CODE DE BONNE CONDUITE

-

CC - 2018

(MISE À JOUR EN MAI 2020)

Les menaces que vous pouvez rencontrer sur la toile sont nombreuses et très variées. Les pirates rivalisent d'ingéniosité pour tromper votre vigilance. Quelques bonnes habitudes peuvent en partie vous protéger des malwares, spywares, espiogiciels, virus et autres logiciels malveillants qui pourraient infecter votre ordinateur.

- **Les emails**

  Vous devez être conscient que la simple ouverture d'un email frauduleux peut infecter votre ordinateur à votre insu ! Il en est de même pour les fichiers contenus dans ces emails ainsi que pour les fichiers joints. Ce qui permettra par exemple aux hackers d'avoir un rapport automatique sur les toutes les touches de votre clavier que vous saisissez, ou encore d'avoir sur son propre ordinateur une copie de votre écran en direct, ou même de pouvoir prendre en main votre ordinateur à distance sans que vous ne vous rendiez compte de quoi que ce soit !

  Pour vous prémunir de cela et dans la mesure du possible, n'ouvrez que les emails dont vous connaissez l'expéditeur et déplacez les autres directement dans vos spams ! Méfiez-vous des titres accrocheurs du type : « ***Au secours…*** », ou « ***Remise incroyable…*** », ou « ***Vous avez gagné ! ...*** ». A priori, vous ne gagnez jamais rien sans avoir jouer au préalable ! Ne renseignez pas votre email dans n'importe quel questionnaire ou sondage sur le net ! Méfiez-vous des titres écrits dans une langue étrangère ou comportant des fautes d'orthographes ! Vous pouvez aussi bloquer les images contenues dans les emails des expéditeurs inconnus qui sont souvent utiles lors de tentatives d'intrusions **(*cf. internet ou la rubrique d'aide de votre FAI*)**.

  Vous pouvez aussi paramétrer votre boîte mail pour qu'elle trie automatiquement vos emails selon vos souhaits **(*cf. internet ou la rubrique d'aide de votre FAI).***

  Une liste des logiciels utiles est téléchargeable dans la section « ***Mentions*** » de notre site.

- **Les supports amovibles**

  Les supports amovibles (***clé usb, carte SD ou micro SD, disque dur externe***…) sont aussi d'excellents moyens de propagation pour les virus et autres espiogiciels ! Il suffit d'un seul ordinateur infecté pour que tous les autres le deviennent ! N'acceptez donc que des supports amovibles provenant de sources fiables.

- **Les cookies et l'historique des navigateurs**

  La description d'un cookie et de son utilité sont résumées dans notre document « ***Politique d'utilisation des cookies*** » disponible sur la page « ***Mentions*** » de notre site internet. Ceci-dit, vous devez savoir que lorsque vous donnez votre autorisation à un site de déposer des cookies autres que pour émettre des statistiques, il vend vos informations à d'innombrables tiers. Prenons par exemple une enseigne telle que les DNA (***Dernières Nouvelles d'Alsace***), qui jouit à priori d'une bonne image et d'une

CC - 2018

bonne réputation. Lorsque vous consultez le site des DNA, vous avez ce petit bandeau en première page :

Si vous cliquez sur « ***J'accepte*** », les données que le site aura récupéré sur votre navigateur sont transmises à **453 sociétés !** (***en date du 05/11/2018***), qui ensuite vont probablement à leur tour vendre ou transmettre vos données à d'autres ! Et nous n'avons évoqué qu'une seule structure bien connue de tous !

Donc plutôt que vous débarrasser du bandeau en cliquant sur « ***J'accepte*** », intéressez-vous à ce que cela implique ! Ne vous demandez plus pour quelle raison telle ou telle société essaye de vous vendre une piscine ainsi qu'une barrière de sécurité alors que vous avez simplement effectuer une recherche pour acheter des palmes sur internet !

Allons un peu plus loin en paramétrant le navigateur internet ! Vous pouvez dans chaque navigateur demander à ce qu'aucun mot de passe ou moyen de paiement ne soit enregistré, évidemment il faudra les saisir à chaque fois mais ils ne pourront pas être dérobés dans votre navigateurs ! Vous pouvez aussi paramétrer votre navigateur pour qu'il efface automatiquement toute trace de votre activité sur la toile à sa fermeture ou n'enregistre aucune information (***cf. internet ou la rubrique d'aide de votre navigateur***).

- **Les sites internet**

  Evidemment, le type de sites internet que vous visitez joue énormément dans les risques encourus ! Les sites pour adultes, les sites de hackings ainsi que les sites de publicités alléchantes en tout genre sont des terrains de jeux pour les hackers ! En ce qui concerne les réseaux sociaux, la plupart transmettent vos données à d'innombrables tiers !

  Par ailleurs, bien que ce ne soit pas une garantie totale, il est fortement conseillé de ne plus visiter les sites internet commençants par « ***http*** » au lieu de « ***https*** » (***regardez dans votre barre d'adresse***).

CC - 2018

- **<u>Les mots de passe</u>**

  Il est fortement conseillé d'utiliser des mots de passe différents pour chacun de vos comptes sur la toile. Par ailleurs, pour être un minimum sécurisé, un mot de passe doit comporter **(*certains sites n'acceptent pas les caractères spéciaux*)** :

  - des chiffres
  - des lettres minuscules
  - des lettres majuscules
  - des caractères spéciaux (:/@ !?., etc …)

  Afin de minimiser les risques d'intrusions sur vos comptes en ligne, ***<u>prenez l'habitude de modifier vos mots de passe tous les 2 à 3 mois maximum</u>*** !

  Par ailleurs, afin de contrer toutes tentatives d'accès malveillantes à vos comptes, il est fortement conseillé ***<u>d'activer l'authentification à 2 facteurs</u>*** au sein de chacun de vos comptes en ligne, surtout pour les comptes sensibles tels que les réseaux sociaux, les sites bancaires ou vos comptes emails.

L'authentification à deux facteurs est une fonction de sécurité qui aide à protéger vos comptes en plus de votre mot de passe. Si vous configurez l'authentification à deux facteurs, vous devrez saisir un code de connexion spécial ou confirmer votre tentative de connexion chaque fois que quelqu'un tentera d'accéder à vos comptes depuis un ordinateur ou un appareil mobile que le site ne reconnait pas. Vous pouvez également recevoir des alertes lorsque quelqu'un essaie de se connecter depuis un ordinateur que le site reconnait pas.

L'authentification à 2 facteurs peut se présenter sous forme de code à durée limitée reçu par sms ou encore sous forme de code à durée limitée disponible par l'intermédiaire d'applications mobiles telles que « ***Google Authenticator, Authy, Authenticator Plus, etc…*** ». Cette technique est à ce jour une des plus sûre pour sécuriser vos comptes sur la toile.

- **<u>Stockage de fichiers</u>**

  Nous avons tous des documents personnels, des photos de familles ou autres présents sur nos ordinateurs. Pour améliorer la sécurité de ces derniers, vous pouvez utiliser des mots de passe pour vos fichiers Word, Excel, PDF, etc… **(*cf. rubrique d'aide de votre logiciel ou sur internet*)**. Il est aussi possible de créer une partition sécurisée par un mot de passe **(*nécessite quelques connaissances*)** à l'aide d'outil comme **« *BitLocker Drive Encryption*** » disponible gratuitement sur de nombreuses versions de Microsoft Windows **(*cf. barre de recherche de votre ordinateur ou internet*)**.

- **<u>Poste de travail</u>**

  Vous ne seriez pas prêt à laisser n'importe qui se servir de votre smartphone, n'est-il pas ? Faites-en de même pour votre poste de travail, limitez en l'accès par des mots de passe et des sessions différentes. Fermez votre session une fois que vous quittez la pièce.