Sécurité sur Internet: êtes-vous bien protégé ?

TEXTE : JULIE FIARD • JFI@EASI-IE.COM
HTTP://WWW.EASI-IE.COM • HTTP://WWW.TWITTER.COM/EASI_IE • HTTPS://WWW.FACEBOOK.COM/EASI.EXPERTSDUWEB
ILLUSTRATIONS : VINCE • VINCENT_DUBOIS@ME.COM

Internet évolue rapidement, les règles de sécurité d'hier ne sont plus celles d'aujourd'hui. Voici un tour d'horizon des bonnes pratiques, en matière de sécurité, sur les réseaux sociaux et sur Internet en général.

Début 2019, le journal *20 Minutes* publie les résultats d'une enquête sur le cyber-harcèlement des jeunes entre 18 et 30 ans, avec *Opinion Way* (**https://urlz.fr/c2G4**). Les chiffres sont inquiétants !

- 53% des 18-30 ans ont déjà subi au moins une situation de cyber-violence sur les réseaux sociaux, un chiffre qui grimpe à 63% chez les 20-24 ans.
- Selon l'enquête, les faits les plus courants sont les insultes (29%), les moqueries (27%), les photos compromettantes (21%), la diffamation (13%), le harcèlement (11%), l'usurpation d'identité (9%) et le «revenge porn» ou publication d'une vidéo à caractère sexuel par vengeance amoureuse (2%).
- *Facebook* est de très loin la plateforme la plus citée comme lieu de harcèlement (81%), suivi de *Messenger* (16%), *Twitter* (15%) et *Snapchat* (8%).

Il n'est pas toujours évident de se prémunir contre ce type d'agressions. Néanmoins, un comportement adapté et quelques règles simples de sécurité peuvent aider.

Tout d'abord, distinguons 2 types de cybercriminalité:

1. des actions malveillantes visant des réseaux informatiques ou des appareils (ordinateurs, téléphones, tablettes,...) plutôt dirigées vers des entreprises et des institutions.
2. des actions visant à nuire à la propriété intellectuelle (par le vol de données personnelles) ou individuelle d'une personne. On parle alors de cyberharcèlement, de vol d'identité, de phishing, de diffusion de contenu interdit ou illégal. Ces actions sont plutôt dirigées vers un public de particuliers.

Il semblerait également qu'avec l'utilisation quotidienne des réseaux sociaux et d'Internet dans nos vies, nous accordons moins d'importance à notre vie privée (selon le cyberbaromètre d'*AXA Partners* - ***https://urlz.fr/c3LI***) et par conséquent, à la protection de nos données.

Protection de vos données numériques

Vous connaissez la chanson, tout le monde le sait mais nous n'appliquons que trop rarement les bonnes pratiques pour protéger nos données numériques. En mettant en place ces simples règles de sécurité, vous éviteriez certaines attaques. Attention ! Ces règles sont un dispositif préventif et malheureusement, elles ne vous protègent pas d'une éventuelle intrusion mais peuvent déjà décourager ses auteurs !

L'une des premières règles concerne le mot de passe. Cependant, et toujours selon le cyberbaromètre d'*AXA* 2019 (une enquête annuelle menée sur un panel d'un millier de belges: ***privacy-assist.be/fr/cyberbarometre***), il apparaît que la population belge connaît les principaux cyberrisques mais n'en tient pas compte ! Par rapport aux chiffres 2018, autant, si ce n'est plus de belges indiquent réutiliser le même mot de passe pour accéder à des comptes différents.

▸ Utilisez un mot de passe différent pour chaque service

Oui, c'est contraignant ! Oui, Internet va vite et nous pousse à vouloir tout tout de suite ! À tel point que nous sommes parfois agacés de devoir rentrer nos données personnelles correctement et que la tentation est grande d'utiliser toujours le même mot de passe, souvent très simplifié, afin de s'en souvenir.

Pour vous aider dans la gestion de vos différents mots de passe et services en ligne, vous pouvez utiliser un gestionnaire virtuel de mots de passe, sorte de coffre-fort numérique, vous permettant de stocker tous vos mots de passe dans un seul et unique endroit.

Pour les utilisateurs d'*Apple*, il est facile de vous fier aux trousseaux d'accès de vos appareils. Cela vous permettra d'utiliser des mots de passe très complexes qui seront gérés et cryptés dans le trousseau de votre appareil principal et que vous n'aurez pas à mémoriser. Le tout accessible via un seul mot de passe.

Consultez plus d'informations à l'adresse suivante:
https://urlz.fr/c3ma

Voici quelques gestionnaires de mots de passe:

- ***www.lastpass.com***
- ***www.dashlane.com***
- ***https://nordpass.com***
- ***www.keepersecurity.com***

N'hésitez pas à tester, chercher et choisir celui qui convient le mieux à votre usage.

▸ Choisissez avec attention vos mots de passe

Choisissez des mots de passe longs, de plus de 12 caractères, avec au moins une majuscule, un chiffre et un caractère spécial autorisé. Évitez les successions de chiffres trop simples telles que 123 ou 000. N'utilisez pas votre prénom, votre nom ou votre date de naissance dans votre mot de passe. Pour vous aider, il existe des générateurs qui vont vous proposer des mots de passe à utiliser en fonction de leur niveau de protection, en voici quelques-uns:

- ***www.motdepasse.xyz***
- ***www.lastpass.com/fr/password-generator***
- ***www.roboform.com/fr/password-generator***

Pour connaître et calculer la force de vos mots de passe, l'*Agence française de la sécurité des systèmes d'information* (*ANSSI*) vous propose un outil en ligne: ***https://urlz.fr/c3rW***

NOTRE CONSEIL: changez vos mots de passe souvent, une fois par an minimum et si possible, tous les 3 mois.

▸ Utilisez la double authentification chaque fois que c'est possible

L'identification à 2 facteurs, comme son nom l'indique, consiste à demander un mot de passe puis une seconde information confirmant que vous êtes le bon utilisateur. Plusieurs méthodes sont proposées: vous recevez un sms avec un code à reproduire à l'écran ou un appel téléphonique vous indiquant le fameux code (cela complexifie les opérations, le deuxième facteur impliquant de toujours avoir son téléphone près de soi pour chaque opération). Le deuxième facteur

>> est obligatoire pour les banques, optionnel sur d'autres plateformes. Vous avez la possibilité de l'activer ou non.

NOTRE CONSEIL: activez-le pour vos accès à des données sensibles. Votre boîte mail principale par exemple, votre compte *Paypal*, le serveur contenant les données de votre site Internet si vous en possédez un.

Sur les réseaux sociaux

Nous sommes 3,7 milliards, soit 48% de la population mondiale à utiliser au quotidien les réseaux sociaux selon les derniers chiffres (source: *We Are Social/GlobalWebIndex*/blog du modérateur). Dans cet ordre, nous utilisons le plus les réseaux suivants: *Facebook*, *YouTube*, *WhatsApp*, *Instagram*, *TikTok* et *Twitter*. Combien sommes-nous à nous préoccuper de savoir si les données que nous confions à ces géants du Web sont bien protégées ? Peu d'entre nous considèrent que surfer sur ces fameux réseaux est risqué et par conséquent, nous n'adoptons pas toujours un comportement sécuritaire mettant à l'abri nos données personnelles. Voici quelques règles simples à appliquer sur la plupart des réseaux.

▸ Ne partagez pas tout et n'importe quoi. Surtout n'importe quoi.

Soyez pragmatique ! Et logique. Pourquoi feriez-vous sur les réseaux ce que vous ne faites pas dans la vraie vie ? Question à vous poser également quand cela ne vous concerne pas directement mais concerne vos enfants, un membre de votre famille, vos amis. Iriez-vous, par exemple, afficher en grand format aux yeux de toute votre société de plus d'un millier de personnes, sur les murs de la cantine par exemple, une photo de vous à la plage en train de courir vers les vagues ? Vous ne le feriez pas ? Et vous avez raison. Alors ne le faites pas quand il s'agit de vos enfants ou de vos proches. Parce que c'est à peu près ce que vous faites quand vous publiez une photo de vous ou d'une autre personne, même si c'est sur votre espace dédié.

+ À lire sur le site de la *VRT*, un article sur l'utilisation cybercriminelle de photos d'enfants: ***https://www.vrt.be/vrtnws/nl/2019/10/15/pano/***

Cela est également valable pour ceci: vous permettez-vous de donner votre avis sur une caractéristique physique d'une personne en vous adressant directement à elle dans la rue, pour lui confier que vous trouvez que son nez est vraiment très grand ? Non, alors ne le faites pas non plus sur les réseaux, si la personne ne vous demande pas votre avis, gardez-le pour vous. Même si la section «commentaires» existe sous quasiment toutes les publications, cela ne veut pas dire qu'il faut donner son avis à tout prix.

Il est également dangereux de partager sur vos réseaux trop d'informations vous concernant, comme la prochaine date de vos vacances, la photo de votre voiture avec sa plaque d'immatriculation, des emplacements géolocalisés où vous vous trouvez, des achats coûteux suscitant l'envie. Toutes ces informations peuvent être entrecoupées entre elles afin de servir à vous voler votre identité numérique, pénétrer chez vous par effraction, vous suivre...

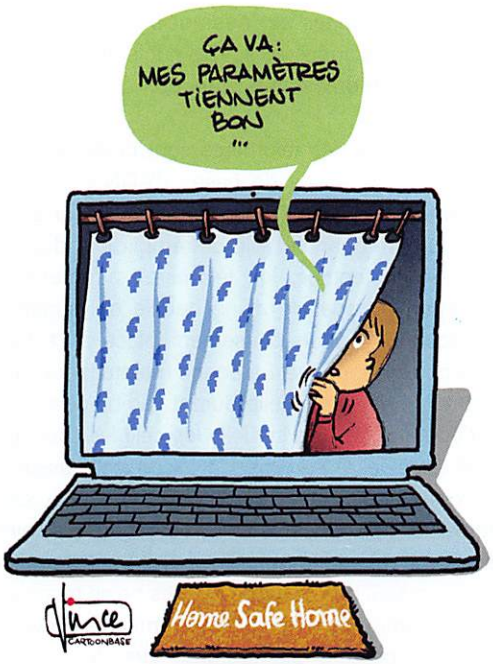
Attention également quand vous envoyez des photos ou des copies de documents officiels, passeport et autre. Assurez-vous d'accorder votre confiance à la personne qui les reçoit et faites également attention d'utiliser les bons canaux de communication pour le faire. Le mail restant le plus adapté pour ce genre de transfert.

▸ Ne niez plus les paramètres de confidentialité

Ces fameux paramètres de confidentialité qui ne cessent d'évoluer ! Des dizaines de pages, pour ne pas dire des centaines, à lire, encore faut-il comprendre ce qu'il y est expliqué. Tout en sachant qu'à chaque mise à jour du service en question, les paramètres de confidentialité sont susceptibles de changer. Oui c'est long, personne n'a le temps et personne n'a envie, MAIS...

Voici ce que vous risquez à ne pas vous en préoccuper. Qui n'a jamais accepté, parmi ses amis «virtuels», une personne qu'elle ne connaissait pas ?! Une fois accepté, vous oubliez que cette personne fait désormais partie de votre réseau et qu'elle a par conséquent accès à toutes les informations personnelles que vous publiez. Elle a d'ores et déjà une fenêtre ouverte sur votre vie, elle peut également vous envoyer des virus par message. Si vous refusez les demandes de personnes que vous ne connaissez pas sur vos réseaux mais que vous ne vérifiez pas vos paramètres de confidentialité et que votre profil est paramétré sur public, le mur sur lequel vous pensez partager des informations personnelles juste à votre réseau agit comme un miroir sur le monde, et n'importe qui a un accès direct sur ce que vous partagez. Pensez-y et repassez en revue les paramètres de tous vos réseaux !

Voici quelques astuces pour vous aider et vous rendre la tâche plus facile. Nous nous sommes concentrés sur le réseau le plus utilisé: *Facebook*. La nouvelle version de l'assistant confidentialité développée sur le réseau en ce début d'année, devrait vous faciliter la tâche.



Pour accéder aux paramètres de confidentialité plus rapidement: ***https://www.facebook.com/help/395495000532167***

Pour télécharger tout ce que vous lui avez transféré sous forme de fichiers: dans votre profil, allez dans «Paramètres» puis, dans la colonne de gauche, cliquez sur «Vos informations *Facebook*».

Pour contrôler qui peut voir ce que vous publiez sur *Facebook*, nous vous conseillons de lire ce guide: ***https://www.facebook.com/help/1297502253597210?helpref=faq_content***

Sachez qu'une fois les conditions d'utilisation acceptées , chaque information que vous donnez sur le site est conservée dans ses bases de données. Sur Internet, quand quelque chose est gratuit, c'est que vous êtes le produit. *Facebook* l'exprime clairement dans ses conditions d'utilisation dont voici un extrait: «*Nous ne vous facturons pas l'utilisation de* Facebook *ou des autres produits et services inclus dans les présentes conditions. À la place, les entreprises et les organisations nous payent pour vous montrer des publicités pour leurs produits et services*» (***https://www.facebook.com/terms***).

Pour aller plus loin, nous avons sélectionné pour vous une liste de sites intéressants à consulter en ce qui concerne la cybercriminalité et la cybersécurité:

- ***www.safeonweb.be/fr*** décrit toutes les situations que vous pourriez rencontrer en cas de problème et comment y faire face. Ce site a été développé à l'initiative de *Centre for cyber security belgium*: ***https://ccb.belgium.be***
- Sur le site *Childfocus*, vous trouverez des informations sur la sécurité en ligne destinées à tous et dont le contenu est adapté pour les enfants et les adolescents (***https://www.childfocus.be/fr/prevention/clicksafe-tout-sur-la-securite-en-ligne***)
- Pour signaler un abus sur Internet, rendez-vous sur: ***https://www.dnsbelgium.be/fr/securite-internet/signaler-un-abus-internet***
- Si vous avez perdu votre téléphone, rendez-vous sur: ***www.safeonweb.be/fr/jai-perdu-mon-smartphonema-tablette***
- Si votre compte est piraté: ***www.safeonweb.be/fr/mon-compte-est-pirate***

Et vous, qu'allez-vous modifier ou mettre en place pour votre cyber-sécurité ? Faites-nous part de vos avancées en nous envoyant un mail à ***contact@easi-ie.com***