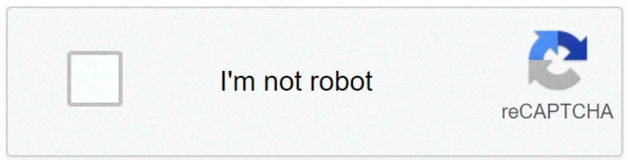

Continue

Cisco email and web security ordering guide 2020

Of Alex Smith the Internet has become part of daily life and any company or individual who wants a strong presence on the web should create a website. Protecting a web address for your site is not complicated. There are many companies that exist to help you in this process. Once you check a particular web address, you'll find it's available or isn't. If not, you may still be able to protect it from the current owner. Switch to a domain registration company, such as GoDaddy, BuyDomains, or NameCheap (see Resources). Enter the Web address that you want to get in the search field on the first page. Click Search to see if the web address you want is available. Select all suffixes of the address you want to buy. Some popular choices are: .com - Commercial .net Sites - Business and Personal Alternative .org - Organization Sites .gov - Government Sites .edu - Educational Sites .info - Multiple Suffix Information Sites can help generate increased traffic. Proceed to the company's payment page once the selection has been made. Enter your personal and credit card details in the appropriate fields to purchase your new web address. Get the contact information for the person who registered the web address you want. Some domain companies will allow you to directly access this information, while others require you to go through an intermediary. Contact the owner and offer to purchase the web address. Negotiate a price that you and the owner are satisfied with. Don't be afraid to bargain and be willing to leave if the price is too high. If a specific prefix (example.com) is taken, others (example.org, example.net) may be available. Buy the web address from the owner once a price has been agreed upon. This purchase can be made with a credit card, cashier's check, bank transfer or any other way you and the owner agree. The owner's domain company can transfer the address to your name and set up hosting if necessary. A new Google-funded study on browser security by security research firm Accuvant Labs has crowned Chrome the champion of security features and ranked Firefox below Internet Explorer in terms of the protection available from web-transmitted threats. Predictably, Microsoft and Mozilla have different opinions about what makes a browser safe and why Accuvant's results are out of base. All this has made us think about which browser is the safest and whether the security features listed in studies like this also matter to the rest of us. How was it the study? Accuvant reviewed three browsers for his study: Mozilla Firefox, Google Chrome, and Microsoft Internet Explorer. All three were tested and examined running on 32-bit Windows 7, and the search was wrapped up in July 2011, so the current release versions of each browser at that time were those included in the report. Accuvant says they left out other like Safari and Opera, to save time, but they plan to update their results on the big three as more data becomes available and each development house improves their application. Accuvant's study of browser security is probably the most comprehensive to date, although other browsers and operating systems have not been included. Researchers will be happy to tell you that they look deeper than bug trackers and vulnerability lists, and try to get a little more information about what makes a browser secure or vulnerable to threats, both current and future. Part of this effort led researchers to examine how each browser worked when an intruder already had access to a machine with each browser installed, and how much information they could get. What did the firm find? Accuvant researchers determined that Google Chrome had the newest and most effective security features aimed at protecting users from malicious code and scripts embedded in web pages, or automatically downloaded and run as part of the sites they visit. They looked at three main areas: sandboxing, or the method by which a browser restricts access to system resources and data beyond browser boundaries, was an area of significant difference. Researchers found that Chrome was more effective than all three browsers in keeping an intruder away from private data not associated with the browser. Internet Explorer also has sandboxing features, but researchers said intruders are provided with some file-reading capabilities even if they are prevented from installing software. Firefox, on the other hand, is simply listed as unimple implemented or ineffective. Just-In-Time (JIT) Hardening, which prevents the browser from compiling JavaScript that cannot run on the user's computer, was another area where Chrome and IE were on par, but Firefox lagged far behind. Plug-In Security was another area where Chrome rose above the competition, denying plug-ins from installing additional software and running scripts that do not require user interaction while on a website. In all three areas, Chrome came out on top. Researchers tied Chrome with Internet Explorer in Sandboxing and JIT Hardening, but pointed out that Chrome was just a little better in both areas. In all three areas, Firefox got the lowest marks. In other areas, however, all three browsers have balanced, and at least in one area, Blacklisting URLs, all three browsers got poor ratings, although researchers pointed out once again that Chrome did better than the other two – only that none of them blacklisted very well. In the end, the of Accuvant gave Chrome the first place, with Internet Explorer just behind it. They pointed to Google's ability to build Chrome from scratch, from scratch, without having to deal with legacy code or shoehorns in older features like Microsoft and Mozilla have with Internet Explorer and Firefox. Essentially Essentially for the search team, Chrome is the safest because Google was able to write it with a new perspective and security in mind, with no luggage to take with it. What do Mozilla and Microsoft say about it? Johnathan Nightingale, Director of Firefox Development at Mozilla, responded to the study in a Forbes article and said: Firefox includes a wide range of technologies to eliminate or reduce security threats, from platform-level features such as address space randomization to internal systems such as our layout frame poisoning system. Sandboxing is a useful addition to that toolbox we're investigating, but no technology is a silver bullet. We invest in security throughout the development process with internal and external code reviews, constant testing and analysis of running code, and quick response to security issues when they emerge. We are proud of our reputation for safety and remain a central priority for Firefox. Similarly, Microsoft pointed to a study by NSS Labs that showed Internet Explorer dominating all of its rivals, including Firefox and Chrome, to protect users' systems from malware. However, just as the Accuvant studio was sponsored and commissioned by Google, NSS Labs studios are often paid for by Microsoft, so there's a lot of skepticism to do. How impartial is the study? Accuvant is a respected security and research company, and they went out of their way to make available not only the full text of the study, but also the tools used and the supporting data behind the study in case other researchers want to examine their findings. Google and Accuvant both explained that even though they commissioned the study, they knew that if the results were in their favor, that fact would cast doubt on the merits of the result. Accuvant explained in an Ars Technica article that Google has given them more than a large berth to do the search, and insisted that the study is an unbiased look at the state of browser security. Accuvant, for his part, has also put his reputation at risk, stating that the firm is representative of their company and its quality of work, and they are behind it. Whether Google was so open about whether the study was independent because they knew the test methodology and the fact that their code base put them ahead is another story, but at the moment no one criticizes Accuvant's results or methodology. The real question, however, is how much interest should it be to you or me? Is anything wrong? What should I do? In the end, the study is important, but the real lynch-pin of browser security is, and always is the user behind the keyboard. Chrome may be on top now, but Microsoft and Mozilla will make changes to deal with as a result of the results. Accuvant's methodology assumes that your system is compromised and also assumes that you have no other protection besides browser browser security to protect you, both are probably not true for most users. Meanwhile, this studio will end up being used as cannon fodder in browser wars, with fans of one browser firing it from another without ever bothering to read it. For the most part, browser security is a matter of user responsibility. Be sure to navigate responsibly and use SSL whenever possible. Don't accept, run, or even download anything if you're not sure what it is or why you've been asked to download a file and only keep the running extensions and add-ons you need on a daily basis. Firefox users can use extensions like HTTPS Everywhere to safely navigate whenever a secure session is available and on services that allow you to enable SSL and use an extension like NoScript to stop malicious JavaScript in its tracks. Chrome users can get similar features with add-ons like NotScript or ScriptNo, which do very similar things. In the end, browser security features only go so far as to protect you, and as long as you take a cautious, skeptical, security-centric approach to browsing, it probably doesn't matter which browser you use. Firefox: Firefox HTTPS extension everywhere, which automatically switches browser to SSL for ... Read moreWhat do you think about the study results? More ammo for browser wars, or does it really distinguish Chrome or Firefox below? Share your thoughts in the comments below. Under.