The Internet you deserve

https://feeltr.io

Porquê usar Feeltr?

O trabalho de Feeltr é filtrar ligações na sua rede, quer seja uma LAN (Local Area Network) ou uma WAN (Wide Area Network).

A filtragem tem três resultados:

- Uma **rede mais enxuta**, como Feeltr bloqueia pedidos des necessários, o que liberta largura de banda e resulta numa ligação mais rápida;
- Uma **rede mais segura**, uma vez que Feeltr bloqueia alguns roubos de dados pessoais e malware;
- Uma **rede menos poluente**, uma vez que Feeltr reduz a utilização da largura de banda e pára algum malware, reduzindo assim o consumo global de C02.

Feeltr é portanto uma resposta adequada aos desafios qualitativos, de segurança e ambientais das redes informáticas em grandes empresas, centros de saúde, escolas e espaços académicos, estados, ligações públicas WIFI, operadores IOT, fornecedores de serviços Internet, etc

Como é que Feeltr melhora a sua rede?

Feeltr é um servidor **DNS seguro.**

A missão de Feeltr é interceptar, na medida do possível, o :

- Inscrição biométrica
- Roubo de dados privados
- Abuso publicitários
- Adware
- Ransomware
- Malware
- Minerware
- Spyware

Inscrição biométrica

Os registos biométricos são informações técnicas, enviadas por uma aplicação de software para a empresa que os desenvolve.

Por exemplo, uma aplicação de telemóvel transmitirá o modelo de um telefone, o seu número de série, o operador, o número de vezes que a bateria foi recarregada, etc.

Para um navegador da Internet num computador, isto poderia ser, por exemplo, os endereços dos sítios visitados.

Roubo de dados privados

O roubo de dados privados é a transmissão de dados nas suas máquinas por software para a empresa que o concebeu.

Por exemplo, uma aplicação para telemóvel, à qual tem acesso autorizado aos contactos do seu smartphone, transmitirá todo o seu livro de endereços (e de facto todos os dados privados dos seus contactos), cujo conteúdo será depois revendido aos corretores de informação, que vendem bases de dados para fins de marketing.

Para computadores, a lógica é a mesma.

Abuso publicitários

A noção de abuso publicitário tem duas definições possíveis:

- Ou é a sobre-exposição à publicidade que degrada a experiência do surf ou mesmo a torna impossível;
- Ou é publicidade que não cumpre as normas que foram definidas pelo ACC ("Acceptable Ads Committee" https://acceptableads.com/committee/).

SOBRE EXPOSIÇÃO: A sobre-exposição de publicidade ocorre quando uma página web tem demasiados anúncios, ou quando os anúncios impedem o acesso ao conteúdo, ou quando uma campanha se dirige demasiado a si (ou seja, mais de 5 anúncios para o mesmo produto por dia).

NORMA ACEITÁVEL DE PUBLICIDADE: Anúncios aceitáveis são anúncios que não são nem intrusivos nem perturbadores. São respeitosos, não interferem com o conteúdo e são claramente identificados pela palavra "anúncio" ou equivalente. Os anúncios não devem interromper a experiência normal de leitura do utilizador. Estes anúncios devem ser colocados acima, para o lado ou abaixo do Conteúdo Principal.

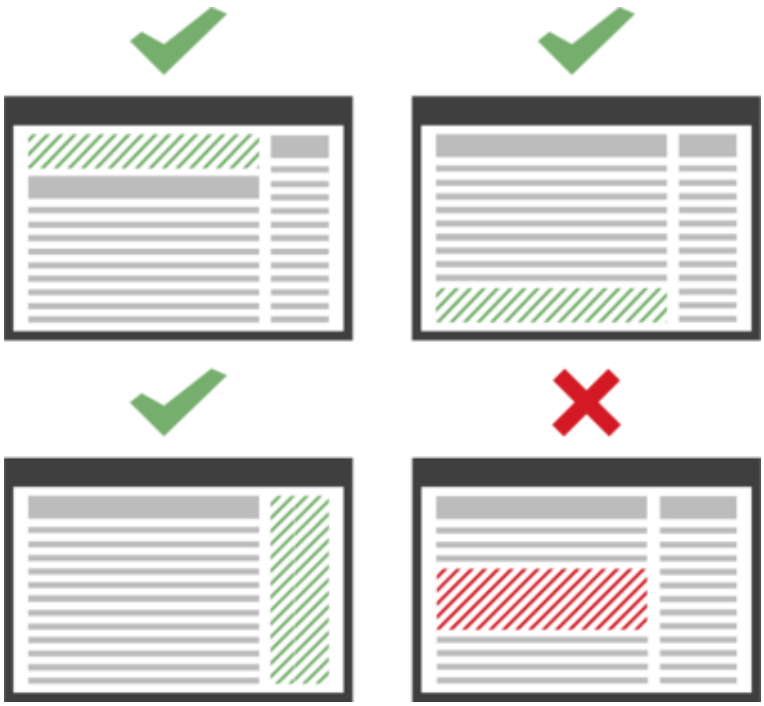

Figure 1- source : https://acceptableads.com/committee/

Os requisitos de tamanho dependem da localização do anúncio:

- Quando colocado acima do conteúdo principal, a altura máxima do anúncio é de 200 pixels.
- Quando colocado junto ao conteúdo principal, a largura máxima do anúncio é de 350 pixels.
- Quando colocado abaixo do conteúdo principal, a altura máxima do anúncio é de 400 pixels.

Os anúncios devem permitir espaço suficiente para o Conteúdo Principal no tamanho padrão do ecrã: 1366 x 768 para computadores, 360 x 640 para dispositivos móveis e 768 x 1024 para comprimidos.

Todos os anúncios colocados acima da linha de água (a parte da página web que aparece primeiro na janela do navegador quando uma página é aberta, com base em tamanhos de ecrã padrão), devem ocupar menos de 15% da parte visível da página web. Os anúncios colocados abaixo da linha de água devem ocupar menos de 25% da parte visível da página web.

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

Adware

Um ADWARE é um programa de computador que exibe anúncios na interface de um programa de software ou através do navegador da Internet sob a forma de janelas pop-up que surgem numa base crónica.

Ransomware

Um RANSOMWARE é um programa informático malicioso que faz reféns os dados, ou melhor, o proprietário dos dados. Faz isto encriptando e bloqueando os ficheiros no seu computador e exigindo um resgate em troca de uma chave para os decifrar. O resgate é um grande risco para a segurança cibernética das empresas.

Malware

Um MALWARE é um tipo de vírus malicioso e agressivo que visa danificar ou desactivar computadores, sistemas informáticos, comprimidos ou dispositivos móveis.

Minerware

Um MINERWARE é um código que efectua cálculos avançados nos seus dispositivos sem o seu conhecimento, a fim de gerar moedas criptográficas do tipo Bitcoin para grupos cibercriminosos. O impacto do MINERWARE é um abrandamento do seu equipamento cujos recursos são monopolizados por este tipo particular de malware.

Spyware

Um SPYWARE é um software que o espiona, por exemplo, tirando fotografias da sua webcam, ou copiando tudo o que escreve no seu teclado, e depois transmitindo informações a estes ciber-criminosos.

O que é que Feeltr oferece?

Feeltr pode proteger **um dispositivo individual** ou proteger **uma rede inteira**, como uma LAN ou WAN, e assim proteger todos os dispositivos ligados a essa rede.

Por dispositivo entendemos :

- Computador
- Tablet
- Telefone
- Dispositivos ligados (equipamento de registo sanitário, equipamento médico, IOT privado, como frigorífico ligado, sonda ou câmara fotográfica profissional IOT, etc.)

Se deseja proteger uma rede individual, subscreva o software através de: https://feeltr.io/index.html

Se quiser proteger uma rede, basta definirFeeltr como o DNS predefinido para a sua rede. Esta é uma configuração extremamente simples de executar nos seus routers. Para uma oferta personalizada, com base nas suas necessidades específicas, contacte-nos por favor por e-mail para feeltr@simpl.team

Feeltr: bom para o planeta

De acordo com a GREENPEACE, o tráfego global na Internet é estimado em

+/- 500 milhões de toneladas de CO2, o que equivale ao **dobro da pegada de carbono de um país como a Espanha.**

Ao reduzir a sua largura de banda, através do uso de Feeltr, reduz a pegada de carbono do seu computador.

Se pudéssemos bloquear, digamos, **25% do tráfego mundial via Feeltr,** isso seria **175 milhões de toneladas** de CO2 poupadas. Para comparação, o esforço global definido durante a COP21, que nem sequer foi alcançado com o encerramento do mundo durante a crise da COVID19, consiste em **reduzir as emissões em cerca de 150 milhões** de toneladas.