# Les dangers et menaces sur Internet
(virus, espions, spams, pirates…)

## Introduction

Aujourd'hui, plus de 23 millions de Français surfent sur Internet et la France est en passe de rattraper son retard en matière d'équipement numérique, avec une augmentation de 12 % des ventes d'ordinateurs en 2003 et une croissance de 123 % des foyers connectés à l'ADSL. Internet est une mine d'informations illimitée. Trouver la recette de son plat préféré, retrouver ses camarades de lycée, regarder le programme télé, rechercher un numéro de téléphone oublié ou le plan pour se rendre en vacances... Sur Internet, quand on cherche... on trouve, même des informations fausses, voire interdites. Infos, fichiers audio et vidéo, achats en ligne, échanges de mails, chats, jeux en réseau, mais aussi virus, espions, spams, piratage, hoax (canulars)…, Internet offre le meilleur comme le pire.

Les journaux télévisés évoquent souvent les dangers et menaces lorsqu'ils parlent d'Internet. Ces dangers sont bel et bien réels, mais avec quelques conseils et astuces, on peut éviter ce genre de tracas et contourner les chausse-trappes. Petit tour d'horizon des principaux risques et recommandations pour surfer avec le maximum de sécurité.

---

## Sommaire

## 1/ Les virus

### Définition

Un virus est un petit programme dont le but est de se dupliquer sur d'autres ordinateurs. L'objectif recherché ou non est de perturber ou d'abîmer plus ou moins gravement le fonctionnement de l'ordinateur infecté, voire donner à un pirate le moyen de le contrôler à distance. Les virus peuvent se propager à travers tout moyen d'échange de données numériques comme l'Internet, mais aussi les disquettes, les cédéroms, etc.

Cette désignation vient de l'analogie avec le virus biologique puisqu'il présente des similitudes dans sa manière de se propager et de se reproduire. À chaque fois que l'utilisateur exécute le programme "infecté" (caché dans un fichier anodin, une image, un logiciel de jeu…), il active le virus qui en profite pour aller s'intégrer dans d'autres programmes exécutables ou se dupliquer via Internet.

Ils peuvent provoquer des dégâts très différents : blocage de Microsoft Office, destruction de fichiers ou de toutes vos données, voire de votre système d'exploitation…

Les virus se propagent surtout par l'Internet et 99 % des attaques s'effectuent aujourd'hui par courriel, notamment par l'intermédiaire des pièces jointes.

**Voici quelques conseils pour déjouer les pièges des virus :**

1. **Ayez un Antivirus À JOUR.**
   Il est indispensable de posséder un anti-virus performant (par exemple : Norton Antivirus ou MacAfee).
   Avec une connexion haut débit que l'on a tendance à laisser ouverte en permanence, le logiciel antivirus est devenu un complément indispensable de votre PC. Son rôle : neutraliser et mettre en quarantaine les virus qui pourraient s'attaquer à votre ordinateur. L'installer ne suffit pas : il faut faire régulièrement des mises à jour sur le site de l'éditeur car de nouveaux virus sont découverts en permanence.
   Certains logiciels gratuits ont des performances qui ne sont pas toujours au rendez-vous. D'autres sont aussi bons que les antivirus payants. Les meilleurs logiciels offrent un taux de détection variant entre 90 et 95 %.

2. **Analysez les pièces jointes avant de les ouvrir.**
   Il ne faut jamais ouvrir le fichier attaché à un courrier électronique si on ne connaît pas l'expéditeur. Il faut supprimer immédiatement les fichiers suspects. (Toujours demander à votre correspondant d'indiquer quel fichier attaché il vous envoie). Si vous jugez que l'extension du fichier est bizarre, ne l'ouvrez surtout pas, même si vous connaissez l'expéditeur, car il a pu être transmis à son insu.

3. **Analysez tous les courriels entrants.**
   N'importe quel antivirus récent propose une option pour analyser les courriels reçus avant même de les afficher dans le logiciel de courrier. Pour contrer les virus qui envoient des messages à votre insu, certains intègrent aussi une option pour scanner les messages sortants. C'est, par exemple, le cas de Norton Antivirus.

4. **Modifiez les réglages de votre logiciel de mail et de votre navigateur.**
   Vous pouvez par exemple transformer votre Outlook Express en barrière infranchissable. En effet, ce logiciel de messagerie propose par défaut des options pour bloquer l'accès aux pièces jointes censées être dangereuses, comme les documents en Word, PDF ou même Tiff. Précisons que ce réglage interdit d'envoyer la plupart des pièces jointes, même sans virus. Vous pouvez personnaliser le niveau de sécurité de votre navigateur en allant sur outils/option Internet.

5. **Mettez à jour régulièrement votre système d'exploitation.**
   Au fur et à mesure, on découvre dans les systèmes d'exploitation, Windows essentiellement, et dans les logiciels comme Internet Explorer, ce que les spécialistes appellent des failles de sécurité utilisées par les créateurs de virus. Il est donc important de faire des mises à jour. Ou même d'en changer. Certains systèmes, comme MacOS ou Linux ont moins de failles de sécurité.

6. **Mac ou PC ?**
   Tous les spécialistes l'admettent : le Macintosh est moins exposé aux virus. Pourquoi ? Tout simplement parce que l'objectif principal d'un auteur de virus est d'infecter le plus grand nombre d'utilisateurs. Or la part d'Apple sur le marché des ordinateurs est limitée à 3 %. L'institut spécialisé en sécurité informatique ICSA Labs le confirme : il a recensé entre 40 et 100 virus Macintosh actifs, alors que près de 50 000 virus sévissent sur les PC. À noter qu' aucun virus n'a été recensé à ce jour sur la version X du Mac OS, sorti en 2001 !

## Les sites utiles

Si vous êtes sur PC, allez régulièrement sur le site de Microsoft pour télécharger les correctifs qui vous mettront (temporairement) à l'abri.
http://windowsupdate.microsoft.com

Service grand public du Forum des droits sur l'Internet, destiné à différents publics : parents, juniors, créateurs de sites… à partir d'une liste de questions fréquemment posées (nombreuses questions autour des virus)
http://www.droitdunet.fr/

Introduction aux virus, sur le site "Comment ça marche", encyclopédie informatique libre.

http://www.commentcamarche.net/virus/virus.php3

Virus, vers, chevaux de Troie...
Les codes malicieux ne cessent d'évoluer et de s'adapter. Souvent, d'élémentaires mesures de précaution suffisent à minimiser les risques, mais la menace, protéiforme, demeure. (Dossier du journal du net)
http://solutions.journaldunet.com/dossiers/virus/sommaire.shtml

*D'autres ennemis de votre ordinateur rôdent sur Internet. Bien que théoriquement moins dangereux que les virus, ils peuvent être vraiment gênants. Ils ont pour nom spam, spyware et hoax. Voici en quoi consistent ces nouvelles menaces.*

## 2/ Le spam

### Définition

Le spam, encore appelé pourriel, junk-mail, ou bombardement, est l'équivalent électronique des prospectus publicitaires qui envahissent nos boîtes aux lettres. Et il se développe à mesure que le réseau grandit. Plus d'un courrier électronique envoyé sur deux est un message publicitaire non sollicité, voire un message illégal à caractère pornographique, raciste…

La différence avec les prospectus, c'est que les spams engorgent les réseaux et peuvent coûter cher, à celui qui le reçoit, en temps de connexion et de nettoyage.
Le spam est l'action d'envoyer des courriers électroniques publicitaires ou promotionnels, en général en grand nombre, à des personnes qui ne les ont pas sollicités. D'une manière générale, est considéré comme du spam tout envoi de messages dans des mailing-lists, des newsgroups ou des boîtes aux lettres électroniques personnelles, afin de "faire de la publicité".

Selon la CNIL (Commission Nationale de l'Informatique et des Libertés), *"l'expression trouve son origine dans un sketch des Monty Python, dans lequel deux personnes parlant de saucisson ("spam"), répètent le mot "spam" tous les deux ou trois mots jusqu'à l'exaspération des spectateurs"*. Ce type de publipostage électronique porte donc bien son nom puisqu'il a pour principal effet de vous agacer par ses messages pourris.
Internet permet de toucher un grand nombre de personnes à moindre coût. La communication de masse est à la portée de tous. Le coût d'envoi d'un mail est en effet estimé autour de 10 centimes contre 1 euro pour un courrier traditionnel. Qui sont les spammeurs ? Des publicitaires ? Des escrocs ? Un peu des deux ! Car les pourriels sont une façon peu coûteuse de toucher rapidement un maximum de clients potentiels. En général, les spammeurs achètent des listes d'adresses à des commerçants indélicats, ou les aspirent à l'aide de logiciels spécialisés sur des sites et des forums. Ou encore ils les "trouvent" aléatoirement grâce à des générateurs automatiques d'adresses.

Même s'il est quasi impossible d'échapper totalement au spam, il y a toutefois une grosse différence entre une boîte complètement submergée de publicités et la réception mensuelle de quelques messages non sollicités. Pour lutter, voici quelques précautions à prendre.

**Conseils pour s'en débarrasser**

**1/ Gardez confidentielle votre adresse principale.**
Cette adresse, celle où vous recevez les messages de vos proches ou de vos contacts professionnels, doit rester vierge de tout spam. Ne la communiquez qu'aux personnes que vous connaissez.

**2/ Adoptez une ou deux adresses poubelles.**
Vous passez beaucoup de temps sur des forums ? Vous achetez souvent en ligne ? De nombreuses situations vous imposent de communiquer votre adresse électronique à des inconnus. Plutôt que de prendre le risque de divulguer votre adresse principale à n'importe qui, ouvrez une deuxième boîte aux lettres chez votre fournisseur d'accès.

**3/ Méfiez-vous des formulaires d'inscription.**
Que ce soit pour profiter d'un nouveau service ou pour télécharger un logiciel, vous devez souvent remplir un formulaire vous demandant des données personnelles, dont votre adresse électronique. Attention, ces formulaires contiennent souvent des cases indiquant que vous consentez à recevoir des promotions ou que vous acceptez que votre adresse soit communiquée à des partenaires commerciaux. N'oubliez pas de décocher ces cases si ne vous souhaitez pas recevoir de publicités.

**4/ Faites attention lorsqu'on vous demande de vous désabonner !**
Tous les spammeurs n'achètent pas leurs fichiers. Certains utilisent des programmes qui génèrent automatiquement des adresses électroniques. Ils envoient leurs messages à toutes ces adresses, sans savoir lesquelles existent vraiment. Le corps du message comprend toujours une procédure (renvoi d'un courrier ou visite d'une page Web) pour faire cesser ces envois et appelée désabonnement ou *unsubscribe* en anglais. Si vous essayez de vous désinscrire en suivant leurs instructions, ils sauront que votre adresse est valide. Ils continueront donc à vous envoyer d'autres messages.

**5/ Filtrez vos messages.**
Que vous consultiez vos courriels à partir d'un site Web ou d'un logiciel de messagerie, vous pouvez à tout moment décider de bloquer les messages en provenance d'un expéditeur.

**6/ Ne répondez jamais à un spam.**
En effet, même s'il est dit qu'une désinscription des listes d'envoi sera effectuée, ceci n'est très souvent pas le cas. Un des buts recherchés par le spammeur est de savoir si l'adresse email est valide. Si une réponse est faite à une sollicitation, l'adresse email sera revendue à d'autres spammeurs qui la spammeront a leur tour.

**7/ Si nécessaire**, vous pouvez écrire votre adresse sur vos sites de façon à ce que les robots ne puissent pas l'utiliser : par exemple, *jean-dupond at france point com* pour jean-dupond@france.com.

## Les sites utiles

Sur son site, la Cnil a publié un dossier consacré au spam. Vous y trouverez de nombreuses informations sur les obligations des commerçants à votre égard en termes de publicité et des conseils légaux pour éliminer le spam.
http:// www.cnil.fr

Ce site regroupe l'ensemble des fournisseurs d'accès à Internet français. Il vous explique en détail comment signaler un spam à votre FAI. Il vous donne également l'adresse de la cellule anti-spam de chacun de ses membres.
http://www.afa-france.com

Vous n'avez besoin d'une adresse que de manière très ponctuelle pour récupérer le code d'activation d'un logiciel téléchargé ou pour faire un achat en ligne ? Le site jetable.org propose de vous en donner une temporaire. Il vous suffit d'indiquer l'une de vos adresses et la durée de validité, de 24 heures à huit jours. Le site génère automatiquement une adresse du type dupont@jetable.org.
http://www.jetable.org/fr/index

## 3/ Les spywares

### Définition

Littéralement, il s'agit de *"logiciels espions"*. Les spywares (ou mouchard) sont des petits programmes qui, installés à l'intérieur d'autres programmes, collectent des informations sur l'utilisateur d'un ordinateur (ses intérêts, ses habitudes de téléchargement et de navigation) et profitent de sa connexion à Internet pour faire leur rapport à des sociétés de marketing. Les données récoltées, notamment les adresses électroniques, serviront à élaborer de nouveaux spams mieux ciblés. Tout cela dans un but exclusivement commercial.

Ces mouchards présents dans de nombreux logiciels gratuits (freewares) ou en version de démonstration (sharewares) s'installent lors du téléchargement et ne sont pas détectables par l'utilisateur. En effet, ils n'apparaissent pas dans la liste des programmes et ne peuvent donc pas être désinstallés.

Pour les repérer, voici quelques sites utiles.

## Les sites utiles

Pour un suivi quotidien de l'actualité des spywares et les différents moyens de les détecter, consultez régulièrement ce site..
http://www.anonymat.org/actualite/

Avant de télécharger un logiciel, vérifiez sur ce site qu'il ne contient pas de spyware (en anglais).
http://www.spychecker.com/

"Comment supprimer les spywares (mouchards) présents dans les versions gratuites de nombreux logiciels ?"
http://www.linternaute.com/0redac_actu/0103_mars/010306maquestion.shtml

## 3/ Les "hoax"

### Définition

Le "hoax" est un canular en français. Ils sont à la frontière entre le spam et le virus. En effet, des petits malins s'amusent à faire circuler sur Internet des messages indiquant que tel fichier présent dans le dossier de Windows est en fait un virus qu'il faut supprimer. Or la suppression dudit fichier peut surtout nuire à votre ordinateur.

Désinformation, faux virus, rumeur… Infos bidon, intox en tous genres circulent sur Internet. Les identifier vous permettra par exemple de ne pas faire de don pour financer des opérations salvatrices d'enfants qui n'existent pas ou encore de ne pas répondre à une super offre commerciale qui n'en est pas une.

### Les sites utiles

C'est le site incontournable qui traque les fausses rumeurs, fausses alertes aux virus, faux messages de soutiens afin de mettre fin aux différents types de hoax, véritables "mensonges électroniques" qui pullulent sur la toile.
http://www.hoaxbuster.com/

### Et pour finir, quelques informations sur les "pirates" :

Le pirate informatique est un expert dans son domaine, capable, entre autres, de trouver les failles d'un système ou de "casser" un code. Il faut bien distinguer ses compétences de ses intentions. En effet, on distingue deux grands courants dans la grande famille du hacking (de hacker - bidouilleur en anglais) :

> les White Hats (chapeaux blancs) hackent afin d'améliorer la sécurité de ce qu'ils visitent. En principe, après avoir fait leur coup, ils prennent contact avec l'administrateur du site ou le créateur du logiciel pour leur communiquer les résultats de leurs investigations.

> les Black Hats (chapeaux noirs) sont une formation de hackers moins moralistes. Diverses motivations les poussent à agir (attention ! à ne pas confondre avec les *script kiddies* piratant plus par désir de se faire remarquer

que de progresser). Là encore on trouve de tout : certains Black Hats versent dans l'hacktivisme tandis que d'autres détruisent sans aucune animosité à l'égard de la cible. Ils sont alors appelés crashers. (Source Wikipédia)