création de n'importe quel programme arbitraire dont les **programmes malveillants**.

Le fait d'attraper un virus n'est donc pas une maladie système ou un programme anormal qui se serait faufilé « magiquement » dans l'ordinateur, mais plutôt un programme comme n'importe quelle autre, dont l'action est plutôt de **détruire** ou de **voler**, que d'apporter des fonctionnalités utiles.

Et ceci permet de laisser libre cours à l'imagination des pirates :

- Un programme pour cacher un autre programme malveillant (cheval de troie)
- Un programme pour chiffrer tous les fichiers de l'ordinateur (rançongiciel)
- Un programme pour récupérer et envoyer à distance les touches tapées au clavier (keylogger)
- Un programme pour afficher de la publicité (adware)
- Etc.

Le rôle de l'antivirus, qui lui aussi est un programme informatique, est de détecter ces actions suspectes et d'éviter qu'elles se produisent (c'est le fameux lancement de l'alerte antivirus qui vous informe d'un souci).

Le système est donc la base, le « bac à sable », permettant toutes sortes de créations, même les plus machiavéliques.

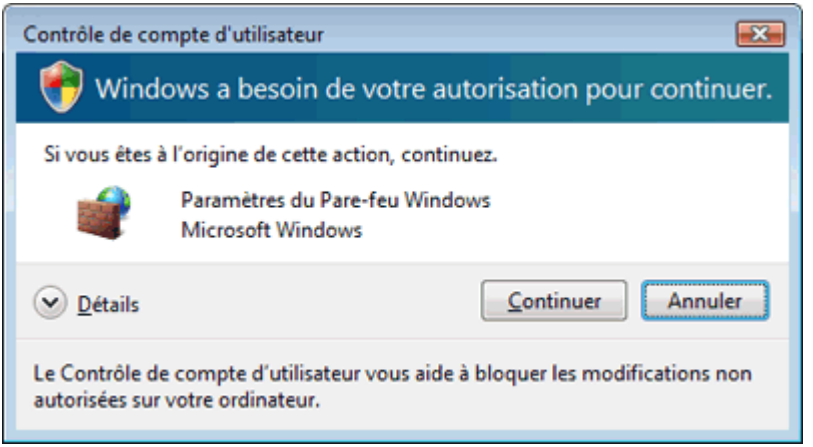
Alors y a-t-il un système immunisé ? Y a-t-il un système plus sûr ?

La réponse est théoriquement **non**. À partir du moment où le système se présente comme un « bac à sable » autorisant diverses créations, les programmes malveillants peuvent exister.

Cela dit, il existe quelques exceptions faisant pencher la balance :

- Si un système est **plus sécurisé**.
- Si un système est **moins ciblé**.

Dans le premier cas, on peut par exemple imaginer que le système demande à l'utilisateur une confirmation explicite pour certaines actions risquées. C'est le fameux message qui demande des autorisations d'administrateur.



Dans le deuxième cas, on peut noter la différence entre les systèmes d'exploitation *Windows*, *Mac*, *Linux* et mêmes mobiles. Par défaut, la plupart des internautes ont un ordinateur avec *Windows*. Le profil type de l'internaute de nos jours utilise *Windows*. De cette façon, les menaces visent en priorité *Windows*.

Mac, *Linux* et d'autres systèmes moins connus gagnent donc en sécurité par le fait que la menace type contre l'internaute type ne vise pas ces systèmes.

Mais cela ne suffit pas pour pouvoir affirmer qu'un système est vraiment plus sûr qu'un autre. Déjà par le fait que le système n'est pas la seule variable : l'être humain compte pour beaucoup. Et également par le fait que l'internaute type peut changer et attirer les menaces vers un nouveau

système.

De façon générale, un système sécurisé est un système à jour, dont l'internaute exploite pleinement les possibilités de sécurisation offertes (séparation entre comptes, bonnes pratiques, etc.). Les internautes les moins sensibilisés ont tout intérêt à choisir un système moins ciblé comme *Mac* ou *Linux*. Mais il faut bien comprendre que les menaces sont souvent **indépendantes du système** (lorsqu'elles passent par exemple par un site web ou par un e-mail).

11.1 Points importants à retenir

- Le système rend possible la création de **n'importe quel programme** dont les virus informatiques.
- Les menaces visent naturellement **les systèmes les plus populaires.**
- Un système peut être mieux protégé par des **bonnes pratiques intégrées** (compte administrateur pour les opérations risquées, mises à jour, etc.).

12 Le meilleur conseil à donner

Tout ce que vous avons vu dans ce guide n'est qu'une infime partie de la sécurité sur Internet. Vous connaissiez peut-être déjà la plupart des conseils, mais il y en a encore tant d'autres. L'informatique vient à nouveau d'évoluer depuis la lecture de la première ligne de ce guide, de nouveaux piratages viennent d'avoir lieu, de nouvelles menaces viennent de voir le jour.

Mais s'il y a bien une défense qui vous permettra de faire face constamment à ces évolutions, **ce sont vos connaissances**. Vous n'avez pas besoin d'un diplôme pour cela, ni de quelconques outils. Les connaissances sont surtout **des bonnes pratiques à acquérir en étudiant le fonctionnement des cyberattaques**. C'est le cœur de ce qu'on appelle le « hacking éthique ».

Et la (vraie) difficulté autour de ces connaissances à acquérir, c'est qu'elles sont souvent désorganisées, éparpillées, obsolètes, fausses, difficile à trouver ou à assimiler etc… C'est pour cette raison que les sites Cyberini et son grand frère *Le Blog du Hacker* existent. La démarche est simple : (ré)organiser, classer et expliquer étape par étape les façons de se protéger sur Internet à destination du

grand public, trop souvent oublié mais tellement concerné.

Les cours vidéo Cyberini sont faits pour vous si :

- Vous êtes un peu perdu(e) avec ces histoires de piratages et de données personnelles.
- Vous souhaitez être guidé(e) et apprendre étape par étape à votre rythme avec des explications simples et efficaces.
- Vous souhaitez naviguer sereinement sur Internet.
- Vous souhaitez mieux maitriser l'informatique de façon générale.
- Vous souhaitez simplement savoir comment ne pas (ou plus) vous faire avoir.

Je vous joins exceptionnellement un code de réduction pour votre premier cours « **JECOMMENCE** » applicable en passant commande aujourd'hui, et valable sur le cours de votre choix.

Excellent apprentissage et à très vite.

Michel.