The Internet you deserve

http://feeltr.io/

Why to use Feeltr ?

Feeltr's job is to **filter connections** on your network, whether it is a LAN (Local Area Network) or a WAN (Wide Area Network).

Filtering has three results :

- A **leaner network**, as Feeltr blocks unnecessary requests, which frees up bandwidth and results in a faster connection ;
- A more **secure network**, as Feeltr blocks some personal data theft and malware ;
- A **less polluting network**, as Feeltr reduces bandwidth usage and stops some malware, thus reducing overall CO2 consumption.

Feeltr is therefore an adequate answer to the qualitative security and environmental challenges of the IT networks of large companies, healthcare centres, school and academic spaces, states, public WIFI connections, IOT operators, Internet service providers, etc.

How does Feeltr improve your network ?

Feeltr is secure **DNS server**:

Feeltr's mission is to intercept, as much as possible, the:

- Biometric recording
- Theft of private data
- Advertising abuse
- Adware
- Ransomware
- Malware
- Minerware
- Spyware

Biometric recording

Biometric recording are technical information, sent by a software application to the company that develops it.

For example, a mobile phone application will transmit the model of a phone, its serial number, the operator, the number of battery charging cycles, etc.

For an internet browser on a computer, this could be, for example, the addresses of websites visited.

Theft of private data

Private data theft is the transmission of data on your machines by software to the company that designed it.

For example, a mobile phone application, to which you have authorized access to the contact on your smartphone, will transmit your entire address book (and de facto all the private data of your contacts), the content of which will then be resold to information brokers, who sell databases for marketing purposes.

For computers, it is the same logic.

Advertising abuse

The notion of advertising abuse has two possible definitions:

- Either it is advertising overexposure that degrades the surfing experience or even makes it impossible ;
- Or it is advertising that does not respect the standards that have been defined by the ACC (« Acceptable Adscommittee » https://acceptableads.com/committee/).

OVEREXPOSURE: Advertising overexposure occurs when a web page has too many ads, or when ads prevent access to content, or when a campaign targets you too heavily (i.e. more than 5 ads for single product per day).

ACCEPTABLE ADVERTISING STANDARD: Acceptable ads are ads that are neither intrusive nor disruptive. They are respectful, do not interfere with the content and are clearly identified by the word « advertisement » or equivalent. Advertisement should not interrupt the user's normal reading experience. This advertisement must be placed above, to the side of or below the Main Content.

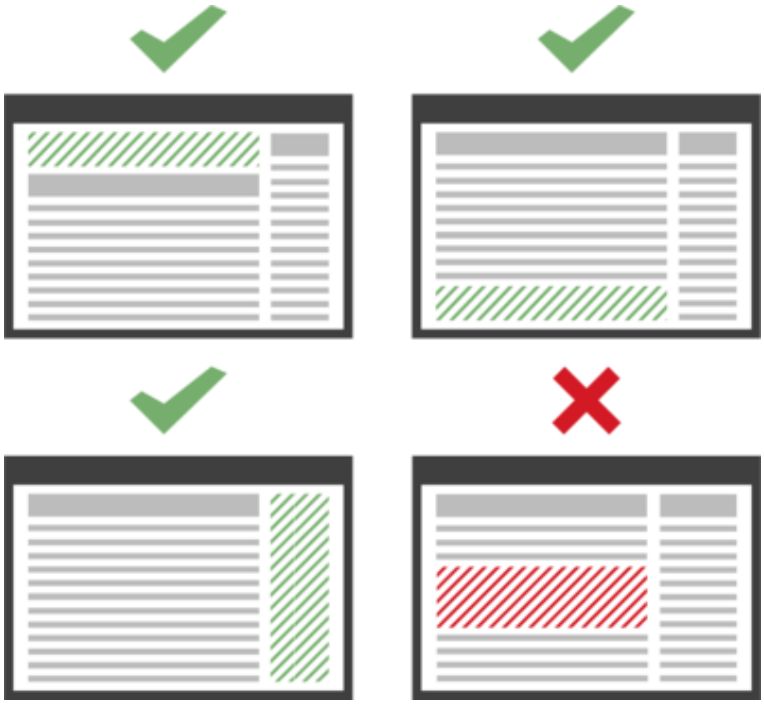

Figure 1- source : https://acceptableads.com/committee/

The size requirements depend on the placement of the ad:

- When placed above the main content, the maximum ad height is 200 pixels.
- When placed next to the main content, the maximum ads width is 350 pixels.
- When placed below the main content, the maximum height of the ad is 400 pixels.

Advertisements must allow sufficient space for the Main Content on the standard screen size: 1366 x 768 for computer 360 x 640 for mobile devices and 768 x 1024 for tablets.

All ads placed above the waterline (the portion of the web page that appears first in the browser window when a page is opened, based on standard screen sizes), most occupy less than 15% of the visible portion of the web page. Ads placed below the waterline must occupy less than 25% of the visible portion of the web page.

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

Adwares

Un ADWARE is a computer program that displays advertisements on the interface of a software program or via the Internet browser in the form of pop-up windows that appear chronically.

Ransomwares

A RANSOMWARE is a malicious computer program that takes your data, or rather the owner of your data, as hostage. It does this by encrypting and locking files on your computer and demanding a ransom in exchange for a key to decrypt them. Ransomware is a major cybersecurity risk for businesses.

Malwares

A MALWARE, is a type of malicious, aggressive virus whose purpose is to damage or disable computers, computer systems, tablets or mobile devices.

Minerwares

A minerware is a code that performs advanced calculations on your devices without your knowledge in order to generate Bitcoin-like currencies for cybercriminal groups. The impact of MINERWARE is a slowing down of your equipment whose resources are monopolized by this particular type of malware.

Spywares

A spyware is software that spies on you, for example by taking pictures from your webcam, copying everything you type on your keyboard, and then passing the information on to these cyber criminals.

What does Feeltr **offer**?

Feeltr can either protect **an individual device** or protect **an entire network**, such as a LAN or WAN, and thus protect all devices connected to that network.

By device we mean:

- Computer
- Tablet
- Phone
- Connected devices (health recording equipment, private IOT such as a connected fridge, professional IOT probe or camera, etc.)

If you wish to carry out individual protection please subscribe to the software via: https://feeltr.io/index.html

If you want to protect a network, you just need to set Feeltr as default DNS for your network. This is an extremely simple configuration to perform on your router. For a customized offer, based on your specific needs, please contact us by email at feeltr@simpl.team

Feeltr in **4** figures?

- **46.093** data thefts blocked
- **49.246** viruses and security theats blocked
- **878.415.517** advertising abuse blocked
- **87.851** tonnes of CO2 saved

Follow the evolution of our project on https://www.feeltr.io/hourra.html