

Score Methodology and Frequently Asked Questions

A browser is a gateway to the web, and given the prevalence of online threats, browser security is very important. Modern browsers tend to have new security features and enhancements that are better suited to help protect users from newer threats. Though a browser cannot guarantee your safety online, the more security features your browser has, the better protected you are from online threats.

The subject of software security is complex, and not all consumers will understand the variety of security technologies present in a browser. Microsoft created a browser feature score that provides a concise view of the security capabilities of a browser on a four point scale. The browser security feature score assesses the trustworthiness of your browser based on the availability of features that help keep you safer online.

We acknowledge that others will have comments, suggestions, and criticisms of the feature score. We've worked hard to make sure the test is fair and have validated the methodology with many others - from consulting independent security researchers to security-focused not-for-profit organizations. If you still consider the security score to be arbitrary, we encourage you to design one better. We are strongly in favor of more dialogue about browser security. The more awareness people have about browser security, the more likely consumers are to pay attention and migrate to a modern browser.

This document helps a reader understand the methodology behind the feature security score. This document is broken down into two sections:

- Score Methodology
- Frequently Asked Questions

Score Methodology

Categorization

The security features in a browser are categorized based on types of online threats they mitigate. The threats and the respective features fall into the categorization below:

- Dangerous Downloads
- Phishing Websites
- Attacks on your Browser and its Plugins
- Attacks on Websites

The browser features are categorized into the above groups because they reflect the online threat landscape. Though the prevalence of each of types of attacks is open to debate, recent data shows that attacks using social engineering techniques such as Phishing and Socially Engineered Malware are increasingly used by attackers. The [Security Intelligence Report Volume 11](#) shows that 45% of the infections cleaned from over 600 million machines were the result of attacks that required user interaction. These types of attacks typically use social engineering techniques. The same report shows that less than 6% of the malware cleaned from these machines used attacks based on vulnerabilities. These attacks rely on techniques similar to the ones used to attack a browser or its plugins and are commonly referred as “Drive-By” attacks. To simplify the scoring, each category was assigned one point.

The browser security feature score for each category is calculated based on the availability and effectiveness of features designed to mitigate online threats. A browser can receive a score of 0, 0.5, or 1 point for each category depending on the number and quality of security features it implements. The security features for each category as well as how the score per category is determined is described below. The sum total of the scores from each category is the final browser security feature score for that browser.

Operating System and Browser Set:

The browser security feature score assesses the current version of Chrome, the supported versions of Internet Explorer, and Firefox versions 3.6 onwards. To make the assessments comparable, the default version of a browser is considered. Customized configuration, extensions and add-ons are not considered when assessing the mitigations. All browsers are assessed on the Windows platform with the latest service packs, updates, and default settings.

Category: Dangerous Downloads

Threats that fall into this category involve malware (malicious software) hosted online that uses social engineering techniques to spread. A full point is awarded if a browser provides both mitigations described below, half a point is awarded if the browser only provides one of the two mitigations, and zero points are awarded if a browser provides no mitigation against socially engineered malware.

Does the browser help protect you from websites that are known to distribute socially engineered malware?

[NSS Labs Socially Engineered Malware Report](#) is used as proxy to measure effectiveness of browser’s capability to block URLs known to host malware. This test assumes that a browser provides mitigation against this attack if the browser is able to block more than 80% of Socially Engineered Malware based on the latest NSS test. If NSS test is not available for a version of the browser, the results from the most recently tested version is used. Because the NSS Labs browser tests are updated approximately every six months, it is reasonable to assume that the most current test result applies to the browser irrespective of the browser version. The reason is that the protection offered by this feature is based on a web service which tells the browser which

URLs are bad and which are good. Though a browser version number may change, this service is likely to persist across versions.

Does your browser provide a distinct warning when you download an application that is of higher risk but not yet confirmed as malware?

A browser receives credit for implementing this mitigation if it contains features that provides a distinct warning when a user downloads an application that is not commonly downloaded and also if the download is of higher risk. In order for these warnings to be effective, the browser should not warn a user every single time the user downloads an application.

[Application Reputation Blog Post](#)

Category: Phishing Sites

Threats that fall into this category involve sites that are phishing scams. There are many types of phishing sites, ranging from sites that mimic banking portals to those that mimic social networks. A full point for this category is given only if the browser implements a mechanism to help detect and block phishing sites.

Does the browser have a feature that can help protect you from phishing sites?

A browser receives credit for implementing this mitigation if it has a mechanism to help detect phishing sites and warn the user appropriately.

[Wikipedia Article on Phishing Sites](#)

[SmartScreen Filter In Internet Explorer](#)

Does your browser help you identify the domain you're on by distinguishing it within the URL?

A browser receives credit for implementing this feature if it can help users identify the domain for a website when a user is browsing to that site.

Category: Attacks on your browser and its plug-ins

Attacks against the browser and its plug-ins (or add-ons) represent the category of malware that exploits vulnerabilities specific to a browser and its extensions. The mitigations for such attacks involve an effective sandbox for the browser and extensions as well as mechanisms to reduce the attack surface area exposed by extensions. Out of the set of mitigations listed below, a full point is awarded if a browser implements at least 5 of the 7 mitigations, half a point is awarded if at least 3 of 7 of the mitigations are implemented and zero points otherwise.

Reducing the attack surface area exposed by extensions

Does the browser have the ability to restrict an extension or a plugin on a per site basis?

A browser receives credit for implementing this mitigation if it allows for fine-tuned control of browser add-ons such as the ability to enable or disable an add-on on a per-site basis.

Does the browser have a system for auto updating browser extensions?

A browser receives credit for implementing this mitigation if it has an auto update mechanism for extensions.

Effective Sandbox

Does the browser process utilize Windows Protected Mode or implement a similar mechanism such that browser processes cannot modify parts of the system that it doesn't have access to?

A browser receives credit for this mitigation if it implements a sandbox that prevents code from modifying or writing to parts of the computer it doesn't have access to.

[Wikipedia Article on Mandatory Integrity Control](#)

[MSDN Article on Mandatory Integrity Control](#)

Does the browser extend the sandbox such that it cannot read data from parts of the system that it doesn't have access to?

A browser receives credit for implementing a sandbox that prevents code from reading parts of the computer it doesn't have access to.

Does the browser benefit from Windows operating system features that protect against arbitrary data execution?

A browser receives credit for this mitigation if it incorporates Data Execution Prevention/NoExecute functionality of the operating system that helps prevent arbitrary code in memory from being executed.

[Data Execution Prevention In Windows.](#)

[Wikipedia Article On Data Execution Prevention.](#)

Does the browser benefit from Windows operating system features that randomize the memory layout to make it harder for attackers to find their target?

A browser receives credit for utilizing a mechanism to randomize the memory layout (ASLR), making it harder for attacks to find their targets.

[Wikipedia Article On Address Space Layout Randomization](#)

[MSDN Article On Defensive Enhancements To Windows](#)

Does the browser benefit from Windows operating system features that protect against structured exception handling overwrite attacks?

A browser receives credit if it utilizes a mechanism to defend against attacks that exploit structured exception handling mechanisms.

[Safe Exception Handling MSDN Article](#)

Category: Attacks on Websites

This category of malware exploits websites and servers that users visit with their browser. The attack vectors can range from potential man-in-the-middle attacks that target mixed content on HTTPS pages to Cross Site Request Forgery or “Click Jacking.” Browsers that implement 4 of the 5 of the mitigations receive full point for this category and browsers implementing at least 2 of 5 mitigations receive half a point. Browsers receive zero points otherwise.

Does the browser automatically block insecure content from secure (HTTPS) pages?

A browser receives credit for this mitigation if it automatically blocks insecure parts (HTTP) from a secure (HTTPS) connection or warns the user if this condition occurs.

Does the browser filter out scripts on the client to help protect against Cross-Site Scripting (XSS) attacks?

A browser receives credit if it contains a filter to mitigate Cross-Site Scripting attacks.

[Wikipedia Article On XSS Attacks](#)

Does the browser implement content security policy that websites can use to mitigate XSS and Cross Site Request Forgery (CSRF) attacks?

A browser receives credit if it implements a Content Security Policy that websites and servers can use to help mitigate XSS and CSRF attacks.

Can the browser sanitize HTML to remove potentially problematic code?

A browser receives credit for this mitigation if it contains a built in mechanisms that web developers can utilize to sanitize scripts from HTML code. An example of this is the ToStaticHTML API implemented by Internet Explorer.

Does the browser have features that websites can use to help protect you from "click jacking" attacks?

A browser receives credit for this mitigation if it contains a mechanism that web developers can utilize to safely make cross domain requests.

[Internet Explorer Cross Site Request Forgery Mitigation](#)

Frequently Asked Questions

Why did you implement a browser security score?

The score was created so that someone with an older browser can easily recognize the need to upgrade to a modern browser. Through the score and the site – [YourBrowserMatters.org](#) we hope to encourage everyone to pay attention to browser security and migrate to a more modern browser.

Will this test lead people into a false sense of security because a perfect score will imply that a user is safe from online attacks?

The score is designed to convey the fact that modern browsers are safer. Newer browsers contain technologies that are much better suited to help protect users from modern threats. People who continue to browse on older browsers are exposing themselves to unnecessary risk and the score is designed to make this point clear.

For example, on a 4 point scale it is easy to distinguish Internet Explorer 6's score of 0 from Internet Explorer 9's score of 4 points and make a strong case for upgrading. As we clearly state in the methodology, no browser can protect you from all threats online; however, a browser with more security features helps mitigate some risks. The score simply highlights this fact easily and clearly.

Is this test biased against browsers other than Internet Explorer?

We've worked hard to ensure that the scoring methodology is as fair and unbiased as possible. The score takes into consideration the major security features found across all browsers. Technologies such as enhancements on top of Protected Mode, a system for auto-updating add-ons, content security policy, and other security features which not found on Internet Explorer are part of the score. Chrome and Firefox receive due credit for implementing features such as these in the browser feature security score.

We've also vetted the test with independent partners such as the [Anti-Phishing League](#), [Identity Theft Council](#), and [Online Trust Alliance](#) and security first groups such as [WhiteHat Security](#) and [Cenzic](#) to ensure that the score is well designed. Only the browsers which do not implement adequate security features receive a poor score. The case in point being Internet Explorer 6 and 7— both receive low scores because they doesn't have most of the features that help protect against modern threats.

Why are the browsers limited to Firefox, Chrome, and Internet Explorer on Windows?

Initially, we decided to limit our focus on the browsers with a majority of the market share on Windows. (These three combined represent [93%](#) of all web browsing on Windows today.) Our focus is to provide a browser score for majority of the population browsing the Internet using a PC.

How did you validate or test for availability of features across browsers?

Most of the security features that were included in the score are publically documented by the browser manufacturers and the presence can be verified directly through the browser itself. Additionally, tools like the Sys Internals process explorer were used to verify the use of DEP, Protected Mode, and ASLR.

How often will you update the test?

The test will be updated on a regular basis as new advancements in security features are made across browsers and as new versions of the browsers are released.

How will you take into account changes to other browsers as vendors release new versions?

The browser security score will be updated on a regular basis, for example when browser versions are updated and new security features are added.

Why are the features bucketed into four categories?

One challenge we faced when creating the score was how to determine the relative importance of each of the features. At a micro level, we considered questions like whether the use of protected mode is more important than auto-updating plugins. Assigning weighting to the features would not only make the feature score more subjective but it would also detract from the original intent to keep the score simple and straightforward. To keep the assessment simple we categorized the features into four buckets.

The four categories were chosen because they are recognized as typical attack vectors used on the internet. Each category is distinct from the others and the browser security features can be classified into these four areas. By categorizing the security features into four areas it is easier to understand the overall capabilities without getting lost in individual security features.

Why are all of the categories worth one point? Aren't some categories more important than others, for example the features that help protect against attacks on browsers may be more important than features that help protect against attacks on websites?

We assigned one point to each category even though there is compelling evidence to suggest that attack vectors that use social engineering techniques are far more prevalent and effective than attack vectors that take advantage of exploits. For example the [Security Intelligence Report Volume 11](#) by Microsoft shows that 45% of the infections cleaned from over 600 million machines were a result of attacks that required user interaction. These types of attacks typically use social engineering techniques. The same report shows that less than 6% of the malware cleaned from these machines used attacks based on vulnerabilities. These attacks rely on techniques similar to the ones used to attack a browser or its plugins and are commonly referred as “Drive-By” attacks.

Based on evidence such as this, it's easy to make a case that features that help protect people from socially engineered attacks should be weighted differently than features that help protect against “Drive-By” attacks – however determining that exact weighting would be complex and again detract from the original intent. To simplify the scoring we opted to assign one point to each category.

I use Firefox with a custom configuration. Why are you not giving credit to users who use add-on like no script or custom browser configurations?

People who are knowledgeable and concerned about browser security do use custom configurations, add-ons, and plugins to enhance the capabilities of the browser. We opted to ignore plugins and

advanced configurations of the browser for two reasons. First, many people do not utilize plugins or custom configurations to secure a browser – simply put a modified configuration of the browser is not representative of the common default configuration. Furthermore, if user who is aware of such advanced use cases is not the intended audience of this score. Second, it is impossible to make comparisons across versions and browsers when considering custom configurations and plugins.

Why are you using NSS Labs test results to determine whether a browser gets credit for implementing features that help protect against socially engineered malware?

Where possible we wanted to measure both quality and the presence of security features. The test results from NSS Labs, an independent research and testing organization, make it possible to gauge the quality of socially engineered malware protection offered by a browser. Holding the browsers to a higher bar ensures that the score is a fair representation of the protection offered by a browser.

How can you say this is accurate when you are using NSS test results from an older version of Chrome and Firefox?

NSS Labs historically has updated its browser test results every 6 months – a frequency that is rapid enough to assert that the most recent test results are current irrespective of the version of the browser. This is because, given the rapid release cycle of Chrome and Firefox, improvements across versions are incremental. More important, the socially engineered malware protection relies on a web based service that tells a browser whether a URL is good or bad. This service isn't likely to change from one version to the next. Therefore, the protection offered by a version of Chrome or Firefox two months ago is roughly the same as the protection offered by the version of Chrome current today.

If NSS Labs stopped performing regular tests of Socially Engineered Malware protection we would reconsider using antiquated test results as a measure of effectiveness of this feature

Chrome has a feature that blocks malicious files. Why doesn't it get credit for this feature under the rule that asks whether a browser blocks risky downloads?

The Chrome feature that helps protect against malicious downloads is URL based. Chrome's ability to help protect against URLs known to distribute socially engineered malware is already considered in the first rule in the Dangerous Downloads category.

The second rule requires a more advanced feature not yet implemented by Chrome or Firefox. This feature should help protect people by warning them about files without an established reputation. The current implementation of Chrome helps protect people against files which are known to be malicious; this feature doesn't warn people about files that are not reputable.

Why do all browsers get credit for implementing a Phishing filter, why doesn't the score differ based on the quality of the phishing filter?

The score doesn't differ based on the quality of the Phishing filter in a browser because there isn't an independent test that measure the quality of the Phishing protection offered by browsers. Therefore, all browsers that implement a Phishing filter get credit for doing so.

Why doesn't domain highlighting receive any credit in the Phishing category?

Though domain highlighting is a useful feature it is not clear whether the feature helps consumers distinguish a phishing site from a legitimate site in practice. In comparison, the phishing filter is a far more powerful mitigation. It is not fair to browser versions such as Firefox 5 to receive a lower score in this category just because it doesn't have a domain highlighting feature even though it implements a phishing filter.

Why doesn't the score give importance to vulnerabilities, for example by taking into account the number of vulnerabilities known for a browser?

Overall the score was designed with one consideration in mind – make it easy for everyone to determine how many security features their browser has. Features that help mitigate the impact of vulnerabilities are given prominence. An entire category, “Attacks Against the Browser” is dedicated to such features.

Counting individual vulnerabilities would be complex because in many cases the vulnerabilities differ from browser to browser, and comparison across browsers would not be fair for vulnerabilities that are specific to one browser. Furthermore, using individual vulnerabilities would be contrary to the purpose and intention of the browser score.

Some features mentioned in the Attacks on Websites category, such as CSRF and Click Jacking protection, push the responsibility of protecting a user to a website, why do browsers get credit for them?

The responsibility to help protect users belongs to both the website as well as the browser. Websites often rely on Browser features to help secure the connection – when considering browser security it's only appropriate to give credit to browsers for implementing features that web site owners can take advantage of.