Protéger son ordinateur

La protection d'un ordinateur passe par l'adoption de bonnes pratiques. N'utilisez que des programmes originaux, téléchargez les mises à jour, et surtout ne vous fiez à personne.

Voici les 6 bonnes habitudes les plus importantes pour ne jamais être victime d'un programme malveillant.

Se créer une session utilisateur

Quand vous paramétrez votre ordinateur la première fois, il est fortement conseillé :

- de ne pas s'attribuer les droits d'administrateur
- d'utiliser une simple session « utilisateur ».

En effet, les sessions « administrateur » disposent de tous les droits pour modifier et installer des programmes. Quand un virus tente une intrusion sur une session administrateur, il peut réussir à s'octroyer les droits d'installation seul car il est au cœur du réacteur !

En revanche, sur une session « utilisateur », il faut systématiquement renseigner un mot de passe avant d'installer tout programme. Si un virus veut infecter votre ordinateur, une pop up vous demandera votre mot de passe. Un non, la demande est rejetée et le virus éloigné !

pour une sécurité encore plus élevée, changez régulièrement votre mot de passe.

Ne faites pas confiance aux fenêtres indésirables

Il arrive, lors de vos pérégrinations sur le Web, qu'une fenêtre de type IFrame ou pop-up apparaisse sur votre écran.

Elle vous signale souvent que votre ordinateur vient d'être infecté, et qu'il vous faut cliquer sur « ce bouton » pour que votre antivirus se mette en marche (ou que vous venez de gagner une villa, un yacht et un chèque de 100 000 €).

Pour savoir s'il ne s'agit pas d'un piège (pour le yacht, sérieusement, vous y aviez cru ?), ouvrez le programme antivirus de votre ordinateur. Ne vous fiez qu'à lui, et à personne d'autre.

Bon à savoir : lisez systématiquement les avertissements, les notifications et autres fenêtres d'information. Si quelque chose vous semble douteux, ne tapez pas votre mot de passe et ne cliquez jamais sur OK/j'autorise sans avoir lu !

Repérez les mails pirates

Parmi les nombreux mails que vous recevez quotidiennement, peuvent se glisser des reproductions très réussies de mails administratifs. Votre banque, votre caisse d'assurance maladie, votre mutuelle ne vous demanderont jamais de leur envoyer des informations personnelles sensibles par mail. Ni vos coordonnées bancaire, ni vos identifiants ou mots de passes ne doivent être envoyés à ces adresses pirates !

Pour repérer ces faux mails administratifs :

·2 L'adresse expéditrice est souvent complexe, avec des chiffres ou des noms frauduleux.

·3 Il y a souvent de nombreuses fautes d'orthographe.

·4 On vous demande souvent de cliquer sur un lien et de renseigner des informations personnelles.

·5 Il est souvent question d'urgence (majuscules, points d'exclamation nombreux, injonctions).

N'ouvrez jamais les pièces jointes avant de vous être assuré qu'elles sont saines, en particulier s'il s'agit de dossiers envoyés par des personnes ne faisant pas déjà partie de votre liste de contacts.

Bon à savoir : ces dossiers contiennent des programmes informatiques qui vont se loger dans votre ordinateur et envoient des données relatives à votre comportement commercial à une société tierce.

L'e-mail est un moyen de communication exploité par tous. Au boulot, à la maison, par les pro, les marques, la famille, les amis, un internaute français reçoit environ 40 e-mails par jour ! 40 occasions de relever de petites erreurs, pourtant faciles à éviter.

Abuser du " répondre à tous "

Pour peu que vous soyez destinataire d'un message groupé, et que tout le monde utilise la fonction « répondre à tous », vous voilà au beau milieu d'un chat !

En effet, si une personne commence à « répondre à tous » pour demander un renseignement ou poursuivre la discussion, l'ensemble de la chaîne se trouve abreuvée de messages qui ne concernent parfois qu'une poignée de personnes.

Pour éviter les abus :

·6 Masquer les destinataires en « CCI ».

·7 Demander aux destinataires de répondre sous la forme d'un « Message privé ».

Répondre comme un SMS

Si vous avez grandi à la naissance du SMS, vous maîtrisez peut-être l'art du langage associé où tous les mots sont réduits à leur phonétique pour économie de temps et d'argent. Seulement, ce langage destiné au portable doit rester sur un portable ! De la même façon, évitez :

- Les réponses du tac-au-tac sans prendre le temps de vous relire. Cela vous jouera forcément des tours !
- Les simples « OK », « Je ne suis pas d'accord. » et autre « Oui », « Non », « Peut-être ». Si le message est court, téléphonez ou levez-vous et allez parler à votre collègue ! Sinon, argumentez et expliquez ce que cela implique.

Bon à savoir : le langage SMS naît d'une volonté de réaliser des économies. En effet, dans les années 90 et au début des années 2 000, le SMS était facturé à l'unité de 160 signes. Il fallait donc trouver un moyen de communiquer en prenant le moins de place possible.

Attendre une réponse immédiate

Il faut vous y faire, tout le monde n'est pas accro aux nouvelles technologies comme vous !

Ce n'est pas non plus parce que votre destinataire peut vous répondre qu'il va forcément le faire : c'est l'avantage du mail et des SMS. Si vous voulez une réponse immédiate, allez parler directement à la personne concernée ou téléphonez-lui !

Un peu impatient ? Apprenez à gérer votre stress !

Envoyer des mails pro le week-end

La règle de bienveillance professionnelle impose de ne pas envoyer de mail le week-end :

- Pour éviter de passer pour un supérieur qui abuse de ses subalternes.
- Pour ne pas risquer de devenir un « accro au travail ».
- Parce qu'en cas d'urgence, le téléphone reste de rigueur.

Lire ses mails le soir rend moins efficace le lendemain

Oublier l'objet

Précipitation ou simple manque d'imagination, le champ « objet » mérite toute votre attention que ce soit pour un message pro ou perso. En effet, il permet :

·13 d'être pris au sérieux par son interlocuteur ;

·14 au récepteur de traiter plus efficacement l'information (urgent – important) ;

·15 à tous de retrouver facilement la discussion.

Bon à savoir : lors de l'envoi d'une candidature, n'oubliez sous aucun prétexte d'ajouter un objet à votre e-mail. En effet, le recruteur classe ses candidats en fonction de l'objet avant d'ouvrir le message.

Abuser des gifs

Les gifs animés peuvent être des smileys mis à votre disposition dans un administrateur d'e-mail, ou des extraits très courts de films ou séries trouvés sur Internet.

Souvent, en utilisant des références communes, des chaînes de mail usent et abusent de ces petits plus ludiques. Mais attention !

·16 Les gifs sont à proscrire des messages professionnels.

·17 Avec parcimonie, c'est drôle, systématiquement, ça l'est moins.

Abuser des majuscules

En langage Internet, l'usage des majuscules symbolise le cri.

Imaginez un instant mener une discussion essentiellement constituée de cris et vous comprendrez pourquoi les majuscules restent incompatibles avec une communication numérique saine !

Ne jamais lire ses mails

C'est tentant quand on sait que bien plus de la moitié des mails qu'on reçoit chaque jour sont des spam... Cependant, le mail étant un moyen de communication répandu et utilisé par les administrations, ne pas ouvrir ses mails peut vous faire rater une information importante.

Bon à savoir : saviez-vous que le mot français pour spam est pourriel ?

Mal écrire les noms propres

Avant d'écrire à une personne, assurez-vous de bien orthographier son nom en vérifiant sur vos documents personnels ou en quelques clics sur Internet.

Une mauvaise orthographe :

·18 Vexe, même les personnes peu susceptibles.

·19 Vous fait passer pour une personne peu consciencieuse.

·20 Vous disqualifie d'office pour un rendez-vous ou toute requête mentionnée dans votre message.

Scannez les clés USB

Un ami vous remet une clé USB avec des fichiers qu'il a téléchargés ? Scannez le contenu de cette clé USB à l'aide de votre antivirus. Cet ami a peut-être téléchargé un programme malveillant sans le savoir…

Même si aujourd'hui le scan par antivirus est devenu automatique pour tout périphérique branché ou tout document téléchargé, vous n'êtes pas à l'abri d'un nouveau virus qui se glisserait entre les mailles du filet. Aussi, si vous avez un doute, ne transférez rien sur votre ordinateur.

Bon à savoir : éjectez systématiquement vos périphériques USB manuellement ! En effet, les systèmes d'exploitation utilisent parfois ces petites extensions de mémoire pour stocker momentanément des données. Si le retrait est brutal, cela peut causer des problèmes de « corruption de données ».

Mettez vos systèmes à jour

Les 2 inconvénients majeurs des mises à jour, ce sont le temps nécessaire à leur installation et la place qu'elles prennent sur votre disque dur. Souvent, elles se mettent en marche au moment où vous avez besoin de toute la mémoire RAM de votre ordinateur…

Mais cela étant dit, en maintenant votre machine à jour, elles permettent de corriger des failles repérées dans le système, le navigateur ou tout autre programme, les rendant plus performants et plus sécurisés. Paramétrez donc les mises à jour en installation automatique !

Bon à savoir : les mises à jour de l'antivirus intègrent des protections contre les nouveaux virus repérés depuis la dernière mise à jour. Bien sûr, si un nouveau virus a été développé le jour même et tente d'infecter votre machine, vous ne serez pas protégé, mais cela reste rare !

Les mises à jour sont indispensables, même pour votre assurance habitation !

N'utilisez pas de copie

Bien sûr on trouve sur Internet des copies de Windows ou Mac OS pas chères, mais elles ne sont pas fiables. Même chose en ce qui concerne les antivirus !

On trouve des programmes « craqués » gratuitement, mais ils sont généralement moins performants que les originaux et leur téléchargement vous expose aux pirates du web !

Note : les ingénieurs qui conçoivent ces logiciels ne sont pas bêtes. S'ils ne peuvent pas empêcher des professionnels de craquer leurs programmes, ils peuvent limiter les fonctions des versions piratées.

4 conseils pour choisir un mot de passe sécurisé

Vos données sur Internet peuvent être importantes. Pour les protéger, il vous faut choisir un mot de passe sécurisé. Voici quelques conseils pour le trouver.

Ne pas utiliser le même mot de passe pour différents sites

50 % des internautes gardent toujours le même et pourtant, c'est une très mauvaise idée !

- Non seulement vous répétez souvent les mêmes frappes sur le clavier et rendez ainsi votre mot de passe plus facile à identifier.
- Mais en plus une fois qu'on l'a trouvé, on peut accéder à tous vos comptes.

Vous pouvez néanmoins utiliser le même mot de passe pour différents sites de moindre importance.

Par exemple, un mot de passe pour les sites marchands, à condition de ne pas laisser vos coordonnées bancaires, un mot de passe pour les forums auxquels vous participez, etc. En revanche, utilisez un mot de passe unique pour les sites à données sensibles : messagerie, réseaux sociaux, banque, Sécurité sociale, etc.

Changer régulièrement de mot de passe

Si vous utilisez le même mot de passe depuis des années, nul doute que des hackers l'ont déjà repéré et que vous l'avez déjà confié à quelques proches.

Pour augmenter la sécurité de vos données, changez de mot de passe régulièrement, surtout pour votre messagerie. En effet, celle-ci contient des données hautement confidentielles, notamment d'autres mots de passe pour différents comptes.

Alors soyez plus prudent que 90 % des internautes !

Choisir un bon mot de passe

Un bon mot de passe, ce n'est pas un mot du langage courant suivi de la lettre 1 ou du symbole ! Ceux-là sont faciles à craquer.

Un bon mot de passe, c'est une suite de lettres, de chiffres et de symboles imprononçables, incluant des majuscules et des minuscules. Malheureusement, ceux-là

sont difficiles à retenir.

Pour vous aider, utilisez un moyen mnémotechnique.

Par exemple, choisissez une phrase dont vous vous souviendrez : « mon premier chat s'appelait Artiste ». Le mot de passe devient : M1cA@!

Les mots de passes proscrits !

Autant sur smartphone que sur ordinateur, des mots de passe reviennent très souvent, pour plusieurs raisons :

- Ils sont faciles et rapides à taper.
- Ils ne débloquent « que » l'écran de veille.
- … mais beaucoup de gens finissent par utiliser ces mots de passe simples de partout !

Quelques mots de passe plus répandus qu'il n'y paraît, et totalement interdits pour un accès sécurisé :

- 123456 ;
- mot de passe ;
- azerty.

Votre ordinateur est certainement l'objet avec lequel vous passer le plus de temps, après votre smartphone. Il est donc primordial de bien sécuriser les différents accès personnels auxquels vous vous connectez.

Il est plus simple que vous ne le croyez de dénicher des indices sur les mots de passe. Aussi, soyez vigilant et n'oubliez jamais de vous déconnecter !

Ne pas se creuser la tête pour inventer un mot de passe comporte des risques pour votre sécurité sur la toile. Le problème? Vous n'êtes ni le premier ni le dernier à avoir eu l'idée. Et les pirates informatiques ne le savent que trop bien. Retour sur les pires mots de passe.

Cette année, le mot de passe « 123456 » est le champion toutes catégories. Cette suite de chiffres a détrôné le mot de passe « mot de passe » (ou « password » qui fonctionne aussi très bien à l'international). C'est le bilan qu'a dressé la société américaine SplashData, spécialisée dans la sécurité informatique. Dans la liste annuelle des mots de passe les plus utilisés, c'est la première fois que « mot de passe » n'est pas premier.

Des mots au hasard avec des chiffres

On retrouve ensuite les cadors comme « 12345678 » à la troisième place pour la version améliorée et moins fainéante du champion. « Qwerty » se place toujours très bien ensuite

(en France c’est « azerty ») suivi de « abc123 » pour ceux qui pensaient pourtant avoir bien trompé leur monde. Très belle et romantique progression du « iloveyou » qui se place maintenant 9e.

SplashData, qui est une société vendant des applications gérant les mots de passe, tient à rappeler que prendre comme mot de passe le nom du site où l’on s’inscrit présente des risques pour la sécurité informatique. Un petit rappel en raison de l’arrivée dans le top des mots de passe tels que « adobe123 » et « photoshop ».

En fait, il est conseillé tout simplement d’utiliser des phrases secrètes faites de mots pris au hasard, avec des chiffres et des variations majuscules/minuscules. Faciles à retenir et difficiles à décoder.

Logiciel à télécharger pour la protection des mots de passe : KeyScrambler