15 astuces pour ne plus se faire piéger sur le Net

Juin 2014

La plupart des internautes savent que surfer sur le Net n'est pas sans risques. Espionnage, arnaque, spam, publicité intempestive, vol de données : les délits du Net sont nombreux et aujourd'hui massivement répandus. Pour y faire face, il faut bien sûr disposer de logiciels de sécurité, mais cela ne fait pas tout. La grande majorité des infections ne dépendent que de la vigilance de l'utilisateur.
Mais avec le temps, les fraudeurs emploient des méthodes de plus en plus subtiles, et ont donc plus de chances de berner l'utilisateur. Chaque jour, de nombreuses personnes sont victimes d'arnaques parfois grossières, mais très profitables pour les fraudeurs. Pour vous aider à repérer et lutter contre ces tentatives de fraudes, nous avons constitué ce dossier répertoriant quinze des principaux pièges à éviter sur Internet. Dans tous les cas, nous vous conseillons également d'utiliser le filtre anti-phishing de votre navigateur, ou bien une solution ou un module dédiés.

Les faux sites

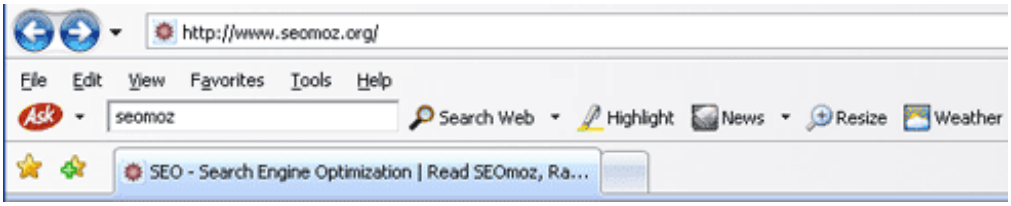
Lorsque vous lancez une recherche sur Internet, il est possible que vous tombiez sur des sites frauduleux (par exemple sur les annonces commerciales des moteurs de recherche). Ces derniers prennent la forme d'un site officiel (logo, pseudo-certifications, etc.), et profitent de la crédulité de l'utilisateur pour lui voler des informations confidentielles (identifiants et mot de passe par exemple, ou encore coordonnées bancaires). Parmi les sites les plus concernés : le paiement en ligne (Paypal, Western Union) et les e-commerçants. Ces sites ont une durée de vie généralement courte, afin d'éviter leur traçabilité. Il en existe de nouveaux chaque jour, mais en cas de doute, vous pouvez déjà vous référer à cette liste de liens frauduleux.

Mails frauduleux (ou « phishing »)

Dans votre boite mail, vous trouverez toujours parmi vos messages des spam (courriers non désirés, le plus souvent à des fins publicitaires). Vous pouvez vous contenter de les supprimer, surtout que toutes les messageries actuelles possèdent un filtre anti-spam plus ou moins efficace. Mais parmi les messages publicitaires ou exotiques, vous pouvez tomber sur des e-mails frauduleux, qui se font passer pour un site officiel (banque, assurance, e-paiement, etc.). Là encore, c'est une méthode pour accéder à vos identifiants ou vos comptes bancaires. Par ailleurs, si le message vous demande de vous identifier en ligne, alors il s'agit probablement d'un courrier frauduleux. Aucune organisation authentique ne demande à ses utilisateurs de s'identifier de cette manière, aucune organisation authentique pratique aussi mal l'écriture du Français. Vous pouvez repérer l'authenticité ou non du lien en glissant le curseur dessus et en vérifiant que l'adresse affichée est bien l'adresse officielle. Surveillez aussi les pièces jointes, qui peuvent contenir des programmes malveillants.

Un exemple de phishing sur Twitter Un autre type de fraude, nommée fraude 419 ou « arnaque nigériane ». Elle joue sur la crédulité et la compassion du lecteur pour lui extorquer de grosses sommes d'argent. Il s'agit de la principale fraude en ligne depuis 10 ans. Enfin, il y a les fameuses chaînes. Ces messages envoyés à une base d'e-mails, où l'on vous demande de renvoyer ce message au plus de monde possible parmi vos contacts, sous des prétextes fallacieux jouant sur la compassion ou la peur. Souvent plus lassantes que dangereuses, ces chaînes peuvent contenir des liens vérolés, diffusés gracieusement par les internautes qui ne prennent pas garde au message.

Les barres d'outils



Intégrés à de nombreux logiciels, les barres d'outils proposent des fonctions supplémentaires plus ou moins utiles pour l'utilisateur, mais sont également un outil de profilage pour les sociétés. Leur but est avant tout de collecter des informations personnelles et de s'en servir pour des activités marketing (vente de fichiers, envoi de messages électroniques ciblés, etc.). Il faut être assez vigilant vis-à-vis de ces barres d'outils, bien souvent cochées par défaut lors de l'installation d'un logiciel. A vous de l'installer ou non en connaissance de cause. Parmi les plus courantes, on retrouve les barres d'outils Google, Ask ou encore Yahoo!. Si vous souhaitez vous débarrasser de barres d'outils indésirables, nous vous invitons à vous rendre sur ce lien.

Les publiciels (adwares)

Il s'agit de logiciel gratuit pour lequel l'éditeur est rémunéré en affichant de la publicité lors de son utilisation. Certains d'entre eux ne contiennent que de la publicité, qui s'affiche de manière intempestive sur votre ordinateur, ce qui en fait donc un programme particulièrement indésirable. En outre, certains logiciels n'indiquent pas la présence de publicités lors de leur installation, ils sont donc considérés comme malveillants. De plus, plusieurs publiciels contiennent des programmes espions. Plusieurs logiciels existent pour éliminer les éventuelles infections, comme Malwarebytes' Anti-Malwares.

Les faux logiciels (rogues)

Descripción - CCleaner

Au cours d'une navigation sur Internet, il n'est pas rare de voir apparaître des messages d'alertes vous signifiant que votre PC est infecté par un grand nombre de menaces. Accompagné d'un scan qui n'est en fait qu'une simple animation, ce message vous propose l'installation - payante - d'un logiciel anti-virus soi-disant capable de nettoyer ces dizaines de menaces qui n'auraient pas été repérées par votre actuel anti-virus. Bien évidemment, tout est faux et télécharger ce logiciel vous délestera de plusieurs dizaines d'euros tout en laissant votre ordinateur et ses données aux mains des fraudeurs. Il existe plusieurs solutions en cas d'infection.

Typosquatting

Ce type de fraude utilise les similitudes entre deux adresses web afin de tromper l'utilisateur et le rediriger vers le site pirate au lieu du site recherché. Pour cela, le « typosquatteur » achète des noms de domaines similaires à celui de sites à fortes fréquentations (par exemple « mcrosoft » au lieu de « microsoft »). Lorsque l'utilisateur fait une faute en tapant l'adresse, il peut se retrouver sur un des sites pirates à l'adresse quasi identique. En plus de détourner le trafic des sites officiels pour attirer les annonceurs, le typosquatting permet aussi de récupérer des données utilisateurs et de rediriger ces derniers vers des sites concurrents avec lequel le site pirate est affilié.

Le HTTPS

Vous l'avez peut-être remarqué, de nombreux sites affichent désormais une connexion « https », visible dans la barre d'adresse. Cela signifie qu'au protocole http classique s'ajoute le « s » (pour « sécurisé »), qui permet au visiteur de vérifier l'identité du site sur lequel il se rend. La connexion HTTPS crypte les données entre le site et l'utilisateur, ce qui limite les intrusions et garantit la confidentialité de ses données. Sont principalement concernés les sites les plus

sensibles tels que les banques, les plateformes de e-commerce ou les réseaux sociaux. Il ne s'agit pas d'une fraude en soit, mais certains sites le désactivent par défaut, comme Facebook lors de sa dernière mise à jour. Il faut alors personnellement cocher la case « chiffrement HTTPS » dans les paramètres.

Les logiciels gratuits mais payants

Descripción - CCleaner

Une autre pratique qui touche les internautes les moins avertis, celle des logiciels officiellement gratuits, mais proposés moyennant quelques euros par certains éditeurs. Plusieurs indices permettent d'identifier le caractère frauduleux du site, comme une interface peu ergonomique, une traduction approximative ou des liens douteux. Le paiement se fait souvent par SMS (surtaxés) via des plateformes de type Audiotel. Prenez-garde donc. Le meilleur moyen d'éviter de se faire rouler est de se rendre sur des sites de confiance, comme les sites des éditeurs / constructeurs.

Les spywares

Véritable plaie du Net, les spywares sont extrêmement présents sur la toile et sont sans cesse plus perfectionnés. La difficulté de ses programmes espions est qu'ils sont relativement difficiles à repérer, par votre anti-virus mais surtout par l'utilisateur, qui doit redoubler de vigilance pour ne pas se faire infecter. Comme toujours, le meilleur moyen de les éviter et de surfer avec précaution. Ainsi, mieux vaut éviter de télécharger des logiciels dont on n'est pas sûr de la fiabilité (et donc peu ou pas connus). De la même manière, mieux vaut éviter de fréquenter certains sites à risque (les téléchargements de fichiers torrents et les sites pornographiques sont très concernés). Certains sites proposent l'installation de programmes (comme des plug-ins) pour lire une vidéo par exemple : c'est probablement un spyware, il vaut donc mieux annuler son

téléchargement. Plus de détails ainsi que des moyens de lutte sont disponibles sur cette page.

Les jeux en ligne

Ces jeux sont devenus très populaires grâce à des licences telles que World of Warcraft par exemple, mais aussi l'équivalent virtuel de jeux de société ou de cartes (comme le Poker). Des individus mal intentionnés profitent de cet engouement pour s'infiltrer dans le jeu et proposer aux joueurs des « aides » afin de progresser plus rapidement. L'appel du gain aidant, de nombreux joueurs se sont fait avoir par ces individus qui proposent davantage de ressources ou d'argent virtuel... contre de l'argent réel. Ces pratiques sont évidemment interdites et peuvent engendrer le bannissement du joueur-tricheur. Ces propositions peuvent se faire directement dans le jeu, ou via des plateformes de vente en ligne comme eBay. Si certains honorent leur part du contrat, d'autres se contentent d'encaisser votre argent avant de disparaitre. On peut également parler des nombreuses annonces de gain par des casinos en ligne, qui s'avèrent être bien évidemment une arnaque, le site vous réclamant plusieurs étapes payantes pour recevoir le prétendu gain, ce qui peut au final vous revenir plus cher et vous embarquer dans un système d'abonnement très difficile à résilier. Bien que ce soit fastidieux, il est impératif de lire les conditions d'utilisation avant de donner le moindre euro, sans quoi vous pourriez avoir de très mauvaises surprises, sans pouvoir vous défendre.

Les High Yield Investment Program (HYIP)

Il s'agit de sites web proposant des programmes d'investissement à haut rendement, avec des taux d'intérêt qui peuvent grimper jusqu'à 3% par jour. Il existe un grand nombre de ces sites, et certains se sont illustrés pour leurs arnaques répétées sous forme de vente pyramidale, notamment de chaîne de Ponzi. La plupart d'entre eux ont une durée de vie très courte, de quelques mois, à cause d'un modèle économique fragile, pour eux, et pour vous. Soyez très vigilants si vous souhaitez investir sur ce type de plateforme, car de tels taux dépendent soit d'un placement très risqué, soit d'une arnaque totale.

La vente bradée d'objets de luxe

Un certain nombre de vendeurs proposent des produits de luxe à des prix défiants toute concurrence. Normal, il s'agit de contrefaçons. On retrouve un grand nombre d'annonces expliquant qu'il s'agit d'un objet familial, et vendu à un prix très attractif. En pratique, ces produits sont fabriqués en Asie pour quelques dizaines d'euros, puis revendus quelques centaines, contre des tarifs en boutique qui se chiffrent plutôt en milliers d'euros. Différents facteurs peuvent vous mettre la puce à l'oreille : le prix bien sûr, les termes de l'annonce (sac à main façon Chanel) ou encore la réticence du vendeur à vous donner des informations claires et crédibles. Il devient difficile de repérer les contrefaçons car les vendeurs affichent des prix plus élevés, ce qui met donc en confiance l'acheteur potentiel, sans parler des détails des produits. Il faut donc procéder à une inspection minutieuse de l'objet, et ne pas hésiter à demander des photos rapprochées du produit.

Les faux profils

Les lieux d'échanges comme les services de messagerie instantanée ou les réseaux sociaux sont aujourd'hui très touchés par le phénomène de « faux-amis », ces profils à l'avatar généralement attrayant qui vous demande en ami. A moins que vous ne reconnaissiez l'adresse ou la personne sur la photo, il est vivement déconseillé d'accepter ce type de demande car ils contiennent potentiellement des logiciels espions qui s'empareront de vos identifiant pour prendre le contrôle de votre compte, à des fins lucratives ou tout bonnement malveillantes. Dans le même genre, faites attention lorsque vous cliquez sur certains boutons de partage comme le bouton « like » de Facebook. Ce dernier active généralement une autorisation qui permet au site d'accéder à des informations vous concernant (des photos par exemple) et de créer du trafic à votre insu en publiant automatiquement des données sur votre profil.

Les abonnements automatiques

Pas vraiment une arnaque, mais cela n'a pas empêché de faire de nombreuses victimes. Lorsque vous vous abonnez à une offre d'essai pour consulter l'offre payante d'un site web, un abonnement est souvent enclenché automatiquement à la fin de l'offre d'essai. Selon les sites, vous pouvez donc être débité pour un mois ou plus, sans aucun moyen de faire marche arrière. Lisez attentivement les modalités lors de votre inscription, et veillez à décocher l'abonnement automatique si cela ne vous intéresse pas. Cela évitera de vous retrouver avec un débit de plusieurs dizaines d'euros pour un contenu qui ne vous satisfait pas.

Protéger ses identifiants

Une astuce pour terminer : veillez à utiliser des mots de passe auxquels seul vous pourrez penser. Si vous devez les partager, veillez à ce que ce soit avec une personne de confiance et de manière confidentielle (donc éviter les réseaux sociaux par exemple). De même, variez les mots de passe pour limiter les chances que vos comptes soient piratés. Notez-les dans un carnet si vous avez peur de les oublier. Enfin, si vous partagez votre ordinateur, veillez à ne pas enregistrer vos identifiants sur le navigateur, sans quoi vous laisserez une véritable porte ouverte aux autres utilisateurs.

A voir également

- Repérer si un site web est fiable