How to Block Inappropriate Websites in a Workplace

Posted on December 29, 2019

Accessing explicit or illegal content from the office network can be a serious liability for your company. Blocking inappropriate websites at a workplace protects your network from malware, legal issues, and low employee productivity.

Monitoring workplace Internet activity manually could be a time-consuming task. Fortunately, the blocking of inappropriate websites can be automated. We'll show you how to block inappropriate websites by using five tricks with varying degrees of reliability.

1. Create a transparent Internet-use policy

Before you enforce any rules on workplace Internet activity, make sure these rules are clearly stated. Your employees need to understand which websites are allowed and which are banned during working hours. This also refers to any non-work-related web content, such as social media, online games, gambling, shopping sites, etc.

Even if you decide to grant access to entertainment sites, illegal content should be off-limits for several reasons. Apart from hindering productivity and being inappropriate, such websites are usually a hotbed of viruses and malware. In certain situations, they can also tarnish your company's reputation.

Your Internet-use policy should be part of the onboarding documentation for every new employee. Also, it should always be readily available to all of your current employees.

2. Block inappropriate websites with DNS filter

Unfortunately, informing employees on the Internet-use policy isn't usually enough to prevent access to inappropriate websites.

So how do you approach it? You can start by setting up a DNS filter. DNS is the Internet protocol that converts the domain name to an IP address. When you set up a filter, this process is prevented for any blocked or explicit content.

This is the quickest and simplest way to block inappropriate websites. Since DNS protocol is a prerequisite to Internet connection, you can use DNS filters on any device and network.

There are plenty of free and affordable DNS filtering services. However, technically savvy employees are able to bypass them. Also, using these services raises privacy concerns with regard to your company's sensitive information.

3. Use a safe-search mode to block Inappropriate content

Another way to block explicit content in the office is to set your search engines to "safe search" mode. In the links below, you can find detailed instructions on how to block inappropriate websites on Google Chrome:

- Google
- Bing
- Yahoo
- YouTube

Thoroughness is the main perk of using a safe-search filter to block inappropriate content. They don't stop at blocking websites. The safe-search mode also filters individual Web pages based on headlines, title, description, metadata, reviews, and sets age-restrictions. These tools also come with features such as limiting screen time and monitoring. Safe search mode works across different platforms and devices, including Android devices and iPhones.

Yet, the reliability of this tool is only moderate. The quality of filtering varies based on location and language. Also, users can easily bypass it by logging out of their accounts or by using alternative search engines.

None of the existing content blockers offer protection against viruses, malware, and phishing.

4. Use filtering apps and extensions to enable safe search

Web browser extensions and web filtering apps are more secure ways to block inappropriate websites. They allow you to block specific websites, categories, or URLs that contain inappropriate terms. These add-ons and apps also come with bonus protection against viruses, malware, and phishing.

Compared to the safe-search mode and DNS filtering, these tools are also more customizable. You can play around with the settings and add entertainment and social media to the list of blocked websites. They work in incognito mode as well.

Web filtering apps are superior to browser extensions because browser add-ons are easily bypassed. Even going as far as adding them to every browser isn't of much help. Employees can easily access inappropriate sites by downloading or by using alternative browsers.

Web filtering apps offer a plethora of possibilities for customization, protection from cyberattacks and malware, as well as limiting access to non-work-related websites.

However, web filtering solutions cannot guarantee 100% safety either.

Safe-search mode, add-ons and web filtering tools often cannot make a difference between allowed and blocked content. Even work-related websites can be mistaken for inappropriate content on the basis of one word or image. This may result in frustration and decreased productivity. An incomplete database of malware and dangerous websites may also put your

company in danger.

5. Use website categorization for 100% protection

Website Categorization API is a tool developed by WhoisXMLAPI. Website categorization helps you block inappropriate websites by analyzing web content in three steps:

- Examining website response during the crawling session
- Analyzing on-page content and keywords based on natural language processing
- Authenticating the results through human supervision

Websites are assigned to 1-3 out of 25 different categories. You can set which combinations belong on the list of blocked categories.

With website categorization API, you won't waste time wondering how to block inappropriate websites effectively. Your web filter will analyze entire domains and individual page content just like a human would. This way, you'll make sure you are not blocking work-related or safe websites. At the same time, inappropriate websites or pages won't be able to break through the barrier.

With website categorization, you can feel confident that your office remains a decent, safe place with a great reputation. Click here for a free demo!