WEB BROWSER SECURITY COMPARATIVE REPORT

Protection Against Phishing

NOVEMBER 16, 2018
Author – Morgan Dhanraj

Tested Products[1]

Google Chrome: Version 69.0.3497

Microsoft Edge: Version 42.17134.1.0

Mozilla Firefox: Version 61

Environment

Windows 10 Enterprise Version 1803

Google Chrome OS: Version 68.0.3440.118

Windows 10 S: Version 1709,Build 16299.611

NSS Labs Web Browser Security Test Methodology v4.0

[1] At the start of testing, each product was updated to the most current version available and given access to the Internet for the duration of the test. The product version reflects the most up-to-date version that was available at the end of the test.

Overview

The results presented in this report were obtained from continuous live testing between September 4, 2018 and September 14, 2018 at the NSS Labs facility in Austin, Texas. This test was conducted free of charge, and NSS did not receive any compensation in return for vendor participation.

This Comparative Report is based on empirically validated evidence gathered by NSS during ten days of continuous testing. Testing was performed every six hours, with new phishing URLs added each test cycle.

Among the most prominent and impactful security threats facing users today are phishing attacks and socially engineered malware (SEM). As such, they have been the primary focus of NSS' continued research and testing of the security effectiveness of browsers. While drive-by downloads and clickjacking are also effective attacks that have achieved much publicity, they represent a smaller percentage of today's threats.[2] [3]

Figure 1 depicts the average percentage of phishing attacks blocked throughout the test.

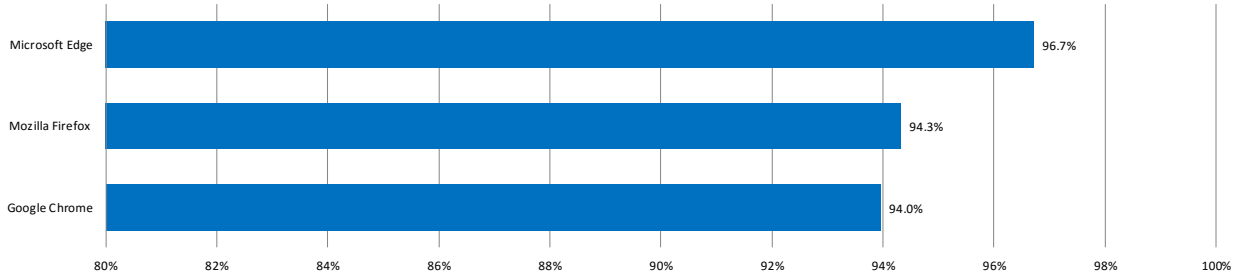


Figure 1 – Average Block Rate for Phishing Attacks (%)

During the test, Microsoft Edge blocked an average of 96.7% phishing URLs; Mozilla Firefox blocked an average of 94.3% phishing URLs, and Google Chrome blocked an average of 94.0% of phishing URLs.

[2] Kaspersky Security Bulletin. Predictions for 2017. Kaspersky Lab

[3] IT threat evolution in Q2 2016. Statistics. Kaspersky Lab

NSS Labs Findings

- Microsoft Edge demonstrated the highest protection against phishing attacks throughout the test, blocking an average of 96.7% of phishing URLs. Mozilla Firefox provided the second highest protection, blocking an average of 94.3% of phishing URLs.
- Microsoft Edge provided the highest zero-hour protection rate (89.5%).
- NSS did not observe any significant difference in block rates between the Microsoft Edge browser running on Windows 10 and running on Windows 10 S.
- NSS did not observe any significant difference in block rates between the Google Chrome browser running on Windows 10 and running on Chrome OS (Chromebook).
- Products that relied upon the Google Safe Browsing API provided a similar level of protection.

NSS Labs Recommendations

- Protection against phishing attacks is just one security attribute of a browser. The capability to block socially engineered malware (SEM) must also be factored into any overall assessment of a browser's security.
- When considering browser security, users should minimize risk by selecting browsers with higher phishing block rates, consistency of protection, and early protection against new threats.
- Augment browser protection with education to protect against attacks that succeed in bypassing browser protections.

Table of Contents

Table of Figures

Analysis

Long before the Greeks hid a group of soldiers in a wooden gift horse (Trojan horse), social engineering was a popular tool for con artists and other criminals deceiving people for their own personal gain. Phishing is the natural application of modern technology to social engineering by criminals perpetrating this proven attack strategy. Web browsers are in a unique position to combat phishing and other criminal activities by warning potential victims that they are about to stray onto a malicious website. Since phishing sites have a short lifespan, it is essential that the site is discovered, validated, classified, and added to the reputation system as quickly as possible. This explains the correlation between average-time-to-block and catch rate. A good reputation system must be both accurate and fast in order to realize high catch rates.

In this report, NSS studied the ability of leading web browsers to protect against phishing. In a companion report, NSS reports the findings of the protection capabilities of web browsers against socially engineered malware. (See NSS' Web Browser Security Comparative Report: Protection Against Socially Engineered Malware.)

The Phishing Threat

"Phishing" attacks can be constructed using two basic methods. The first type of attack attempts to persuade a victim to provide personal information to the attacker. The information may be credit card details, login information for email or social media accounts, or other personal information that can be used for identity theft and other information-based attacks. The second type of phishing attack attempts to lure users into installing a malicious application or navigating to a website where malicious software will be installed through the exploitation of vulnerable software. Common to both phishing attacks is that they arrive via email, instant messages, SMS messages, and links on social networking sites.

Phishing attacks pose significant risk to individuals and organizations alike, by threatening to compromise or acquire sensitive personal and corporate information. The Anti-Phishing Working Group (APWG) reported a total of 264,483 unique email phishing campaigns in the second quarter of 2018.[4] Phishing attacks are becoming increasingly complex and sophisticated, making them harder to detect and more difficult to prevent.

Web Browser Security

The evolution of the browser can be compared to the evolution of antivirus software. Where antivirus software once detected only self-replicating threats, and then Trojans, and eventually diverse types of threats, browsers initially dealt primarily with annoyances such as pop-ups and cookies and then were required to tackle more serious security issues. Phishing websites are among the top threats that the browser must protect against. This report examines the abilities of three different web browsers to protect users from live phishing attacks.

To protect against phishing, browsers utilize cloud-based reputation systems that scour the Internet for malicious websites and then categorize content accordingly, either by adding it to blacklists or whitelists, or by assigning it a score (depending on the vendor's approach). These categorization techniques may be performed manually and/or automatically.

[4] APWG Phishing Activity Trends Report

The second functional component of protection against phishing involves the web browser requesting reputation information from the cloud-based reputation systems about specific URLs and then warning against or blocking specific URLs.

If results indicate that a website is "bad," the web browser redirects the user to a warning message explaining that the URL is malicious. Some programs also include additional educational content. Conversely, if a website is determined to be "good," the web browser takes no action and the user remains unaware that a security check was just performed by the browser.

Test Composition

Data in this report spans a testing period of nine days between September 4, 2018 and September 14, 2018. All testing was performed at the NSS testing facility in Austin, TX. During the test, NSS engineers routinely monitored connectivity to ensure the browsers under test could access the phishing URLs, as well as browser reputation services in the cloud.

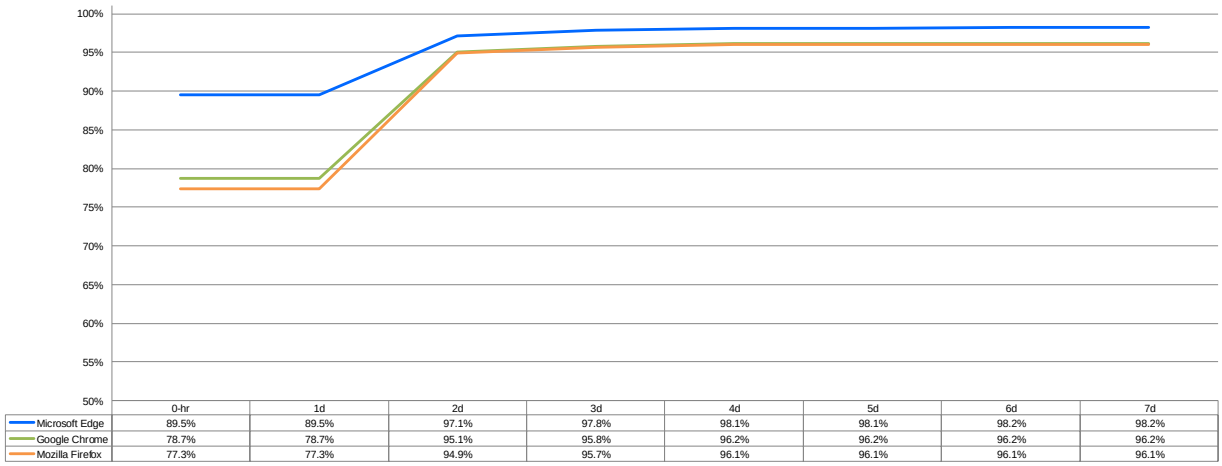
The test comprised 56,669 test cases that included 2,943 unique and suspicious URLs. Ultimately, 790 URLs met the NSS validation criteria (i.e., active and malicious) and were included as part of the test. On average, 21 new validated URLs were added to the test set per day; the number of URLs added varied according to fluctuating levels of criminal activity. Testing was performed every six hours, with new phishing URLs added each test cycle.

Protection Metrics

The average block rate for phishing attacks is a key metric against which browsers are tested. Consistency of protection, the amount of time required to add protection for new URLs, and zero-hour protection are also important metrics and thus are included in this report.

Zero-Hour Protection

Immediate protection against new phishing URLs is critical. As phishing sites are discovered, they are taken down, and often within a relatively short amount of time. Products that fail to add protection in a timely manner may be too late to counter a threat. Figure 2 shows how long each browser took to block a phishing site once the threat was introduced into the test cycle. Within the seven-day window, cumulative protection rates are calculated each day until threats are blocked.



	0-hr	1d	2d	3d	4d	5d	6d	7d
Microsoft Edge	89.5%	89.5%	97.1%	97.8%	98.1%	98.1%	98.2%	98.2%
Google Chrome	78.7%	78.7%	95.1%	95.8%	96.2%	96.2%	96.2%	96.2%
Mozilla Firefox	77.3%	77.3%	94.9%	95.7%	96.1%	96.1%	96.1%	96.1%

Figure 2 – Zero-Hour Protection Histogram

During the test, Microsoft Edge demonstrated a zero-hour protection rate of 89.5% against phishing attacks. Microsoft Edge blocked 10.8% more phishing attacks than Google Chrome and 12.2% more phishing attacks than Mozilla Firefox during zero-hour protection testing. By the end of the seventh day of testing, Microsoft Edge was maintaining a 2% lead over Google Chrome and a 2.1% lead over Mozilla Firefox.

Weighted Protection Score

Once the time to add protection is known, NSS can better represent a web browser's protection against phishing attacks by assigning a greater value (or weighting) to those browsers adding protection more quickly than those browsers adding protection more slowly. By applying this weighting to the protection score over the seven-day period, the zero-hour protection of a browser. can be more accurately depicted. Figure 3 depicts the weighted protection score for each browser.

Time to Protect	Microsoft Edge	Google Chrome	Mozilla Firefox
0-Hour	89.0%	79.0%	77.0%
1 day	89.0%	79.0%	77.0%
2 days	97.0%	95.0%	95.0%
3 days	98.0%	96.0%	96.0%
4 days	98.0%	96.0%	96.0%
5 days	98.0%	96.0%	96.0%
6 days	98.0%	96.0%	96.0%
7 days	98.0%	96.0%	96.0%
Protection Score	**93.6%**	**87.9%**	**87.0%**

Figure 3– Weighted Protection Score

Consistency of Protection Over Time

Throughout the test, new phishing URLs were added daily, and URLs that were either no longer reachable or no longer delivering phishing URLs were removed. Each data point represents protection at a specific point in time. If a URL was blocked early on, this improved a browser's score for consistency of protection over time. Alternatively, if the browser did not block the URL, this lowered its score.

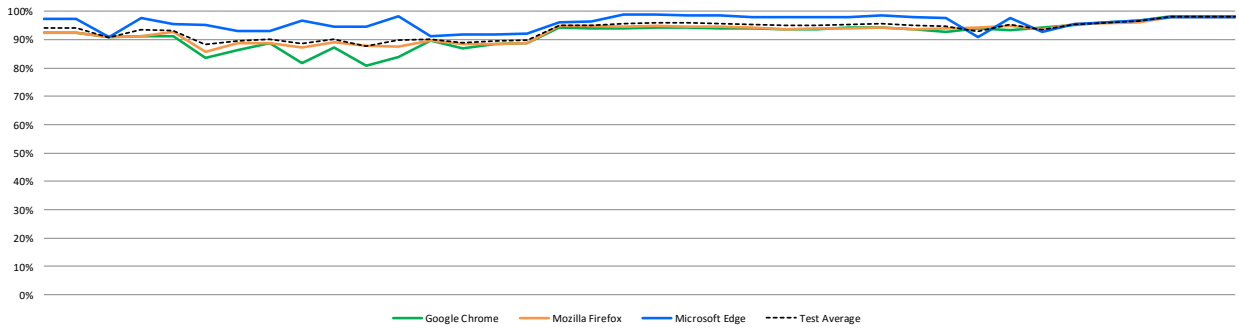


Figure 4 – Consistency of Protection Against Phishing Attacks Over Time

Safe Browsing Products and Windows Defender SmartScreen Products

Google Chrome, Apple Safari, and Mozilla Firefox use the Safe Browsing API to provide protection against phishing Attacks. NSS measured the efficacy of phishing protection across browsers that rely on the Safe Browsing API and concluded that there were only minimal differences in the scores.

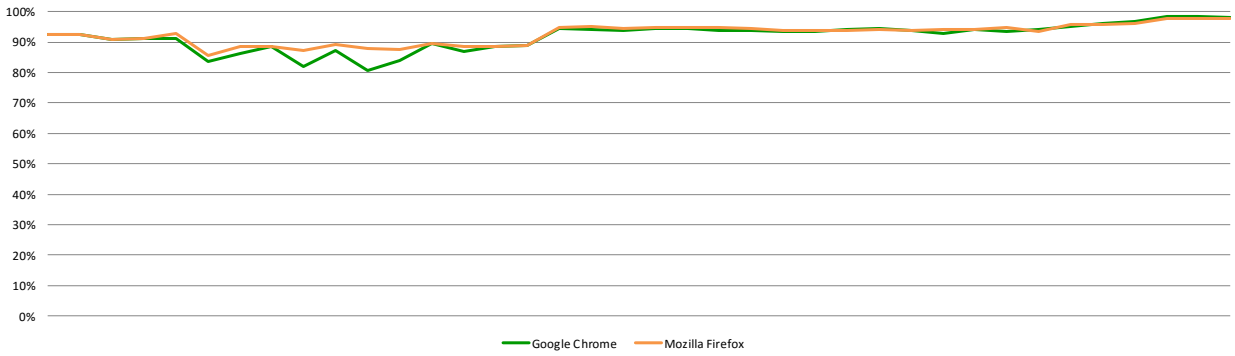


Figure 5 – Phishing Protection Over Time – Products Using Google Safe Browsing

Microsoft Edge relies on Windows Defender SmartScreen to provide protection against phishing attacks.

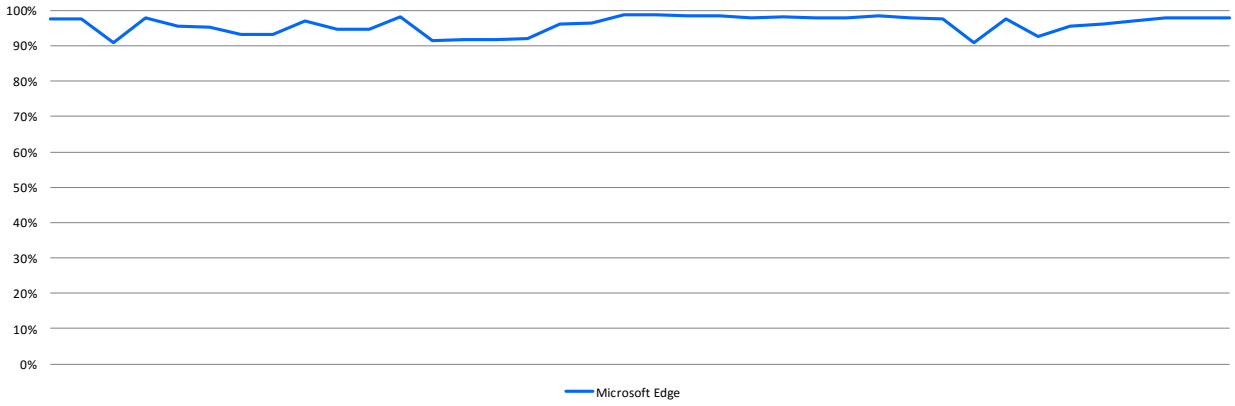


Figure 6 – Phishing Protection Over Time – Products Using Windows Defender SmartScreen

Chrome OS (Chromebook) vs. Windows 10 S

NSS received a large number of requests from clients in the education sector to evaluate the security of Chrome OS (Chromebooks) and Windows 10 S. NSS measured the security efficacy of running Google Chrome on Windows versus running Google Chrome on Chromebooks. Additionally, NSS measured the security efficacy of running Microsoft Edge on Windows 10 versus running Microsoft Edge on Windows 10 S. Figure 7 depicts the results for protection against phishing.

No significant differences were observed between the Edge browser running on Windows 10 or Windows 10 S, but Microsoft Edge on Windows 10 S performed better than Google Chrome on Chrome Pixel.

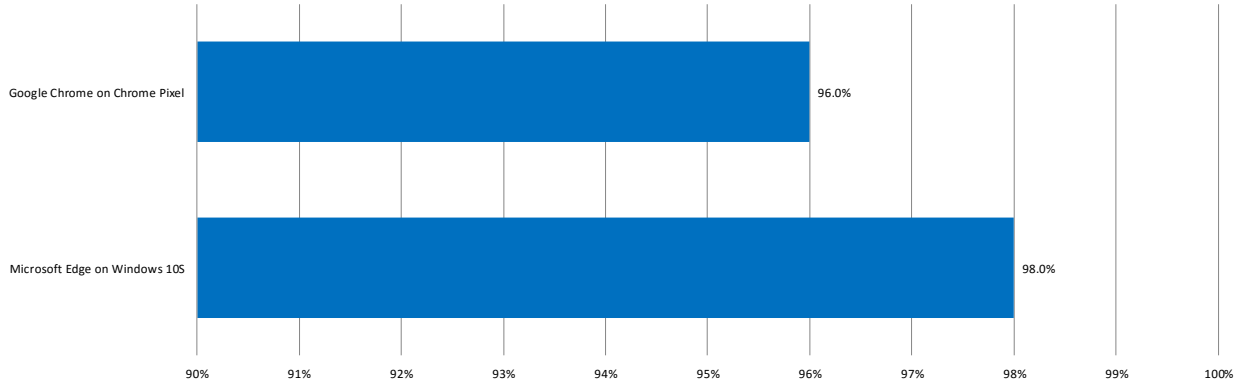


Figure 7 – Chromebook vs. Windows 10 S

Test Methodology

Web Browser Security Test Methodology v4.0

A copy of the test methodology is available at www.nsslabs.com.

Acknowledgement

NSS Labs acknowledges PhishLabs for providing the samples used in this test.

Contact Information

NSS Labs, Inc.
3711 South MoPac Expressway
Building 1, Suite 400
Austin, TX 78746-8022
USA
info@nsslabs.com
www.nsslabs.com