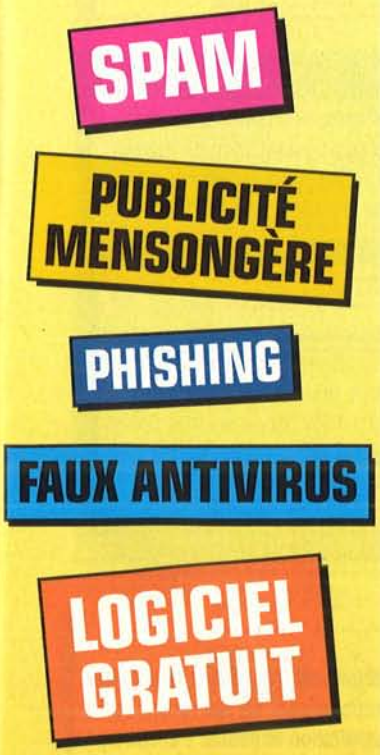
Comment éviter...

Les 1 pièges d'Intern

Sommaire

Dossier réalisé
par Alexandre Carneiro avec la rédaction

0 nouveaux et



Les pirates n'ont pas de répit et ils cherchent de plus en plus à vous voler vos données perso ou à utiliser votre PC à des fins mercantiles. Nous avons décrypté leurs dernières méthodes pour vous éviter de tomber dans leurs pièges.

En informatique, s'il y a bien un domaine qui ne connaît pas la crise c'est bien l'imagination des hackers et autres pirates. La question de la sécurité reste donc toujours d'actualité et c'est une problématique qui ne cesse d'évoluer. Évidemment, pour se protéger il y a les antivirus et les suites de sécurité qui les accompagnent. Au cours des derniers mois, nos différents tests sont catégoriques: les éditeurs maîtrisent bien leur sujet. De nombreux antivirus utilisent les mêmes moteurs, et la plupart des solutions disponibles sont finalement assez équivalentes en termes de protection et de détection des menaces. La différence se fait le plus souvent sur l'ergonomie du logiciel et sur la fréquence des mises à jour. Les pirates savent tout cela, et ils attaquent donc la seule variable qui peut encore faillir: vous!

La porte d'entrée, c'est vous!

En listant les nouvelles menaces, l'une des premières constatations est que la plupart d'entre elles ont pour objectif de vous duper ou de tromper votre vigilance. Et c'est finalement assez normal, car comme nous le disions plus haut, les ordinateurs d'aujourd'hui sont globalement bien armés face aux classiques attaques insidieuses. Pour continuer leur trafic, les pirates sont donc contraints de vous pousser à la faute. Et ils ne manquent pas de ressources pour atteindre leur but! C'est donc à la fois une mauvaise et une bonne nouvelle. Une mauvais parce que les menaces sont toujours aussi présentes si ce n'est plus encore. Une bonne, car vous êtes en mesure de les contrer en adoptant quelques règles de base. Suivez nos indices pour les identifier et surtout les éviter. Et mettez en pratique les astuces de la rédaction.

> **“ Internet génère en permanence de nouveaux pièges liés à vos différents usages. ”**

Une question de bon sens

Pour repérer les nouvelles menaces susceptibles de vous atteindre, nous avons pris comme point de départ tous les différents usages d'Internet. Le constat? Pour chacun d'entre eux, il existe un danger. Vous téléchargez des logiciels? Méfiez-vous, les logiciels contrefaits et truffés de malwares sont légions. Vous passez du temps à partager avec vos amis sur les réseaux sociaux? Attention les hackers ont flairé cet engouement et ils n'hésitent plus à se faire passer pour l'une de vos connaissances pour encore mieux vous duper. La liste est longue… Dans la plupart des cas, un peu de bon sens suffit à détecter la supercherie ou le piège. Ainsi, si vous recevez un mail de votre grand-père dans un français approximatif, où il vous parle de son immense joie suite à sa récente découverte d'un site d'e-commerce chinois ou les iPad sont vendus 80 euros, vous pouvez sans trop de risque deviner qu'il s'agit probablement d'un piège. Et par la même occasion que l'ordinateur de votre grand-père est certainement infecté. Certaines tentatives sont parfois tellement ridicules qu'elles en deviennent pathétiques… Mais comme un utilisateur averti en vaut deux, plongez-vous dans ce dossier pour vous mettre à jour sur les dernières menaces en date. ■

3000

C'est le nombre de sites qui référencent des fausses versions du logiciel VLC.

Le piège du logiciel gratuit

N°1 le plus hypocrite

Les pirates n'hésitent pas à créer de faux sites pour vous proposer des logiciels gratuits. Leur but: vous faire installer des logiciels espions et vous soutirer de l'argent. Voici comment les éviter.

C'EST QUOI ?

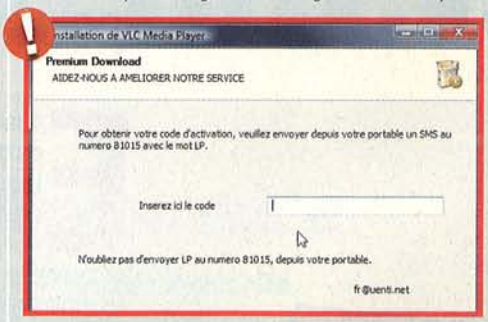
Il existe des logiciels gratuits pour faire à peu près tout. Le problème c'est que certains d'entre eux sont victimes de leur succès. En effet, de petits malins n'hésitent pas à fabriquer de faux sites pour proposer ces logiciels incontournables en téléchargement. En plus de s'accaparer le travail d'autres développeurs, ces pirates incorporent des systèmes de paiement qui vous sollicitent au moment de l'installation et souvent des logiciels espions qui causent de graves dommages à votre PC. Le pire dans tout ça, c'est que lorsque vous faites une recherche dans Google les premiers résultats renvoient souvent vers ces sites véreux.

Vous tombez dans le panneau !

1 Vous avez reçu une vidéo que vous n'arrivez pas à lire. VLC Media Player est capable de lire les vidéos sans installation de codecs. Vous tapez son nom dans Google et choisissez le premier résultat.

2 Vous tombez sur un site de téléchargement du logiciel. Indices du piège: les fautes d'orthographe. Le site a été réalisé en traduction automatique. Lors de l'installation, c'est le début des grosses surprises.

3 Le logiciel vous propose d'installer des options comme une barre d'outils (Yahoo ou Google). Ensuite, il demande de l'argent via un code AlloPass: un comble pour un gratuit ! Il s'agit d'une arnaque.

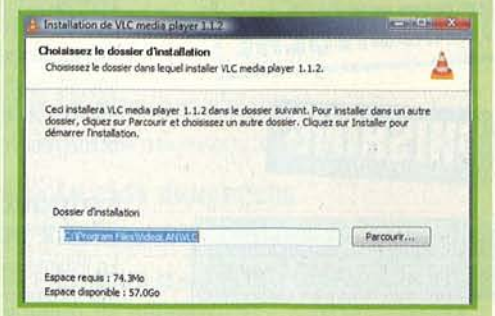


Vous évitez le piège !

1 Quand vous cherchez un logiciel gratuit, méfiez-vous des liens sponsorisés. N'hésitez pas à ajouter « officiel » à vos mots de recherche pour arriver sur le véritable site de l'éditeur.

2 Téléchargez le logiciel quand vous êtes sûr de son origine. Choisissez **Enregistrer sous** plutôt qu'**Exécuter** pour ne pas installer le logiciel automatiquement et pour le passer à l'antivirus.

3 Une fois sûr de vous, vous pouvez lancer l'installation. Ici pas d'installation de logiciel superflu et aucune sollicitation monétaire. Le logiciel est gratuit et le reste jusqu'à la fin.



TOP 10

DES LOGICIELS GRATUITS CONTREFAITS

- Spybot – Search & Destroy
- VLC media Player
- Winrar
- Adobe Reader
- FileZilla
- OpenOffice
- Avira Antivir
- Gimp
- Avast Antivirus
- Sopcast

LES 4 CONSEILS microactuel

1 Assurez-vous d'être sur le site officiel de l'éditeur. Vous y trouvez l'historique du logiciel.
2 Évitez les liens sponsorisés dans Google et les adresses alambiquées. Dans notre exemple VLC, l'adresse était **www.vlcplayer.2010fr.biz** alors que l'officielle est **www.videolan.org**.
3 Lors du téléchargement, choisissez **Enregistrer sous** plutôt qu'**Exécuter** pour ne pas lancer automatiquement l'installation et passer l'antivirus.
4 Si vous n'êtes pas sûr, passez par un site de téléchargement connu comme **www.telecharger.com** qui vous aiguille vers une source fiable.

5 secondes

C'est le temps nécessaire pour qu'un faux site remplace à l'identique celui déjà ouvert.

Le piège du Tab Jacking

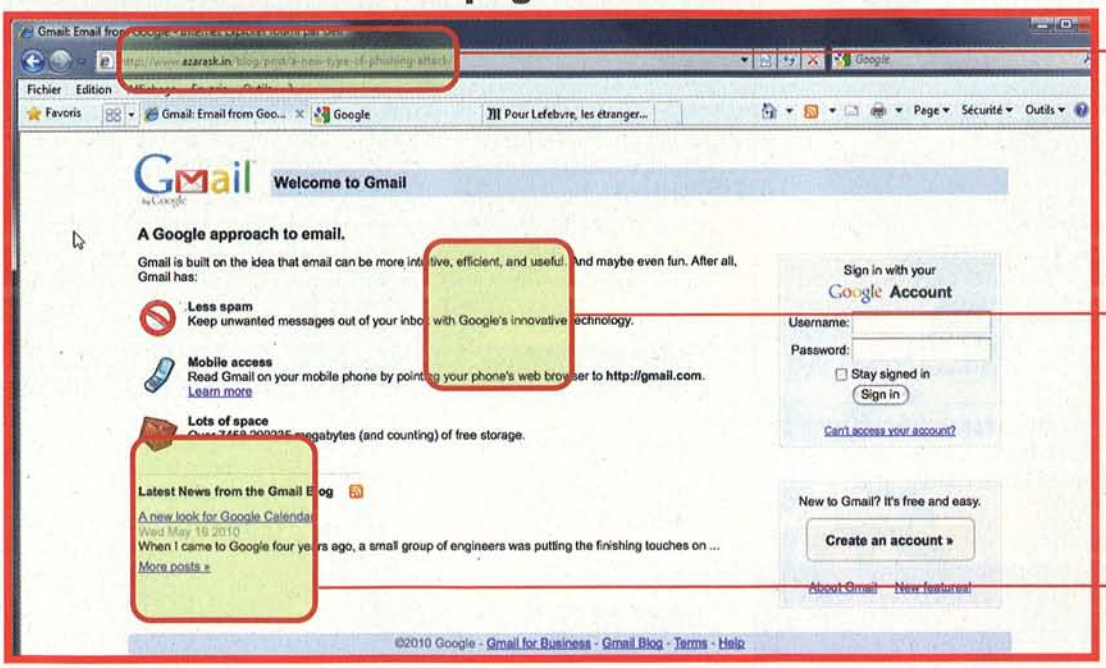
N° 2 le plus rusé

Pour subtiliser vos infos les pirates n'ont dans certains cas même plus besoin d'infecter votre ordinateur. Une simple page web peut transformer votre navigateur en véritable piège indétectable.

C'EST QUOI ?

Le Tab Jacking est une technique d'attaque qui touche certaines versions du navigateur Firefox ainsi que la dernière version de Chrome. L'ennemi c'est un code JavaScript malicieux caché dans une page. Un exemple, vous ouvrez votre page Gmail, Facebook ou autre, puis vous changez d'onglet. Un code JavaScript malicieux détecte que vous n'êtes plus sur votre page initiale et la remplace par une fausse page Gmail, Facebook ou autre. Quand vous revenez sur l'onglet de départ, vous êtes sur une page d'accueil Gmail ou Facebook sur laquelle vous n'êtes plus connectée. Naturellement, vous retapez vos mots de passe. Vous êtes tombé dans le piège: vos mots de passe sont récupérés par le pirate.

Reconnaître une fausse page web



Indice 1

Avant de rentrer vos identifiants, regardez la barre d'adresse. Vous avez beau être sur la page d'accueil de Gmail, l'adresse indiquée n'a rien à voir avec celle du service de webmail de Google.

Indice 2

Ne vous fiez pas au contenu de la page. Comme toute bonne attaque de phishing, la page reproduit au pixel près la page d'accueil originale de Gmail. Soyez prudent si vous avez l'habitude d'ouvrir de nombreux onglets.

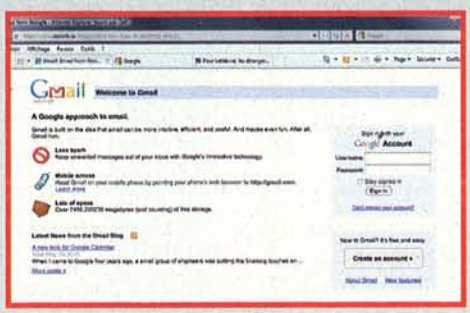
Indice 3

Le texte est ici en anglais alors que si vous utilisez Gmail à partir de la France le texte d'accueil est toujours en français. Si vous avez un doute, la meilleure précaution est de ne jamais entrer vos identifiants.

Vous tombez dans le panneau !

1 Vous surfez en utilisant la navigation par onglet. Cette pratique consiste à ouvrir au sein d'une même fenêtre du navigateur plusieurs pages internet. Sans le savoir, vous arrivez sur une page contenant un script de Tab Jacking. Tant que vous êtes dessus, la page se comporte normalement. Cela se complique si vous changez d'onglet.

2 Le script le détecte et change le contenu de la page sans que vous vous en rendiez compte. Lorsque vous revenez dessus, la page vous affiche une page de connexion vers un service comme Gmail, Facebook ou Hotmail. Croyant être déconnecté, vous rentrez vos identifiants qui sont ainsi révélés au pirate à l'origine du script.



QUE RISQUEZ-VOUS ?

- ✔ Vous faire subtiliser vos identifiants et vos mots de passe sans vous en rendre compte.
- ✔ Vous faire voler des infos perso qui mènent à une usurpation d'identité.
- ✔ Être la victime de spams personnalisés sur vos boîtes mails.
- ✔ Perdre l'accès à vos boîtes mails et à vos différents comptes utilisateurs.

160€

Prix d'un boîtier pirate qui décrypte les réseaux Wifi dans un rayon de 2 km. Illégal!

Le piège du Wifi

N°3 le plus discret

Chez vous, avec le Wifi vous vous connectez partout. Pourtant, mal sécurisé votre réseau devient accessible à vos voisins. Si l'un d'entre eux est malintentionné c'est vous qui risquez d'en faire les frais.

C'EST QUOI ?

Vous vous connectez à votre routeur ou à votre box via le Wifi. Si votre connexion n'est pas correctement sécurisée, il est possible pour un utilisateur mal intentionné de se connecter à votre accès internet. Outre le problème d'avoir sur votre réseau local un pirate capable d'accéder aux contenus de vos ordinateurs, c'est aussi ce qu'il fait de votre connexion qui peut être dangereux. En effet, si l'idée lui venait de télécharger des contenus protégés ou immoraux, c'est vous qui seriez accusé. Avec la mise en marche de l'autorité de lutte contre le piratage (Hadopi), il devient de plus en plus nécessaire de protéger votre accès contre tous les types d'intrusions.

Vous tombez dans le panneau!

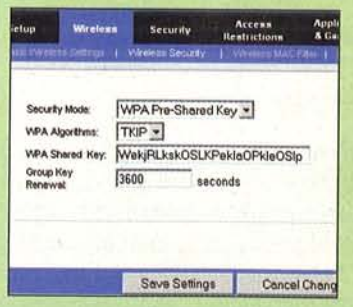
Ici, votre réseau Wifi sans protection (ou mal sécurisé) est accessible à un voisin malintentionné.

Vous évitez le piège!

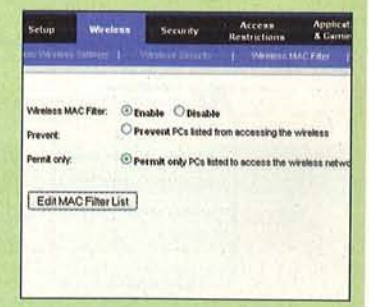
Ici, votre réseau est bien protégé. Votre voisin n'a pas la possibilité de s'y connecter.

4 astuces pour sécuriser votre Wifi

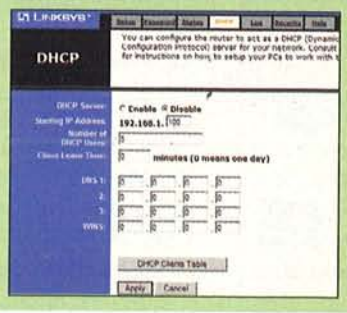
1 Privilégiez les clés WPA aux clés WEP. Les clés WPA ou WPA2 (Wifi Protected Access) sont les plus sécurisées. Privilégiez leur utilisation. Le protocole WEP est à éviter ou à associer à d'autres mesures de sécurité. Avec quelques utilitaires disponibles sur le Net couplés à un PC puissant il ne faut que quelques minutes pour cracker une clé WEP.



2 Utilisez le filtrage par adresse MAC. L'adresse MAC (Média Access Control) identifie l'ordinateur par sa carte réseau (Ethernet ou Wifi). Cette adresse unique est définie par le constructeur. Une fois ce filtrage activé, seuls les ordinateurs dont l'adresse a été renseignée peuvent se connecter.



3 Désactivez le serveur DHCP. Dans votre routeur ou box, le serveur DHCP fournit les adresses IP à vos périphériques. Il est possible de le désactiver et de créer manuellement une adresse pour chaque périphérique en fonction de son adresse MAC. Un périphérique non renseigné n'obtient pas d'adresse et donc pas de connexion.



4 Désactivez la diffusion du SSID. Pour se connecter sur un réseau Wifi, le PC a besoin du nom du réseau (SSID). Le point d'accès le diffuse en permanence. Une fois votre réseau configuré, vous pouvez activer la fonction **Cacher le SSID**, présente dans tous les routeurs ou box, afin de rendre votre point d'accès invisible depuis l'extérieur.

À SAVOIR

AVEC HADOPI, À VOUS DE DONNER DES PREUVES

La loi sanctionne la négligence de sécurisation de la ligne. En clair, si vous n'avez pris aucune mesure pour sécuriser votre ordinateur et que celui-ci est utilisé par un pirate pour télécharger illégalement des films, par exemple, vous êtes tenu pour responsable. Ce sera alors à vous de démontrer la preuve de l'intrusion. Des logiciels de sécurisation labellisés devraient être proposés cet automne et, à terme, ces solutions pourraient être intégrées directement dans les box des fournisseurs d'accès à Internet.

Hadopi

Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet

N°4 le plus fouineur

46 Le piège des réseaux sociaux

46 Pourcentage des utilisateurs Facebook qui acceptent des inconnus pour amis.

Les réseaux sociaux ont la cote. Le problème c'est que beaucoup de pirates sont à l'affût. Paramétrez vos pages pour limiter l'accès à vos seuls amis et n'exposez pas trop votre vie privée.

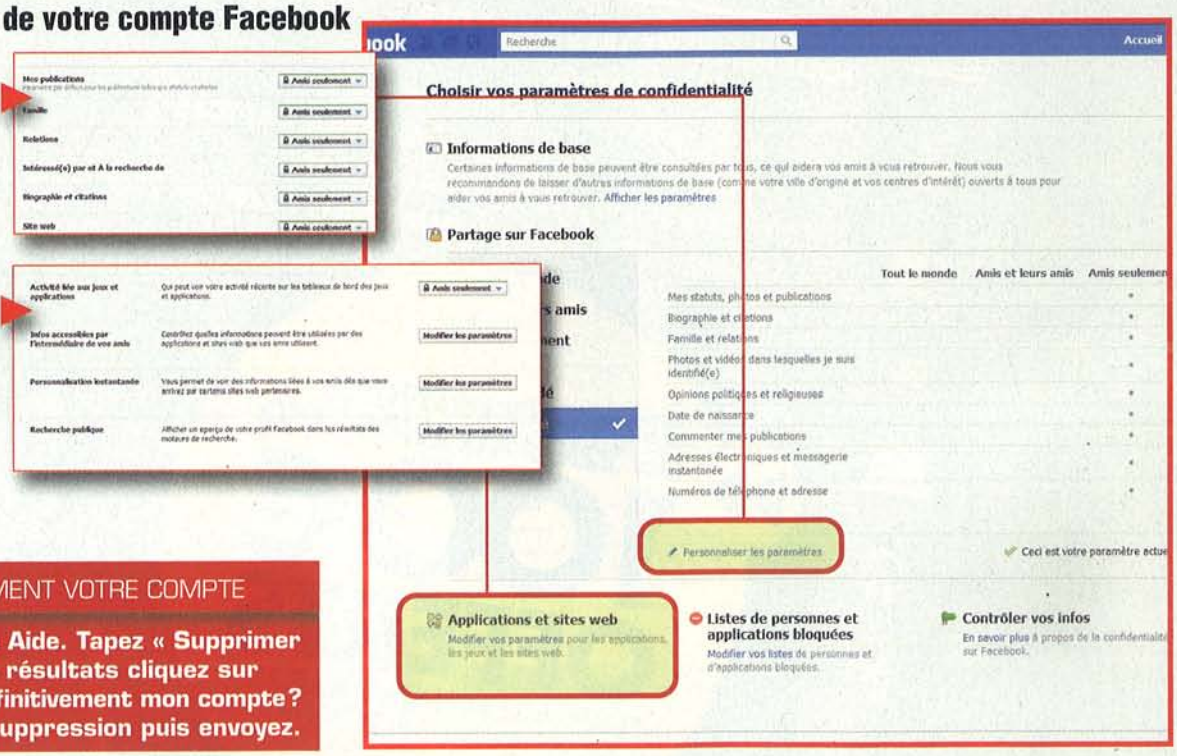
C'EST QUOI ?

Les principaux problèmes liés à l'utilisation des réseaux sociaux restent l'usurpation d'identité et la récupération de données personnelles. Deux méthodes sont utilisées par les hackers pour récupérer vos identifiants : soit au travers de certaines procédures décrites dans ce dossier (malware, Tab Jacking…) soit par la diffusion d'applications nuisibles sur les réseaux sociaux. Si vous utilisez Facebook, vous avez certainement remarqué que la plupart des applications liées à ce réseau social réclament un droit d'accès à vos informations. Si vous n'êtes pas sûr de leur origine, n'acceptez surtout pas ou vous risquez d'avoir de bien mauvaises surprises.

Les données sensibles de votre compte Facebook

À partir de cette page, vous pouvez définir qui aura accès au contenu de votre profil. Notre conseil : réglez au minimum chaque paramètre sur Amis seulement.

Cette page est souvent négligée et pourtant c'est une véritable porte ouverte vers votre profil. Vérifiez attentivement les informations de votre profil auxquelles les pirates ont accès via vos amis.



ASTUCE

SUPPRIMEZ DÉFINITIVEMENT VOTRE COMPTE

Allez dans Compte puis Aide. Tapez « Supprimer compte » puis dans les résultats cliquez sur Comment supprimer définitivement mon compte ? Faites la demande de suppression puis envoyez.

4 astuces pour bien paramétrer votre compte Facebook

1 Protégez vos informations de contact

Nous vous déconseillons de rentrer vos informations de contact comme votre adresse ou votre numéro de téléphone dans Facebook. Il n'y a pas grand intérêt à partager ce type de renseignement avec vos amis car, a priori, ils savent déjà où vous habitez et comment vous joindre.

2 Sécurisez votre profil

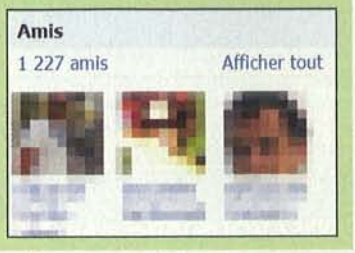
Réservez les infos comme votre statut ou vos photos à vos seuls amis en choisissant l'option **Amis seulement**. Si vous laissez ouvert un statut comme « En vacances » jusqu'à la fin du mois, cette info combinée à votre adresse pourrait être utilisée à mauvais escient par des personnes mal intentionnées.

3 Réservez les applications de votre profil

Dans le menu de paramétrage, sélectionnez **Amis seulement** pour toutes les applications que vous utilisez, les jeux auxquels vous jouez et les informations disponibles via vos amis.

4 N'étalez pas toute votre vie privée

N'acceptez pas n'importe qui comme ami et il est primordial de ne pas trop en dire, d'autant que Facebook est de plus en plus utilisé par les chargés de recrutement et autres organismes.



N°5 le plus envahissant

81 %

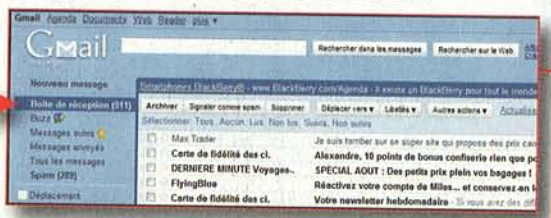
Pourcentage d'e-mails qui se sont révélés être du spam en 2009.

Le piège des nouveaux spams

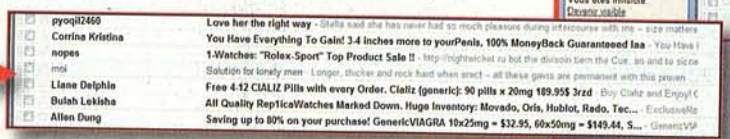
Même s'il recule légèrement, le spam envahit encore les boîtes mail. Pour vous tromper, les diffuseurs de ces messages n'hésitent plus à se faire passer pour vos connaissances.

C'EST QUOI ? Le spam, que l'on appelle aussi pourriel ou polluriel en français est une communication électronique non sollicitée envoyée par e-mail, et plus récemment par SMS, MMS ou messages vocaux sur les téléphones mobiles. Il s'agit en général d'envois en grande quantité effectués à des fins publicitaires pour des produits, des services ou pour promouvoir des sites. Une grande partie de ces offres s'avère être des arnaques. Surtout ne répondez jamais à un spam. Vous serez alors repéré en tant que personne physique derrière votre adresse e-mail et vous n'échapperez pas à l'invasion de centaines de pourriels et d'annonces publicitaires incongrues.

Le spam, c'est vous et vos amis



Les spams proviennent aussi d'utilisateurs que vous connaissez ! Si le PC d'un de vos amis est infecté, vous risquez de recevoir des mails de sa part qui n'iront pas dans votre dossier Spam, mais dont le contenu ne fait aucun doute. Ce spam n'est pas reconnu comme tel et apparaît dans la boîte de réception classique.



Pour vous pousser à ouvrir les mails publicitaires, les diffuseurs de spams vont jusqu'à se faire passer pour vous. Dans ce cas de figure, le mail provient de « Moi » comme si vous vous étiez envoyé un mail vous-même. Ici la messagerie détecte que c'est c'est un pourriel et le range dans le dossier Spam.

Les sites pour lutter contre le spam

La CNIL

Le site de la CNIL propose aux victimes de spams de le signaler. Par le biais d'un formulaire simple d'utilisation, vous obtenez les infos nécessaires pour lutter contre ces nuisances.
www.cnil.fr/vos-libertes/plainte-en-ligne

Hoaxbuster

Si vous avez un doute sur la nature ou la légitimité d'un mail, n'hésitez pas à aller faire un tour sur ce site qui note toutes les dernières rumeurs, fausses bonnes affaires et spams à la mode.
www.hoaxbuster.com

Arobase

Ce site est la référence pour tout savoir sur le mail en général. Dans sa rubrique « SOS e-mail » vous trouvez tout pour reconnaître un spam et surtout apprendre à vous en débarrasser.
www.arobase.org

LES 3 CONSEILS microactuel

1 Évitez de laisser traîner votre adresse web n'importe où. En effet, des « robots » écument le Web à la recherche d'adresse mail à spammer.

2 Ne communiquez pas votre adresse mail personnelle à des sites douteux. Pour cela, l'idéal est de créer une adresse pour des usages ludiques.

3 Paramétrez finement le filtre antispam de votre suite antivirus.

55 000

C'est le nombre de PC infectés par Mumba, spécialisé dans le vol d'infos perso.

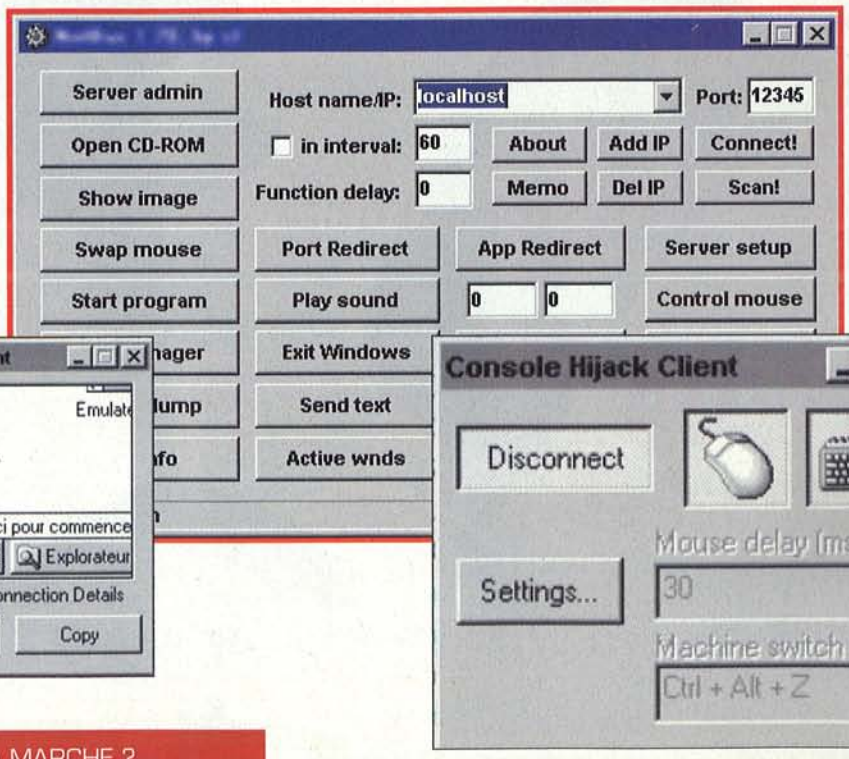
Le piège des malwares

Chevaux de Troie, keyloggers... pour éviter les programmes nuisibles, il est toujours important de faire très attention à ce que vous téléchargez et aux sites sur lesquels vous vous rendez.

C'EST QUOI ? Les malwares, ou logiciels malveillants, englobent toute une catégorie de programmes diffusés à des fins néfastes. Parmi les plus populaires on compte les chevaux de Troie (trojans), qui installent des fonctions nuisibles dans votre ordinateur sans autorisation. Mais aussi les rootkits qui sont des ensembles de programmes qui dissimulent l'activité nocive d'un malware, ou encore les keyloggers qui sont de petits logiciels capables d'enregistrer tout ce qui est tapé au clavier pour le renvoyer ensuite vers les pirates à l'origine de leur diffusion. Les hackers disposent ensuite de tous les moyens nécessaires pour voler vos secrets et même votre argent.

La dangerosité d'un cheval de Troie

L'une des particularités des chevaux de Troie est leur simplicité d'utilisation y compris pour des apprentis pirates. Sur certains sites de hackers, des packs complets et prêts à l'emploi sont disponibles facilement. Ici, un clic suffit pour ouvrir à distance sur votre PC le lecteur de CD (Open CD-Rom) ou encore lancer un programme (Start program).



Certains de ces chevaux de Troie assurent une prise de contrôle totale de l'ordinateur infecté avec la possibilité entre autres d'afficher votre Bureau à distance et de suivre toutes vos actions quand vous utilisez votre ordinateur.

Des interfaces simples, à la portée de tout pirate débutant, vont même jusqu'à offrir la prise de contrôle de la souris et du clavier du PC infecté.

À SAVOIR

UN CHEVAL DE TROIE : COMMENT ÇA MARCHE ?

Un cheval de Troie est une catégorie de nuisible en plein essor depuis 2005, date à laquelle ils ont dépassé les virus en termes de diffusion. Contrairement aux virus, ils ne se reproduisent pas par eux-mêmes. Ils sont récupérés au cours d'un téléchargement à partir d'une source peu fiable, via un mail ou bien dissimulés dans une image ou un programme à l'apparence légitime. Généralement, ils servent à introduire une porte dérobée sur un ordinateur. Ensuite, le pirate informatique à l'origine de sa diffusion peut à tout moment prendre à distance, via Internet, le contrôle de l'ordinateur. Le pirate contrôle la totalité du PC afin de récupérer des infos ou alors l'utiliser en tant que machine zombie pour diffuser des spams ou d'autres types de malwares.

LES 3 CONSEILS micro actuel

1 En complément de votre antivirus, un firewall ou coupe-feu en français est indispensable. En effet, celui-ci bloque le transfert de données vers le pirate à l'origine de sa diffusion.

2 Soyez très prudent dans l'utilisation de votre boîte mail. Évitez de télécharger les fichiers exécutables. Normalement, la plupart des webmails empêchent leur envoi, mais si vous en recevez faites très attention.

3 Le même type de précaution est à prendre quand des images sont en pièces jointes aux mails. Ces dernières peuvent inclure toutes sortes de malwares.

150 000

C'est le nombre de tentatives d'hameçonnage par jour en France.

Le piège du phishing

N°7 le plus cupide

Le phishing est l'une des méthodes de vol de données personnelles les plus utilisées sur Internet. Heureusement, la plupart du temps, il est facile de la repérer. Restez vigilant.

C'EST QUOI ? Le phishing (ou hameçonnage en français) est une technique utilisée par les pirates pour obtenir vos renseignements personnels. La technique consiste à vous faire croire, lorsque vous surfez sur le Net, que vous vous adressez à un tiers de confiance, le plus souvent une banque ou une administration. Mais le faux site sert de paravent afin de vous soutirer des informations clés comme vos mots de passe, votre numéro de carte de crédit ou vos identifiants bancaires. Généralement, l'hameçonnage peut se faire par le biais de courriers électroniques ou par des sites web falsifiés. Soyez attentif à certains détails et vous ne tomberez pas dans le piège.

Vrai et faux site : le jeu des différences

Ici la page originale de gestion des coordonnées bancaires. Pour l'atteindre, il est nécessaire de se rendre sur le site officiel de Free et de s'identifier au préalable. En aucun cas l'opérateur ne vous enverra un mail pour modifier vos informations ou les confirmer.

L'exemple type de la tentative de phishing envoyée par mail : la confirmation des coordonnées bancaires. Remarquez que la fausse interface est une reproduction fidèle de celle du site de Free, seule différence notable l'absence du bandeau publicitaire.

Les sites pour être au courant des tentatives de phishing

Les Arnaques

Ce site référence une bonne partie des arnaques ayant cours sur le Web. L'intérêt du site réside dans son forum où les membres recensent une grande partie des mails douteux circulant sur la Toile et menant vers des tentatives de phishing.
www.lesarnaques.com

Sécurité informatique

Le portail de la sécurité informatique du gouvernement publie des alertes concernant les menaces qui peuvent vous toucher. En plus de ces informations, le site comporte des fiches d'autoformations proposées sous la forme de modules interactifs.
www.securite-informatique.gouv.fr

Escrocs

Un site qui suit au quotidien l'actualité des fraudes sur le Net. Le site propose une liste d'adresses mail d'escrocs et vous permet de dénoncer un mail frauduleux afin d'avertir les autres utilisateurs du site. Le ridicule de certaines tentatives vaut le coup d'œil.
www.escrocs.net

REPÉREZ LES ARNAQUES EN 4 POINTS

1 Les banques et autres organismes n'envoient jamais de mails vous demandant de rentrer vos coordonnées.
2 Les mails de phishing comportent régulièrement des fautes d'orthographe qui sont un signe flagrant de fraude.
3 La barre d'adresse doit mentionner « https » devant « www » et un cadenas doit apparaître sur la page.
4 Les pirates reproduisent souvent l'adresse du site copié en changeant 1 ou 2 caractères.

30 millions

C'est la quantité d'ordinateurs infectés par de faux antivirus.

Le piège du faux antivirus

N°8 le plus menteur

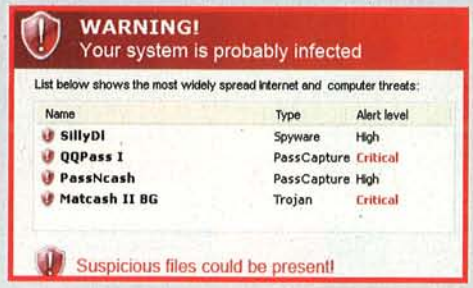
Le faux antivirus est l'une des armes préférées des pirates. Sous prétexte de décontaminer votre ordinateur, ces logiciels vous soutirent de l'argent et installent des malwares dans votre PC.

C'EST QUOI ?

Vous naviguez tranquillement sur Internet quand un pop-up apparaît avec un message alarmant: votre ordinateur est infecté ! Si ce message ne provient pas de votre antivirus, il y a toutes les chances qu'il s'agisse d'une arnaque. Surtout si le message vous invite à cliquer sur un lien pour télécharger une solution. Cela peut paraître anodin, mais il existerait tout de même près de 7000 variantes de faux antivirus installées sur plus de 30 millions d'ordinateurs. Les internautes qui tombent dans le piège verseraient en moyenne 50 euros pour ces fausses solutions de sécurité. Une menace qu'il ne faut pas prendre à la légère.

Vous tombez dans le panneau !

1 Vous surfez quand un message apparaît sous la forme d'un pop-up et vous informe que votre PC est infecté par un virus ou un spyware. Le pop-up vous propose un lien pour télécharger un outil apte à résoudre ce problème.



2 Vous cliquez sur le lien. Vous téléchargez la solution et bien que celle-ci soit annoncée comme gratuite dès que vous l'utilisez, vous devez payer pour passer à la version complète.

3 Une fois installés, ces logiciels sont assez difficiles à supprimer et dans les pires cas de figure, ils installent eux-mêmes des virus et des chevaux de Troie dans votre ordinateur.

Paramétrez correctement votre antivirus

ÉTAPE 1 — Optez pour les paramètres par défaut.
Au moment de l'installation choisissez les paramètres par défaut. Une fois l'installation achevée, procédez à un redémarrage de votre ordinateur.

ÉTAPE 2 — Vérifiez le bon fonctionnement des mises à jour.
Si vous avez la possibilité de régler la fréquence de ces dernières, optez pour au moins une fois par jour pour une meilleure efficacité.

ÉTAPE 3 — Planifiez l'analyse de votre micro
Dans la partie planification, déterminez des plages horaires pendant lesquelles votre ordinateur sera scanné. Une fois par mois pendant la nuit est un bon choix.

ÉTAPE 4 — Ne cumulez pas les solutions de sécurité
N'installez jamais deux logiciels antivirus, sous peine de ralentissements. Si votre antivirus arrive à échéance, il est important de le désinstaller.

LE CHOIX microactuel

3 antivirus gratuits

Antivir Personal Edition
Disponible pour tous les systèmes d'exploitation (sauf Mac OS), Antivir est un excellent antivirus qui dispose d'une bonne détection des menaces.

Avast Home
Avast fonctionne sous Windows et propose un bon niveau de protection. Le logiciel vous demande de vous enregistrer afin de profiter des mises à jour.

Microsoft Security Essentials
L'antivirus de Microsoft a deux avantages : sa simplicité d'emploi et sa très faible utilisation de ressources système.

N°9 le plus racoleur

1000000e

C'est vous le millionième internaute qui avez droit à un cadeau exceptionnel!

Le piège de la pub mensongère

Vous avez été confronté à une publicité en ligne vous annonçant que vous aviez gagné une maison? Méfiez-vous, si vous répondez, ce que vous risquez de gagner, ce sont des spams dans votre boîte mail!

C'EST QUOI? Sur Internet vous êtes certainement déjà tombé sur des bannières clignotantes vous indiquant que vous êtes le 1 000 000e visiteur et que vous venez d'être sélectionné pour remporter une voiture. Une fois arrivé sur le site vers lequel cette publicité vous redirige, le discours n'est plus le même… Vous avez seulement gagné le droit de participer à un tirage au sort. Et «gagné» est un grand mot, car sans avoir vu cette bannière et en rentrant juste l'adresse du site vous auriez eu exactement le même droit. Le but de ces manœuvres est surtout de vous amener à remplir des formulaires pour récupérer votre adresse mail au sein d'une base de données qui servira ensuite à des envois groupés de spams.

Une voiture à gagner: plus une malchance qu'une réelle chance

Voici typiquement le genre de publicité mensongère que l'on peut trouver sur la Toile. Et oui, vous êtes le millionième visiteur et, sans même jouer, vous avez déjà gagné!

En revanche, une fois que vous suivez le lien vous vous apercevez que vous avez surtout le devoir de remplir un formulaire détaillé pour participer à un tirage au sort.

LES 2 CONSEILS micro actuel

Ne perdez pas de temps avec ces vrais/faux jeux concours, néanmoins si vous souhaitez tenter quand même votre chance:

1 Évitez d'utiliser votre adresse mail principale sous peine de la voir être spammée.

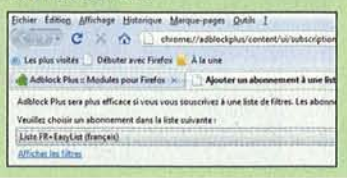
2 Créez-vous une adresse sur un webmail gratuit comme Hotmail ou Gmail que vous réservez à cet usage.

Évitez les publicités mensongères

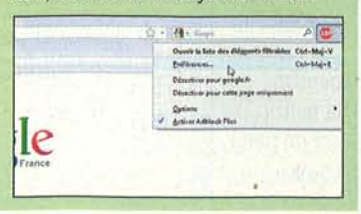
ÉTAPE 1 Ouvrez votre navigateur Firefox. Rendez-vous ensuite à l'adresse **https://addons.mozilla.org/fr/firefox/addon/1865/**. Sur cette page, cliquez sur le lien **Ajouter à Firefox**.

ÉTAPE 2 Dans la nouvelle fenêtre qui s'ouvre cliquez sur **Installer maintenant**. Le téléchargement se lance et l'installation s'effectue automatiquement. Vous êtes ensuite invité à redémarrer le navigateur. Cliquez sur **Redémarrer Firefox**.

ÉTAPE 3 Au redémarrage, une fenêtre vous indique que vous avez la possibilité de souscrire à une liste de filtres. Laissez les paramètres par défaut et cliquez en bas de la page sur **Ajouter l'abonnement**. Adblock est maintenant activé et il apparaît sous la forme d'un panneau d'obligation marqué des lettres ABP.



ÉTAPE 4 Pour régler le plug-in, cliquez sur la flèche à droite du panneau. Vous aurez par exemple la possibilité de le désactiver ou d'établir finement vos préférences. Néanmoins, si la pub reste acceptable ne la désactivez pas sur les sites que vous aimez. Pour certains d'entre eux, c'est le seul moyen d'exister.



16 août

Adobe délivre en urgence un patch correctif pour Reader et Acrobat suite à une faille détectée.

Le piège de la faille

N°10 le plus opportuniste

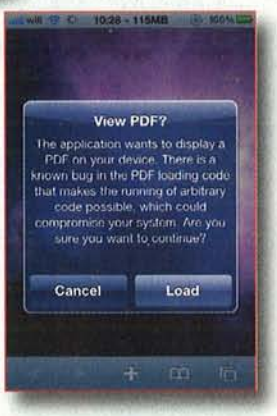
Certains logiciels, très largement installés sur vos ordinateurs, sont des portes d'entrée pour toutes sortes de nuisances en provenance du Net. Elles peuvent endommager votre PC.

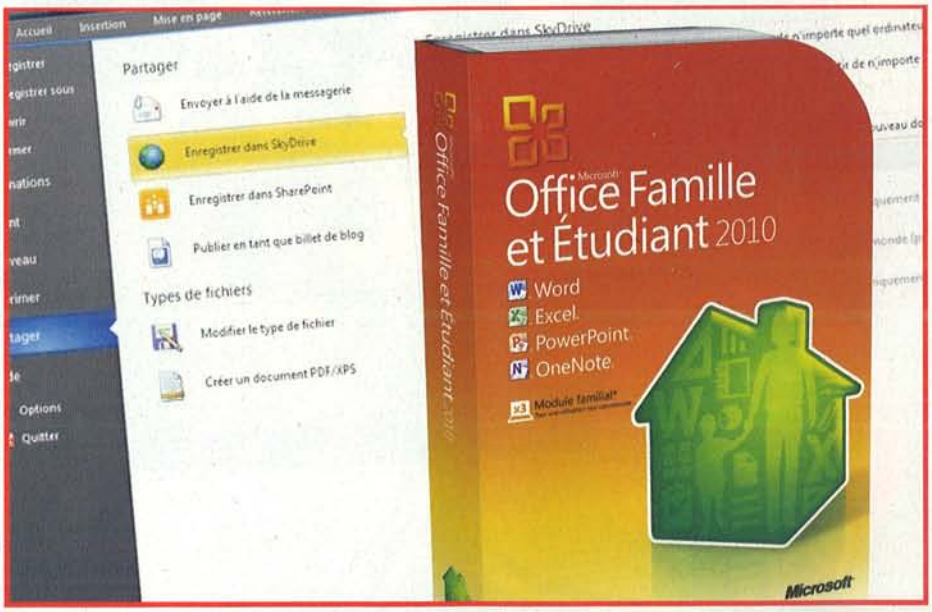
C'EST QUOI ? Sur votre ordinateur, vous disposez presque tous de certains logiciels incontournables: une suite bureautique, un lecteur de fichier PDF ou un éditeur d'images par exemple. Les pirates le savent bien et ils ciblent tout particulièrement les failles de ces logiciels largement distribués pour être certains de toucher le plus grand nombre de victimes potentielles. Pour contrer ce type d'attaques, il est vraiment indispensable que vous soyez équipé d'un antivirus à jour pour une parfaite efficacité. Il est important également de vérifier que tous vos logiciels sont eux aussi à jour pour rester à l'abri de ce type de piratage.

Acrobat et Office: deux logiciels à « faille »

En 2010, Acrobat et plus généralement les produits Adobe ont été la cible de plusieurs attaques directement liées aux failles présentes dans les logiciels de la marque.

Ce type de faille ne s'arrête pas à l'univers des ordinateurs. Les téléphones portables qui se rapprochent de plus en plus d'un ordinateur en sont aussi victimes. Dernièrement, c'est la faille sur les documents PDF qui a ouvert la voie au piratage de l'iPhone.



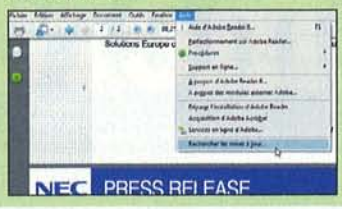


Office et ses composants sont aussi régulièrement la cible d'attaques. Il est donc nécessaire de régulièrement procéder aux mises à jour de la suite sous peine d'être victime d'attaque via des codes malicieux insérés dans les documents Office.

Mettez à jour vos logiciels

ÉTAPE 1 Commencez par ouvrir le logiciel que vous souhaitez mettre à jour. Pour cet exemple nous avons choisi Acrobat Reader qui a été au centre de l'actualité récente à cause d'une faille permettant de lancer un code malicieux caché au cœur d'un PDF.

ÉTAPE 2 Après avoir ouvert le logiciel, cliquez sur **Aide** dans le menu qui s'ouvre choisissez **Rechercher les mises à jour**. Une fenêtre s'ouvre et vous indique les mises à jour disponibles. Cette manipulation est valable pour la plupart des logiciels.



ÉTAPE 3 Cliquez sur **Installer maintenant** pour appliquer les mises à jour. Il est important de maintenir à jour la totalité de vos logiciels. Aucune méthode ne garantit une sécurité à 100, mais alliées à un antivirus bien paramétré, ces mises à jour assurent une meilleure protection.

LES 2 CONSEILS microactuel

Les logiciels vous proposent souvent une mise à jour quand vous les utilisez, ce qui vous pousse à l'annuler. Un conseil: agissez méthodiquement.

1 À un moment précis, faites les mises à jour de votre système et des logiciels.

2 Planifiez ces tâches automatiquement. Une fois par mois est une bonne moyenne et cela vous assure de disposer d'un système « up to date » !