A propos de sécurité et de mes Pages perso

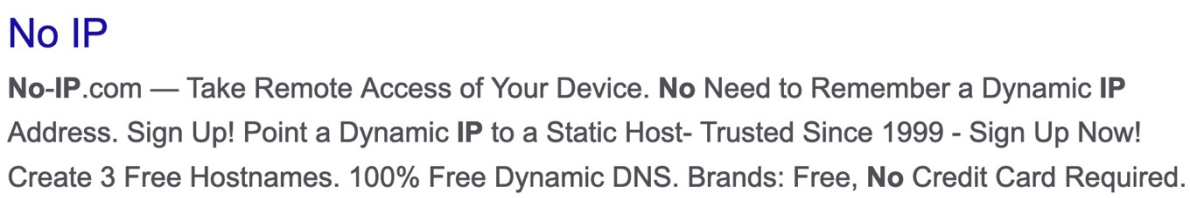
Christian me signale qu'au moment d'encoder son adresse mail, une fenêtre apparaît avec une alerte de sécurité disant que ses identifiants pourraient être compromis.

Je vous explique ……..

Cette alerte est due au fait que la connexion avec mes pages passe par un site de **redirection** pour aboutir chez moi et que l'adresse de mon **serveur** n'est pas répertoriée comme sécurisée. Cela demande un peu d'explication.

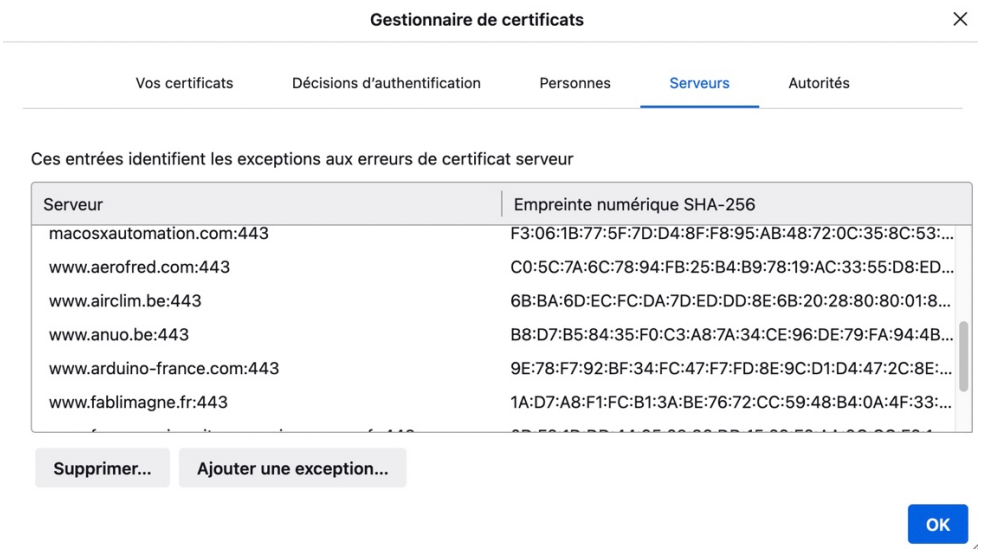
Les communications internet doivent répondre à un protocole technique pour que cela fonctionne, le protocole **IP** (*internet protocole*). A cet effet, chaque machine correspond à un **numéro IP**. Ce numéro, composé de 4 chiffres entre 0 et 255 dont une partie représente le numéro de réseau (côté serveur) et une autre un numéro de machine (*côté client*). D'un côté, il y a le client (*vous*) et de l'autre un serveur (*votre fournisseur d'accès à internet*).
Ce système permet la communication avec de nombreux clients.
Supposons un réseau utilisant un seul des 4 chiffres, cela permet la connexion de 256 x 256 x 256 clients sur les 3 chiffres restants (*près de 17 millions de clients*). Cela permettrait de connecter toute la Belgique sur un seul réseau mais, évidemment, le serveur aurait bien du mal à s'occuper de tout le monde en même temps. Ce n'est donc généralement pas comme cela que votre fournisseur d'accès travaille. De même, votre fournisseur transmet votre demande de connexion à un autre serveur (par exemple google.com) qui doit aussi répondre à de nombreuses demandes en les répartissant vers une série de machines.
Lorsque vous vous connectez à internet, votre fournisseur d'accès vous attribue un **numéro IP** qui est variable (*il change de temps à autre*). Un numéro IP fixe a des avantages mais coûte plus cher. Cela vous permet de créer une communication entre votre ordinateur et un ou plusieurs autres car votre adresse est alors connue (*http://200.150.12.2 par exemple, pour y abriter un site web*).
Votre fournisseur d'accès ne vous fait pas seulement payer plus cher en raison de cet avantage mais aussi parce qu'un numéro IP fixe est bloqué pour un seul client même si le client ne s'en sert pas. Pour le fournisseur d'accès, il s'agit d'un canal de communication en moins à répartir entre les clients du serveur.
Pour ne pas avoir à payer plus cher, il existe une solution gratuite : passer par une **redirection**. Il s'agit de se faire attribuer un nom de domaine par une société qui redirige gratuitement les demandes envoyées à ce nom de domaine vers votre serveur personnel.

Personnellement, mon **nom de domaine** est hébergé chez NO-IP :



Et mon **nom de domaine** est **smot.webhop.me** (*c'est moi qui ai choisi la partie avant le premier point*).
Mon adresse IP n'est pas fixe mais elle est régulièrement et automatiquement envoyée chez No IP par une petite application qui fonctionne en tâche de fond dans mon ordinateur. De cette manière vos demandes de consultation de mes pages perso sont envoyées à **smot.webhop.me** (*chez No ip qui détient le nom de domaine **webhop***) et les **redirige** vers **mon adresse IP du moment**.
La **redirection** est un système qu'utilisent aussi des pirates pour se cacher en passant au travers d'une flopée de machines ayant des numéro IP provisoires garantissant ainsi une certaine anonymité.
Les navigateurs internet comme Firefox, Outlook, Chrome et d'autres avertissent donc les utilisateurs d'un manque de sécurité en fonction de **certificats** des serveurs.

Voici une vue de mon **gestionnaire de certificat** (*Firefox*)



Lorsqu'à la suite d'un avertissement de sécurité vous décidez de poursuivre, le gestionnaire de certificat de votre navigateur inscrit votre confiance en l'adresse du site comme exception à l'erreur de certificat serveur. Cela évitera une nouvelle alerte de sécurité à chaque fois que vous vous adresserez à ce serveur. Voilà pourquoi vous pouvez recevoir un avertissement de sécurité totalement injustifié en consultant mes **Pages perso**.

A propos de sécurité, sachez que votre **mot de passe** est sécurisé par **hachage sha256**.
Voici une partie des explications trouvée ici https://www.dcode.fr/hash-sha256.

Le *SHA-256* est une norme de hachage (issu du SHA-2 Secure Hash Algorithm), un standard du gouvernement fédéral des États-Unis qui permet de faire correspondre à une donnée binaire quelconque, une empreinte de 64 caractères hexadécimaux qui la caractérise de manière quasiment unique.
Le chiffrement *SHA256*, comme toute fonction de hachage, étant basé sur des fonctions non linéaires (non réversibles), il n'existe pas de méthode de déchiffrement.

De tout cela découle le fait que je suis totalement incapable de lire votre mot de passe et qu'en conséquence je ne peux pas vous le rappeler. MAIS ce n'est pas un problème car si vous perdez votre mot de passe il suffit de vous inscrire à nouveau. Lors d'une nouvelle inscription, vous recevez un mail de confirmation et j'en reçois une copie. Dès lors, je supprime votre ancienne fiche d'inscription, simplement pour ne pas avoir de doublon encombrant. Voici à quoi ressemble mon mot de passe personnel dans ma fiche d'inscription :

Je paie un pot à celui qui le décode !