Se protéger des sites malveillants et pornographiques

Objectif : éviter de tomber sans le vouloir sur un mauvais site

L'objectif est d'éviter que l'on tombe *sans le vouloir* sur des sites malveillants ou pornographiques. Cette mesure fonctionnera comme une barrière d'autoroute : en cas d'erreur, on ne tombera pas dans le fossé.

C'est probablement une des mesures à prendre en premier, car elle est assez simple à mettre en place et se situe au point d'entrée même d'internet dans la maison (Wi-Fi) ou dans l'assistant personnel (smartphone, tablette, …).

Les mesures complémentaires comme activer Safe Search sur tous les navigateurs disponibles, ou installer un contrôle parental sont intéressantes, mais sont plus éloignées du point d'entrée des données.

Annuaires d'Internet qui référencent tous les sites

Internet est constitué d'une constellation mondiale de systèmes informatiques connectés entre eux.

Lorsque l'on clique sur un lien ou que l'on tape dans la barre de recherche l'adresse d'un site, par exemple, https://www.youtube.com/, le système informatique que nous utilisons (notre assistant personnel, notre ordinateur), va demander à un annuaire où trouver YouTube.

Ces annuaires sont nommés des DNS pour Domain Name Server, et il en existe plusieurs. On leur demande où se trouve "www.youtube.com", et le DNS va répondre quelque chose comme 74.125.135.93 ou 2607:f8b0:400e:c08::88, c'est à dire les coordonnées informatiques précises de l'endroit où se trouve YouTube (ces coordonnées sont nommées adresse IP, pour "Internet Protocol").

Par analogie, si l'on donnait "18, avenue Charles de Gaulle, le Pecq", l'annuaire répondrait par la latitude et longitude 48°53'15.6"N 2°06'07.6"E.

Annuaire qui connait les sites malveillants et pornographiques : Cloudflare

Par défaut, notre téléphone ou notre ordinateur utilise un annuaire qui connait l'intégralité de tous les systèmes informatiques du monde, qu'ils soient bons ou mauvais. Pour les téléphones Android, l'annuaire est celui de Google, et a pour adresse IP 8.8.8.8.

Il existe aussi des annuaires qui répertorient les sites malveillants et pornographiques, et lorsque qu'on demande leurs coordonnées, ils répondent par l'adresse IP 0.0.0.0 qui ne correspond à rien du tout. Par analogie, ils répondraient longitude 0 et la latitude 0, c'est-à-dire au milieu de l'océan où il n'y a personne, si l'on demandait l'adresse d'une maison close.

Le plus connu de ces annuaires Cloudflare. Cloudflare répertorie tous les sites existants et est un annuaire très efficace. Cloudflare for Families élimine les sites malveillants et pornographiques.

Note : je télétravaille avec Cloudflare for Families depuis des mois, cela fonctionne parfaitement avec tous les outils de ma société (Teams, Zoom, Confluence, Jira, Office 365, etc.).

Procédure de configuration de Cloudflare for Families

Constater (sans risque) qu'avant son utilisation, on n'est pas protégé

Pour cela, utiliser deux URL de sites fictifs qui ne contiennent aucun mauvais contenu, mais qui sont répertoriés comme tel par Cloudflare.

- Site fictif malveillant : https://malware.testcategory.com/
- Site fictif pornographique : https://nudity.testcategory.com/

Le DNS configuré par défaut donnera leur adresse réelle.

Vous devriez donc obtenir *"This is a test website provided by Cloudflare Gateway. If you expected this category to be blocked, please check…*" dans votre navigateur.

Comment appliquer les procédures Cloudflare for Families

Comme expliqué, l'annuaire (DNS) qui nous intéresse est Cloudflare pour Families. L'annuaire Cloudflare standard connait l'intégralité de tous les sites web de la planète.

Or, dans les procédures données par Cloudflare, la version Cloudflare for Families n'est pas toujours clairement explicitée. Notez que la procédure est la même, il faut simplement remplacer les adresses comme 1.1.1.1 et 1.0.0.1 qui sont l'annuaire Cloudflare complet, par les adresses qui se terminent par un **3**, ou qui contiennent le mot **familly** comme listées ci-dessous.

Adresses à utiliser pour Cloudflare for Families :

- 1.1.1.**3**
- 1.0.0.**3**
- 2606:4700:4700::111**3**
- 2606:4700:4700::100**3**
- **family**.cloudflare-dns.com

Configurez votre boîtier Internet

Objectif : toute personne se connectant à Internet par votre Wi-Fi (ou par un câble Ethernet) sera protégé, quel que soit le smartphone ou ordinateur utilisé.

Note : si vous n'avez pas le temps de configurer votre boîtier Internet, vous pouvez directement sauter à la configuration de chaque ordinateur ou téléphone plus bas.

Boîtier Internet qui permet de changer le DNS : Free box uniquement ?

Pour les quelques boîtiers Internet qui le permettent, c'est-à-dire probablement toutes les versions de Freebox (à confirmer), il suffit de changer le DNS via son interface d'administration. C'est la situation idéale.

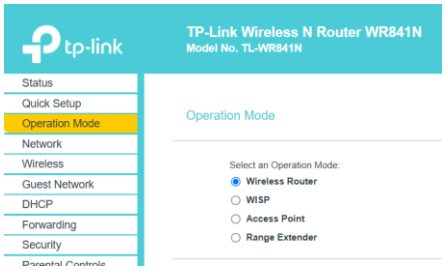
Merci à ceux qui ont une Freebox d'indiquer si la procédure suivante est correcte, car elle n'a pas été vérifiée.

1. Aller sur l'interface d'administration de la Freebox : http://mafreebox.freebox.fr/ et s'identifier
2. "Paramètres de la Freebox" puis "Mode avancé" puis "DHCP".
3. Dans paramètres DHCP, 5 champs permettant de renseigner les adresses des serveurs DNS.
4. Déplacer les adresses IP actuelles des champs "DNS 1" et "DNS 2" vers les "DNS 4" et "DNS 5"
5. Saisissez les adresses IP **Cloudflare for Families 1.1.1.3 et 1.0.0.3** dans "DNS 1" et "DNS 2"
6. Validez en cliquant sur "OK".
7. Éteindre, puis rallumer la FreeBox

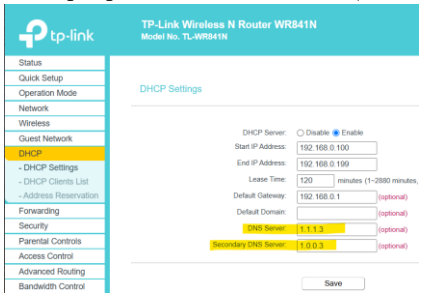
Boitiers Internet qui ne permettent pas de changer le DNS : LiveBox Orange, BBox Bouygues, SFR

Les boitiers Internet LiveBox Orange, BBox Bouygues et SFR n'autorisent pas de changer de DNS. Il va falloir rajouter un nouveau point d'accès Wi-Fi qui remplacera l'accès Wi-Fi celui du boitier Internet.

1. Rajouter un petit routeur accès Internet comme le TP-Link TL-WR840N à 20€
   (TP-Link est une bonne marque pour ce type de matériel)
2. Le brancher avec un câble RJ-45 court
   (doit venir avec le routeur, sinon en acheter un)
   a. Le configurer en mode "Wireless router"
      - Exemple pour le TP-Link N300 (toutes les interfaces TP-Link sont similaires) :



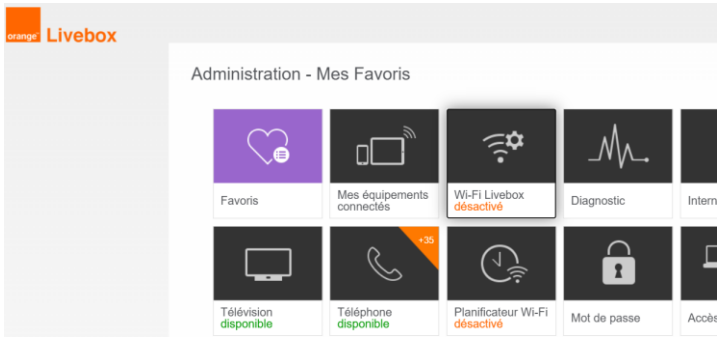
   b. Lui donner le DNS Cloudflare for Families
      - Suivre https://developers.cloudflare.com/1.1.1.1/setup/router/
      - Exemple pour le TP-Link N300 (toutes les interfaces TP-Link sont similaires) :



3. Désactiver le Wi-Fi de votre boitier Internet (il ne s'agit pas d'appuyer sur le bouton Wi-Fi pour l'éteindre)
   a. S'y connecter en tant qu'administrateur
   b. Désactiver tous les réseaux Wi-Fi

- Exemple avec la LiveBox Orange : tout passer sur OFF

- Ensuite, le tableau de bord Livebox doit montrer ceci :



4. Vérifier que la configuration tient en éteignant puis rallumant votre boitier Internet
5. Vérifier que vous êtes protégé avec les deux URLs de sites fictifs
6. Configurez tous vos téléphones pour qu'ils cherchent à se connecter à votre nouveau Wi-Fi par défaut

Vérifiez que vous êtes maintenant protégé

1. Site fictif malveillant : https://malware.testcategory.com/
2. Site fictif pornographique : https://nudity.testcategory.com/

Le DNS CloudFlare répondra donc 0.0.0.0 pour ces deux sites, le navigateur affichera donc quelque chose comme "Ce site est inaccessible".

Configurer chacun de vos téléphones et tablette

Objectif : lorsque vous utilisez un téléphone en dehors de la maison, ou si le Wi-Fi est éteint à la maison, il se connectera à Internet via la 4G ou 5G, il ne sera plus protégé par votre boitier Internet de la maison.

Note : en l'absence de signal, éviter de se connecter à des Wi-Fi publics. Le protocole Wi-Fi étant faiblement sécurisé, il y a toujours un risque de se faire pirater son appareil.

Depuis assez récemment, il est devenu très facile de configurer le DNS des assistants personnels (smartphones).

Configuration pour :

- Android : https://developers.cloudflare.com/1.1.1.1/setup/android/
  - Note : pour un Android ancien (< 9), installer l'application "1.1.1.1:Faster Internet"
- Apple (iOS) : https://developers.cloudflare.com/1.1.1.1/setup/ios/
  - Note : nécessite l'installation de l'application "1.1.1.1: Faster Internet"

Dans les deux cas, suivre : *Block malware and adult content with 1.1.1.1 for **Families***

Une fois fait, vérifier que vous êtes protégé :

1. Désactiver le Wi-Fi de votre téléphone et assurez-vous que vous êtes connecté par 4G ou 5G uniquement
2. Ouvrir les deux sites de test
    - Sites malveillants : https://malware.testcategory.com/
    - Pornographie : https://nudity.testcategory.com/
3. Réactiver le Wi-Fi de votre téléphone si besoin

Configurer chacun de vos ordinateurs portables & consoles de jeu

Objectif : l'ordinateur portable peut être utilisé sur le Wi-Fi d'une famille amie ou sur le Wi-Fi d'une école qui n'a pas encore protégé son accès Internet.

Consoles de jeu

Les consoles de jeu récentes peuvent accéder à Internet (XBox, Sony PlayStation, Nintendo).

Configuration : https://developers.cloudflare.com/1.1.1.1/setup/gaming-consoles/

Ordinateurs portables

Suivre les procédures suivantes :

- Windows : https://developers.cloudflare.com/1.1.1.1/setup/windows/
- MacOS : https://developers.cloudflare.com/1.1.1.1/setup/macos/
- Linux : https://developers.cloudflare.com/1.1.1.1/setup/linux/

Wi-Fi publics = Danger

Note : éviter de se connecter à des Wi-Fi publics. Comme déjà expliqué, le protocole Wi-Fi étant faiblement sécurisé, il y a toujours un risque de se faire pirater son ordinateur.

À la place, utiliser le partage de connexion de Wi-Fi de votre téléphone portable, dont le mot de passe doit être long et difficile à deviner, car la sécurité ne repose que sur la longueur du mot de passe. Par exemple, choisir plusieurs mots faciles à retenir, comme "rosace céleri ristourne nettoyage".

Limitations

1. Habitué à rechercher sans risque sur Internet, si j'utilise un autre ordinateur non protégé, je suis moins vigilant, le risque est donc probablement plus important pour moi. Apprendre à configurer Cloudflare for Families à ses grands enfants et à son conjoint peut donc être intéressant.
2. Les prises RJ-45 des boitiers internet sont toujours accessibles et non protégées par le DNS Cloudflare for Families (sauf Freebox), mais il faut le vouloir pour s'y connecter directement, et disposer d'un portable avec prise RJ-45, ou d'un adaptateur USB vers Ethernet.

En cas de difficulté ou de question

Contactez-moi par courriel : vincent.agami@gmail.com