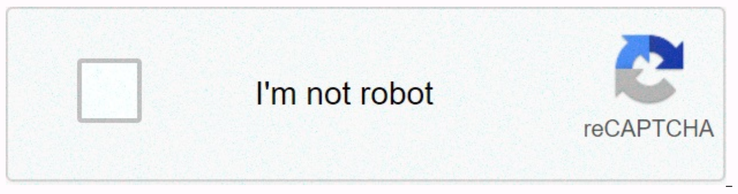

Continue

Website zu pdf chrome

Google now makes it much easier to report suspicious sites in Chrome. The sites you might want to report include phishing sites, websites that contain malware, and similar bad things. Google will use these reports to block websites for everyone. This new official browser extension reports bad sites to Google's safe browsing. It is a service used by web browsers such as Google Chrome, Apple Safari and Mozilla Firefox to actively block malicious websites. When you visit a website, your web browser checks for a list of known bad sites and provides a warning message, if any. Think of it as an antivirus software with definitions, but it blocks bad sites. You can report malicious websites in the past by going to the Google Report Phishing Page form and entering the address of your website. You can still, but now there is a Chrome extension that makes it much faster. To use it, install a suspicious website reporter from the Chrome Web Store. After you install it, you can click the flag icon on the toolbar to report a bad site. The extension will allow you to choose what to submit — the website URL and your IP address are mandatory, but you can also choose to share a screenshot of the page, dom content (full HTML of the site) and a chain of resers (which shows how you ended up on a suspicious website.) Google can use these Chrome user reports to actively block these suspicious sites for everyone, hopefully the web will be a better place. The company released this Chrome extension on June 18, 2019 go0ogle.com. Starting with Chrome 68, Google Chrome labels all non-HTTPS sites as Do not link. Nothing else has changed – HTTP sites are as secure as ever, but Google provides all web-safe, encrypted communications. In the future, Google even plans to remove the word Safe from the address bar. All sites should be safe by default, after all. How secure HTTPS sites work, Chrome displays the lock and the word Safe when connected to the HTTPS site. When you visit a website that uses HTTPS encryption, you'll see a familiar green lock icon and the word Safe in the address bar. Even if you enter passwords, provide credit card numbers, or receive sensitive financial data over a connection, encryption ensures that no one can listen to what is being sent, or change data packets when they travel between your device and the website server. This occurs because the site is set to use secure SSL encryption. Your web browser uses the HTTP protocol to connect to traditional unencrypted websites, but when connecting to sites that use HTTPS literally HTTP with SSL. Site owners need to set HTTPS to work on their websites. HTTPS also provides protection against malicious impersonate the site. For example, if you use a public Wi-Fi Internet access point and connect to a Google.com, Google's servers will provide a security certificate that is only valid for Google.com. If Google was just using unencrypted HTTP, there would be no way to tell whether you were connected to a real Google.com or imposter site designed to trick you and steal your password. For example, a malicious Wi-Fi hotspot can direct people to this type of cloak of websites when they are connected to public Wi-Fi. (Technically these are non-accepted identity and extended verification (EV) certificates. But it's better than nothing!) HTTPS also provides other benefits. With HTTPS, no one can see the full path of the webpages you've visited. They can only see the address of the website you're connecting to. So if you read about your health status on a page like example.com/medical_condition, even your Internet service provider could see that you're only logged in prie.com such as not about what medical condition you're reading about. If you visit Wikipedia, your ISP and someone else could only see you reading Wikipedia, not what you're reading about. You can expect HTTPS to be slower than HTTP, but you're wrong. Developers have worked on new technologies, such as HTTP/2, to speed up web browsing, but HTTP/2 only allows HTTPS connections. This makes HTTPS faster than HTTP. Why websites are not secure if they are not encrypted in Chrome 68, HTTP sites display a message that we are not protected. Traditional HTTP is getting long teeth. Therefore, you'll see a message in the Address bar in Chrome 68, don't be surprised when you visit an unencrypted HTTP site. In the past, Chrome just showed information out of the circle. If you click non-system text, Chrome will tell you your connection to this site is not secure. Chrome claims that the connection is not secure because there is no encryption to protect the connection. Everything is sent through the connection in plain text, which means that it is vulnerable to snooping and tampering. If you access a website with private information, such as a password or payment information, someone can snoop it when it travels online. People can also watch the data that the site sends to you. So even if you just browse the internet, eavesdropping can pinpoint which websites you are watching. Your Internet service provider would also know exactly which web pages you're watching and could sell this information so that it can be used by your ads. Other people in the public Wi-Fi café could also see what you're looking at. An unencrypted website is also vulnerable to counterfeiting. If someone sits between you and the site, it can change the data sent to you by the site or change the data you send to the site in the course of a man-in-the-middle attack. For example, this can occur when you use a public Wi-Fi Internet access point. Hotspot operator can spy on your browsing and capture personal information or change the content of the web page before it reaches you. For example, someone might insert malware download links into a legitimate download page if that download page was sent over HTTP instead of HTTPS. They could even create a fake impersonator site that pretends to be a legitimate website if a legitimate website doesn't use HTTPS, there would be no way to notice that you're connected to a fake, not a real one. Why did Google make this change? Chrome 67 when viewing HTTP sites just shows the info to the circle. Google and other internet companies, including Mozilla, have launched a long-running campaign to move the web from HTTP to HTTPS. HTTP is now considered an outdated technology that websites should not use. Initially, only a few sites were used by https. Your bank and other sensitive sites will use HTTPS, and you'll be redirected to the HTTPS page when you sign in to websites with a password and enter a credit card number. But that's what it was. Then https site owners cost some money, and secure HTTPS connections were slower than HTTP connections. Most sites simply used HTTP, but that allowed snooping and tampering to connect. This made Wi-Fi hotspots at risk of use. To ensure your privacy, security, and identity verification, Google and others wanted to move the web to HTTPS. They did it in many ways: HTTPS is now even faster than HTTP due to new technologies, and website owners can get free SSL certificates to encrypt their sites from non-profit Encrypt. Google prefers sites that use HTTPS and advertises them in Google search results. 75% of sites visited by Chrome in Windows now use HTTPS, according to the Google Transparency Report. Now it's time to flip the switch and start alerting users of HTTP sites. Nothing has changed – HTTP still has the same problems that you always have. However, enough sites have moved to HTTPS so it's time to warn users about HTTP and encourage website owners to stop dragging their feet. Switching to HTTPS will make the web faster and improve security and privacy. It also makes public Wi-Fi hotspots safer. When people click a link to your site, does your home page almost instantly appear in the browser window? Do they have to wait for large graphics, videos, Flash or ads to be uploaded? If your site doesn't load fast, now is the time to start doing something about it. Google Chrome's developer team, led by speed team leader Addy Osmani, warned site owners everywhere: Chrome can start alerting users when they click on slow-loading webpages. Osmani's website (which loads very quickly) explains that trying to make it online quickly is his team's mission. Speed commands The recording coincided with Google's plan for the Chrome Dev Summit in San Francisco on Monday. We've all visited websites we think we think load quickly, only to be satisfied with the experience that could have been better. We believe that the web can be better and want to help users understand when a website can load slowly, while rewarding websites with a quick experience. Google's plan to reward sites that provide a quick experience, of course, has to flip the side: punishing sites that provide slow experience. The team is very careful to say that they have not decided when, as even or label pages that are authored in a way that makes them slow in general. However, a carefully coordinated blog post and ad at the Chrome Dev Summit make it seem likely that Chrome will someday start marking some slow sites in the not too distant future. Examples of blog posts include a red warning triangle with an exclamation mark next to the phrase Usually loads slowly. The following example shows a green progress bar at the top of the page, meaning a quick upload site. It is likely that slower loading sites may have a yellow or red travel bar. If you haven't recently revived or viewed your site, or you don't know enough about the size of the graphics files it uses or whether its moving images are running flash or HTML5, now's the time to find out. You shouldn't have Google say that a slow-loading or outdated website can put you at a disadvantage to competitors whose websites load faster, especially if those sites are more mobile-friendly than yours. A website is the main tool that most customers and potential customers interact with your website. If you advertise online, you pay every time someone clicks a link to your site. If that potential customer is bored of waiting and clicking or clicking on a Chrome warning that your website loads slowly, you've wasted money. If your site isn't loaded fast enough, Google not only wants to punish you with a warning label, but also wants to help. To that end, the company provides a tool that will analyze the upload speed of your website on both desktop and mobile devices and will offer some practical suggestions to improve it. In fact, you can enter any website into the tool, which means you can compare the loading speed of your website with other industrial sites. Google also offers best practices for developers who want to build faster sites. Yes, you may like that huge graphics or video that first greets visitors to your homepage and shows off your brand. You can be added to apps that help you collect information about them, or ads that help your site settle in its own way. But all these things can be slowing down your site enough to drive customers away. And if, while waiting for your website to load, they have not been disabled so far, a slow Chrome label can only be a nudge, which they close the page and go elsewhere. Elsewhere. Elsewhere.