

**Internet : Des conseils pour contrer les menaces de l'Internet.**

**Internet**

Post   par : JPilo

Publi  e le : 29/3/2013 13:30:00

Quelle que soit la solution de protection antivirale install  e sur un PC, la premi  re barri  re aux malwares et autres "cancrelats" du Net consiste    respecter quelques r  gles, voici donc des conseils afin d'  viter la catastrophe.   Le plus risible dans tout cela, c'est que ces conseils, nous les connaissons   tous sur le bout du pouce.

**Alors, r  p  ter des conseils portera bien un jour ses fruits.**

**1. N  ouvrez jamais les pi  ces jointes aux e-mails.**

L  e-mail n  a pas   t   invent   pour envoyer des fichiers et encore moins des programmes ou des archives comportant des programmes. M  fiez-vous   galement des photos jointes aux e-mails, certaines pouvant masquer des intentions malveillantes.

**2. Ne r  pondez pas aux e-mails ind  sirables ou spontan  s.**

Si vous recevez un e-mail automatique d   une liste de diffusion    laquelle vous ne vous   tes pas abonn  , ne r  pondez pas et ne vous d  sabonnez pas non plus. Vous ne ferez qu   indiquer au spammer que vous avez re  u et lu son e-mail : vous risquez alors de recevoir bien plus de spams.



**3. N  achetez jamais rien qui vous a   t   recommand   par un e-mail ind  sirable.**

Les offres relayées par des spams semblent souvent trop séduisantes pour être honnêtes, et c'est généralement le cas ! Evitez d'acheter tout produit ou service recommandé par un e-mail douteux.

**4. Ne cliquez jamais sur les liens d'e-mails qui vous pressent de faire quelque chose.**

Face à un message super urgent ou si l'on vous fait une offre incroyable (sur le point d'expirer), ne cliquez jamais sur le(s) lien(s) proposés et ne divulguez jamais d'information. Supprimez l'e-mail.

**5. Votre banque ne vous enverra et ne vous demandera jamais d'informations personnelles par e-mail.**

Si vous recevez un e-mail de votre banque vous demandant des informations personnelles ou vous invitant à valider des détails personnels, ne répondez pas. Jamais une banque ne procéderait ainsi par e-mail.

**6. Ne répondez à aucun e-mail qui vous demande des informations personnelles ou confidentielles.**

Quoique l'on vous promette en échange d'informations personnelles, ne donnez pas suite. L'utilisation potentielle de vos données risquerait de vous porter préjudice.

**7. Utilisez des mots de passe compliqués à deviner.**

Créez des mots de passe complexes, difficiles à deviner. Cliquez ici pour obtenir des conseils de création de mots de passe.

**8. Utilisez des mots de passe différents pour vos différents comptes.**

Plus vous aurez de mots de passe, plus il sera difficile pour un hacker ou voleur d'obtenir l'accès à vos différents comptes.

**9. N'enregistrez jamais votre mot de passe sur un ordinateur qui ne vous appartient pas.**

Pour vous inciter à revenir plus facilement, certains sites vous proposent d'enregistrer vos identifiants sur l'ordinateur utilisé. Ne cochez pas cette option si vous n'utilisez pas votre propre PC ou terminal sécurisé.

**10. N'installez pas tous les programmes que l'on vous suggère.**

Les sites Web vous proposent fréquemment d'installer des programmes « gratuits ». Ces pratiques occasionnent parfois des dommages collatéraux. Avant de télécharger quoi que ce soit, assurez-vous que l'entreprise ou le produit proposé sont de confiance.

**11. Utilisez un antivirus.**

Ne facilitez pas la vie des cybercriminels. Il existe des solutions antivirus gratuites et payantes pour toutes les plates-formes.

**12. N'utilisez pas n'importe quel dispositif USB vous tombant sous la main.**

Les dispositifs USB (clés, cartes SD, disques durs, etc.) contiennent souvent des programmes malveillants qui s'activent dès que vous connectez le dispositif à un ordinateur. Faites toujours

un scan de vérification de ces dispositifs avant de les utiliser.

**13. Verrouillez l'accès à votre ordinateur quand vous n'êtes pas à proximité.**

Ne laissez jamais votre espace de travail ou votre bureau inoccupé sans verrouiller votre ordinateur. En protégeant l'accès par un mot de passe, vous éviterez qu'un tiers ne s'infilte dans vos fichiers.

**14. Protégez l'accès à votre Smartphone et configurez-le pour qu'il s'auto-verrouille.**

Protégez toujours votre Smartphone par un mot de passe ou un geste et programmez-le pour qu'il s'auto-verrouille au bout d'une minute d'inactivité. Ainsi, en cas de vol, il sera plus difficile pour quiconque d'accéder à vos données.

**15. Les Smartphones sont de petits ordinateurs, à utiliser avec prudence.**

Les Smartphones ne sont rien de moins que de petits ordinateurs qui offrent des capacités comparables de connectique, de mémoire et de vol d'informations personnelles. Oh ! Et ils permettent aussi de passer des appels téléphoniques et d'envoyer des SMS.

**16. Vous ne devez pas manquer à personne sur les réseaux sociaux.**

Les e-mails expéditeurs connus ou inconnus qui prétendent que vous leur manquez sont probablement des spams. Vous savez quoi faire des spams : les supprimer.

**17. Vous n'êtes jamais le millionième visiteur.**

Vous avez déjà vu ces bannières clignotantes sur des sites Web qui vous informent que vous êtes le millionième visiteur et que vous avez donc gagné un prix incroyable ? Eh bien, ces bannières affichent toujours le même message. Et il n'y a jamais rien là-dessus.

**18. Ne publiez jamais de photos embarrassantes sur Facebook.**

Même si vous n'avez que peu d'amis en ligne, vos photos (embarrassantes ou non) risquent d'être vues par des personnes dont vous ne voudriez pas qu'elles les voient. Des proches, votre patron, etc.

**19. Ne vous prenez jamais nu en photo ; même si vous êtes agréable à regarder.**

Une fois que de telles photos ont quitté votre ordinateur ou votre Smartphone, il devient impossible de les récupérer et elles risquent bien de revenir vous hanter un jour ou l'autre.

**20. Internet n'oublie jamais.**

La capacité de stockage d'informations sur Internet est illimitée. Vos documents ou photos pourraient bien se rappeler à vous au moment où vous vous y attendez le moins. Même si vous supprimez l'original, il est fort probable que quelqu'un l'ait enregistré et copié quelque part.