The Internet you deserve

https://feeltr.io

Pourquoi utiliser Feeltr ?

Feeltr a pour mission de **filtrer les connexions** de votre réseau, qu'il s'agisse d'un LAN (Local Area Network) ou d'un WAN (Wide Area Network).

Le filtrage a trois résultats :

- Un **réseau allégé**, puisque Feeltr bloque les requêtes non nécessaires, ce qui induit une libération de la bande passante et donc une connexion plus rapide ;
- Un **réseau plus sécurisé**, puisque Feeltr bloque certains vols de données personnelles et certains logiciels malveillants ;
- Un **réseau moins polluant**, puisque Feeltr en diminuant l'occupation de la bande passante et en stoppant certains logiciels malveillant, diminue la consommation en C02 globale.

Feeltr est donc une réponse adéquate aux enjeux qualitatifs, sécuritaires et environnementaux, des réseaux informatiques des grandes entreprises, des centres de soins de santé, des espaces scolaires et académiques, des états, des connexions WIFI publiques, des opérateurs IOT, des fournisseurs d'accès à Internet, etc.

Comment Feeltr améliore votre réseau ?

Feeltr est un serveur **DNS sécurisé**.

La mission de Feeltr est d'intercepter, autant que possible les :

- Relevés biométriques
- Vols de données privées
- Abus publicitaires
- Adwares
- Ransomwares
- Malwares
- Minerwares
- Logiciels espions

Relevés biométriques

Les relevés biométriques sont des informations techniques, envoyées par un logiciel, à l'entreprise qui le conçoit.

Par exemple, une application d'un téléphone mobile va transmettre le modèle d'un téléphone, son numéro de série, l'opérateur, le nombre de cycle de recharge de la batterie, etc.

Pour un navigateur internet, sur un ordinateur, cela peut-être par exemple, les adresses des sites web visités.

Vols de données privées

Les vols de données privées sont la transmission, par un logiciel, de données présentes sur vos machines, à l'entreprise qui le conçoit.

Par exemple, une application d'un téléphone mobile, à laquelle vous avez autorisé l'accès aux contacts de votre smartphone, va transmettre tout votre carnet d'adresse (et de facto toutes les données privées de vos contacts), dont le contenu sera ensuite revendu à des brokers d'information, qui commercialisent des bases de données à des fins marketing.

Pour les ordinateurs, c'est la même logique.

Abus publicitaires

La notion d'abus publicitaire a deux définitions possibles :

- Soit il s'agit d'une surexposition publicitaire qui dégrade l'expérience de surf, voire qui la rend impossible ;
- Soit il s'agit de publicité qui ne respecte pas les normes qui ont été définies par l'ACC (« Acceptable Ads Committee » https://acceptableads.com/committee/).

SUREXPOSITION : la surexposition publicitaire est effective quand une page Internet propose trop de publicités, ou quand les publicités empêchent l'accès au contenu, ou quand une campagne vous cible trop fortement (soit plus de 5 publicités pour un même produit par jour).

NORME D'UNE PUBLICITE ACCEPTABLE : les publicités acceptables sont des publicités qui ne sont ni intrusives ni dérangeantes. Elles sont respectueuses, ne s'immiscent pas dans le contenu et sont clairement identifiées par le mot « publicité » ou un équivalent. Les publicités ne doivent pas interrompre la lecture normale de l'utilisateur. Ces publicités doivent être placées au-dessus, sur les côtés ou en dessous du Contenu Principal.

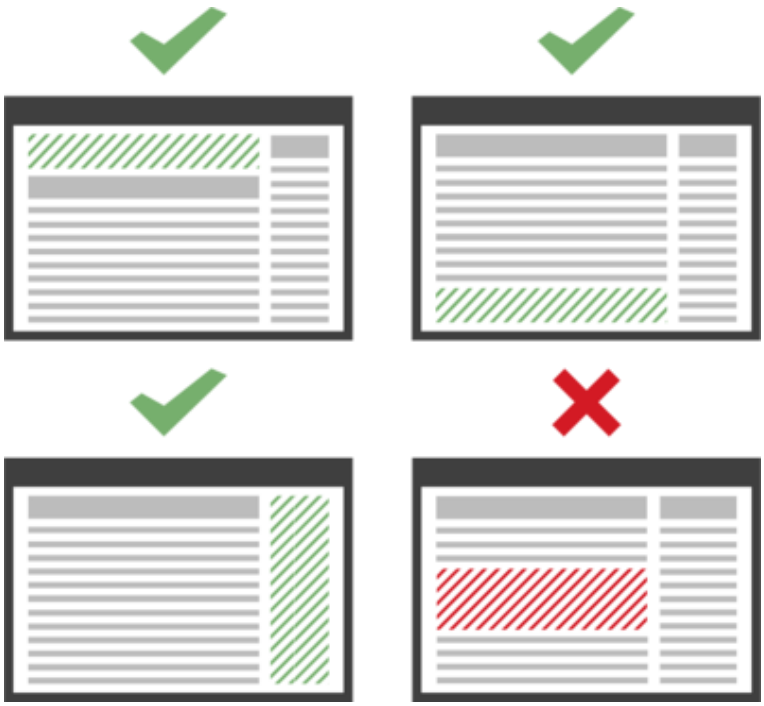

Figure 1- source : https://acceptableads.com/committee/

Les exigences relatives à la taille dépendent de l'emplacement de l'annonce publicitaire :

- Lorsqu'elle est placée au-dessus du contenu principal, la hauteur maximale de l'annonce est de 200 pixels.
- Lorsqu'elle est placée à côté du contenu principal, la largeur maximale de l'annonce est de 350 pixels.
- Lorsqu'elle est placée sous le contenu principal, la hauteur maximale de l'annonce est de 400 pixels.

Les publicités doivent laisser suffisamment d'espace pour le Contenu Principal sur la taille standard d'écran : 1 366 x 768 pour les ordinateurs, 360 x 640 pour les appareils mobiles et 768 x 1 024 pour les tablettes.

Toutes les publicités placées au-dessus de la ligne de flottaison (portion de la page Internet qui apparaît en premier sur la fenêtre du navigateur lorsque l'on ouvre une page, selon les tailles standard d'écran), doivent occuper moins de 15 % de la portion visible de la page Internet. Les publicités placées sous la ligne de flottaison doivent occuper moins de 25 % de la portion visible de la page Internet.

Figure 2- source : https://acceptableads.com/committee/

Adwares

Un ADWARE est un programme informatique qui affiche des publicités sur l'interface d'un logiciel ou via le navigateur Internet sous forme de fenêtres pop-up qui jaillissent de façon chronique.

Ransomwares

Un RANSOMWARE est un logiciel informatique malveillant, prenant en otage les données ou plutôt le propriétaire de ces données. Pour ce faire, il crypte et bloque les fichiers contenus sur votre ordinateur et demande une rançon en échange d'une clé permettant de les déchiffrer. Le ransomware est un risque majeur pour la cyber sécurité des entreprises.

Malwares

Un MALWARE est un type de virus malveillant, agressif, dont le but est d'endommager ou de mettre hors service les ordinateurs, les systèmes informatiques, les tablettes ou les appareils mobiles.

Minerwares

Un MINERWARE est un code qui réalise des calculs avancés à votre insu, sur vos appareils, afin de générer des cryptomonnaies de type Bitcoin, pour des groupes de cyber criminels. L'impact du MINERWARE est un ralentissement de vos équipements dont les ressources sont monopilisées par ce type particulier de malware.

Logiciels espions

Un LOGICIEL ESPION est un logiciel qui vous espionne, par exemple en prenant des photos depuis votre webcam, ou en copiant tout ce que vous saisissez au clavier, pour ensuite transmettre des informations à ces cybers criminels.

Quelles sont les offres de Feeltr ?

Feeltr peut soit protéger **un appareil de façon individuel**, soit protéger **tout un réseau**, de type LAN ou WAN, et de facto protéger tous les appareils connectés à ce réseau.

Par appareil nous entendons :

- Ordinateur
- Tablette
- Téléphone
- Appareils connectés (équipements de relevé de santé, équipements médicaux, IOT privé de type frigo connecté, IOT professionnel sonde ou caméra, etc.)

Si vous désirez réaliser une protection individuelle, merci de souscrire au logiciel via : https://feeltr.io/index.html

Si vous désirez protéger un réseau, il suffira de placer Feeltr comme étant le DNS par défaut de votre réseau. Il s'agit donc d'une configuration extrêmement simple à réaliser sur vos routeurs. Pour une offre personnalisée, sur base de vos besoins spécifiques, merci de nous contacter par email sur feeltr@simpl.team

Feeltr : c'est bon pour la planète

Selon GREENPEACE, le trafic du réseau Internet mondial représenterait **+/- 500 millions de tonnes de CO2**, soit l'équivalent de **deux fois l'empreinte carbone d'un pays comme l'Espagne**.

En allégeant votre bande passante, via l'utilisation de Feeltr, vous allégez l'empreinte carbone de votre informatique.

Si nous pouvions bloquer, via Feeltr, par exemple **25% du trafic mondial**, cela représenterait **175 millions de tonnes** de CO2 d'économisé.

A titre de comparaison, l'effort mondial définit pendant la COP21, qui n'a même pas été atteint en mettant le monde à l'arrêt pendant la crise du COVID19, est de **diminuer les émissions d'environ 150 millions** de tonnes.