



Internet Gazette

Site : <http://aviquesnel.free.fr/Mederic>

20 octobre 2008

Numéro 81

Sommaire

<i>Spam : comment piéger l'internaute</i>	1
<i>Google fait du bien aux personnes âgées</i>	2
<i>Quelques informations à propos de l'encre des imprimantes</i>	2
<i>Flash Player comment votre webcam peut se retourner contre vous</i>	2
<i>Envoyez un message vide dans GMail</i>	3
<i>CPL : le courant porteur en ligne</i>	3
<i>Google invente la protection contre le mail désespéré de fin de soirée</i>	4
<i>Déplacer automatiquement la souris sur le bouton par défaut - Windows Vista</i>	5
<i>Microsoft s'attaque aux arnaques sécuritaires par pop-up</i>	5
<i>Les principaux formats d'image</i>	6
<i>Les principaux formats vidéo</i>	6
<i>Les principaux formats audio</i>	7
<i>Vista : contrôle des alertes UAC par Norton</i>	7
<i>Paris, Lyon, Lille, Toulouse, Marseille et Nice dans Google Street View</i>	8

Spam : comment piéger l'internaute

Des chercheurs de BitDefender viennent de découvrir un nouveau moyen utilisé par les spammeurs pour récupérer des adresses e-mails valides. Cette nouvelle tactique combine en fait trois techniques réunies au sein d'un même message électronique, ce qui diminue d'autant les chances des internautes abusés de passer au travers des mailles du filet.

La première technique mise sur l'accusé de réception. Si l'internaute destinataire clique

sur cet accusé de réception, qui normalement sert à confirmer à l'expéditeur que son message a bien été reçu et/ou lu, cela permet au spammeur de confirmer que l'adresse ciblée est bien valide, et sera donc en mesure de recevoir tout un flot de nouveaux spams.

Si l'internaute choisit de ne pas utiliser l'accusé de réception, c'est là qu'intervient la deuxième technique du spammeur : un lien dans l'e-mail renvoyant vers une image stockée sur un serveur distant. Le client de messagerie bloque habituellement automatiquement ce genre de contenu. Pour le débloquer,

l'internaute doit accepter le chargement de l'image. S'il le fait, le spammeur reçoit confirmation que l'adresse utilisée est bien valide.

La validation d'adresse, "l'arrêt de mort de la boîte mail"

Si l'utilisateur ne succombe toujours pas à ces pièges, le spammeur joue sa dernière carte : le faux lien de désinscription cliquable. Bien sûr, celui-ci est fictif et ne sert qu'à confirmer, une fois de plus, la validité de votre adresse e-mail.

Cette mise en garde de BitDefender sert surtout à rappeler à tous les internautes

que le spam est un danger à prendre au sérieux. "La validation de leur adresse e-mail par les utilisateurs revient à signer 'l'arrêt de mort' de leur boîte de messagerie", précise Vlad Valceanu, directeur du centre de recherche anti-spam de BitDefender.

"Le prochain mail envoyé par les spammeurs pourra contenir un malware ou un code malveillant qui peut effacer leur disque dur ou récolter des informations confidentielles et les faire sortir de l'ordinateur, comme par exemple les numéros de cartes bancaire qui sont utilisés pour les achats en ligne", poursuit-il.

Google fait du bien aux personnes âgées

Qui l'eut cru ? Faire des recherches sur Google pourrait améliorer l'activité cérébrale, surtout auprès des personnes âgées. C'est en tout cas l'avis très sérieux de chercheurs du [Center on Aging](#) de l'Université de Californie à Los Angeles (UCLA) qui en est venu à la conclusion que rechercher des informations sur Internet était bon pour stimuler le cerveau.

Internet, un stimulant avéré

Les chercheurs ont mené une étude sur des sujets âgés de 55 à 76 ans. Ils ont séparé ces personnes en deux groupes bien distincts : ceux qui ont l'habitude de surfer sur le Web et les néophytes.

Tous ont subi un examen IRM afin de déterminer l'action de

leur surf sur leur cerveau. C'est ainsi qu'ils ont pu constater que rechercher des informations sur le Web stimule terriblement le cerveau, notamment les aires dédiées au choix et au raisonnement. Le professeur Gary Small indique que ces résultats sont très encourageants et que la technologie pourrait bien être bénéfique à l'effort mental.

Quelques informations à propos de l'encre des imprimantes

Les cartouches génériques vous font gagner entre 30 et 50% sur le prix d'achat. Pour plus de sécurité il vaut mieux se fier aux grandes marques telles Armor ou Pelikan.

Si vous voulez recharger vos cartouches avec les kits de remplissage et leur seringue, sachez que ce sont les imprimantes Canon qui supportent le mieux ce procédé (plus de 50% d'économie), quasiment impossible avec les Epson.

Flash Player comment votre webcam peut se retourner contre vous

Une faille dans le lecteur vidéo permet à des pirates de prendre le contrôle de votre webcam et de votre micro grâce à la méthode du clickjacking.

Comment pouvez-vous perdre le contrôle de votre webcam en utilisant le lecteur vidéo Flash Player ? Tout simplement en étant victime d'une nouvelle forme de piratage, le clickjacking.

Son but : attirer, à son insu, un internaute vers un code malicieux pour finalement prendre le contrôle de son ordinateur ou de ses périphériques en l'amenant à cliquer sur des boutons dangereux. Les navigateurs Web et Flash Player jouent ici le rôle d'appât.

Dans le cas du lecteur vidéo d'Adobe, un hacker peut tout à fait à distance changer les paramètres de Flash Player pour lui permettre d'activer l'envoi de flux vidéo et audio pour que ce pirate puisse accéder à la webcam de l'internaute usurpé.

Comment ce piratage se déroule-t-il ? Un page HTML vient discrètement se superposer à la première, tout en demeurant invisible aux yeux de l'utilisateur. Quand celui-ci clique sur la première fenêtre, ses clics sont automatiquement propagés sur la deuxième page HTML cachée.

Ensuite, un simple clic sur une fenêtre de lecture Flash permet au pirate d'accéder au propriétaire de Flash Player pour lui permettre de déclencher à distance la webcam et le micro, pour pouvoir vous filmer et vous écouter à votre insu.

Averti de cette faille, Adobe pense qu'il faudra attendre la version 10 de son lecteur vidéo pour que le problème soit résolu. En attendant, [l'éditeur donne quelques conseils](#) pour ne pas être victime de clickjacking via son Flash Player.

Il suffit de se rendre dans le gestionnaire des paramètres, de se rendre dans l'onglet "Paramètres globaux de contrôle d'accès" et de choisir l'option "Toujours refuser" pour empêcher les sites Web d'accéder, ou de demander l'autorisation d'accéder, à la webcam ou au microphone

Une extension du navigateur Firefox baptisée NoScript permet de se préserver du clickjacking.

La nouvelle version Firefox 3.1 a l'objectif de bloquer les scripts qui pourraient permettre à un éventuel hacker de prendre le contrôle d'une machine via son navigateur Web. Il faut savoir que ce type d'attaque permet à un pirate de détourner les clics de l'utilisateur d'un PC contre son gré.

Envoyez un message vide dans Gmail

Est-ce qu'il vous arrive d'envoyer des courriels dans lesquelles il n'y a qu'un objet et où le corps de votre texte est vide? Des courriels du genre: es-tu libre pour déjeuner? Ou: je suis en retard.

Si vous faites parvenir ce genre de message à vos contacts depuis Gmail, vous savez qu'il vous préviendra que le corps de votre texte est vide. Il existe une astuce qui vous permet d'envoyer le message directement sans que Gmail n'affiche cet avertissement. Tout ce que vous devez faire c'est d'ajouter EOM ou eom à la fin de votre objet. EOM

signifie End of message.

CPL : le courant porteur en ligne

Le principe de fonctionnement du CPL est relativement simple. Il consiste à superposer au courant électrique de votre domicile (le signal 50 Hz du courant électrique européen) un signal à plus haute fréquence transportant des informations numériques. Le CPL se propage alors sur l'installation électrique et peut être reçu par tout récepteur s'y trouvant relié. Il est ainsi possible de créer un réseau local Ethernet à partir des prises électriques de votre domicile. On parle alors de CPL haut débit, par opposition au CPL bas débit, qui, lui, est utilisé par des applications domotiques, par exemple pour piloter votre chauffage ou vos volets roulants.

2. Comment savoir si le CPL haut débit va fonctionner chez moi ?

C'est impossible. Sauf à connaître l'état de votre installation électrique, comme la longueur des câbles qui relie deux prises. Mais, dans de très nombreux cas, ça fonctionne. En effet, les signaux numériques ont une portée théorique de 1 000 mètres avant qu'ils ne soient totalement atténués. Et, en règle générale, la portée efficace du CPL est de 300 mètres... Ça devrait donc marcher sans souci dans un appartement ou une maison récente. En revanche, si vous habitez dans une vieille maison ou dans un appartement ancien, par exemple là où deux

compteurs électriques existent, rien n'est garanti.

Rappelons enfin que, comme les fils électriques n'ont pas été conçus pour véhiculer des données numériques, ils peuvent être perturbés par des flux électromagnétiques. Et ici inutile de lutter. Ces perturbations peuvent tout aussi bien venir d'un écran d'ordinateur, d'un transformateur électrique ou de tout type d'émetteur-récepteur, comme la radiodiffusion, les communications civiles, les radios amateurs...

3. Peut-on installer plus de deux prises CPL sur son installation ?

Oui, mais... Le fait de relier une troisième prise divise théoriquement par deux le débit. Dans la pratique, le débit d'une prise CPL est aléatoire. Par exemple, si vous utilisez le CPL pour « streamer » des flux vidéo haute définition entre la box de votre FAI et un téléviseur, il est fort possible que l'ajout d'une troisième prise fasse que cela ne fonctionne plus. Mais, s'il s'agit de relier plusieurs PC à Internet, cela ne devrait pas poser de problème. Si, bien entendu, vous disposez à la base d'un débit satisfaisant.

4. Comment brancher sa prise CPL ?

Avec précaution. C'est tout le problème du CPL. L'installer sur une prise multiple est à éviter absolument. Pour deux raisons. La première, c'est que les prises multiples sont protégées par un parasurtenseur. Donc le CPL ne passe pas. La seconde, c'est que les adaptateurs électriques, par définition, perturbent le

signal CPL. Les pires sont en général les adaptateurs des téléphones portables. L'idéal est donc de ne rien relier d'autre que son adaptateur CPL à une prise électrique. Et, au pire, il faut utiliser un doubleur de prise. D'un côté vous y reliez l'adaptateur, de l'autre, une multiprise disposant d'un câble de 1 mètre au moins. Ainsi, vous éloignerez d'autant les perturbations venant des autres alimentations électriques.

5. Comment relier plusieurs appareils sur une même prise CPL ?

Avec une multiprise CPL. C'est l'innovation du moment. [Le constructeur Zyxel](#) vient de commercialiser une grosse multiprise supportant le CPL et offrant la possibilité de relier jusqu'à quatre appareils en Ethernet. Si l'idée est ingénieuse, le CPL n'étant pas perturbé par les appareils électriques, elle a le défaut de diviser le débit Internet des appareils ainsi reliés.

6. Peut-on utiliser des prises CPL de marques différentes ?

Oui, mais... Ce n'est pas tant la marque qui compte, que la technologie. En général, quand on ne sait pas ou que l'on ne veut pas s'embêter, il est préférable de prendre des adaptateurs de même marque. Ne choisir que du Homeplug AV 200 Mbits, en attendant la normalisation du CPL.

7. Comment relier le routeur de son FAI en CPL ?

Bêtement, pour l'instant. La solution est ici très simple : vous reliez l'une des prises

Ethernet du routeur à l'une des prises électriques de votre domicile..

8. Quel est le vrai débit du CPL 200 ?

Le défaut du CPL, c'est l'atténuation du débit à mesure que vos adaptateurs s'éloignent l'un de l'autre (il s'agit de la longueur réelle du câblage électrique entre deux prises). Là-dessus, vous ajoutez le mensonge outrancier des vendeurs de prises CPL. Car le débit du CPL 200 n'est pas de 200 Mbit/s mais de légèrement plus de 50 Mbit/s, c'est-à-dire 6,25 Mo/s.

9. Peut-on utiliser du CPL et du Wi-Fi sur son réseau domestique ?

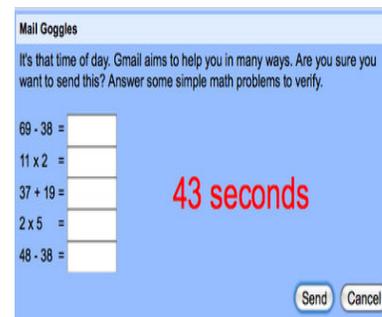
Oui. L'idéal est même d'utiliser conjointement les deux technologies en fonction des obstacles à contourner. Le CPL et le Wi-Fi peuvent être utilisés pour apporter des solutions originales, comme [celle proposée par Bewan](#) pour étendre la portée du Wi-Fi. Mais, comme cette solution est presque dépassée (le Wi-Fi est en 802.11b/g, le CPL du 85), on attendra des versions plus évoluées (802.11n et CPL 200) pour y trouver un réel avantage.

10. Le CPL est-il sécurisé ?

Parfois. Le compteur électrique n'est pas un pare-feu. Même s'il est - comparativement au Wi-Fi - improbable de voir son réseau CPL piraté, les adaptateurs disposent de systèmes de cryptage activables par la simple pression d'un bouton. L'amusant est de voir [qu'EDF utilise le CPL sur ses](#)

[nouveaux compteurs électriques pour les relever.](#)

Google invente la protection contre le mail désespéré de fin de soirée



Voilà une trouvaille des labos de Google qui risque fort de rendre service à ceux vivant un chagrin d'amour. Ce système permet en effet d'éviter le mail affligeant envoyé à son ex un soir de déprime et que l'on regrette instantanément.

Du calcul mental pour calmer les esprits

Le principe est simple : imposer à l'expéditeur un temps de la réflexion. Comment ? En imposant des opérations de calcul mental au moment de l'envoi du mail ! Trouver la réponse à 69 - 38, 37 + 19, ou 48-38 à deux heures du matin sans avoir forcément les idées claires, ça calme. Et ça donne surtout le temps de relativiser le geste que l'on est en train de faire pour éviter un drame.

L'application est simple à configurer, il suffit de se rendre dans les réglages Gmail, puis Labs, puis de sélectionner l'option Mail Goggles [comme](#)

[expliqué dans cette page](#). On pourra ensuite la programmer pour être active les soirs de son choix. Google sauveur des histoires d'amour qui finissent mal ? En général...

Déplacer automatiquement la souris sur le bouton par défaut - Windows Vista

Pour gagner du temps, vous pouvez faire en sorte que le pointeur de la souris soit automatiquement placé sur le bouton par défaut des boîtes de dialogue que vous manipulez. Il vous suffira alors de cliquer sur le bouton gauche de la souris pour valider l'opération, sans avoir à bouger la souris.

1. Cliquez sur le bouton **Démarrer** puis sur **Panneau de configuration**.
2. Cliquez ensuite sur l'option **Souris** de la rubrique **Matériel et audio**.
3. Ouvrez ensuite l'onglet **Options du pointeur**.
4. Dans la zone **Alignement**, cochez alors la case **Déplacer automatiquement le pointeur sur le bouton par défaut dans la boîte de dialogue**.

5. Cliquez enfin sur le bouton **OK**. Désormais, le pointeur de la souris sera placé automatiquement sur le bouton par défaut dans les boîtes de dialogue.

Microsoft s'attaque aux arnaques sécuritaires par pop-up

Sécurité - L'éditeur porte plainte aux Etats-Unis contre plusieurs sociétés qui vendent de faux logiciels de sécurisation de PC. Leur arnaque : convaincre leurs victimes que leur ordinateur est compromis en faisant apparaître sur leur écran un message d'alerte.

Qui n'a jamais vu sur son écran apparaître un pop-up qui prévient d'un problème grave dans le système Windows et propose un logiciel soit-disant miracle pour réparer la faille, contre quelques dizaines d'euros.

C'est contre ce type d'arnaque que Microsoft et le procureur général de l'État de Washington ont lancé l'offensive : ils ont conjointement porté plainte contre plusieurs sociétés américaines coupables de ce type d'offres frauduleuses, et d'autres malfaiteurs encore anonymes.

Ce pop-up utilise une fonction baptisée Windows Messenger (rien à voir avec la messagerie instantanée de Microsoft), qui est censée permettre aux administrateurs d'envoyer des messages à des PC connectés à un même réseau. Sous prétexte d'avoir découvert une faille, il propose alors une vérification complète du système, puis un logiciel payant, capable de sécuriser à nouveau l'ordinateur.

Des logiciels payants qui n'apportent rien

Ces logiciels s'appellent Registry Cleaner XP, Scan & Repair, Antivirus 2009, Malware Core, WinDefenderXPDefender.com ou WinSpywareProtect.

Bien sûr, leur action est nulle. « Il s'agit d'une véritable arnaque des consommateurs », a expliqué Rob McKenna, le procureur général de l'État de Washington. « Les utilisateurs sont amenés à faire un semblant de scan de leur ordinateur et conduits à payer pour un logiciel dont ils n'ont pas besoin. »

Les messages d'alertes pouvaient apparaître de façon très répétée, certaines adresses IP recevant plus de 200 pop-up par jour, expliquent les plaintes. Selon le Computer Spyware Act américain, adopté en 2005, les suspects risquent jusqu'à 2 000 dollars d'amende par infraction commise, plus des dommages et intérêts. De plus, les particuliers qui s'estiment lésés sont invités à porter plainte de leur côté, a précisé Microsoft.

Les principaux formats d'image

Nom / extension	Utilisation	Logiciels à utiliser
JPEG / .jpg	Ideal pour mettre et échanger des photos sur Internet. Pour la retouche, attention au niveau de compression.	Tous. Les visionneuses Windows (aperçu), diaporamas, tous les logiciels de retouche...
TIFF / .tiff	Trop lourd pour Internet. A utiliser pour de l'impression et retouche.	Aperçu Windows, logiciels de retouche (Photoshop, PaintShop...)
PNG / .png	Très bon sur Internet, gère les transparences. Bonne qualité mais un peu plus lourd que le JPEG.	Aperçu, diaporama. Pour la retouche, privilégier Fireworks dont c'est le format natif
GIF / .gif	Très utile et léger sur Internet : schémas, cartes, icônes, petites animations. A oublier pour l'impression.	Se lit avec tous les logiciels, se retouche et se crée avec ImageReady, Fireworks, etc.
PSD / .psd	Pas pour le Web. A utiliser pour la retouche sous Photoshop	Format natif de Photoshop
PSP / .psp	Idem que le PSD, mais pour PaintShop Pro	Format natif de PaintShop Pro
BMP / .bmp	Format non compressé à éviter. Est connu uniquement car c'est le format par défaut sous Paint.	Format Bitmap pour Windows, principalement utilisé avec Paint.

Les principaux formats vidéo

Format / extension	Utilisation	Logiciel / support
AVI / .avi	Dans un fichier AVI, chaque composante audio ou vidéo peut être compressée par n'importe quel codec (DivX et mp3 par exemple). C'est un "conteneur" très pratique, le plus utilisé.	Normalement tous les logiciels de lecture vidéo.
WMV / .wmv	Un format conteneur de Microsoft et sa famille de codecs vidéo. On le trouve souvent chez des vidéos en streaming ou en téléchargement.	Nécessite Windows Media Player.
MOV / .mov	Format conteneur d'Apple, pouvant contenir un très large choix de codec, y compris haute définition.	Nécessite Quicktime.
DivX et Xvid	Les codecs vidéo les plus utilisés. Permet de diviser par 6 la taille d'un film en DVD sans trop de perte de qualité. Xvid est le concurrent libre de DivX.	Nécessite l'installation des codecs DivX / Xvid à jour, qui sont inclus dans de nombreux lecteurs vidéo.
MKV / .mkv .mka .mks	Format conteneur russe, pouvant contenir de très nombreux codecs.	Se lit avec VLC, Media Player Classic et quelques autres après l'installation des Codecs.
H264 / MPEG 4 AVC	C'est le Codec utilisé pour la haute définition.	Se retrouve dans les Blu-ray. Se lit avec la majorité des lecteurs vidéo à jour.
FLV / .flv	Le format Flash Video, utilisé en quantité sur Internet (comme Linternaute Video).	C'est le format natif d'Adobe Flash Player, s'ouvre parfaitement avec VLC.

Real Video /
.rmvb Codec video propriétaire de Real Networks.

S'ouvre avec RealPlayer ou
RealAlternative

Les principaux formats audio

Format / extension	Utilisation / intérêt	Logiciel / lecteur
WAV / .wav	Le WAV est un format ancien, lourd et peu pratique. Il reste incontournable sous Windows puisque c'est dans ce format qu'on extrait / lit les morceaux d'un CD.	Tous les lecteurs. Audacity pour les modifications.
MP3 / .mp3	Le plus connu des codecs audio. Permet de diviser par 6 ou 8 la taille d'un fichier WAV sans trop de perte.	Tous les lecteurs
WMA	Format de compression audio de Microsoft. Assez répandu sur Internet.	La majorité des lecteurs et baladeurs lisent les WMA
OGG Vorbis / .ogg .ogv, .oga, .ogx	Le concurrent libre et plus efficace que le MP3. Il compresse avec perte.	Se lit sans problème avec les lecteurs du monde du logiciel Libre (Foobar2000). Pour les autres, il faut souvent installer des codecs.
FLAC	Format très apprécié puisqu'il compresse sans perte de qualité. En contrepartie, la réduction de taille est moindre, de 30 à 70 %.	Nécessite le plus souvent l'installation de plug-ins spécifiques.
AAC	Format de compression audio (avec perte de qualité) utilisé par Apple. Les morceaux achetés sur iTunes Music Store sont compressés en AAC. Il existe depuis peu sans perte : Apple's Loseless (ALAC).	Se lit avec iTunes. Format musical pour iPod.

Vista : contrôle des alertes UAC par Norton

UAC = User Account Control = contrôle du compte utilisateur

Norton UAC Tool est un utilitaire qui redonne à l'utilisateur le contrôle des alertes UAC. Jusqu'ici, l'utilisateur avait le choix entre garder UAC et ses alertes, désactiver UAC et perdre ses sécurités, ou accepter un fonctionnement de l'UAC silencieux mais peu efficace et générateur d'autres alertes dans le système.

Norton UAC Tool fait qu'il est possible de créer une version plus intelligente d'UAC. Le programme permet de conserver toutes les sécurités liées à l'UAC (DEP, isolation IE, contrôle des accès système, etc.) en limitant au strict minimum les alertes utilisateur. Notamment en permettant à l'utilisateur de choisir les fonctions clés du système qui ne méritent pas de générer une alerte.

- Téléchargez le logiciel en suivant [-- ce lien --](#) (le programme existe en version 32 et 64 bits)

- Installez-le et redémarrez le PC.

- Une fois le logiciel installé, les alertes UAC seront désormais gérées par Norton et prennent le nouveau look que montre l'illustration.

- Cette boîte donne des informations précises sur le processus qui déclenche l'alerte:

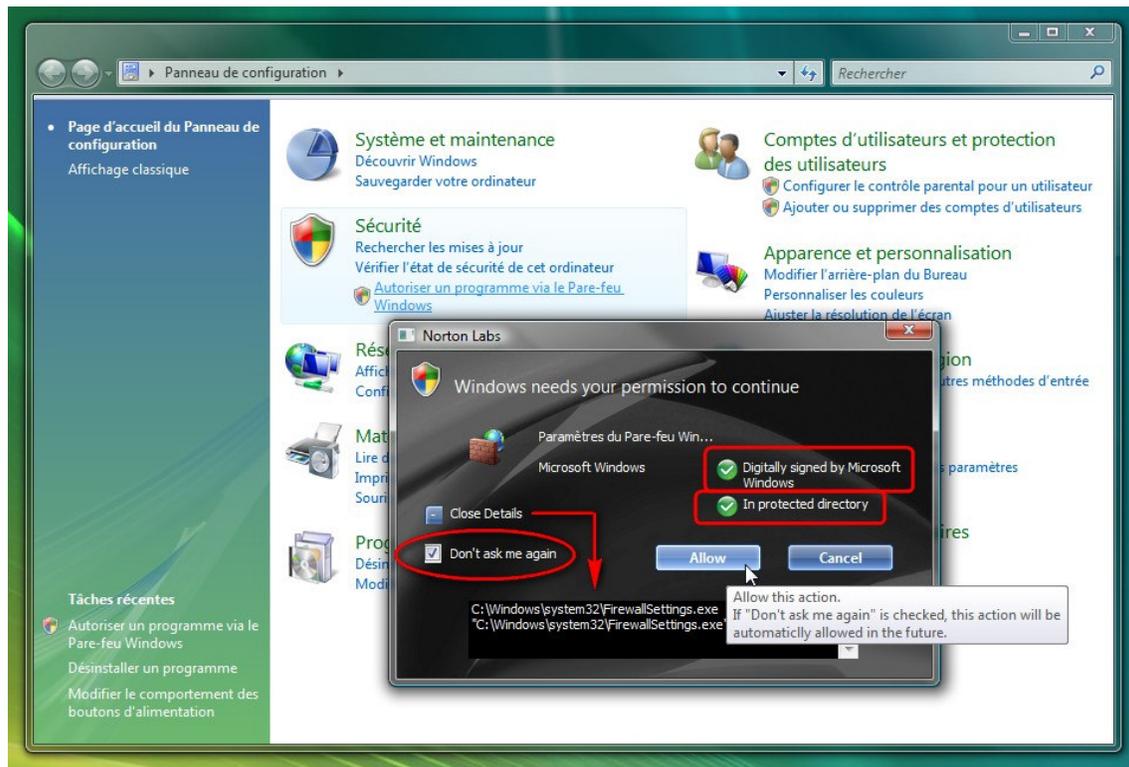
* Le logiciel indique si l'application est signée par Microsoft (**Digitally signed by Microsoft**)

* Si celle-ci provient d'un répertoire protégé (à priori, aucun malware n'atteint un tel répertoire)

* Les fichiers et processus déclencheurs de l'alerte (en cliquant sur **View Details**)

- Si Norton UAC connaît déjà l'application qui déclenche cette UAC et la reconnaît comme fiable et saine, il n'affichera pas l'alerte.

- Lorsque l'alerte est affichée (notamment sur les fonctions à élévation de privilèges du système), il suffit de cocher **Don't ask me again** ("Ne plus me demander") pour que cette fonction système ne déclenche plus d'alertes UAC. - Au bout de quelques jours, vous constaterez que les alertes sont beaucoup moins fréquentes et beaucoup moins intrusives. Vista n'en devient que plus agréable à utiliser!



Paris, Lyon, Lille, Toulouse, Marseille et Nice dans Google Street View

Google élargit son service de géolocalisation Street View, intégré à Google Maps, à plusieurs grandes villes françaises, comme le laissaient anticiper des [véhicules repérés dans la capitale](#). L'Hexagone est ainsi le premier pays européen à obtenir une couverture du service de Google, même si elle reste limitée à 6 villes : Paris, Lyon, Lille, Toulouse, Marseille et Nice.

En juillet dernier, le moteur de recherche avait donné un aperçu de Street View pour la France, en proposant des vues du [parcours du Tour de France](#).

Comme aux Etats-Unis, pour respecter la vie privée, Google s'efforce de flouter les visages ou les éléments d'identification tels que des plaques d'immatriculation de véhicules, apparaissant sur les clichés de Street View. [Le service avait fait l'objet de plaintes](#) à ce sujet à son lancement. Cet effort de confidentialité a été [salué par la Cnil](#), qui a donné son feu vert au service en France.