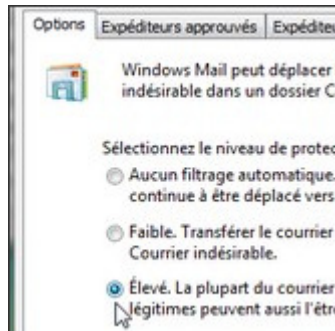


Internet : Internet Explorer

Le Top 10 des astuces pour limiter le spam

Selon diverses études, le spam aurait représenté plus de 95% du trafic Internet des emails en 2007! "*Fléau*" semble désormais un terme bien insuffisant pour décrire l'ampleur du phénomène... Outre l'évidente perte de temps qu'ils engendrent, les spams sont aussi les premiers vecteurs de codes malveillants. S'il paraît bien impossible de les éradiquer intégralement, on peut tout de même lutter efficacement contre. Voici 10 conseils pratiques à mettre en oeuvre dès aujourd'hui.

Étape 1/10



1- Ne jamais répondre à un email non sollicité

Vous ne devez jamais répondre à un email non sollicité. Répondre, c'est le meilleur moyen de confirmer l'existence de votre adresse email (certains spams sont envoyés à des adresses générées automatiquement par des algorithmes) et d'en recevoir davantage encore. En outre, l'adresse d'expédition est parfois celle d'un pauvre innocent qui se prend alors votre email en spam supplémentaire.

Étape 2/10

2- Ne jamais cliquer sur les liens d'un email non sollicité

Ne pas répondre à un spam, cela signifie également ne jamais cliquer sur l'un des liens compris dans l'email. Grâce à ces liens, les cybercriminels:

- savent que votre adresse est réelle.
- peuvent envoyer un code malveillant exploitant les failles de votre système et infecter votre machine.
- peuvent vous amener à saisir des informations personnelles qui seront détournées à d'autres fins.

Notamment, il ne faut jamais cliquer sur les liens "*se désinscrire*" ou "*unsubscribe*" puisqu'ils vous redirigent vers un site géré par les spammeurs. N'oubliez pas que bien des antivirus actuels ne vous protègent pas des attaques Web de type "*WebStorm*" ou "*Drive-by Download*".

Étape 3/10

3- Utiliser plusieurs adresses email

Tous les FAI vous permettent de définir plusieurs adresses email.

Dans l'idéal, vous devriez avoir :

- Un compte email FAI pour correspondre avec vos amis.
- Un compte email FAI pour tout ce qui a trait aux transactions bancaires.
- Un compte email type WebMail (Gmail, Hotmail) pour les newsletters auxquelles vous souhaitez être abonné sans pour autant être certain de conserver l'abonnement longtemps.

Étape 4/10

4- Utiliser les Webmails temporaires

Utilisez, et même au moindre doute abusez, des services Internet qui vous fournissent une adresse email dont la durée de vie, en général, ne dépasse pas la journée.

Ces comptes temporaires sont vraiment très pratiques pour tout ce qui est inscription dans les forums, inscription sur les sites, inscription dans un logiciel, activation de logiciels gratuits, etc. En effet, la plupart du temps, il est nécessaire de confirmer la validité pour valider l'inscription. Mais une fois l'inscription validée, il n'y a aucune raison que l'éditeur/le site ait encore besoin de vous contacter, sauf pour des emails non sollicités et la plupart du temps indésirables!

Le principe de ces services temporaires est simple: vous vous connectez sur le service, celui-ci vous attribue une adresse temporaire, vous l'utilisez pour vous inscrire sur le forum, le site ou le logiciel. Le service vous permettra de consulter tout email arrivant sur l'adresse temporaire afin que vous puissiez valider les inscriptions. Une fois que vous quittez le service, l'adresse disparaît automatiquement. C'est pratique, discret, et terriblement efficace contre le spam.

Il existe de nombreux services Webmails temporaires dont les plus connus sont:

www.Kasmail.com
www.GuerillaMail.com
www.10minutemail.com

Étape 5/10

5- N'affichez jamais les images des emails HTML

Ne demandez jamais l'affichage des images dans les emails HTML. La plupart des clients de messagerie modernes (Outlook, Windows Live Mail, Vista Windows Mail, Thunderbird 2, mais aussi Yahoo Mail ou Hotmail) n'affichent pas les images des emails HTML. Ils bloquent également les cookies et codes Javascripts incorporés dans ces emails HTML. Mais certains utilisateurs modifient le comportement de leur client de messagerie pour les afficher. C'est une très mauvaise idée car ces images sont utilisées pour analyser votre comportement, récupérer votre IP, valider votre email, etc.

Étape 6/10

6- Ne publiez jamais votre adresse sur le Web

Ne publiez jamais votre adresse email réelle sur le Web, que ce soit sur votre blog, sur votre page personnelle (Homepage), sur les forums, etc.

En effet, des moteurs automatiques balayent la toile à longueur de journée pour récolter des adresses. Si vous voulez vraiment que l'on puisse vous contacter par email, utilisez soit des systèmes de formulaires de saisie (notamment sur votre propre site Web), soit des adresses "*alias*" (de fausses adresses publiques qui redirigent ensuite les emails vers une véritable adresse). Si le spam devient trop important, il suffit simplement de supprimer l'adresse "*alias*" et d'en créer une nouvelle.

Exemple de services fournissant des "*Alias d'emails*":

www.jetable.org
www.spamgourmet.com
www.sneakemail.com

Étape 7/10

7- Activez l'antispam de votre FAI

Aujourd'hui, tous les FAI (ou presque) proposent une option "antispam" sur le compte email. Attention, nous ne parlons pas des services antispam payants que l'on doit installer sur son PC, mais bien d'un système antispam incorporé aux serveurs de messageries qui se charge de nettoyer les flux d'emails avant qu'ils n'atteignent votre messagerie. Ces options sont souvent gratuites et désactivées par défaut. Pensez à vous connecter sur le site du FAI pour valider l'option.

Un nettoyage au niveau des serveurs de messagerie du FAI est très pratique:

- Ils sont efficaces et suppriment 90% des spams qui vous sont destinés.
- Ils limitent la quantité de courriers inutilement téléchargés et envoyés vers votre PC. N'oubliez pas que la plupart des Webmails proposent également un tel service antispam.

Étape 8/10

8- Utilisez un client de messagerie avec antispam

Microsoft Office Outlook, Windows Live Mail et Vista Windows Mail possèdent en standard un mécanisme antispam/antiphishing plutôt efficace. Pensez à l'activer. Mozilla Thunderbird 2 possède également une fonction antispam. Sans être efficace à 100%, ces filtres intégrés transfèrent automatiquement vers un dossier "Courrier indésirable" la très grande majorité des spams que vous recevez. Cela dit, pensez à utiliser très régulièrement Windows Update, car les mécanismes antispam des clients de messagerie de Microsoft sont régulièrement mis à jour par ce biais. Certaines suites de sécurité disposent également d'outils antispam qui peuvent s'avérer parfois supérieurs à ces mécanismes standards. Il existe également de nombreux outils antispam gratuits et différents services dédiés à la lutte contre le spam. Si vous continuez à recevoir beaucoup trop de spams, songez à les mettre à l'essai...

Étape 9/10

9- Refusez les envois lors des inscriptions

La plupart du temps, lorsque vous devez remplir un formulaire d'inscription sur un site, un service ou un logiciel, on vous demande de cocher une case (parfois même, celle-ci l'est par défaut) autorisant la société à envoyer des informations par email. Lisez très attentivement le message (certains sont tournées de telle sorte que c'est en décochant que vous autorisez l'envoi des courriers!) et agissez de façon à refuser tous les types d'envoi suggérés. Et surtout, rappelez-vous: n'utilisez jamais votre véritable adresse email, mais soit un alias soit un email jetable.

Étape 10/10

10- Ignorez les "Delivery Failures" et ne participez pas aux chaînes Ignorez systématiquement tous les emails qui vous disent que tel ou tel email soi-disant envoyé par vous n'a pas été reçu ou a été détecté comme infecté. Jetez ces emails, inutiles de les lire! C'est encore un vecteur de spam... ou le fruit d'un virus ayant infecté une autre machine que la vôtre (celle d'un de vos contacts). Et surtout, ne participez pas à la diffusion des "chaînes", ces fameux emails qui soit: - vous annoncent un super-nouveau-hyper-méga-violentissime-dangereux virus, - vous annoncent des changements de service, l'annulation d'un service, la refonte d'un service et qui sont soi-disant signés par le président de Microsoft, MSN, Yahoo, Google ou n'importe quelle autre entreprise publique, - vous annoncent mille et un bonheurs et merveilles, et qui dans tous les cas vous encouragent à envoyer l'email au plus grand nombre, ou à vos 10 amis les plus chers, etc. Refusez systématiquement ces chaînes... Ne participez pas, vous aussi, à la multiplication des emails indésirables sur le réseau! Ne perdez jamais de vue que la sécurité d'Internet est aussi l'affaire de tous, et que nous y jouons tous un rôle par notre naïveté, notre excès de confiance, ou notre manque de vigilance...