The Internet you deserve

https://feeltr.io

¿Por qué usar Feeltr?

El objetivo de Feeltr es filtrar las conexiones en tu red, ya sea una LAN (red de área local) o una WAN (red de área amplia).

El filtrado ofrece tres resultados:

- Una **red** más **ligera**, ya que Feeltr bloquea las peticiones innecesarias, lo que libera el ancho de banda para una conexión más rápida;

- Una **red** **más segura**, ya que Feeltr bloquea algunos intentos de robos de datos personales y ciertos malwares;

- Una **red** **menos contaminante**, ya que Feeltr reduce la ocupación del ancho de banda y detiene ciertos programas maliciosos, reduciendo así el consumo global de C02.

Feeltr es, por tanto, una respuesta adecuada a los desafíos cualitativos, de seguridad y medioambientales de las redes informáticas de grandes empresas, centros sanitarios, escuelas e instituciones académicas, estados, conexiones WIFI públicas, operadores de IoT, proveedores de servicios de Internet, etc.

¿Cómo mejora Feeltr tu red?

Feeltr es un servidor **DNS seguro**.

La misión de Feeltr es interceptar, en la medida de lo posible, los:

- Registros biométricos
- Robos de datos privados
- Abusos publicitarios
- Adwares
- Ransomwares
- Malwares
- Minerwares
- Programas espía

Registros biométricos

Los registros biométricos son información técnica enviada por una aplicación informática a la empresa que la diseñó.

Por ejemplo, una aplicación de telefonía móvil transmitirá el modelo del teléfono, el número de serie, el operador, el número de ciclos de carga de la batería, etc.

En el caso de un navegador de Internet en un ordenador, podrían ser, por ejemplo, las direcciones de los sitios web visitados.

Robo de datos privados

El robo de datos privados es la transmisión de datos presentes en tus máquinas por medio de un software a la empresa que lo diseñó.

Por ejemplo, una aplicación de telefonía móvil, a la que usted ha autorizado a acceder a los contactos de tu smartphone, transmitirá toda tu agenda (y de facto todos los datos privados de tus contactos), cuyo contenido será revendido a intermediarios de información, que venden bases de datos con fines de marketing.

Para los ordenadores, es la misma lógica.

Abuso publicitario

La noción de abuso publicitario tiene dos posibles definiciones:

- O bien se trata de una sobreexposición publicitaria que degrada la experiencia de navegación o incluso la hace imposible;
- O se trata de publicidad que no respeta las normas definidas por la ACC ("Acceptable Ads Committee" https://acceptableads.com/committee/).

SOBREEXPOSICIÓN : La sobreexposición publicitaria se produce cuando una página web tiene demasiados anuncios, o cuando los anuncios impiden el acceso al contenido, o cuando una campaña se dirige a usted de forma excesiva (es decir, más de 5 anuncios del mismo producto al día).

NORMAS DE PUBLICIDAD ACEPTABLE : Los anuncios aceptables son aquellos que no son ni intrusivos ni molestos. Son respetuosos, no interfieren con el contenido y están claramente identificados con la palabra "publicidad" o equivalente. Los anuncios no deben interrumpir la experiencia de lectura normal del usuario. Estos anuncios deben colocarse encima, al lado o debajo del Contenido Principal.

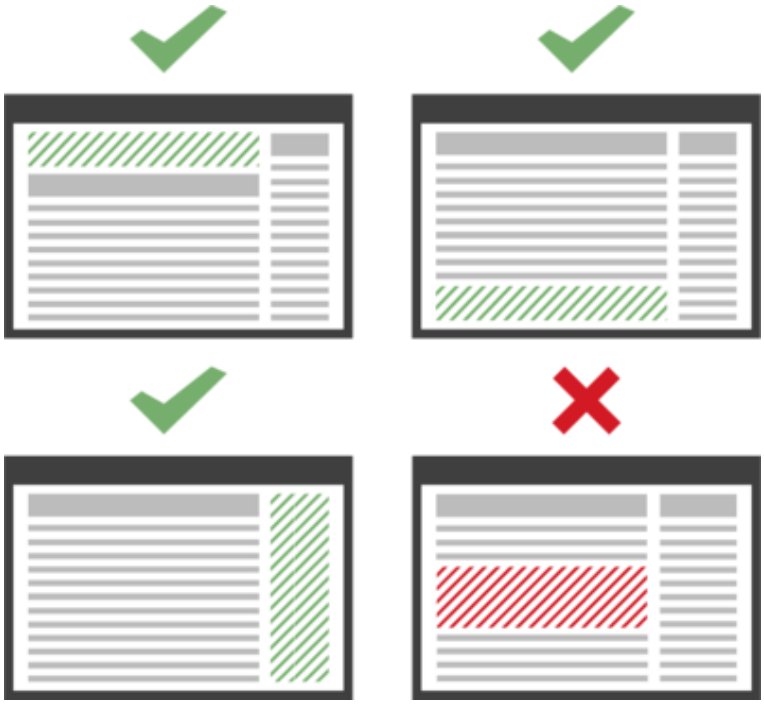

Figure 1- source : https://acceptableads.com/committee/

Los requisitos de tamaño dependen de la ubicación del anuncio:

- Cuando se coloca sobre el contenido principal, la altura máxima del anuncio es de 200 píxeles.

- Cuando se coloca junto al contenido principal, la anchura máxima del anuncio es de 350 píxeles.

- Cuando se coloca debajo del contenido principal, la altura máxima del anuncio es de 400 píxeles.

Los anuncios deben dejar espacio suficiente para el contenido principal en el tamaño de pantalla estándar: 1366 x 768 para ordenadores, 360 x 640 para dispositivos móviles y 768 x 1024 para tabletas.

Todos los anuncios colocados por encima de la línea de flotación (la parte de la página web que aparece en primer lugar en la ventana del navegador cuando se abre una página, según los tamaños de pantalla estándar), deben ocupar menos del 15% de la parte visible de la página web. Los anuncios colocados por debajo de la línea de flotación deben ocupar menos del 25% de la parte visible de la página web.

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

Adware

Un ADWARE es un programa informático que muestra publicidad en la interfaz de un programa informático o a través del navegador de Internet en forma de ventanas emergentes que aparecen de forma crónica.

Ransomware

Un RANSOMWARE es un programa informático malicioso que toma como rehenes a los datos, o más bien al propietario de los mismos. Lo hace encriptando y bloqueando los archivos de tu ordenador y exigiendo un rescate a cambio de una clave para desencriptarlos. El ransomware es un riesgo importante para la ciberseguridad de las empresas.

Malware

Un MALWARE es un tipo de virus malicioso, agresivo, cuyo objetivo es dañar o inutilizar los ordenadores, los sistemas informáticos, tabletas y aparatos móviles.

Minerware

Un MINERWARE es un código que realiza cálculos avanzados en tus dispositivos sin que lo sepas, con el fin de generar criptomonedas como Bitcoin, para grupos cibercriminales. El impacto del MINERWARE es una ralentización de tus equipos cuyos recursos son acaparados por este tipo particular de malware.

Programas espías

Un PROGRAMA ESPIA es un programa que te controla, por ejemplo tomando fotos desde tu webcam o copiando todo lo que escribes en tu teclado, para luego pasar la información a los ciberdelincuentes.

¿Cuáles son las ofertas de Feeltr?

Feeltr puede proteger un dispositivo de manera individual o proteger toda una red, de tipo LAN o WAN, y en consecuencia proteger todo dispositivo conectado a esta red.

Por dispositivo entendemos:

- Ordenador
- Tableta
- Teléfono
- Aparatos conectados (equipos de reconocimiento de estado de salud, equipos médicos, IOT privados como neveras conectadas, IOT profesionales sonda ocámara, etc.)

Si deseas una protección individual, suscríbete al programa vía: https://feeltr.io/index.html.

Si deseas proteger una red entera, bastara con definir Feeltr como DNS principal en tu red. Se trata entonces de una configuración extremadamente simple que realizar en tu router. Para una oferta personalizada, según tus necesidades especificas, contáctanos a la dirección e-mail: feeltr@simpl.team

Feeltr: es bueno para el planeta

Según GREENPEACE, el tráfico mundial de Internet se estima en **+/- 500 millones de toneladas de CO2**, lo que equivale al **doble de la huella de carbono de un país como España.**

Al reducir su ancho de banda, mediante el uso de Feeltr, reduce la huella de carbono de su informática.

Si pudiéramos bloquear, por ejemplo, el **25% del tráfico mundial** a través de Feeltr, se ahorrarían **175 millones de toneladas** de CO2.

A modo de comparación, el esfuerzo global definido durante la COP21, que ni siquiera se logró al confinar el mundo durante la crisis de COVID19, es **reducir las emisiones en unos 150 millones** de toneladas.