How to make the internet safer for the users of your public Wi-Fi.

It is true that no Wi-Fi filtering system is infallible. Even good filters require human monitoring and response protocols. However, filtering is an important tool and may be part of your due diligence as an organization providing publicly accessible internet. Unprotected public internet access may be used for **criminal or illegal purposes**, and you, as the provider, may be liable. Having filtering, using a DNS (Domain Name System) service, may be part of your risk management.

SIMPLEST SOLUTION:

FREE DNS – DNS translates your request for a website into an IP address and searches the web for that address. It connects you and the website. If it deems the website unsafe it will not connect you. Here are two FREE options you can configure on your Wi-Fi router or firewall:

OpenDNS

https://www.opendns.com/home-internet-security/

You will see that they have a Family Shield package which is pre-configured to block adult content. They also have a set up guide right on the sign-up page.

Ultra DNS

https://www.publicdns.neustar/

They have a product called Family Secure. When you click on "Get Set Up Now," it will take you to a page with set up instructions for routers, computers, and mobile devices.

(You can even use both for better protection)

NEXT LEVEL SOLUTION:

As part of your firewall solution, you could activate the **Unified Threat Management** package from your firewall vendor. There would likely be a cost for this and may require additional hardware resources.

ANOTHER OPTION:
Another option is to use software-based filtering, like NetNanny, https://www.netnanny.com/. However, software of this type has a cost and is easily disabled.

Choose Change is an annual campaign of Defend Dignity. It focuses on reducing the ease of access to sexual violent images, pornography. Visit us at choosechangecanada.org

#choosechangecanada #pornharms #choosechangelocal