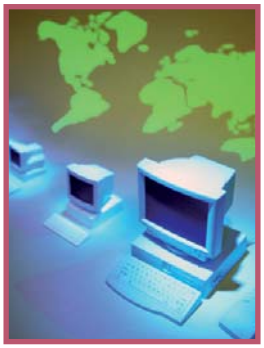


SÉCURISER ET PROTÉGER SON ORDINATEUR

85% des menaces pouvant mettre en péril la sécurité de votre ordinateur viennent d'Internet et 200 000 nouvelles menaces apparaissent chaque jour. Pas de panique ! en adoptant le bon comportement et en privilégiant la prévention, vous limitez les risques sans bien évidemment pouvoir les exclure totalement.

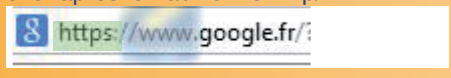
La bonne attitude

Règle numéro 1 : conserver son autonomie d'action, c'est-à-dire ne jamais faire quelque chose parce que l'on vous le propose, mais uniquement parce que vous l'aurez décidé.
Règle numéro 2 : lorsque l'on a des doutes sur une action, on ne la fait pas !

A suivre, pêle-mêle, quelques conseils permettant d'éviter un certain nombre de désagréments :
- Réserver un PC à l'usage professionnel.
- A propos des téléchargements :
Être sûr de ce que l'on télécharge. Il y a souvent d'autres logiciels ou toolbars qui s'installent en même temps. Il est donc important de bien lire et de décocher tout ce qui ne fait pas l'objet du téléchargement choisi.

ASTUCE !
Après un téléchargement, allez vérifier les derniers logiciels installés en allant dans : panneau de configuration/programmes/ installer-désinstaller un programme/ et cliquer sur la date pour classer par date de téléchargements. Vérifier qu'à la date précise de votre téléchargement il n'y ait pas d'autres logiciels installés. Si oui, supprimez les.

- Ne pas cliquer trop vite sur des liens (même et surtout dans les mails) ou sur les pop-up (fenêtres intempestives qui s'ouvrent sans action de votre part), même et surtout si celles-ci vous proposent d'améliorer les performances de votre ordinateur.
- Vérifiez que le site sur lequel vous êtes est sécurisé : dans ce cas un "s" va s'afficher après le traditionnel http/



- Bien choisir vos mots de passe (un mix de majuscules, minuscules, chiffres). Une banque ou une administration ne vous demanderont JAMAIS de leur communiquer.
- Sauvergardez régulièrement votre PC et faites des sauvegardes sur des supports externes. Ces derniers doivent être vérifiés de temps en temps par votre antivirus.
- Soyez méfiant, mais pas parano. Ex : un mail d'un correspondant, avec qui vous correspondez en français, écrit en anglais devra forcément vous inspirer de la méfiance.
- Pour vos achats évitez les petits sites peu connus et/ou à l'étranger. Préférez ceux qui ont pignon sur rue.
- Le phishing : encore appelé le hameçonnage est une technique utilisée par les fraudeurs pour tenter de récupérer des coordonnées bancaires ou toute autre donnée personnelle dans un but d'utilisation frauduleuse (codes d'accès à votre boîte mail, identifiants de connexion sur divers espaces personnels...). Pour cela, ils se font souvent passer pour une boutique en ligne, une banque, un fournisseur d'accès Internet ou encore des organismes gouvernementaux comme les impôts ou la CAF par e-mail. Les pirates ont beaucoup d'imagination et toujours un temps d'avance. Sachez repérer les signes suspects :
• De nombreuses fautes d'orthographe (mais ils ont pris des cours et il y en a de moins en moins).
• Des logos ou données obsolètes.
• Des liens pointant vers une adresse inconnue qui vous paraît douteuse.
• Des messages comportant des histoires irréalistes comme un héritage soudain ou une offre exceptionnelle ou ayant un caractère d'urgence.
• Faites attention à l'adresse e-mail complète de l'expéditeur : ce qui est après l'@ comporte un nom de domaine par ex @ celui de votre banque et non l'inverse : le nom de la banque avant @.
• Une demande des données personnelles comme des codes personnels.

Un PC bien protégé

Pour être correctement protégé, il faut :
- **Commencer par faire un check-up** de ce qui est installé sur son ordinateur en allant dans Panneau de configuration/système et sécurité/ centre de maintenance/ clic sur la flèche pour ouvrir "sécurité". Vous aurez ainsi l'indication de ce qui est activé ou pas.
- **Vérifiez que vos mises à jour programmes** ont bien été faites régulièrement, sinon faites-les. Ces dernières (ou up-date) servent à améliorer les performances et la sécurité des logiciels

SÉCURISER ET PROTÉGER SON ORDINATEUR- suite

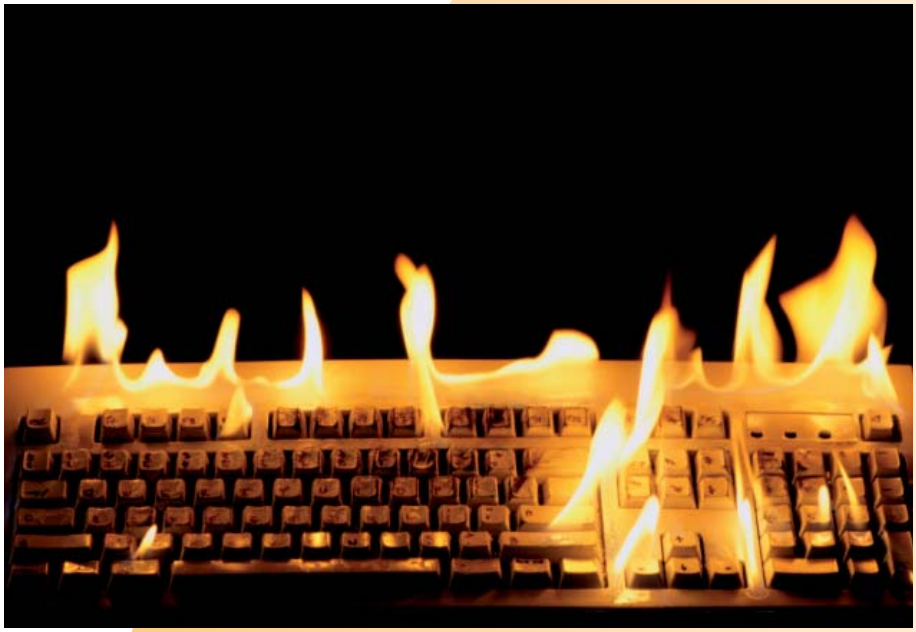
installés sur votre ordinateur. Outre les logiciels propres à votre activité, on peut noter les logiciels suivants à mettre à jour régulièrement : Windows, l'antivirus et les antimalwares, Adobe Reader, Java.

- **Avoir un antivirus et un seul.** Les logiciels gratuits comme AVAST, AVG, WINDOWS Essentiels sont généralement suffisamment performants. Attention lorsque l'on installe un antivirus, il est utile de procéder à quelques paramétrages.
- **Ainsi qu'un pare-feu ou encore firewall** : il fonctionne comme une porte coupe-feu et vérifie toutes les connections avec l'extérieur. On peut se contenter de celui de Windows 7 et 8.
- **Enfin un antispyware et un antimalware :** le premier sert à éliminer les logiciels espions et le second les logiciels qui, entre autres, essaient de récupérer vos données personnelles. Ils viennent compléter l'antivirus. Il est possible d'en installer plusieurs. On notera "Spybot search and destroy" ainsi que "Malwarebytes" et "Rogue Killer".

Leurs téléchargements peuvent se faire sur les site 01.net ou Clubic, où le téléchargement est légal. Lorsque l'on télécharge un logiciel, il est bon de vérifier s'il est en français, s'il est gratuit, sur quel système d'exploitation il fonctionne, s'il est souvent téléchargé, etc. Le fait de télécharger légalement un logiciel gratuit n'exclue toutefois pas le risque d'introduire des éléments malveillants dans son ordinateur.

Outre le fait de protéger son ordinateur avec un antivirus, il est conseillé de verrouiller sa session par un mot de passe et de protéger son réseau wi-fi par une clé WPA et non WEP.

- Pour prémunir sa boite mail, on peut utiliser un antispam.
- **Nettoyer régulièrement son PC** : avec un outil de nettoyage comme C Cleaner.■



ASTUCE !

Conserver sur une clé les logiciels Rogue Killer et Malwaresbytes. S'il n'est plus possible de démarrrer le PC normalement suite à un "virus", et a fortiori de les télécharger pour résoudre le problème, il sera fort utile de les lancer au démarrage de l'ordinateur en mode sans échec par exemple.

ASTUCE !

Consultez le portail de la sécurité informatique du gouvernement en cliquant sur le lien ci-dessous

http://www.securite-informatique.gouv.fr/gp_rubrique34.html