FAVICONE - INFO

Si vous avez installé Mozilla Firefox 3, vous avez peut-être été intrigué, comme moi, par un de ces messages s'affichant lorsque l'on clique sur l'habituel favicon :

- Ce site Web ne fournit pas d'informations concernant son identité.
- Vous vous trouvez sur xxxxxxx.com dont le détenteur est xxxxxx
- Votre connexion vers ce site est chiffrée afin d'empêcher l'interception des informations transmises
- Échec de la connexion sécurisée xxxxxxx.com utilise un certificat de sécurité invalide
- Ce certificat n'est pas sûr car il est auto-signé

Ne trouvant aucune explication complète au fonctionnement à ce nouveau système de sécurité instauré par Firefox 3, j'ai décidé de traduire cet article anglais. Bonne lecture !

Cet article est traduit et adapté de l'article anglais :
http://www.dria.org/wordpress/archives/2008/05/06/635/
Il a été écrit par Deb Richardson (alias dria) le 6 mai 2008, la traduction a été réalisée avec son accord.
Pour signaler une erreur de traduction, merci de me contacter

Informations sur les captures d'écrans : Les catpures ont été réalisées sous Macintosh et Kubuntu Linux, il se peut que l'interface soit légèrement différente pour votre plateforme.

Veiller à ce que les utilisateurs soient en sécurité et protégés lorsqu'ils qu'ils naviguent sur le Web est un des plus grands défis auxquels les développeurs de navigateurs Internet travaillent. Sécuriser un navigateur est un équilibre délicat entre la protection des utilisateurs contre les dangers du Web et la restriction excessive de la liberté de l'utilisateur de faire ce qu'il souhaite.

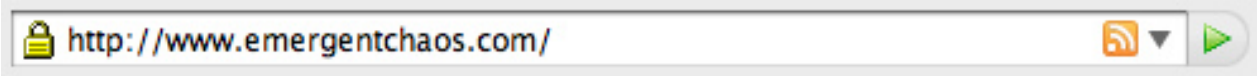
Un de mes nouveaux éléments de sécurité favoris de Firefox 3 est le bouton d'identification du site. Ce bouton remplace le fameux "cadenas", icône qui a si longtemps été le principal témoin de sécurité utilisé pour de nombreux navigateurs. Firefox 2, par exemple, indique que la connexion à un site est cryptée en changeant la couleur de fond de la barre d'adresse et en affichant ce "cadenas" :

Le majeur problème avec ce cadenas, c'est que beaucoup de gens lui font confiance plus que ce qu'il n'en offre. C'est d'ailleurs exactement ce que je pensais jusqu'à ce que j'ai une longue discussion avec Johnathan Nightingale (Gourou de la sécurité de l'interface utilisateur chez Mozilla et l'initiateur de cette fonction) qui m'explique que ce cadenas signifiait simplement "page cryptée" et non "page sécurisée". Là où ce cadenas donnait un sens bien précis quant-à la sécurité du navigateur, je lui avait donné un sens plus large qu'il ne méritait pas vraiment.

Mais alors quelle est la différence entre "crypté" et "sécurisé"?

Il s'avère qu'il n'est pas du tout difficile de créer un site Web faisant afficher ce cadenas à un navigateur. En fait, c'est même tellement facile, que tout le monde peut le faire, y compris les personnes malhonnêtes pour vous voler votre identité, vos coordonnées bancaires ou toute autre information intéressante qu'ils vont trouver. Certes, le cadenas signifie "transaction cryptée", mais ne donne aucune information sur la sûreté du domaine -auquel vous êtes en train de faire confiance, ndt- ni sur l'identité des personnes situées de l'autre côté de la connexion sécurisée.

Il est même possible d'usurper facilement ce cadenas, en voici un exemple :



Le cadenas n'est pas au bon endroit, et il n'est pas exactement celui du navigateur, mais beaucoup d'utilisateurs ne le remarqueront pas, et tomberont dans le panneau en se disant "cadenas égal sécurité". C'est une tromperie très simple et maladroite (le cadenas affiché ici n'est alors qu'un simple favicon -un favicon est une petite image choisie par le webmaster qui représente son site, ndt-), mais il suffit pour piéger certains utilisateurs.

C'était donc clair : ce procédé devait être amélioré.

Comment Firefox 3 rend les choses meilleures ?

C'est là que le nouveau bouton d'identification de site de Firefox 3 entre en jeu. Plutôt que de simplement afficher un petit cadenas quelque part, Firefox 3 dévoile autant que possible l'identité du site que vous êtes en train de consulter et fait en sorte que cette information soit facilement accessible par un simple bouton situé à l'extrémité gauche de la barre d'adresse.

Le bouton peut prendre un fond gris, bleu ou vert et affiche la boîte de dialogue d'identification de site lorsqu'on le clique. Celle-ci montre un "agent de passeports" gris, bleu ou vert, et montre un résumé des informations disponibles sur l'identité du site.

Au final, au lieu d'avoir un seul indicateur qui indique que la connexion est cryptée ou non (le cadenas), Firefox 3 vous fournit toutes les informations nécessaires pour distinguer différents niveaux de sécurité.

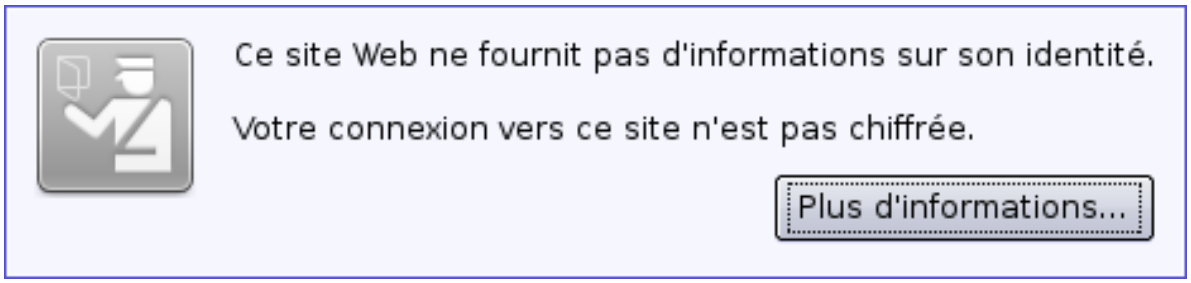
Voici ce que ces couleurs signifient :

Gris - Aucune information sur l'identité

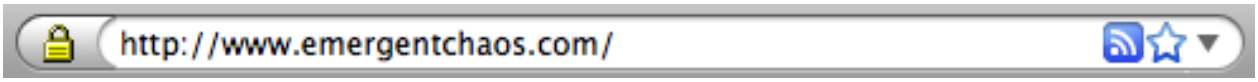
L'icône d'identification de site grise indique que le site en question ne fournit aucune information d'identité et également que la connexion entre le navigateur est en claire ou seulement partiellement cryptée. Il se peut qu'un inconnu espionne les données que vous échangez avec ce site.

La plupart des sites Web ont une icône grise, car ceux-ci, ne transmettant pas d'informations sensibles, n'ont ni besoin de donner d'information d'identité ni d'utiliser une connexion sécurisée.

Note : Si vous échangez des informations sensibles avec une site (coordonnées bancaires, numéros de sécurité sociale, etc) le bouton d'identification de site ne doit ABSOLUMENT pas être gris, mais au minimum bleu voire vert.



Si le bouton d'identification est gris mais que vous aperçevez un cadenas dans la barre d'adresse, ce cadena ne signifie donc même pas que le connexion est sécurisée, c'est une tromperie (et si le webmaster du site essaye de vous trompez avec un faux cadenas de connexion sécurisée, ça en dit beaucoup sur son honnêteté, ndt).



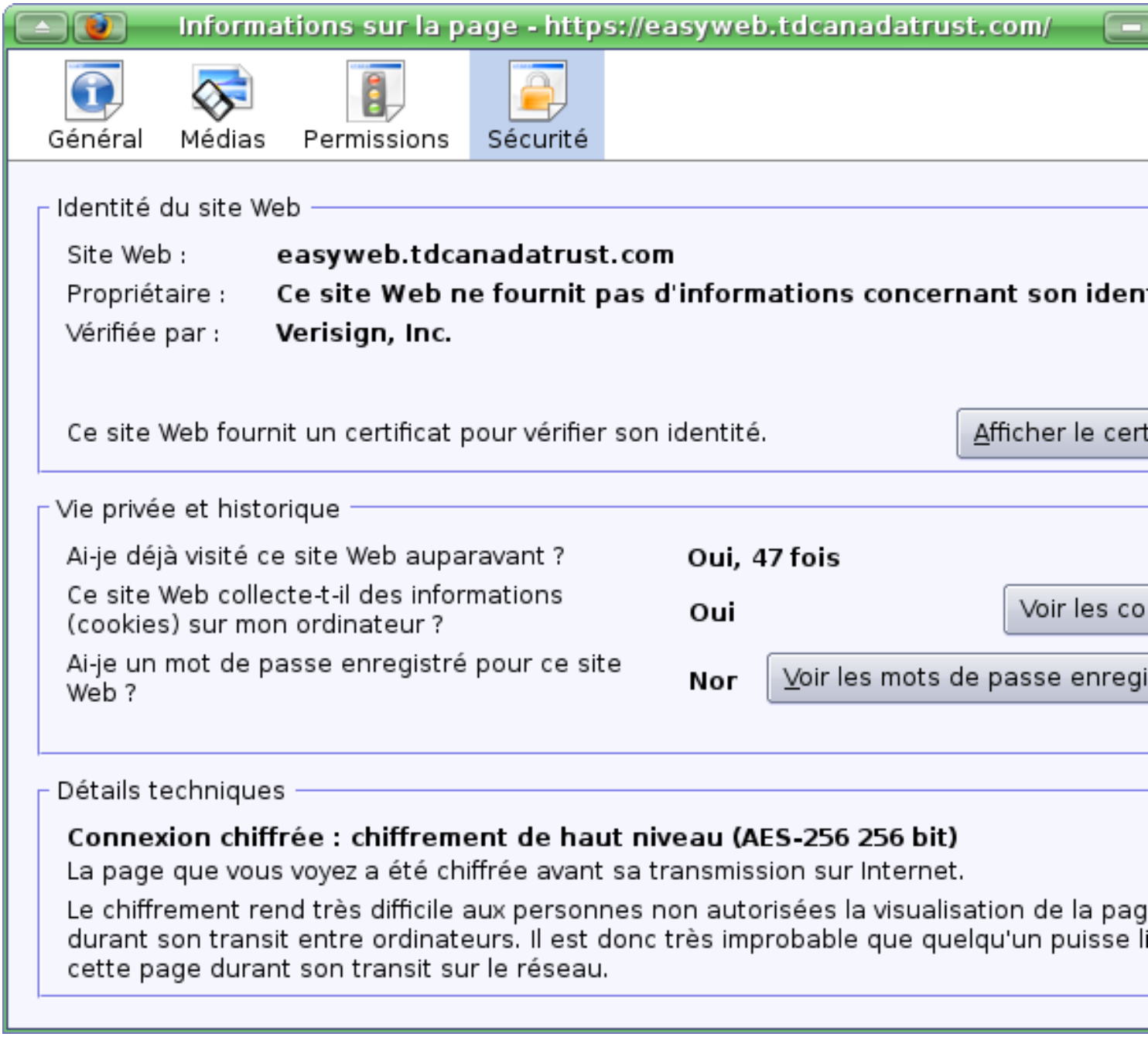
Bleu - Informations basiques d'identité

L'icône d'identification de site bleue indique que le domaine a été vérifié et que la connexion entre le navigateur et le serveur est cryptée et donc protégée contre l'écoute.

Un domaine vérifié signifie que le webmaster du site a acheté un certificat prouvant qu'il possède ce domaine et que celui-ci n'est pas falsifié. Par exemple, le -supposé- site de l'établissement bancaire *Toronto Dominion* possède un certificat et communique avec l'internaute au travers d'une connexion cryptée, Firefox 3 affiche donc une îcone bleue. Lorsque l'on clique sur le bouton d'identification de site, on sait que easyweb.tdcanadatrust.com a été vérifié comme étant parenté de tdcanadatrust.com, tel que certifié par *RSA Data Security Inc*. Il nous assure aussi que la connexion (entre le serveur de *TD Canada Trust* et l'internaute, ndt) est cryptée donc que personne ne peut espionner notre échange d'informations bancaires.

Ce qui n'est pas vérifié dans cette situation c'est **qui** est effectivement propriétaire du domaine en question. Il n'existe aucune garantie que le domaine tdcanadatrust.com est actuellement détenu par la banque *Toronto Dominion*. Tout ce qui est garanti, c'est que le domaine est valide, et que la connexion à celui-ci est cryptée.

Si je reste méfiant lorsque Firefox 3 affiche une îcone d'identification de site bleue, je peux même cliquer sur le bouton "plus d'informations". Ici, je peux consulter le site du certificat d'identité, si j'ai déjà visité ce site auparavant (NDT: utile lorsque vous avez l'habitude de consulter régulièrement votre banque ou un autre site circulant des infos sensibles et qu'il vous semble que quelque-chose dans la présentation, dans le nom du site, dans son contenu etc, est différent de d'habitude et vous semble louche : il peut s'agir d'une simple modification de la part de votre banque ou bien d'une tentative de copie ratée de la part d'un usurpateur, dans le deuxième cas, Firefox 3 vous indiquera que vous n'avez jamais consulté ce site, et là c'est plus que louche !), et si des cookies ou mots de passe ont été enregistrés pour ce site.

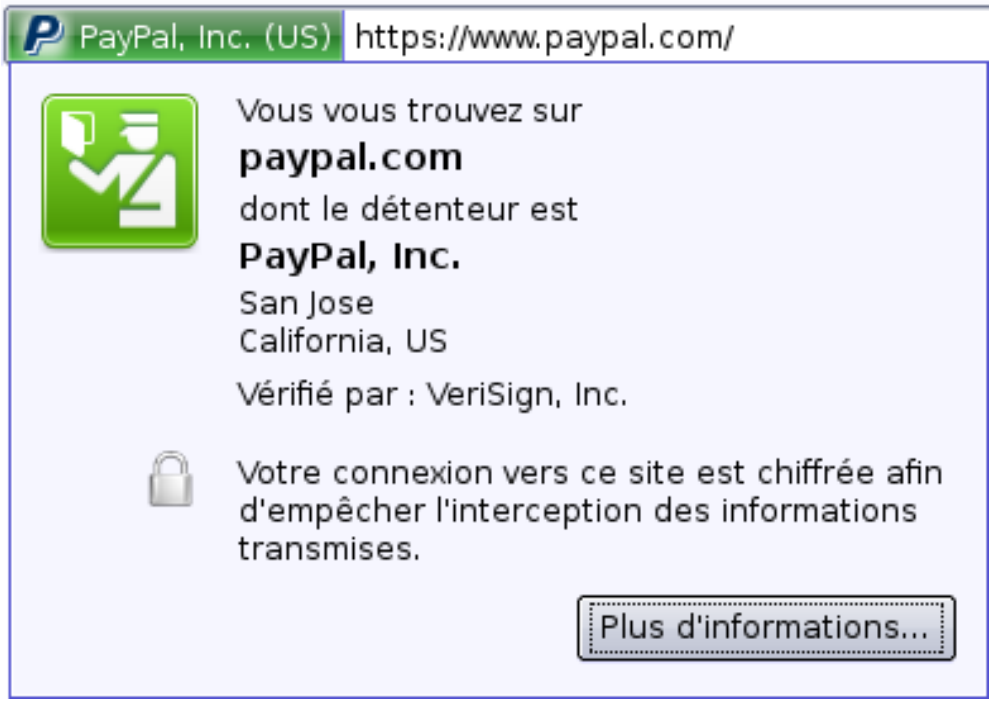


Vert - Informations d'identité complètes

L'icône d'identification de site verte indique que le site a été complètement vérifié quant-à l'identité de son propriétaire et que la connexion est cryptée.

Cela signifie que ce site utile utilise un "certificat de validation étendu" (EV pour *Extended Validation certificate*). Vous pouvez lire tous les certificats EV sur le lien Wikipedia ci-dessus, mais pour faire court, les certificats de type EV nécessitent un très rigoureux processus de vérification d'identité, beaucoup plus stricte que pour les autres types de certificats. Ainsi, si l'icône bleue indique que le domaine n'est pas usurpé, mais ne permet pas de vérifier les informations sur les propriétaires du domaine, l'icône verte indique que le domaine est valide et que les propriétaires du domaine sont bien ceux que vous croyez sans aucune ambiguïté possible.

Prenons Paypal pour exemple, l'îcone d'identification de site vous indique que le certificat EV est détenu par Paypal Inc. Non seulement celle-ci est verte pour Paypal, mais elle vous permet également d'obtenir des infromations très détaillées sur le détenteur du certificat.



On peut comparer ce nouveau système avec celui de Firefox 2 affichant un simple cadena et n'affichant que bien peu d'information quant-au détenteur du certificat -Et idem pour d'autres navigateurs concurrents, mais ne craigniez rien, à l'heure qu'il est, les concurrents sont probablement en train de s'aligner à ce système innovant , ndt-

Mais attendez, ce n'est pas tout!

Dans d'autres cas, l'agent de passeports apparaît avec deux autres couleurs possibles, mais cela ne donne pas vraiment d'informations sur la sécurité sur le site en question.

Jaune - Certificat invalide

Autre chose que vous pouvez rencontrer avec Firefox 3 : l'agent de passeport avec une icône jaune. Bien que le bouton d'identification du site ne soit pas lui-même jaune, l'agent des passeports jaune apparaît qu'il y a un problème avec un certificat d'identité.

Le site ne se charge pas mais une autre page apparaît à la place (voir capture ci-dessous). Cette page est en fait générée par Firefox 3 lui-même, et son but est de vous empêcher de se rendre dans un site qui a un certificat d'identité invalide. Tout comme les permis de conduire et les passeports, les certificats d'identification doivent être renouvelés avant expiration (NDT: pour les permis de conduire ce n'est pas le cas en France). Et tout comme votre passeport n'est valable qu'avec vous-même, chaque site doit présenter sa lettre de créance.

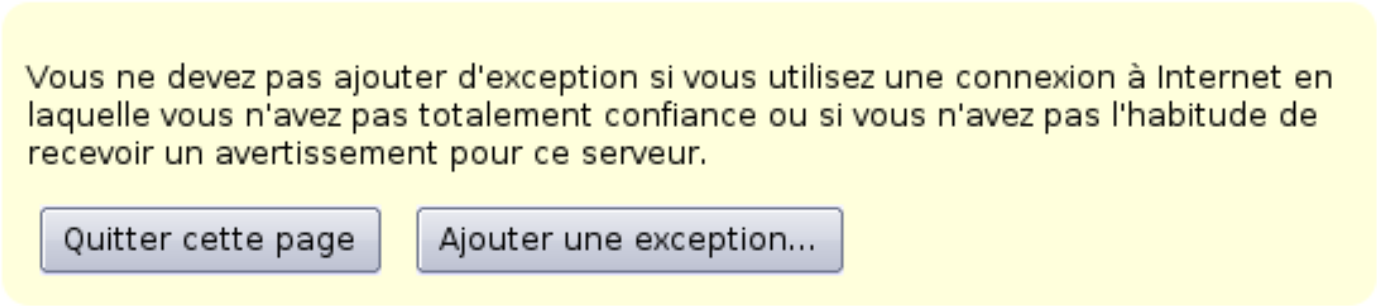
Si l'erreur détaillée est *sec_error_ca_cert_invalid*, le problème que Firefox a rencontré, c'est que le site a lui-même signé son certificat d'identité. C'est en gros comme si vous vous étiez fait vous-même un passeport fait-maison : ce genre de certificats ne signifie rien, personne ne les as vérifiés, et bien que les informations qu'ils fournissent puissent être exactes, Firefox tient à vous informer que le certificat n'a pas été validé.

NDT: Dans la capture réalisée pour konqi.fr (*ssl_error_bad_cert_domain*), le certificat utilisé n'est pas valable pour le domaine konqi.fr. En réalité ce site n'est pas prévu pour utiliser des connexions sécurisées (aucun échange d'informations sensible).

Il existe de nombreux sites parfaitement sérieux qui utilisent des certificats auto-signés simplement pour leur permettre d'utiliser une connexion sécurisée, et ces sites ne sont pas forcément néfastes ou malhonnêtes. C'est la raison pour laquelle Firefox 3 vous permet d'ajouter des exceptions pour les sites qui ont auto-signé leurs certificats lorsque vous avez vérifié que le site sur lequel vous naviguez est sûr.

L'ajout d'une exception est un processus simple qui doit être fait pour chaque site avec un certificat auto-signé et qui ne doit pas être pris à la légère.

En bas de la page "Échec de la connexion sécurisée" qui bloque l'accès au site (voir capture ci-dessus), il y a un lien qui se lit comme suit: "Ou vous pouvez ajouter une exception…". En cliquant sur ce lien vous passerez à l'étape suivante pour vérifier que vous êtes sûrs de ce que vous faites.



Cliquez sur "Ajouter une exception" pour poursuivre l'ajout de l'exception.

Si vous souhaitez ajouter l'exception temporairement, assurez-vous que le "Conserver cette exception en permanence" au bas de la boîte de dialogue est décochée. Cliquez ensuite sur "Confirmer l'exception de sécurité", et Firefox 3 ne vous empêchera plus de visiter ce site.

L'agent de passeport jaune peut s'afficher dans de nombreuses autres situations qui génèrent un problème avec le certificat. La page d'avertissement vous explique alors le problème en détail.

Rouge - Site rapporté comme étant dangereux

L'agent de passeport rouge possède un panneau d'interdiction au lieu d'un passeport entre ses mains.

Ceci fait partie du système de protection de Firefox 3 contre les tentatives frauduleuses et l'hammeçonage, système de protection qui protège ces utilisateurs du danger provenant de sites signalés -l'auteur de l'article signale qu'il détaillera cette procédure de signalement plus tard-. Pour l'instant, soyez assuré que si vous rencontrez l'agent de passeports rouge, vous êtes protégés d'éventuelles attaques, ce n'est pas directement pour vous empêcher de consulter ce site mais pour vous protéger.

Ce nouveau système de Firefox 3 beaucoup plus convivial et informatif en matière de sécurité est largement supérieur aux anciens systèmes qui se basent exclusivement sur un cadenas pas très signifiant. Non seulement le panel des indicateurs de sécurité a été élargi et amélioré, mais il est désormais également beaucoup plus facile de comprendre les niveaux de sécurité rencontrés sur Internet. Aucun système n'est parfait, bien sûr, mais Firefox 3 fait un pas important vers l'amélioration de votre sécurité sur le Web