Comment détecter un site web frauduleux ?

Chaque jour de nombreux sites web apparaissent sur la Toile, augmentant le terrain de jeux des cybercriminels. Quel que soit le type de site que vous consultiez (blog, site commercial, site de téléchargement ou encore de musique ou de vidéo), il est recommandé de prendre quelques précautions.

En effet, si esthétiquement parlant ces sites peuvent paraître clean, certains d'entre eux cachent un loup qui va s'infiltrer, voler vos données ou à infecter votre machine pour en prendre le contrôle au moindre clic de votre souris.

- Vous risquez de communiquer votre numéro de carte bancaire à des escrocs.
- Vous risquez de payer de la marchandise qui ne vous sera jamais livrée
- Si vous utilisez le même mot de passe partout sur Internet, vous risquez que les escrocs vous piratent vos différents comptes utilisant ce mot de passe.
- Un site web frauduleux est susceptible d'endommager les ordinateurs clients car il charge des scripts malicieux de code malveillant.

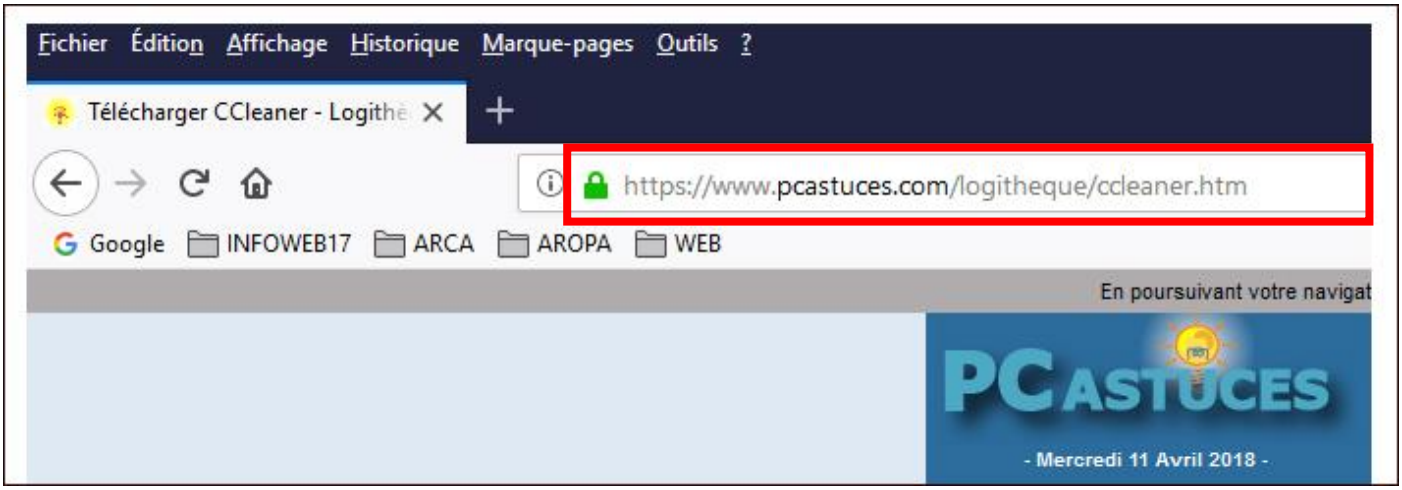
Ainsi, avant de consulter, d'acheter ou de télécharger sur un site Internet mieux vaut s'assurer de sa fiabilité, à commencer par vérifier l'URL.

Une URL c'est quoi ?

Une URL (de l'anglais : Uniform Resource Locator, littéralement « localisateur uniforme de ressource »), souvent appelée « Adresse web » est une chaîne de caractères pour indiquer à un logiciel, l'adresse d'une ressource Internet propre à chaque type de protocole de communication.

Cette adresse sert à désigner une ressource présente sur le web par une suite de caractère ASCII. Les ressources peuvent être variées (page web, vidéo, son, image, animation, adresse email ...).

Chaque navigateur web dispose d'une « barre d'adresse » affichant l'URL de la ressource consultée. Il est en outre possible de saisir une URL dans cette barre d'adresse pour consulter une ressource dont on connaît l'URL.



Quelques exemples pratiques d'URL :

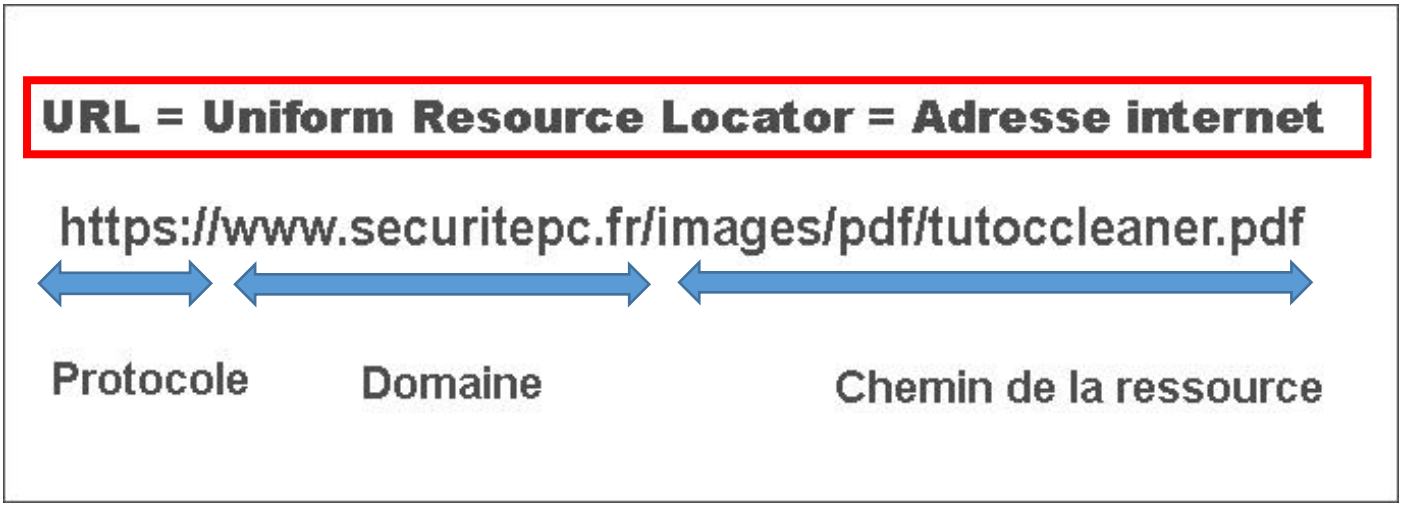
- URL de PCAstuces : http://www.pcastuces.com

- URL d'un lien (mailto) vers une adresse courriel : mailto:nom.prenom@gmail.com
- URL d'un fichier sur un site FTP : ftp://ftp.rfc-editor.org/in-notes/rfc2396.txt
- URL d'un forum de discussion : news:fr.comp.infosystemes.www.auteurs

Les URL ont été inventées pour indiquer aux navigateurs web comment accéder aux ressources d'Internet.

- Exemple 1 : https://www.pcastuces.com/logitheque/ccleaner.htm est une URL permettant de télécharger un logiciel
- Exemple 2 : http://www.micro-mole.com/fic_pdf/2_1778_sauvegarde_indos_10.pdf est une URL permettant de télécharger un fichier PDF présent sur le web

Structure d'une URL standard



Une URL n'est pas anodine et peut être décomposée en plusieurs parties:

- Le protocole: http, https (sécurisé ssl), ftp, mailto ...
- Le nom du serveur : www.pcastuces.com
- Le nom de domaine et sous domaine : pcastuces.com
- L'extension de nom de domaine : fr, com, org, net, uk, be,
- Le chemin vers la ressource hébergée : dossier / fichier

Se protéger en analysant le domaine de l'URL

Exemple avec le site Amazon.fr

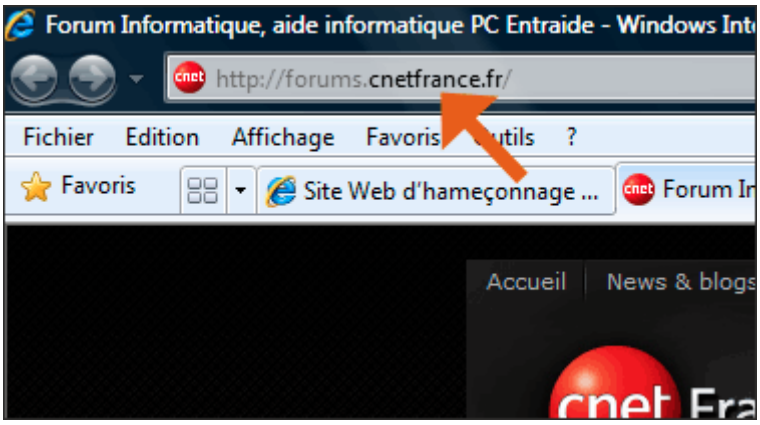
Avant de cliquer, en survolant le lien dans l'email ou une fois sur le site malveillant on peut s'apercevoir que le nom de domaine (l'URL) n'est pas celui d'Amazon. Mais certains noms de

domaines et sous domaines complexes peuvent facilement berner un utilisateur en contenant le nom du service visé. En effet par le jeu des sous-domaines il est très simple de créer des domaines très courts de 5 ou 6 lettres et de placer un nom donnant confiance dans la barre d'adresse du navigateur.

amazon.fr qui est le seul domaine légitime d'Amazon peut également s'afficher en sous domaines tels que "http://connexion.amazon.fr" ou "http://compte.amazon.fr". On remarque que le vrai nom de domaine est placé juste avant l'extension finale .fr , il s'agit donc bien du site appartenant à amazon.fr.

Un sous domaine frauduleux peut prendre une forme très proche de ces adresses. Exemple avec le sous domaine "abcfr.com" qui n'appartient pas à Amazon mais que son propriétaire pourrait utiliser pour créer des sous domaines tels que : "http://www.amazon.abcfr.com" ou "http://compte.amazon.abcfr.com". Ces deux sous domaines qui inspirent pourtant confiance ne sont pas des domaines appartenant à Amazon mais des "sous-domaines" du domaine "abcfr.com" .

Vous l'avez compris, seul le mot placé avant l'extension finale désigne le domaine. Internet explorer met en évidence le vrai nom de domaine dans la barre d'adresse :



Conseil : Adopter le principe de précaution en accédant aux sites par les favoris

Le moyen le plus sûr de se protéger contre le phishing est donc tout simplement de ne jamais se connecter à un compte important (boutique, banque, email etc ...) en cliquant sur un lien depuis un site web ou un email. Pour éviter les manipulations et d'avoir à saisir les adresses manuellement à chaque connexion, l'internaute prudent prendra soin de se constituer une une liste de favoris enregistrés pour accéder à ses principaux services en ligne.

Détecter URL code malveillant :

1. **VirusTotal**

   VirusTotal est un service en ligne gratuit qui analyse les fichiers et URL suspects, et facilite la détection rapide des virus, vers, trojans et tous types de malwares.

2. **Google** dispose d'un outil de détection pour savoir si un site Web en particulier présente un danger, **cliquez sur ce lien** pour tester une adresse web. **Exemple**.

Pour chercher en sécurité, les résultats ne doivent pas être pris au pied de la lettre. Ce ne sont que des avis de robots. Ils donnent des pistes d'analyses qui doivent être interprétées par des recherches avancées. Une URL déclarée probablement inoffensive peut ne pas l'être et une URL déclarée dangereuse peut ne pas l'être.

Se souvenir qu'une analyse robotisée, quel qu'elle soit, ne peut jamais déclarer un objet sain, mais simplement déclarer qu'elle n'a rien trouvé et qu'il y a de fortes probabilité que l'objet soit sain, mais rien de plus. Jamais aucun antivirus ne déclare un objet sain, mais qu'il n'a rien trouvé. Sans être paranoïaque, le doute doit toujours vous habiter sur le Web. Ne vous reposez pas sur la présence d'outils de sécurité dans votre ordinateur, n'abaissez pas votre seuil de vigilance.

Vérifications complémentaires :

1. **Vérifier les mentions légales**

   Sur un site marchand, les mentions légales sont obligatoires. Elles sont composées du nom, des coordonnées ainsi que du numéro de Siret du propriétaire dudit site. Si jamais vous ne trouvez pas de page « mentions légales », fuyez.

2. **Les conditions générales de vente ou CGV**

   Tout site de confiance marchand dispose de sa page affichant ses conditions de vente ou d'utilisation. Généralement, il s'agit d'une suite d'articles où sont expliqués les conditions d'envois, de rétractation ou encore le temps de livraison voire le prix.

3. **Le protocole https**

   C'est le premier réflexe à avoir à l'affichage d'un site web. Pour le repérer c'est simple, il se trouve en première position dans votre barre de recherche. Le protocole https (sécurisé SSL) est d'autant plus important sur les pages de paiement. Si le sigle https n'apparait pas sur la page, quittez immédiatement sous peine de vous faire détrousser.

4. **L'orthographe**

   Cela peut sembler bête et pourtant… Un faux site aura tendance à comporter des fautes d'orthographe ou de grammaire. C'est plutôt facile à repérer : il suffit de faire un tour sur le dit site. Si vous remarquer un français approximatif, vous savez ce qu'il vous reste à faire.

5. Consulter le WHOIS

Littéralement « who is ? » soit « qui est ? ». Ce service vous permet de pratiquement tout savoir d'un site Internet. Cela vous permet donc de savoir si le site que vous visitez est un vrai ou une arnaque. Et pour utiliser le WHOIS, rien de plus simple. Il vous suffit juste de rechercher « whois + nom du site ».

Attention, si jamais vous ne trouvez aucune information via le WHOIS, le site que vous visitez est probablement un faux.

Les liens hypertextes et URL

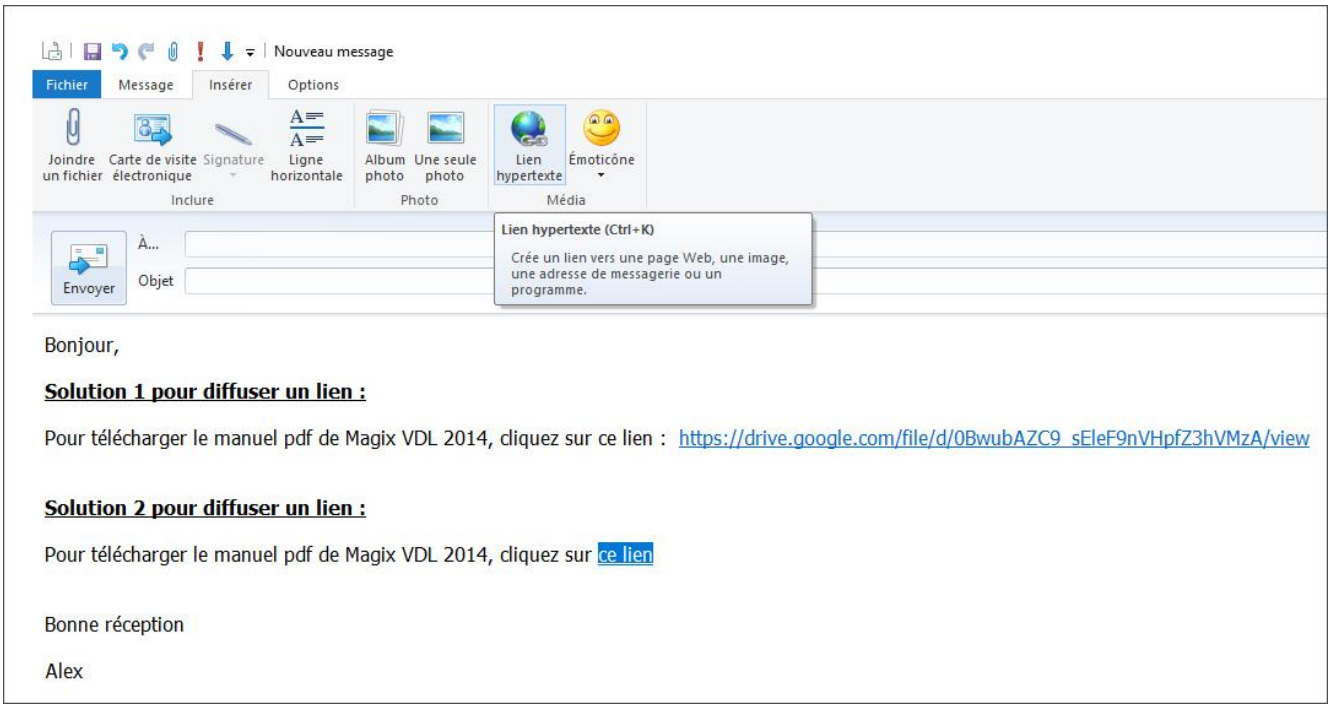
Créer un lien dans un courriel avec Windows Live Mail ou dans une page Word :

- **Solution 1 pour diffuser un lien : Exemple :**

  Pour télécharger le manuel pdf de Magix VDL 2014, cliquez sur ce lien : https://drive.google.com/file/d/0BwubAZC9_sEleF9nVHpfZ3hVMzA/view

- **Solution 2 pour diffuser un lien : Exemple :**

  Pour télécharger le manuel pdf de Magix VDL 2014, cliquez sur ce lien



Un lien texte ou image peut donc pointer sur n'importe quelle URL, des plus légitimes aux plus frauduleux capable d'infiltrer du code malveillant.

Notes

https://www.pcastuces.com/pratique/internet/raccourcir_url/page1.htm

https://www.pcastuces.com/pratique/internet/verifier_url_reduite/page1.htm

http://www.tomsguide.fr/faq/id-2868251/savoir-site-frauduleux.html

https://arnaqueinternet.com/arnaque_sur_le_web/rancongiciel/

https://defense-du-consommateur.ooreka.fr/fiche/voir/419001/signaler-un-site-frauduleux

http://www.toucharger.com/articles/comment-distinguer-un-site-frauduleux-dun-site-fiable_168.htm

https://www.securitepc.fr/images/pdf/tutoccleaner.pdf

https://plone.unige.ch/distic/pub/messagerie/secu/identifier-phishing

https://www.one.com/fr/domaine/creation-nom-de-domaine