

Cloudmark : Cinq conseils de protection contre les attaques de SPAM

S curit 

Post  par : JPilo

Publi e le : 26/11/2010 14:00:00

Aussi bien au bureau qu   la maison, le spam engendre maux de t te et perte de temps, vous obligeant   parcourir votre bo te mail pour trier les messages l gitimes des ind sirables. C est aga sant, fastidieux et souvent dangereux pour la sant  de votre ordinateur.

D apr s une r cente  tude internationale r alis e par **Harris Interactive pour Cloudmark**, pr s de la moiti  des utilisateurs europ ens (44%) d clarent avoir re su davantage de spams en 2010 et affirme qu il est de plus en plus difficile de les distinguer des messages l gitimes.

Afin de surmonter les probl mes croissants li s aux pourriels, Cloudmark, le sp cialiste de solutions anti-spam, a publi  un guide pour aider les internautes   r duire, identifier et g rer les messages ind sirables.

1) Prenez garde aux spams provenant de r seaux sociaux



CLOUDMARK

AntiSpam

En raison de la popularit  grandissante des r seaux sociaux, la prolif ration de spams envoy s par ce biais s accro t chaque mois. Des techniques d ting rie sociale sophistiqu es compliquent la distinction entre messages l gitimes et malveillants. De plus, elles permettent aux spammeurs d obtenir plus de d tails sur la vie priv e de leurs cibles et ainsi de nuire davantage   leurs victimes. Selon l tude Cloudmark, 35 % des adultes en Europe attestent avoir re su des spams via les r seaux sociaux d une mani re ou d une autre (comme une invitation   rejoindre un groupe d amis sur Facebook ou MySpace) ces 12 derniers mois. Les spams envoy s sous la forme d un message provenant d un r seau social populaire peuvent  tre beaucoup plus difficiles   distinguer que les spams classiques. Ainsi, attention   toujours vous connecter correctement   votre r seau social pour r pondre aux messages et d ajouter des amis, par exemple, au lieu de cliquer directement sur des liens dans un message suspect.

Outre l envoi de faux messages, les spammeurs exploitent  galement les r seaux sociaux pour envoyer directement leurs spams. Bien souvent, un faux compte est cr  , puis le spammeur attend d avoir de nombreux amis pour envoyer les spams via ces sites. Alors,

assurez-vous de toujours connaître la personne que vous ajoutez, au lieu de chercher à augmenter le nombre de vos contacts!

2) Sachez répondre correctement

Si vous recevez effectivement des spams, prenez garde à ne pas y répondre. Cloudmark révèle que parmi les utilisateurs européens ayant répondu à un spam, 54% déclarent en avoir reçu davantage par la suite. Au lieu de répondre à un pourriel, vous pouvez signaler le message à votre fournisseur d'accès à Internet (FAI) anti-spam, en général en cliquant sur le message et en le marquant comme un message indésirable.

Vous inscrire auprès d'un organisme spécialisé comme Signal spam par exemple qui vous alerte si des activités malveillantes sont menées en votre nom constitue également une bonne initiative.

3) Ne cliquez pas sur les liens des messages non fiables à 100%

Envoyer des messages malveillants avec de fausses pièces jointes et /ou liens constitue toujours l'un des outils principaux des fraudeurs. Pour eux, c'est souvent très particulièrement simple de masquer l'adresse e-mail d'envoi et de falsifier le lien sur lequel ils souhaitent que vous cliquiez. Ainsi, si vous recevez un message contenant des liens de votre banque, d'un site de commerce en ligne sur lequel vous vous rendez ou d'un site de réseau social ; au lieu de cliquer sur les liens du message, rendez-vous directement sur votre navigateur pour effectuer l'action demandée. Cette méthode vous permet de découvrir rapidement si cette demande est légitime et vous évite de vous rendre sur un site de phishing [1] ou sur un site web injectant un code malveillant sur votre ordinateur. Agissez avec la même prudence pour les messages provenant des de vos amis : les spammeurs sont de plus en plus rusés et peuvent souvent infecter un ordinateur en envoyant des messages semblant provenir des adresses e-mails de votre carnet d'adresses afin de paraître plus légitimes.

4) Maintenez à jour le système d'exploitation et le logiciel de sécurité de votre ordinateur

Même si vous disposez d'un logiciel de sécurité performant (comme un antivirus, un antimalware, etc.), celui-ci ne vous protégera que s'il est mis à jour régulièrement. Ainsi, pensez à autoriser votre logiciel à se mettre à jour automatiquement depuis Internet. La majorité des logiciels de sécurité offrent désormais des mises à jour régulières conçues pour répondre aux dernières vulnérabilités. Ainsi, si votre logiciel ne propose pas cette option, envisagez d'en changer : il existe de nombreuses versions gratuites et performantes pour les utilisateurs. Vous devriez également vous assurer que vous disposez des dernières mises à jour de votre système d'exploitation (XP, Windows 7, etc.), de vos applications (en particulier les visionneuses de PDF) et de vos navigateurs Internet (comme Internet Explorer, Firefox et Chrome).

5) Installez une application anti-spam dédiée

Installer simplement un antivirus sur votre ordinateur ne vous protégera pas des spams, il est ainsi primordial d'installer un filtre anti-spam distinct pour garantir que seuls les messages légitimes arrivent dans votre boîte de réception. Les spams ne constituent pas seulement une nuisance, mais peuvent souvent être également dangereux. Un volume significatif d'attaques de phishing et de virus provient en effet des messages (comme les liens vers des sites infectés intégrés dans un message). 44% des adultes européens ayant reçu des spams déclarent qu'il est de plus en plus difficile de distinguer les spams des messages légitimes. Cependant, 35% de ces personnes affirment qu'ils ne disposent d'aucune forme de protection anti-spam sur leur ordinateur sur lequel ils utilisent le plus souvent leur messagerie.

Voilà une statistique très inquiétante.