

# Que fait votre Voisin Ou Protégeons Nos Réseaux

Merci **HADOPI**

Haute Autorité pour la Diffusion des Œuvres et la  
Protection des droits sur Internet



# Obligation de sécuriser son WIFI

« Le développement et l'essor du numérique font de nous des « êtres connectés ». Néanmoins pour être connecté à Internet de manière responsable il est indispensable de sécuriser son accès à internet (et à son réseau local). Au regard de la loi Hadopi, chaque internaute a pour obligation de veiller à ce que son accès soit sécurisé..... »

Source du site HADOPI



# On est tous des Admins Réseaux

« Face à des méthodes qui ne cessent de se développer : virus, cheval de Troie, ver, spam, hameçonnage (phishing), canular, arnaque... vous devez être vigilant et veiller à la sécurité de vos installations. La première chose à faire pour s'assurer de l'utilisation qui est faite de l'accès à internet est de discuter au sein du foyer, afin que tout le monde soit **sensibilisé** à la sécurité informatique et au respect du droit. »

Source du site HADOPI



# Le Wifi n'est pas Sur !!!

VOUS RISQUEZ LA SANTION SUPREME

## PLUS D'INTERNET

La HADOPI surveille les réseaux P2P afin de relever les IP servant aux téléchargements illégaux.

Un délit de non sécurisation de réseaux WIFI a été créé spécialement Pour Vous !!!!

Les ondes WIFI se captent bien au delà de vos Murs, et casser une clé wifi ne demande que du temps, pas vraiment de technicité.

# La sécurisation des Box

Tous les FAI sont à égalités, leurs modem/routeurs sont dans les mêmes standards de sécurité.

- Prédominance du WPA2.
- Le WEP est à Bannir
- Filtrage par adresse MAC de la carte wifi optionnel.

Le filtrage MAC peut être floué en changeant notre adresse physique de la carte Réseau, cela ralentie juste l'attaque...ou la dissuade....un peu.



# Le syndrome du Tout Fait

Attention certains algorithmes de création de clé WPA ont été cassés ce qui permet de trouver le code WIFI en connaissant le SSID.

Exemple les box Thomson que l'on retrouve dans certaines Bouygues BOX.

## CONSEIL

- Changer le nom de votre réseau WIFI (le SSID)
- Utiliser un SSID caché
- Mettre un vrai mot de passe (admin et clé wifi)  
(Lettre, Chiffre, Symbole, minimum 8 caractères)

Exemple : 0123456789 ou azertyuiop



# Le choix du Mot de Passe

- Utilisez un mot de passe distinct pour tous les comptes importants.
- Utilisez un mot de passe composé de lettres, de chiffres et de symboles (AkUyHgF1,65;9# »).
- Créez un mot de passe difficile à deviner (AZERTY).
- Assurez-vous que les options de récupération de mot de passe sont à jour et sécurisées (question secrète autre que le nom de jeune fille de maman).
- Gardez vos mots de passe à l'abri des regards indiscrets... évitez le post-it sur l'écran.
- Essayez de ne pas les enregistrer dans le butineur.

SOURCE GOOGLE



# Le Wifi Communautaire...Méfiance

- Disponible en premier chez Neuf, Il permet d'accéder à internet de la box d'un tiers, avec des identifiants personnels.
- Tous les opérateurs proposent ce service.
- Même si le débit réduit et les ports P2P sont bloqués pour certains (ex : sfr), la consultation de site interdit peut vous être imputé.
- **Les réseaux Wifi sont séparés, le problème provient de l'adresse IP publique qu'HADOPI relève et attribue à votre Box.**
- Orange et Free attribuent des IP publiques différentes, pourtant des freenautes ont reçu des mails d'avertissement d'hadopi, infondés selon eux.



# Wifree connect

**Wifreeconnect** vous permet de vous connecter aux WIFI Ouverts des différents opérateurs sans avoir de compte chez eux.

Basé manifestement sur l'exploitation de failles, wifreeconnect est un soft payant sous Windows.

Ce logiciel vous est cité à titre d'avertissement pour que vous deveniez des utilisateurs avertis de ce type de service.

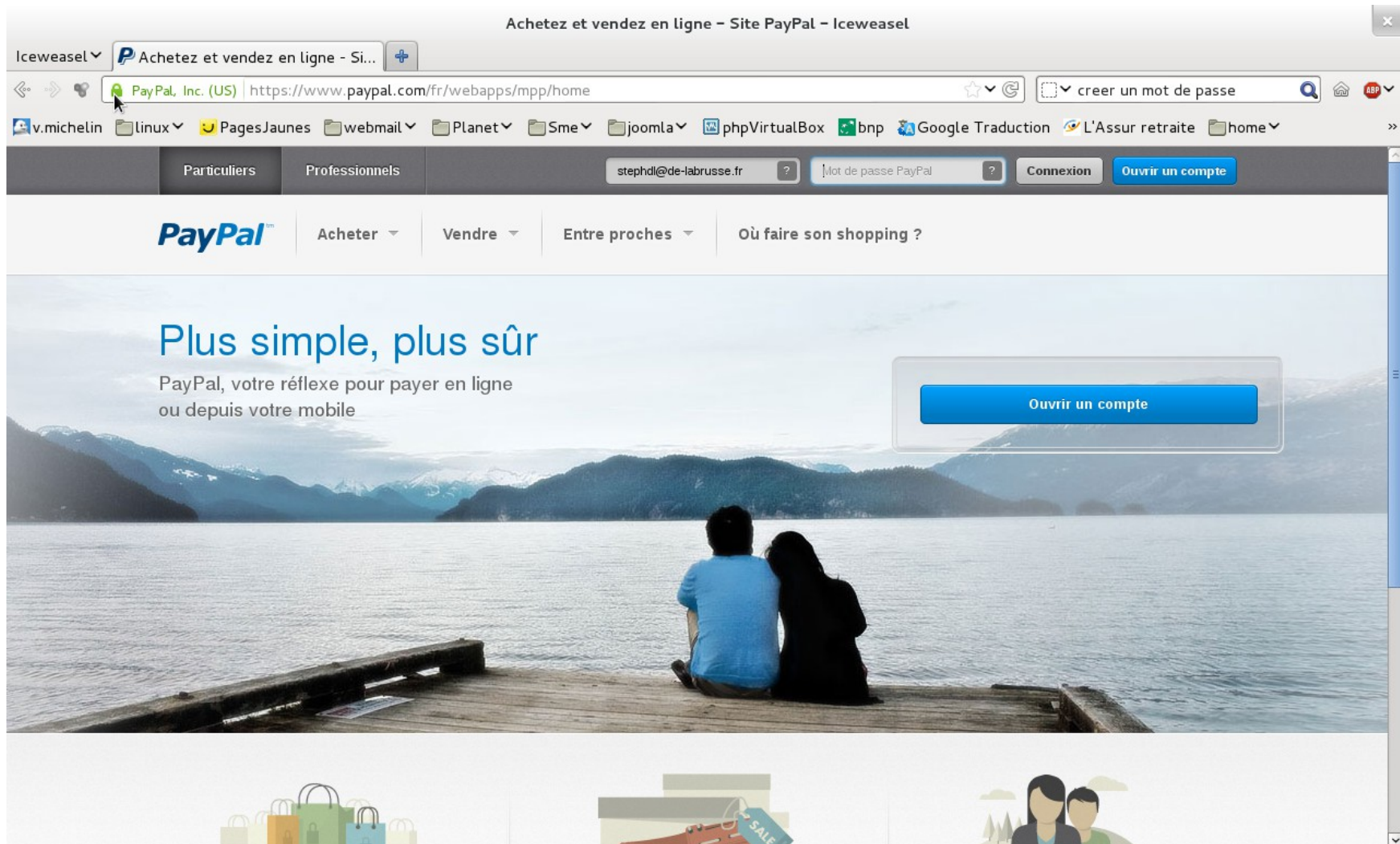


# Surfez Couvert

- Utilisez Firefox car sa base de données de sites vous empêchera de surfer sur un site malveillant.
- Vérifier l'URL, l'adresse Internet des Sites que vous visitez pour éviter le phishing.
- Les sites de banque achètent des certificats **Verisign** qui les identifient, vous pouvez vérifier l'authenticité du certificat dans la barre d'adresse de Firefox.
- Évitez les sites de Fesse ou utilisez MAJ+CTRL+P pour pas que maman le sache (navigation privée recommandée par la **CNIL**).



# Exemple de certificat



# L'ingénierie Sociale ou Social Engineering

L'ingénierie sociale est une forme d'acquisition déloyale d'information et d'escroquerie, utilisée en informatique pour obtenir d'autrui, un bien, un service ou des informations clefs.

Cette pratique exploite les failles humaines et sociales de la structure cible, à laquelle est lié le système informatique visé.

La faille humaine est plus facile à exploiter que la faille informatique : **Hacker croll**, le français qui pirata Twitter.....**mode d'emploi !!!!**



# L'hameçonnage ou Phishing

Le phishing, est une technique utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité. La technique consiste à faire croire à la victime qu'elle s'adresse à un tiers de confiance afin de lui soutirer des renseignements personnels :

**Mot de passe, numéro de carte de crédit,  
informations personnelles**

Les responsables de l'élysée trompés en mai 2012...Sarkozy sauvé car il n'avait pas d'ordinateur.



# Fin...Place au Hack

La faille est toujours entre le clavier et la chaise

