COMMENT SÉCURISER MON ORDINATEUR ? 1

« Plus faibles sont les risques, meilleure est l'entreprise », disait le philosophe grec Sophocle. Évidemment, vous n'êtes pas en possession d'un super-ordinateur capable de déclencher une guerre nucléaire mondiale, comme dans le film *Wargames* de 1983, en plein conflit américano-soviétique. La menace est certes moindre sur ce plan qu'il y a trente ans, mais, dans le même temps, nos ordinateurs nous ont imposé de nouvelles responsabilités individuelles. Commençons par ce qui paraît évident, a priori…

La première règle absolue est de restreindre l'accès à l'ordinateur à soi seul. Pour cela, vous devez être le seul à connaître son mot de passe. Pour des raisons de sécurité, il convient de ne le partager avec personne, même avec votre conjoint. Les mêmes règles s'appliquent à votre smartphone.

« *Comment puis-je obtenir le mot de passe de mon mari ? Je sais qu'il me trompe et j'ai besoin de savoir la vérité.* » Cette question anodine est posée sur un forum en ligne et à laquelle certains répondent encore aujourd'hui avec des méthodes de « pirate » pour débutants. Vous êtes prévenu !

Au passage, sachez que 7 Français sur 10 utilisent régulièrement un seul et même mot de passe pour tous leurs comptes (banques, réseau social, messagerie…), selon une enquête de l'institut CSA de 2017. Apprenez à changer !

Les mises à jour du navigateur (le programme qui vous permet de « surfer » et d'ouvrir des pages) doivent être effectuées régulièrement, et le système d'exploitation (ce qui permet de faire tourner ensemble les différents programmes et logiciels de votre machine) ne doit pas être obsolète. En 2017, le virus « Wannacry » ciblait une ancienne version du célèbre système d'exploitation de Windows et infectait des centaines de milliers d'ordinateurs à travers le monde.

Quelques règles simples, dans cette bataille que vous devez mener face au risque de négligence :

– Commencer par installer un antivirus (BitDefender, Norton, ESET, AVG…), ils arrivent à bloquer de nombreux virus ou

logiciels malveillants. Toutefois, ne refusez pas les mises à jour de la base de virus, et ne passez pas outre les mises en garde (formez vos enfants notamment).

- Il faut aussi activer le Firewall ou Pare-Feu en français, qui en surveillant les échanges de données avec Internet, est capable de vous alerter en cas de tentatives d'intrusions extérieures ou de flux de données étranges. Pour une meilleure sécurité, il peut être avantageux d'utiliser des logiciels spécialisés (GlassWire, ZoneAlarm, Comodo, WFC…) plutôt que le firewall par défaut fourni sur Mac ou Windows.
- Apprendre à régler les paramètres de sécurité de son navigateur pour éviter les sites vérolés (ceux qui sont truffés de logiciels malveillants). Les procédures varient bien selon le navigateur mais restent assez similaires. Trouvez un onglet « paramètres », ou « outils », qui vous permettra d'accéder à un menu. Chercher dans ce menu une section comportant des termes comme « confidentialité » ou « sécurité ».

Le reste est assez intuitif et permet de : gérer vos archives de navigation (l'historique de vos utilisations d'Internet), permettre ou non l'usage de « cookies » par les sites, bloquer les fenêtres « Pop ups » ou activer des contrôles parentaux. Tout ceci est expliqué dans cet ouvrage.

- N'oubliez pas, vous n'êtes pas seul face à l'écran ! Sur Google, lancez des recherches avec des termes comme « paramètres sécurité navigateur untel », ou « régler mon compte mail avec untel navigateur ». Le Web regorge de notices de ce genre, souvent bien faites.
- Créez différents comptes d'utilisateurs dans les paramètres de votre système d'exploitation. Vous pourrez ainsi faire une distinction entre les utilisateurs adultes ou enfants (accès restreint) et imposer des règles de contrôle parental, quant aux applications accessibles et à leur durée maximum d'utilisation journalière. En France, 53 % des parents le mettent en place. (Fédération française des télécoms avec Harris Interactive, 2017).
- Utiliser la double authentification pour vos services les plus sensibles (email…) : elle consiste à utiliser deux modes d'identification et de vérification complémentaires : un mot de passe puis une autre preuve d'identité. Généralement, vous recevez par email un code secret à rentrer dans l'interface pour prouver

votre identité. L'intérêt de cette technique est que si vous vous faîtes voler le mot de passe, le pirate devra avoir aussi accès à votre boîte email pour accéder à votre ordinateur Mais même cette méthode n'est pas infaillible. À l'été 2018, certains comptes anglophones de l'application de photos Instagram ont été piratés, et ce malgré la double authentification par SMS ou email (ceux-ci peuvent être interceptés). Instagram a annoncé travailler sur de nouvelles méthodes de double sécurité. Pour les plus prévoyants, il est possible d'utiliser en double authentification une clé de sécurité, qui s'insère au port USB de votre ordinateur (Yubikey, Neowave, Key-ID…).

Dans notre lexique sécurité : Cookies, NFC, Wifi, Bluetooth.

Pour aller plus loin : « Guide d'Hygiène informatique ». ANSII (Agence nationale de la sécurité des systèmes d'information).

2 COMMENT SÉCURISER MON MOBILE ?

Une journée, 24 heures. C'est le temps, par mois, que nous passons sur les petits écrans de nos téléphones. Et avec 20 h 52 passées sur les seules applications du téléphone et 3 h 47 sur les sites, l'ordinateur devient largement secondaire (Médiamétrie/Netratings, mai 2017). Bien sûr, la sécurité d'un mobile a des points communs avec celle de son prédécesseur. Mais il est désormais d'un usage quasi permanent, voire addictif. Pire, il vous suit à la trace.

Désormais, des myriades d'applications (« apps ») sont disponibles sur ce support. Beaucoup sont gratuites et séduisantes, mais, en pratique, il est assez difficile de savoir concrètement ce qu'elles font. Accepter de les installer, c'est parfois faire entrer un cheval de Troie sur votre mobile (donnant au pirate les pleins pouvoirs sur votre téléphone), par leur nature même ou par des défauts dans leur programmation. Aussi est-il conseillé de limiter leur nombre, de vous enquérir sur les forums d'utilisateurs avant une installation, et de les mettre à jour régulièrement.

Évitez bien sûr les applications piratées, elles sont souvent infectées.

Idéalement, les interfaces sans-fil (Bluetooth et Wifi) ou utilisant la communication en champ proche (à proximité de quelqu'un ou d'un objet de type terminal) doivent être désactivées lorsqu'elles ne sont pas utilisées.

7 règles faciles à suivre pour votre sécurité :

- Personnalisez votre code PIN, qui protège de l'usage de votre carte SIM. Nous sommes encore nombreux à laisser le code par défaut, à savoir 0000 ou 1234. De la même façon, évitez les codes très simples, comme ceux basés sur votre date de naissance par exemple.
- Verrouillez votre téléphone avec un mot de passe. Si vous possédez un mobile équipé d'un lecteur d'empreinte digitale ou de la reconnaissance faciale. C'est la fonctionnalité de sécurité la plus sûre pour un terminal mobile. Sur Android : « Paramètres/Choisir Écran verrouillage/sécurité/choisir Mode de déverrouillage/choisir empreintes/suivre les indications pour enregistrer l'empreinte de son doigt ». Sur les iPhones, cela se trouve dans « Réglages » et « Touch ID ».

– Configurez le verrouillage automatique du terminal au bout de 5 minutes maximum d'inactivité.
– Là aussi, penser à mettre à jour votre système d'exploitation, comme sur un ordinateur fixe, c'est vital pour éviter les virus répandus sur mobile.
– Si le fabricant de votre téléphone les possède quoi qu'il arrive, protégez à minima vos données personnelles grâce au « chiffrement » ou cryptage (des systèmes d'exploitation sur mobile, – celui des iPhones d'Apple principalement –, propose le cryptage automatique des données. Pour les autres sous Android, il est possible de télécharger des applications tierces).
– En moyenne en France, nous installons un peu plus de 90 applications sur un téléphone, d'après les chiffres du spécialiste AppAnnie. Mais seulement une trentaine par mois sont utilisées, soit un tiers. Du coup, un geste simple : le nettoyage saisonnier.
– Enfin le problème de la localisation de votre téléphone. L'option permet de le retrouver, mais également de vous suivre à la trace, et vous pourriez vouloir soit la suspendre entièrement, soit empêcher certaines applications de faire remonter des informations personnelles. Pour désactiver la localisation sous Android : « Paramètres », puis « Sécurité et confidentialité », « données de localisation ».

Chaque application, souvent très curieuse, se commande de manière indépendante. Pour restreindre ces informations à certains de ces services : « Paramètres », « Applications », faites votre choix, puis « Autorisations », et retirer « Informations de localisation ». Dans de nombreux cas, vous ne pourrez toutefois le faire, parce que pour commander un chauffeur, une pizza ou une livraison, vous serez alors obligés de la réactiver.

Le principe est très similaire sur les autres systèmes, comme l'IOS d'Apple. N'oubliez pas que vous avez la main sur vos appareils, pas l'inverse : vous les contrôlez, sinon ils vous contrôlent…

Dans notre lexique : chiffrement, données de localisation.

Pour aller plus loin : ANSII « Note technique. Recommandation relative aux ordiphones ».

3 QUE FAIRE EN CAS DE PERTE DE MON MOBILE ?

Le vol de téléphone portable est une véritable petite industrie. Dans les grandes villes comme Paris, les vols sont fréquents et la revente auprès d'un complice peu scrupuleux est quasi immédiate. En 2014, les derniers chiffres officiels donnent 678 000 vols de téléphone sur un an en France, soit près de 2 000 par jour.

- Il faut d'abord suspendre votre ligne (vol/perte).
- Porter plainte en cas de vol. Il vous faudra fournir aux autorités le numéro IMEI du téléphone. Ce numéro est composé de quinze chiffres. Il figure sur l'étiquette du coffret d'emballage et votre espace client.
- Donner le plus de détails possibles dans votre dépôt de plainte, car cela pourrait permettre de faire jouer l'une de vos assurances (en vérifiant bien les conditions de votre police si possible, avant la rédaction de la plainte). Vous pourriez par exemple avoir une assurance contre le vol avec agression. Mentionnez donc précisément les circonstances du vol.
- Contacter l'assurance (si le cas de figure est couvert par votre police).

Certains opérateurs téléphoniques et revendeurs proposent une assurance permettant le remplacement du téléphone en cas de perte. Une franchise doit généralement être payée. Une telle assurance n'est pas obligatoire.

Si vous n'avez pas assuré votre téléphone, le lieu du vol lui-même (votre voiture ou votre domicile) peut parfois aussi vous faire bénéficier d'une assurance idoine. La carte bleue avec laquelle vous avez réalisé l'achat du téléphone peut aussi l'assurer, dans certains cas.

Généralement, il ne peut pas s'écouler plus de 48 h entre la perte et la déclaration de vol. La perte ou le vol d'un téléphone portable peut éventuellement constituer des cas permettant la résiliation anticipée d'un abonnement. Il faut vérifier si ce cas est prévu dans votre contrat.

Une fois votre ligne suspendue, vous pouvez généralement continuer à consulter votre répondeur depuis un autre téléphone. Pour cela, il suffit d'appeler directement votre numéro de mobile, ou de le renseigner

après avoir appelé un numéro spécial, de taper # pendant l'annonce de votre répondeur, puis de suivre les instructions demandées.

Sachez que la plupart des appareils récents permettent d'effacer à distance vos données personnelles (photos, SMS…). Pensez à prendre les devants en sauvegardant régulièrement, vos données personnelles sur le Cloud de votre système d'exploitation ou de votre opérateur. En cas de perte ou de vol, vous accéderez à vos données en vous connectant via Internet.

À lire : https://www.service-public.fr/particuliers/vosdroits/F34123

4 QU'EST-CE QU'UN BON MOT DE PASSE ?

Le champion du monde des mots de passe, au moins depuis deux ans, est, sans surprise, « 123456 ». Il est suivi par « password » et sa variante « 12345678 » ou encore « iloveyou » (étude Splashdata, 2018). Hélas, un mot de passe raisonnablement sûr comporte un mélange de 12 chiffres et lettres, avec des minuscules et des majuscules, idéalement même des caractères spéciaux (@ &! …). Il est impératif que le mot de passe n'ait pas de lien évident avec soi, même si nous avons souvent l'intuition inverse. À proscrire donc : prénom, ou nom de proches, d'enfants, code postal, adresse, date de naissance…

Il faut établir au minimum un mot de passe « fort » pour ses services les plus exposés : les comptes PayPal et email, son accès bancaire en ligne, son mobile. Une déclinaison de ce mot de passe pourra être employée pour accéder à un gestionnaire de mots de passe (type « Dashlane » ou KeePassX), nous y reviendrons à la question suivante.

Un deuxième (ou troisième) mot de passe devra impérativement être utilisé pour les sites suspects ou à niveau de sécurité incertain (petits sites e-commerce…). Le fait d'avoir plusieurs mots de passe, que vous changez en plus régulièrement, vous évitera, par exemple, quelques sueurs froides si vous recevez par email le nouveau « scam » (arnaque) star de l'année 2018. En objet d'email, votre mot de passe justement et en texte : « *Nous avons accès à tous vos comptes et avons une vidéo de vous en train de regarder une vidéo pornographique, nous avons les meilleurs moments et allons l'envoyer à vos amis et votre famille si vous ne nous payez pas 500 €…* » « Sextortion scam », c'est le nom de cette nouvelle escroquerie opérée grâce au piratage d'anciens mots de passe.

En effet, lors du piratage en 2017 du site « Ashley Madison », spécialisé dans les rencontres adultères, les mots de passe de 11 millions d'usagers ont été piratés suite à une faiblesse dans l'encodage de ces mots de passe par le site. Il suffit alors aux pirates de tester ce mot de passe sur Facebook, Gmail, Amazon… pour accéder à de quoi vous extorquer.

Dès lors, comment créer un bon mot de passe ? Un bon mot de passe est difficile à retrouver même à l'aide d'outils automatisés. La force d'un mot de passe dépend de sa longueur et du nombre de possibilités existantes pour chaque caractère le composant. De ce fait, si quelqu'un tente de le découvrir, c'est techniquement beaucoup plus difficile.