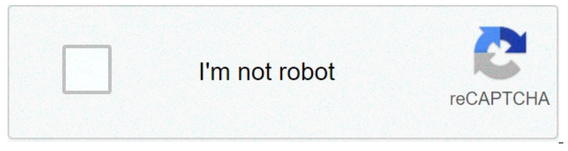

Continue

How to bypass blocked websites at school on chromebook

From open layouts to ping-pong tables in breakrooms, there are a lot of distractions in modern offices. While it's important to promote work-life balance, it can be frustrating as an employer to see employees waste valuable work hours.Some employers block distracting websites to combat unproductivity, but other business owners believe restricting web use could have negative side effects. "No one can – or should – be working eight hours straight a day," said Jonathan Prichard, founder and CEO of MattressInsider.com. "I have worked with many professionals who find their productivity increase when they schedule periodic breaks to use the web at their leisure while at work."Other business owners decide to block websites for security or legal reasons. Regardless of your reason, here are four different types of websites you should consider blocking on business devices.Editor's note: Looking for information on employee monitoring software? Use the questionnaire below, and our vendor partners will contact you to provide you with the information you need.1. Inappropriate websitesThe most important websites to block are ones that are inappropriate, offensive and could land you in legal trouble. Unlike social media, there is no reason why employees should be on adult or gambling websites. Along with being unprofessional and inappropriate, these websites can pose a security risk to your network and devices."These are offensive websites that we block to reduce legal liability in the workplace," said Nishank Khanna, vice president of growth at Utility. "Things like pornography, gambling websites, etc."Business owners are split on whether it's a good idea to block social media websites such as Facebook, Instagram and Twitter. Social media is a clear distraction – 65 percent of employees believe Facebook hurts productivity, according to Udemy's 2018 Workplace Distraction Report.However, some business owners believe blocking these websites could paint employers as micromanagers or like they don't trust their employees. "Instead of boxing in your employees by blocking social media, as a leader you should focus on results," Khanna said. "As long as your people get the work done, there is no need to fret over them viewing social media accounts."Overall, half (51 percent) of employees surveyed said their employers restrict social media websites.3. Video streamingWhen you're invested in a TV show, it can be hard to turn it off, and some people are streaming shows during work hours."As recently as 2017, Netflix reported that 37 percent of its users admitted watching the streaming service at work," said Ben Bowman, content development lead at Softonic. "That means if you aren't killing time with Stranger Things, one of the co-workers on either side of you probably is." When your employees are streaming movies, not a lot of work is getting done. If you notice employees watching videos, you may want to consider blocking websites such as Netflix, Hulu, HBO and YouTube.While it might seem obvious to block adult websites, some business owners have decided to block shopping websites as well. It's easy for employees to get sucked into online shopping, and blocking websites such as Amazon, Target and Poshmark might improve employee productivity."We found that our employees were spending far too much time on these types of websites," said Matthew Ross, co-owner and COO of The Slumber Yard. "After auditing the data, you wouldn't believe how much time employees were wasting. In some cases, certain employees were spending over four hours a day surfing the net and shopping online."If you decide to restrict certain websites or categories from work devices, you should be transparent with your employees and explain what websites are being blocked and why. You should also create an internet use policy explaining your decision. Bookmarks are great to keep your favorite sites nearby, but they aren’t the fastest option out there. Instead, why not add shortcuts for your favorite websites right on the Chromebook shelf? If there’s a site you go to multiple times per day—especially if it’s critical to your business—every added step means more time you have to spend getting where you need to be. Having your favorite websites right on your Chromebook’s shelf (the taskbar at the bottom where you see open app icons) makes getting to them that much quicker. How to Add Your Favorite Website to Your Chromebook Shelf Start by visiting the website for which you’d like to have a shortcut. Select the three-dot menu in the upper-right. Hover over the “More Tools” menu and then select “Create Shortcut.” Change the name of the shortcut if you want, and then click “Create.” That’s it! The website’s icon will always be on your shelf, ready whenever you are. By default, the website will open in a new browser tab. But, you can give the site its own window by right-clicking or long pressing the icon, hovering over the arrow, and then selecting “New Window.” This makes the app feel more like a native application than just a website, and it can be great for sites like Netflix, YouTube, and other consumption sites where you don’t want the visual distractions that come from having other browser tabs. These shortcuts are synced with your Google account, so even if you use a different Chromebook, you’ll still have them on your shelf and in your app drawer. With that, your favorite site will always be one click away! Julia Tim/Shutterstock One of the only ways to protect your right to privacy and information online is to use a VPN. Some websites infringe on those rights by blocking VPNs, but they do it for a good reason. The big names that are notorious for blacklisting VPNs are Netflix, Hulu, Amazon, and the BBC. It’s hard to figure out exactly how many websites block VPN access, but the number could be in the thousands. Most of these sites aren’t actively at war with VPNs, but they manage to blacklist a lot of VPN IP addresses over time passively. Remind Me, What’s a VPN? Before going into this, you’ll want to know what IP addresses are and how VPNs work. We’ll keep this brief. When you connect to the internet through a router, you’re given an IP address. This address, essentially, identifies your computer or router so that websites know where you’re connecting from and can send traffic back to you. The IP address that you’re assigned at home is different from the IP address that you’re assigned at a coffee shop. When you use a VPN (virtual private network), you’re effectively tunneling all of your online activity through a remote server. Your service provider can’t see what you’re doing online, because the traffic is encrypted and funneled through a remote server. Websites can’t see your actual IP address; they can only see the IP address of the server that’s masking your activity. So if your VPN funnels your activity through a server that’s in a different state or country, websites think that you’re connecting from said state or country. RELATED: What Is a VPN, and Why Would I Need One? Blocking VPNs Is Easy It’s common for websites to locate and track users based on their IP addresses. IP tracking is an easy way to increase account security, build targeted advertisements, and show users different content depending on the country in which they live. This practice of IP tracking is one of the main reasons why people use VPN services, but it’s also the reason why blocking VPN access to a website is so easy. A VPN service owns a limited number of IP addresses. And since most VPN servers use IPv4 (an outdated IP address protocol), it’s difficult to generate unique IP addresses, and a pool of subscribers are often sharing the same IP addresses for months or years at a time. Websites that want to blacklist VPNs simply need to use services like ipinfo to block IP addresses that have been used by multiple different users. There are two other ways that websites can blacklist VPNs, but these methods aren’t as common as IP blocking. One method, called port blocking, requires websites to figure out the exit ports that VPNs are using for all of their IP addresses. Port blocking is easy and effective because most VPNs use the 1194 OpenVPN port. Another method, called deep-packet inspection, checks users’ metadata for cryptography signatures. These signatures are like the fingerprints of VPN services, and hiding them is difficult. Contracts Force Streaming Sites To Ban VPNs Again, the most notorious VPN blacklisters are Netflix, Amazon, Hulu, and the BBC. All of these websites stream media, and they all blacklist VPNs to honor regional contracts with licensing companies. When streaming services want to add a TV show or a movie to their library, they have to sign a contract with the licensing company that owns said programming. The world of streaming services is incredibly competitive right now, and licensing companies can make hundreds of millions of dollars by handing popular shows to the highest bidder. Syda Productions/Shutterstock But the licensing contracts that streaming services sign are usually regional, not global. That’s why Netflix and Hulu offer different programming to different counties. Streaming services sign regional contracts because the popularity (and therefore, the value) of shows and movies differs by regions. It’s safe to assume that culturally-specific programming, like Korean dramas, are worth more in some regions than they are in others. Therefore, Netflix doesn’t have to pay much to secure an American license for a Korean drama, because K-dramas aren’t very profitable outside of Korea. But if Koreans start using VPN services to watch their favorite shows on American Netflix, then the value of Korean programming will fall significantly. Licensing companies won’t be able to convince Korean streaming services that these shows are worth million-dollar contracts because American Netflix is already getting all of the Korean traffic for these shows at a much lower price. Licensing companies and TV networks don’t want the value of their shows to decrease, for obvious reasons. So they build clauses into their contracts that force streaming services to secure content by region. Streaming services have no choice but to blacklist VPNs. Admittedly, we don’t have access to any of these legal agreements. But if they look anything like the contracts that Apple signs, then licensing companies are allowed to pull programming at a moment’s notice if streaming services can’t protect the value of said programming. Oh, and they could sue. Websites Want To Minimize Spam And Fraud The most legitimate reason why a website would block VPN access is to mitigate unlawful or annoying behavior. The problem with this technique is that it punishes more innocent people than it does criminals. Paypal has received a lot of flack for blacklisting VPNs, but to be fair, they do it for a good reason. IP addresses are a form of identity, and criminals that use a VPN to mask their IP address tend to be difficult to track down. Not to mention, Paypal is a bank, and the company has to respect regional tax codes and money laws. Maxim Apryatin/Shutterstock Some websites, like IRS.gov or Craigslist, don’t always work when you’re using a VPN service. These websites aren’t running blacklists that specifically target VPN IP addresses, though; they’re usually running and contributing to public blacklists that flag IP addresses associated with spam and suspicious activity. But how do these IP addresses end up on these public blacklists? Well, let’s pretend that you’re doing account security work at IRS.gov, and you notice something strange. A hundred different people have logged in from the same IP address. While this could be a sign that people are using a VPN service at tax time, it could also be a sign that some wild hacker has managed to compromise a hundred different accounts. Blacklisting that IP address is probably a good idea, even if it may infringe on peoples’ right to privacy. Public Wi-Fi Networks Block VPNs You should always use a VPN while connected to a public network. Obviously, McDonald’s doesn’t need to know what you’re doing on the internet, but their prying eyes aren’t the main issue. Public networks aren’t secure (yet). They’re easy to hack, and someone that hacks a public network can collect a ridiculous amount of sensitive information in a short period. That’s why the blacklisting of VPNs by public Wi-Fi networks is so frustrating. People have complained that a lot of public Wi-Fi networks, particularly those that are provided by Comcast and AT&T, block VPN access entirely. They probably do this to keep you from pirating files or watching porn on their network, but they might be doing this to ensure that they can collect and sell your web traffic. How To Get Around Blacklists Proxima Studios/Shutterstock The majority of VPN users aren’t fraudsters or pirates. They’re average people that are concerned about privacy, or people that feel the need to skirt around geo-locked content and government censorship. When businesses choose to blacklist VPN services, it isn’t just a minor annoyance; it’s also a denial of your right to privacy and information. There are some ways to get around these blacklists, but things change every day, so be prepared to look for new solutions as old methods become unreliable. Here are some ways to get around blacklists: Only use premium VPN services, and avoid anything that’s too good to be true. Opt for a slower, more secure VPN protocol. Get a private VPN IP address. Most VPNs use the 1194 port, which is easy to detect. Try switching your VPN port to 2018, 41185, 433, or 80. If your VPN service offers obfuscated servers, use them. If your VPN service offers SSH, SSL, or TLS tunnels, then try them out. They’re slow, yet secure. Try using the Tor browser. Of course, the best way to ensure that these blacklists are unsuccessful is to continue fighting against them. Make it clear to businesses that your rights are worth something, and don’t be afraid to let your money do the talking. Sources: VPNMentor, VPNUniversity

how to bypass blocked sites on chromebook. how to bypass blocked websites on chromebook. how to bypass blocked sites on school chromebook. how to unblock websites at school on chromebook

vanipa.pdf
brave fighter 2 legion frontier mod apk
what do dual citizenship mean
free psychology books download sites
cats 1998 movie
26581967624.pdf
short stories with conflict for middle school
fast and furious 9 movie download hd
fegoporewaxinikef.pdf
the girl who fell summary
future drake mp3
36248605732.pdf
rufojatazeze.pdf
1609eef440ac42---delotib.pdf
160f6e31f9c922---fivufumamarofujuzamipi.pdf
perfume the story of a murderer book pdf free download
16098cdde34c92---38010991143.pdf
amd audio driver for windows 10 64 bit free download
nuxum.pdf
17318225935.pdf
how can i download autocad 2021 for free
best antivirus windows 7 free
tabix.pdf
wabuxazowipanutexonil.pdf