LA SECURITE INFORMATIQUE

Malware en approche, à vos claviers !

ZARIKIAN HAYK-LIS AMBRE

Vous venez de décrypter un document. Vous vous demandez sans doute ce que cela signifie, nous y reviendront plus tard. Avant cela, il est important de savoir comment sécuriser un mot de passe.

Voici quelques conseils pour sécuriser vos mots de passe :

- Mélangez majuscules, minuscules, chiffres, lettres, caractères spéciaux (. / # &).
- Le mot de passe doit avoir au moins 12 caractères.
- Evitez les suites de chiffres comme 1234, ainsi que les évidences comme votre date de naissance. Préférez des mots de passe originaux.
- Changez régulièrement vos mots de passe (tous les 6 mois idéalement), évitez de l'enregistrer et n'utilisez pas les mêmes mots de passe.
- Activez la double authentification quand c'est possible.

La « **double authentification** », permet d'ajouter un niveau de sécurité supplémentaire à un réseau social, site ou autre compte généralement en utilisant votre numéro de téléphone.

Définissons dans un premier temps ce qu'est la « ***sécurité informatique*** ».

C'est un ensemble de moyens techniques, technologiques ou juridiques mis en place afin d'empêcher des personnes malveillantes d'utiliser l'informatique dans le but de nuire à d'autres personnes.

Ce sont des « **hackeurs** ». Des spécialistes de l'informatique qui recherchent des moyens de contourner les protections de l'informatique ou le matériel informatique en utilisant ses failles.

Il existe 2 types de hackeurs. Le hackeur « malveillant » et le hackeur « bienveillant ».

Le hackeur dit « **éthique** », va aider à sécuriser les systèmes informatiques. Il peut être embauché par des entreprises par exemple afin qu'elles puissent sécuriser leurs données ou leurs transactions d'argent.

Le hackeur dit « **malveillant** » va utiliser ses compétences informatiques afin de nuire aux autres. Dans le but de soutirer de l'argent, de se venger de quelqu'un qui lui aurait fait du mal, par curiosité ou simplement par envie de nuire.

Ces pirates informatiques peuvent revendre des informations illégales ou confidentielles d'entreprises, utiliser les cartes bancaires d'autres personnes pour gagner de l'argent, etc. C'est ce que l'on appelle le « **hacking** ».

Il existe de nombreuses manières d'hacker. Virus informatiques, Vers, Adwares, logiciels d'espions, ransomwares, robots, rootkits, chevaux de Troie etc.

Le « **virus informatique** », permet de perturber le fonctionnement de l’ordinateur en l’infectant de façon plus ou moins grave. Un peu comme un virus infecterait le corps humain. Il peut être importé dans une publicité ou bien encore un lien de téléchargement.

Les **2 types de virus** les plus utilisés sont les suivants :

Le « **ransomware** », c’est un virus destiné à « **chiffrer** » nos données personnelles pour les rendre inaccessibles.
Un « **chiffrement** » est un procédé permettant de rendre la compréhension d’un document illisible à toute personne qui n’a pas la clé pour le déchiffrer.
Le ransomware a donc pour but de demander une rançon à la victime qui se fait hacker. On lui demande de l’argent contre la récupération de ses données.
Les ransomwares peuvent notamment être envoyé via nos mails.

L’ « **hameçonnage** » (ou phishing), c’est une technique destinée à duper une personne en l’incitant à communiquer ses données personnelles. (Mots de passe, coordonnées bancaires etc.) en se faisant passer pour quelqu’un de confiance.

Si vous souhaitez en savoir plus sur les types de virus, ouvrez-moi !

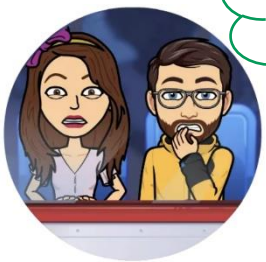
Les pirates informatiques peuvent effectuer un autre type de hacking. Il s’agit du « webcam hacking ».

On installe dans votre ordinateur un malware qui permet d’accéder à distance à votre caméra. Les hackeurs vendent ensuite vos images. Cette technique est assez compliquée pour les hackeurs mais il en existe une autre qui est bien plus simple à utiliser.

Une faille du plugin Adobe Flash sur nos navigateurs internet. Un plugin permet d’ajouter des fonctions supplémentaires à un logiciel principal (dans cet exemple, c’est le navigateur internet).

Cette faille permet d'allumer à distance nos webcam ainsi que les micros qui y sont intégrés. Il faut donc particulièrement faire attention à cela mais attention, ne devenez pas paranoïaque pour autant et pas d'inquiétudes car il existe des solutions !

Pour éviter le piratage de vos webcams :

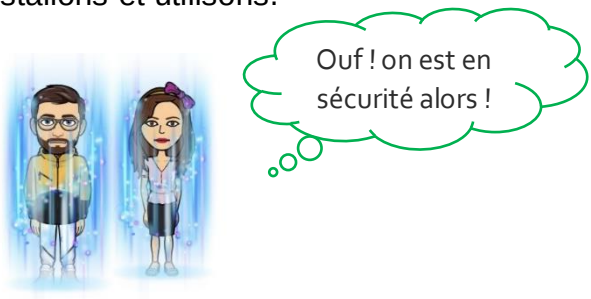


Afin de se protéger des virus informatiques, de nombreuses solutions peuvent être mises en place.

Les « **anti-virus** » par exemple sont là pour prévenir, identifier et effacer les virus ou bien les chevaux de Trois. Il y a certains virus que l'anti-virus ne peut pas détecter car ils sont trop subtils.

Les « **systèmes d'exploitation** » sont des ensembles de programmes qui dirigent l'utilisation des capacités de notre ordinateur par des logiciels. Les systèmes d'exploitation Windows ou Mac OS possèdent un anti-virus intégré. Ils sont assez puissants pour lutter contre les virus donc il n'y a pas besoin d'en installer un autre.

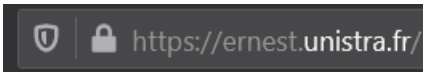
Mais comme l'a dit le développeur web **SAMMY MAHFOUDH**[1], « le plus puissant des anti-virus est celui qui se trouve derrière son écran et son clavier. »
Nous sommes donc les mieux placés et nos propres maîtres de nos protections via ce que nous téléchargeons, installons et utilisons.



[1] Employé de la société SAS WEBAGENCELILLE

Rappelons qu'il est important de faire attention à sécuriser nos comptes sur les sites que nous visitons en créant des mots de passe à sécurité élevée ou bien de simplement de faire attention aux sites sur lesquels nous nous rendons.

Voici une petite technique pour savoir si notre site est sécurisé ou non.



Le protocole HTTPS (Hyper Text Transfer Protocol Secure) est une extension de HTTP. Le « S » pour « Secured » (sécurisé) signifie que les données échangées entre le navigateur de l'utilisateur du site et le site sont chiffrées et ne peuvent pas être espionnées ou modifiées.

Le cadenas situé à côté du https implique que nos informations, comme nos mots de passe, numéros de carte de payement sont privées lorsqu'elles sont transmises à ce site.

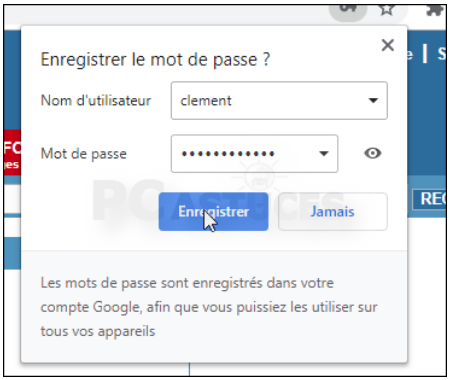
Afin que nos mots de passe soient sécurisés, ils doivent contenir environ 12 caractères, des majuscules, minuscules, chiffres, lettres et caractères spéciaux.

Ils ne doivent pas se référer à des choses personnelles telles qu'une date de naissance, le nom de votre chien ou bien de votre grand-mère.

Il ne faut JAMAIS communiquer son mot de passe et TOUJOURS mettre des mots de passe différents sur chaque compte.
De plus, pour éviter de se faire hacker il ne vaut mieux pas l'enregistrer. Il est plus difficile de le retenir mais plus prudent pour vos données.
Attention : tous les comptes ne sont pas forcément à protéger. Il ne s'intéressera pas à votre mot de passe Marmiton[2]…Mais tout ce qui concerne vos comptes bancaires, c'est comme les bonbons pour un enfants. C'est un trésor.

[2] Site de recettes de cuisine

Pour retenir vos mots de passe vous pouvez les écrire sur un papier et le mettre dans un endroit sûr par exemple.



Google vous propose souvent ces petits encadrés. Si vous y enregistrez vos informations, les hackeurs auront donc accès plus facilement à vos informations même si vos sites sont sécurisés.

Si vous devenez le patron d'une grosse entreprise dans le futur…il vaudra donc mieux éviter d'enregistrer au maximum vos mots de passe sur Google…

Afin d’en savoir plus sur les mots de passe et leur sécurité :

Pour en revenir aux entreprises, afin de sécuriser leurs données, elles embauchent des informaticiens spécialisés, des experts en sécurité informatique. Ils peuvent être aidés d’hackeurs éthiques. Le rôle de ces experts est d’empêcher les hackeurs malveillants de voler les données des entreprises.

Les hackeurs éthiques jouent un grand rôle dans la sécurité informatique, en infiltrant volontairement le système de l’entreprise il permet à toute son équipe de pouvoir anticiper d’une meilleure manière les virus mais aussi de les prévenir.

Une autre solution permettant de sécuriser nos informations consiste à « **crypter nos données** » ou les « **chiffrer** ». Les hackeurs peuvent utiliser cette technique contre nous mais nous pouvons aussi l’utiliser contre les hackeurs. Rappelons que le cryptage sert à rendre illisible nos informations.

Toute personne n'ayant pas la clé pour décrypter ne peut pas accéder à ces informations. Il est donc important de ne pas perdre sa clé de décryptage car sans elle vous ne pourrez plus accéder à vos propres fichiers.

Pour en apprendre plus scannez moi :

Nos données sont donc très importantes pour les hackeurs. Le danger en informatique n'est pas seulement présent via les hackeurs mais via internet et l'informatique en général. Sur les réseaux sociaux par exemple les contenus de nos fils d'actualités sont créés pour nous rendre dépendants. Afin de nous manipuler.
On nous montre beaucoup de fausses informations. Pourtant les créateurs des réseaux sociaux ne sont pas des pirates informatiques.
Pour en savoir plus sur les dangers des réseaux sociaux, vous pouvez regarder le documentaire « **Nos écrans de fumées**. »

Rassurez-vous il n'y a pas que des dangers en informatique et nous avons vu qu'il existe des moyens de les contrer !

Il faut savoir que dans les cas les plus graves, les hackeurs encourent des peines pénales. Il vaut donc mieux se ranger du côté des hackeurs gentils et non du côté obscur de l'informatique.

Ce crime s'appelle en fait la « **cybercriminalité** ». C'est une infraction pénale qui peut être punie d'une peine de 2 ans de prison et de 30 000 euros d'amende selon la gravité de l'infraction. Notamment lorsque les hackeurs s'attaquent à nos cartes bancaires, à l'incitation au terrorisme etc.

Cliquez vite, un cybercriminel est en approche !

Si l’informatique vous intéresse et plus particulièrement la sécurité informatique, il existe de nombreux métiers liés à la sécurité informatique comme expert en informatique, hackeur éthique ou tout simplement développeur/ développeuse des systèmes d’information.
Vous pourrez peut-être développer de nouveaux anti-virus, les améliorer ou bien tout simplement contribuer à la protection d’informations.

Voici quelques liens de descriptions et d'études à faire pour ces métiers :

Expert en sécurité informatique

Hackeur éthique

Développeur/ Développeuse sécurité des systèmes d'informations

Le domaine de l'informatique et de la sécurité informatique est donc très vaste et très intéressant. Il ne cesse d'évoluer et ne cessera d'évoluer dans le futur. C'est pourquoi il est important de prendre conscience du danger de l'informatique et de sécuriser les outils que nous utilisons.