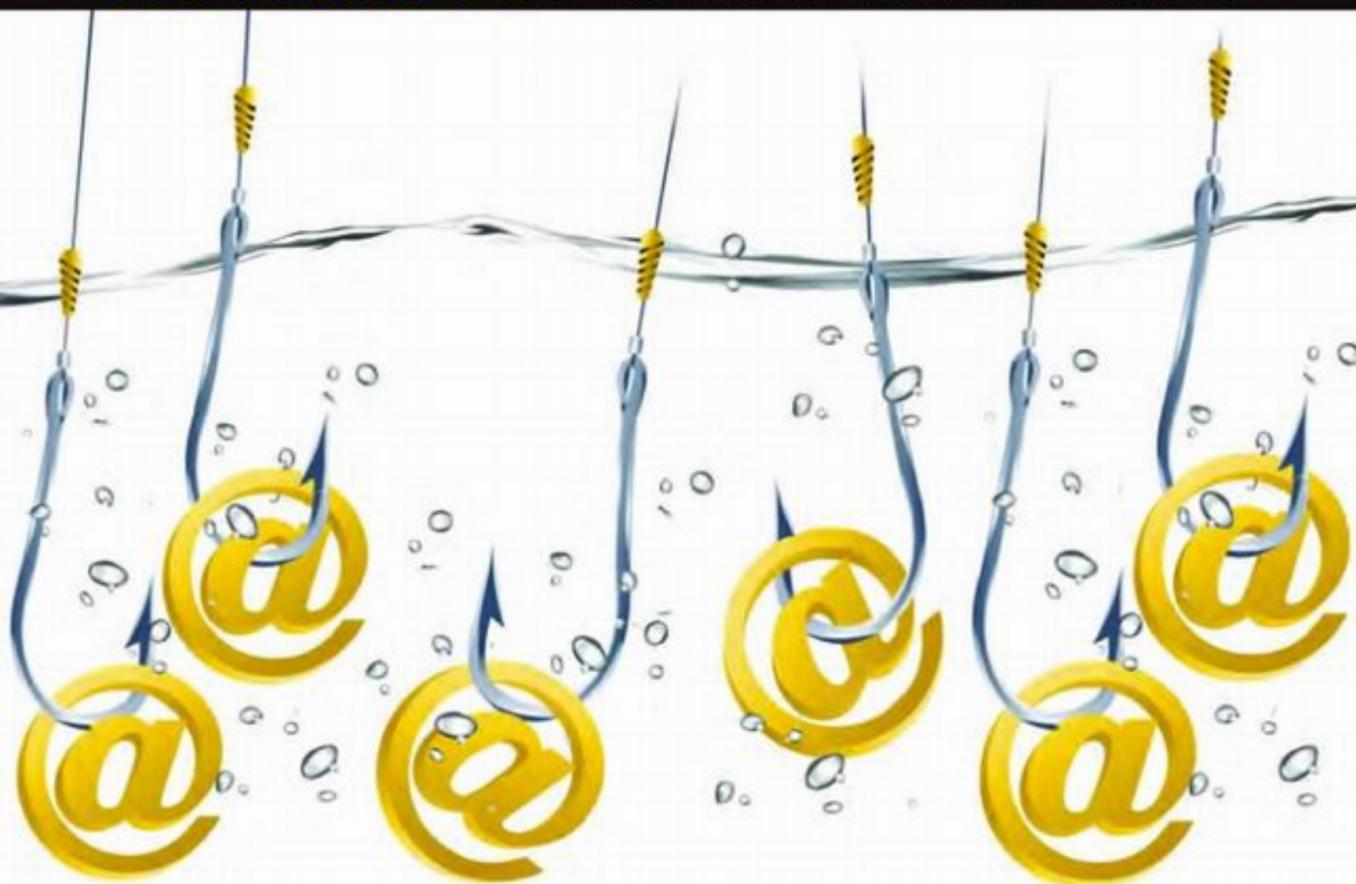


Évitez les pièges du Net les plus grossiers

Pour vous convaincre que certaines fenêtres ou messages imprévisibles surgissant à l'écran ne vous veulent pas du bien, nous avons volontairement mis notre ordinateur en mode faillible pour vous prouver que les tentatives d'atteinte à votre sécurité numérique ne sont pas à prendre à la légère.

NOS 5 CONSEILS POUR PRÉVENIR LES PIÈGES



1 Lisez mieux vos mails
Tant qu'un de nos lecteurs se fera encore « gentiment » avoir par un mail faussement prometteur, nous répéterons inlassablement ces mises en garde de bon sens : aucun établisse-

ment public ou privé (banque, fournisseur d'énergie...) n'est censé vous demander de mettre à jour vos informations à partir d'un lien indiqué dans un courrier électronique. De la même manière,

ne croyez pas une seconde que l'on vous offre de l'argent ou des cadeaux de valeur sans contrepartie.

2 Vérifier l'adresse
Admettons que vous ayez ouvert le mail pour prendre connaissance de son contenu. Sans aucune action sur le courrier concerné, regardez bien l'adresse de l'expéditeur, surtout si le doute s'est installé à propos d'une demande de mise à jour d'informations personnelles. Vous constaterez alors que l'adresse diffère totalement du prétendu expéditeur : ni Microsoft, ni Paribas à l'horizon mais une

Ne croyez pas une seconde que l'on vous offre de l'argent ou des cadeaux de valeur sans contrepartie.

DES CADEAUX « EMPOISONNÉS »

Nouvelle venue dans la liste des fausses promesses, la fenêtre qui surgit sur des sites de confiance, en vous proposant de répondre à une enquête rapide. Seules quatre questions sont au programme avec à la clé l'un des quatre cadeaux possibles à choisir librement. Passons sur la crème anti-âge ou le kit de cigarettes électroniques pour lesquels vous ne paierez que les frais de livraison et concentrons-nous sur les deux cadeaux de valeur, rien de moins qu'un appareil photo numérique ou une tablette. Méfiance, car ces cadeaux cachent en réalité un abonnement à près de 80 euros par mois, où vous devrez répondre régulièrement à des quiz pour d'hypothétiques récompenses. Un conseil ? Bannissez le site www.rockyfroggy.com de vos favoris.

Nous vous proposons les offres spéciales suivantes pour votre participation. Vous pouvez choisir un (2) seul produit de la liste ci-dessous. Merci pour votre participation à notre sondage! Disponible Aujourd'hui seulement:



Tablet Android®
Prix courant €109,85
Le vôtre est: **gratuit***
Ne payez que les frais d'expédition: € 1
Quantité disponible: (1)

Sélectionner ce don



Nikon Coolpix Appareil Photo ©
Prix courant €89,85
Le vôtre est: **gratuit***
Ne payez que les frais d'expédition: € 3
Quantité disponible: (1)

Sélectionner ce don

adresse internet totalement fantaisiste, du moins dans sa rédaction.

3 Ne cliquez pas au hasard
Si vous n'avez pas respecté la consigne précédente, rien n'est perdu tant que vous n'allez pas plus loin que la seule lecture de l'objet du message. Les pièges sont généralement accompagnés d'un lien hypertexte qui s'active donc d'un seul clic. Dans la majorité des cas alors, vous êtes redirigé vers une page factice (reproduisant le logo d'une banque ou d'un site administratif officiel) qui vous incite à renseigner plusieurs champs. Or, il est déjà trop tard, car un clic sur le premier lien est enregistré par le site pirate, et vous en recevrez du coup d'autres ultérieurement. Il va sans dire qu'il est fortement interdit de remplir en plus quelque formulaire que ce soit.

4 Vérifiez l'orthographe
Que ce soit dans l'intitulé du mail ou dans son contenu, il est assez aisé de déceler un piège sans être champion d'orthographe ou de grammaire. Si les pirates sont assez talentueux pour faire tomber certains d'entre vous dans le panneau, ils ne perdent pas de temps à rédiger en bon français et ont dans la plupart des cas recours à des logiciels de traduction automatique dont le moins que l'on puisse dire est que le résultat est plus qu'approximatif. Soit les phrases sont mal construites, soit de nombreuses lettres et symbole ponctuent la prose au point de la rendre illisible.

5 Utilisez les filtres
Le fait de déclarer un courrier électronique dans la catégorie indésirable ne suffit pas toujours à éloigner les tentatives de tous poils. Si la messagerie de votre fournisseur d'accès vous le permet, sélectionnez quelques termes que vous désirez bannir de votre boîte de réception. Ces derniers peuvent provenir d'une adresse ou de l'intitulé du mail. Attention toutefois, car si vous interdisez le mot cadeau, vous risquez de passer à côté de courriers inoffensifs envoyés par l'un de vos contacts.

FERMEZ TOUTES LES FENÊTRES PRÉSENTANT DES RISQUES

Si certaines fenêtres publicitaires ont un malin plaisir à dissimuler la croix qui permet de les fermer, ce n'est pas le cas de celles qui proposent de fausses mises à jour de logiciels existants. Mais les pirates sont malins et s'attaquent en priorité aux applications que vous utilisez ou connaissez de nom. Windows Media Player, Java ou Adobe sont des marques ou des noms familiers qui vont être détournés par les faussaires, soit par omission d'un terme (Media Player sans le mot Windows) soit en choisissant un logo qui ressemble de près à l'original dans sa forme et sa couleur. Regardez à titre d'exemple ces magnifiques « faux Java » et « Flash » que l'on vous incite à mettre à jour : c'est à s'y méprendre. Pire, en saisissant flash Video Player dans votre moteur de recherche préféré, le piège se referme, car vous tombez sur un site aux allures tout à fait correctes, mais qui nécessite une lecture attentive. L'intégralité de la page est issue d'une traduction vers le français pour le moins approximative. Même le mot télécharger contient un e venu d'on ne sait où. Une seule solution : ne pas utiliser le site www.telechargers.net, le piège est grossier. Les exemples sont légion de ces alertes qui peuvent déboucher sur un clic malheureux et imposer ensuite une restauration du système en espérant que quelques bouts de code malveillants ne se sont pas déjà glissés au cœur de votre version de Windows.

Flash Video Player

À propos de :
Flash® Video® Player est un module externe de navigation léger et une application d'exécution sur Internet riche qui offre des expériences cohérentes et engageante pour l'utilisateur, la lecture audio/vidéo et un principe de jeu étonnant.

Conditions :
En cliquant sur le bouton « Télécharger maintenant », vous reconnaissez que vous avez lu et accepté le [Télécharger Flash](#)

Remarque : votre antivirus doit vous permettre d'installer le logiciel.

Télécharger dès maintenant

Votre Version 11.7.800.236
[Télécharger des](#) [Maintenant télécharger la nouvelle version de Flash](#)

vos système:
Windows, française

Version 11.9.900.701 [Télécharger](#)

Que dire de cette fausse application ? Le mot Flash peut piéger certains d'entre vous, bien que le logiciel Flash Vidéo Player n'ait rien à voir avec la musique.

obsolète Java plugin détecté

Vous utilisez actuellement un plugin Java qui peut être obsolète
S'il vous plaît mettre à jour à la dernière version de Java (recommandé)

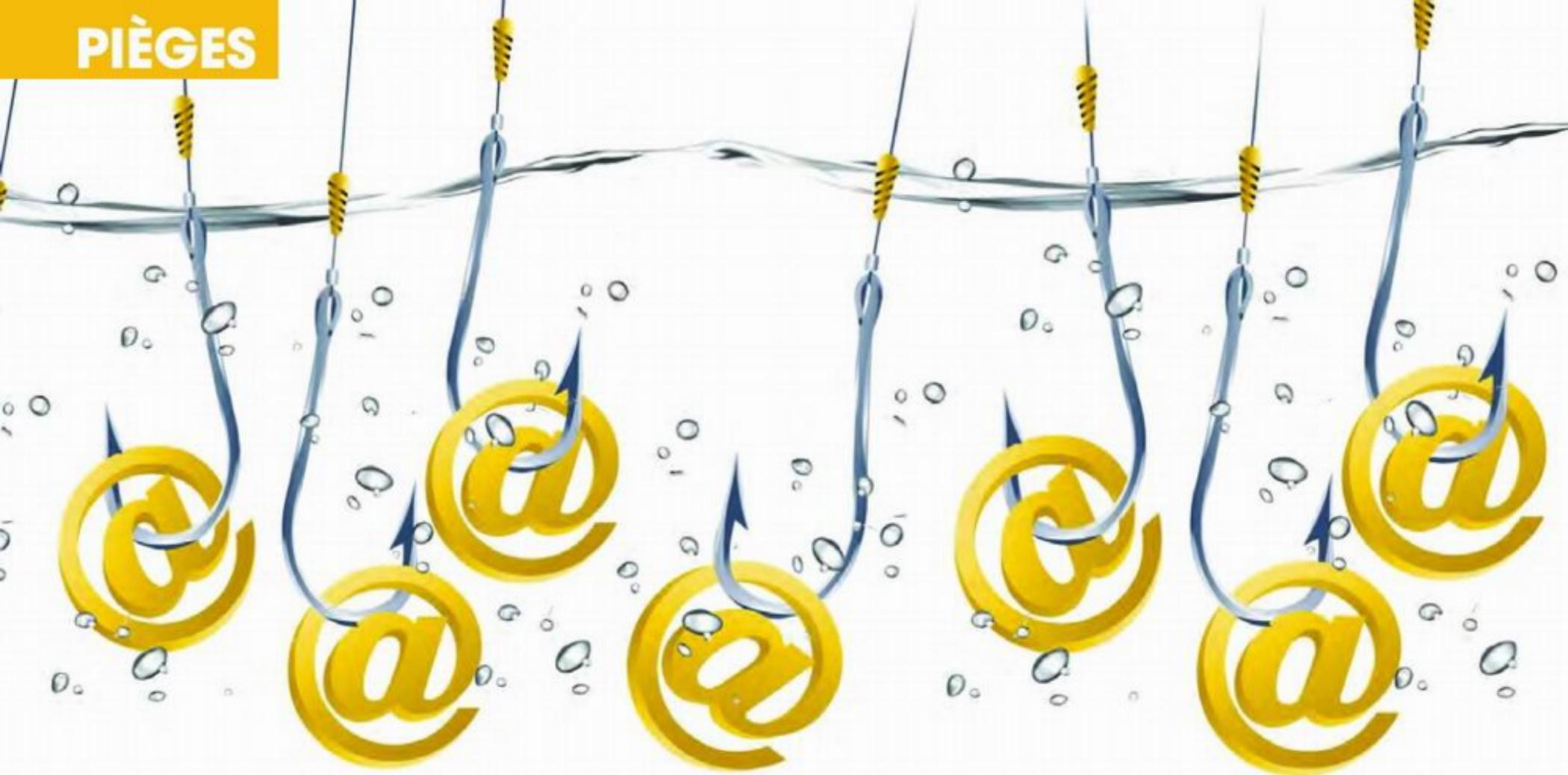
Télécharger Java pour Windows

La version recommandée 7 jour 25 (taille du fichier: 882 KB)

Accepter et démarrer le téléchargement libre

En téléchargeant Java, vous reconnaissez que vous avez lu et accepté les termes du contrat de licence d'utilisateur final

Que dire de cette fausse application ? Le mot Flash peut piéger certains d'entre vous, bien que le logiciel Flash Vidéo Player n'ait rien à voir avec la musique.



Mettez en œuvre la protection rapprochée

Les applications qui génèrent des fenêtres inopportunes ont parfois été installées à votre insu, et passé ce constat, il faut agir pour se débarrasser de toutes ces alertes encombrantes. Suivez le guide.

A force de naviguer sur la toile ou de télécharger des utilitaires sans risque pour votre système, vous êtes de plus en plus gêné par des messages de mise en garde, dont vous ne mesurez pas toujours la dangerosité. Pour partie malheureusement, vous êtes responsable de cette situation. Car la nouvelle mode de certains sites de téléchargement légaux (qui proposent des centaines d'utilitaires vérifiés) est de reconditionner les programmes d'origine (on appelle alors cela Repackaging ou Repack)

en ajoutant à l'archive quelques barres d'outils et autres déclencheurs de fenêtres publicitaires. Le site légal est bien entendu rémunéré pour cette discrète diffusion et vous bien embêté ! D'une manière générale, choisissez de préférence l'adresse internet de l'éditeur d'origine et en cas de doute, ne passez pas par une autre plateforme. Dans tous les cas, avant l'installation d'un programme de nettoyage, parcourez l'intégralité de la fenêtre d'accueil et veillez à décocher tous les termes « toolbar » et autres « browser ». Dans le cas contraire, l'utilitaire

ajoute des barres d'outils pénibles et peut même vous suggérer un nouveau navigateur internet par défaut. Si vous ne comprenez pas l'anglais, répondez no à toutes les demandes connexes à l'installation. Par précaution, créez un point de restauration après l'installation, et si d'aventure le logiciel ne répond pas efficacement à votre demande, revenez au jour précédent. Enfin, soyez attentifs lors du téléchargement : certains boutons « télécharger » ne concernent pas l'application demandée, mais envoient en réalité à des programmes parasites. La bonne parade consiste malheureusement à ne pas utiliser les liens commerciaux des moteurs de recherche, qui ont tout intérêt à vous gaver insidieusement d'applications inutiles. ■

Vous êtes parfois responsable de la venue de fenêtres publicitaires ou de fausses alertes de sécurité.

HALTE AUX NUISIBLES !

Bien que les annonces commerciales ne soient pas des pièges en elles-mêmes, leur accumulation à l'écran devient juste pénible. Certaines fenêtres contiennent tout de même une petite icône de désabonnement mais il est rare que cela soit définitif. D'autres sites permettent la suppression permanente, mais vous devrez parfois suivre des liens entièrement en anglais.

Regroupés sous le terme anglais Adware, les programmes qui font surgir des publicités sont le plus souvent incorporés dans des utilitaires ou le résultat de votre navigation (S'agissant de Google, voir les réglages de ce dernier dans le dossier page 24). Notre sélection d'outils ci-contre devrait venir à bout de la majorité de nuisances que vous vivez au quotidien.





4 utilitaires très efficaces

Pour lutter contre toutes formes de nuisances, ces utilitaires gratuits ou abordables feront l'affaire, à la condition de les récupérer directement chez l'éditeur d'origine.

Rogue Killer

A partir de cette bonne adresse, cherchez dans software puis sélectionnez le français. L'utilitaire gratuit Rogue Killer va prendre en charge le nettoyage de votre ordinateur, allant même jusqu'à traquer certaines informations contenues dans la base de registre de Windows. www.adlice.com



Spybot

Cet incontournable utilitaire gratuit s'installe en quelques secondes et procède à une analyse minutieuse de votre système. Sa détection est parfois spectaculaire. En revanche, pour corriger toutes les erreurs détectées, vous devrez le lancer en tant qu'administrateur. www.safer-networking.org/



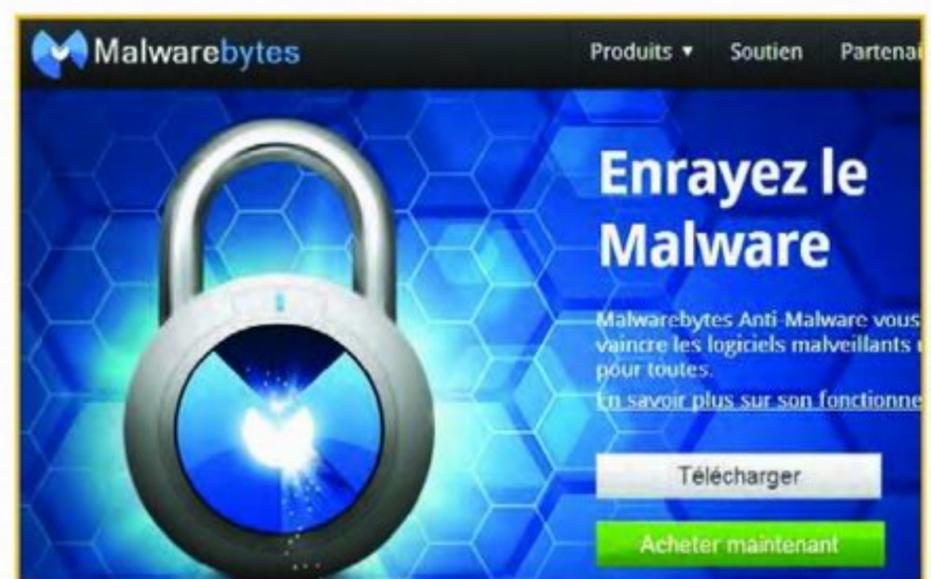
Adwcleaner

Pour chasser toutes les publicités inopportunes, cherchez dans la rubrique « Download » et vous trouverez votre bonheur. En quelques minutes seulement, l'application fait un ménage efficace. En contrepartie, vous devrez l'utiliser régulièrement en le relançant. www.bleepingcomputer.com



Malwarebytes

Dans sa version gratuite, le logiciel est imparable mais doit être lancé manuellement. L'acquisition payante à vie coûte moins de 25 euros (cherchez les promotions) et traite chaque jour en temps réel le mal en profondeur. L'investissement vaut le coup. <http://fr.malwarebytes.org/>



MÉFIEZ-VOUS DES IMITATIONS

Si le logiciel SbyBot est incontestablement performant et inoffensif, son presque synonyme Spy.Zbot est autrement plus néfaste. Ce cheval de Troie espion qui tente d'aspirer vos mots de passe s'infiltrer dans des publicités déjà infectées, spécialement dans les réseaux de téléchargement illégal. Nos utilitaires ci-dessus peuvent en venir à bout,

mais ce ne sera pas sans conséquence, et il vous faudra probablement supprimer tous vos points de restauration antérieurs à l'issue du nettoyage puis en créer un flam-bant neuf pour repartir du bon pied.