

# Dossier sécurité : Spam et Phishing

La démocratisation d'Internet et du haut débit a fourni aux Français de nouveaux moyens de communication et d'information puissants et rapides. Malheureusement, Internet n'est pas sans failles et sans risque pour ses utilisateurs, loin de là même. Ils doivent désormais être particulièrement vigilants quant aux actions qu'ils entreprennent et aux informations auxquelles ils accèdent. La faute à des personnes malintentionnées qui exploitent les failles et parfois la naïveté d'internautes pas suffisamment informés pour les polluer, ou pire, les arnaquer.

Aujourd'hui, sur Internet, la pollution et l'arnaque sont réunies et désignées, sous deux principaux termes : le SPAM et le « phishing ». Dans ce dossier/article, nous avons donc décidé de vous exposer les tenants et les aboutissants de ces deux « phénomènes néfastes » afin de vous informer au mieux. Nous évoquerons également une « partie pratique » pour vous aider à vous protéger de ces menaces d'un nouveau genre.

## Le SPAM, qu'est ce que c'est ?

À l'origine, le SPAM désigne une marque de pâté américaine / jambon en boîte réputée bon marché, mais de mauvaise qualité. Cette marque a été évoquée à l'occasion d'un sketch des Monty Python dans lequel le mot SPAM envahit la conversation et le menu d'un petit restaurant.

En informatique, il désigne également quelque chose de néfaste et de mauvais : la distribution en masse de courriers électroniques à caractère publicitaire et non sollicités. Si le SPAM (pourriel chez nos amis québécois) rime très bien avec pollution numérique, c'est qu'il est difficile de s'en défaire une fois pour toutes.

En effet, une fois qu'un « Spammeur » a inscrit votre adresse mail dans ses listes de distributions, vous allez recevoir de façon hebdomadaire ou journalière, des courriers publicitaires redondants. Attention toutefois à ne pas confondre les listes de distribution classiques (newsletter, promotions de magasins...) avec du SPAM. La principale caractéristique qui différencie le SPAM et ces listes de distributions « légales » se situe au niveau des possibilités de désinscriptions. Avec des listes de distributions classiques, il est généralement très facile de se désinscrire pour ne plus recevoir des mails provenant de tel ou tel site ou de tel ou tel magasin. Pour cela, il suffit généralement de cliquer sur un simple lien placé dans l'un des mails reçus.

Dans le cas du SPAM, le lien en question peut être absent et s'il est présent (simplement pour des raisons légales), les demandes de désinscriptions sont tout bonnement ignorées. Ainsi, l'utilisateur continu, malgré ses demandes répétées, à recevoir des courriers qui vantent les vertus, les prix particulièrement bas, l'exclusivité de certains sites commerciaux, de médicaments miracles ou de tel ou tel produit révolutionnaire. Bien entendu, ces annonces pour attirer le chaland sont, n'hésitons pas à le dire, purement et simplement des arnaques ! Cliquer sur un supposé lien de désabonnement dans un SPAM est d'ailleurs une très mauvaise idée, car cette action peut permettre au spammeur de savoir que sa publicité a été bien reçue et bien lue, du coup il n'hésitera pas une seconde à vous "bombarder" avec d'autres email. Il pourra également diffuser votre adresse à d'autres spammeurs ...

Le SPAM est né quelques temps après l'émergence du courrier électronique aux États-Unis au milieu des années 90. La démocratisation d'Internet dans le monde a été suivie par une vague de « spammeurs » qui a pris de l'ampleur avec le temps. Ainsi, aujourd'hui, il n'est pas rare qu'un internaute reçoive plusieurs dizaines, voire plusieurs centaines d'emails « SPAM » dans sa boîte

électronique chaque jour ! Ce qui provoque rapidement un ras-le-bol quand il s'agit de classer / trier son courrier électronique... Comme si les nombreux prospectus en tout genre reçus dans la boîte aux lettres, physique elle, ne suffisaient pas !

Une issue au problème ?

Conscientes des problèmes divers et variés que peut provoquer le SPAM, plusieurs grandes entreprises et plusieurs gouvernements se sont penchés sur cette pollution numérique. Cela a donné naissance à quelques projets / lois, comme la CAN-SPAM aux États-Unis qui visent à s'attaquer directement aux responsables d'envois de SPAM.

Malheureusement, ces actions / lois n'ont pas été totalement couronnées de succès. Certes, certains Spammeurs ont arrêté leurs activités, mais pour le moment le phénomène du SPAM a atteint une telle ampleur que les autorités, entreprises et utilisateurs ont l'impression de se battre contre une hydre : coupez une source de SPAM, il y'en a cinq autres qui poussent à la place... Le problème vient principalement du fait que de nombreuses sources qui génèrent du SPAM proviennent de plusieurs pays asiatiques (20% des SPAM viennent de Chine et de Corée du Sud). Ces pays se sont engagés à lutter contre le SPAM, mais les résultats et les actions concrètes dans ce domaine continuent à se faire attendre, malheureusement !

Pour le moment, il est utopique d'espérer un avenir proche sans SPAM, alors que peut faire l'utilisateur contre cette pollution ? La réponse est finalement assez simple : installer et configurer un client antispam sur son ordinateur ! Nous allons donc vous exposer maintenant comment installer, configurer et exploiter une telle solution logicielle.

## **Le Phishing : « tu te fish de moi ? »**

Le « phishing » ou « hameçonnage », est un nouveau type d'arnaque qui s'appuie sur Internet et sur le courrier électronique. Son nom provient du terme anglais « Fishing » qui désigne la pêche et qui en reflète particulièrement bien le principe de fonctionnement. Pour l'internaute, l'aspect premier du « phishing » prend généralement la forme d'un email classique. Le corps du texte de l'email incriminé vous informe d'une information « importante » qui concerne votre compte en banque, votre compte d'enchères ou tout autre compte menant à des données personnelles sensibles. Ces textes sont toujours accompagnés d'un lien hypertexte qui cache en réalité une véritable supercherie.

Théoriquement, les liens en question doivent conduire au site d'un établissement bancaire ou alors à celui d'un site marchand. La réalité est évidemment bien différente et ils conduisent en définitive à de parfaites copies de sites légitimes ! Comme les sites originaux, ces copies vous proposent d'entrer vos identifiants pour accéder à vos données personnelles. Seulement, une fois entrés, ces identifiants ne sont pas dirigés vers un serveur sécurisé : ils sont interceptés par des utilisateurs malintentionnés qui procèdent ainsi au vol d'informations importantes comme votre mot de passe ou votre numéro de carte de crédit, qu'ils pourront utiliser à votre place en toute impunité.

La supercherie pourrait être facile à débusquer si les liens envoyés par mail n'étaient pas « truqués » pour faire apparaître dans le texte une adresse tout à fait sécurisée comme « [www.bnp.fr](http://www.bnp.fr) ». Bien sûr, il n'est alors pas question de vous emmener sur le site de la fameuse banque, mais bien vers une toute autre adresse. En règle générale, les emails liés au « phishing » sont distribués en masse comme un véritable SPAM. Pour se protéger, le plus simple est de toujours se poser la question de l'authenticité d'un message théoriquement en provenance d'une banque ou d'un site marchand : pourquoi ce dernier voudrait-il vous contacter et pourquoi vous envoie-t-il un lien direct vers votre compte ?

De manière générale, pour se protéger des arnaques par « phishing » voici les quelques règles élémentaires à suivre :

- Lorsque vous recevez un courrier électronique, ne cliquez jamais sur un lien conduisant à un site bancaire / marchand : préférez taper l'adresse manuellement dans votre navigateur.
- Posez-vous la question de savoir si oui ou non vous avez déjà communiqué votre adresse de courrier électronique à cet établissement / site.
- Sur les sites supposés de confiance, vérifier qu'un cadenas est présent en bas dans la fenêtre de votre navigateur au moment d'entrer un numéro de carte bancaire. Cela signifie que le site en question exploite une connexion sécurisée / cryptée. Les « faux sites » ne peuvent, a priori, pas exploiter de telles connexions. Mais se baser sur ce seul critère peut être parfois dangereux, si jamais un site "malveillant" arrive à mettre en place une "fausse connexion sécurisée".
- Vérifiez dans les emails reçus si des données personnelles (numéro de client, numéro d'agence...) sont indiquées. Si ces données sont présentes, il est peu probable que l'email soit un courrier dédié au « phishing ». Les emails liés au « phishing » sont généralement formatés pour ne contenir que des données classiques (nom ou prénom, adresse email...), mais il est très rare qu'ils contiennent des informations très précises et vérifiées.
- Si vous identifiez un email comme étant un courrier formaté pour le « phishing », n'hésitez pas à l'ajouter à votre filtre « antispam » : cela n'éliminera pas définitivement les emails « phishing », mais permet tout de même de mettre en place un obstacle supplémentaire à leur réception.

À noter que la loi commence à s'attaquer sérieusement aux « amateurs de pêche aux internautes ». Ainsi, en France, l'auteur d'une telle escroquerie a été condamné à un an de prison avec sursis, il a également été dans l'obligation de verser une amende de 8500 euros à titre de dommages et intérêts. Cet étudiant a abusé 12 clients du Crédit Lyonnais, dont il avait détourné les identifiants et mots de passe avec une copie du site Web de la banque. Il aurait ainsi pu récupérer la somme de 20 000 euros. Malgré les multiples plaintes déposées à travers le monde, il faut tout de même savoir que les arnaques par « phishing » explosent littéralement !

Les responsables de serveurs placés sur Internet doivent également être particulièrement vigilants au niveau de la sécurité de leurs machines. Certains pirates n'hésitent pas à détourner les contenus de certains sites (à l'issue de leurs responsables), en exploitant certaines failles, pour y placer des copies de sites qui serviront la cause du "phishing". Non seulement la pratique pose des problèmes légaux, mais les responsables des sites ainsi piratés s'exposent à des plaintes pour contrefaçon, qui peuvent être entamées par les responsables des établissements bancaires ou des services d'enchères, d'annonces, de ventes ...

Les développeurs de logiciels commencent à se pencher sur le problème posé par le phishing et plusieurs clients emails / navigateurs devraient aider l'utilisateur à éviter et à repérer ces arnaques, Mozilla Thunderbird, Netscape 8 et Internet Explorer 7 devraient proposer de telles possibilités. En attendant, la meilleure arme de l'internaute reste la vigilance. A noter que certains navigateurs comme Firefox ou Internet Explorer 6 (avec les dernières mises à jour) sont capables de détecter les adresses avec redirection.

Inutile toutefois de sombrer dans la paranoïa. Après avoir lu ce dossier et en respectant les différentes règles de base que nous vous proposons, vous devriez être à l'abri de ces mauvais tours. N'hésitez d'ailleurs pas à « éduquer » et à « sensibiliser » vos proches à ce sujet... Plus que jamais, un internaute averti en vaut deux !