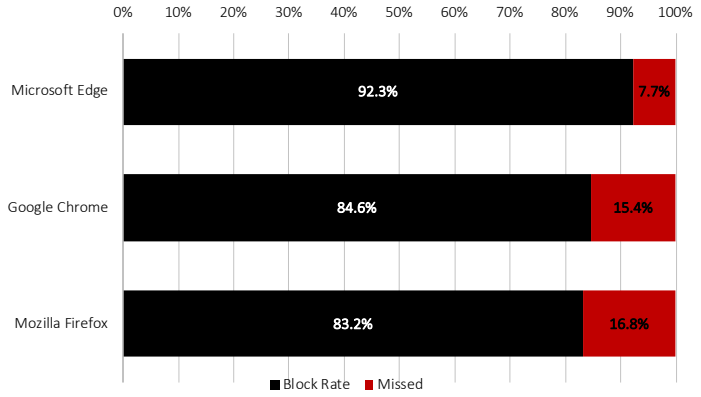
Q2 2021 Web Browsers vs. Phishing

Overview

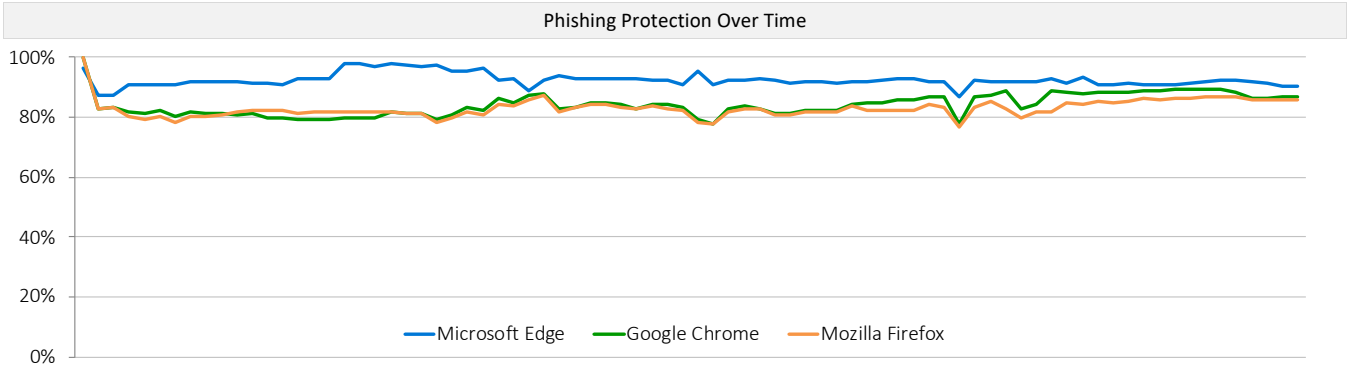
During Q2, 2021, CyberRatings.org performed an independent test of phishing protection offered by web browsers. The tests ran for 20 days with 80 discrete test runs. To protect against phishing, Microsoft Edge uses Microsoft Defender SmartScreen; Google Chrome and Mozilla Firefox use the Google Safe Browsing API.

Microsoft Edge offered the most protection, blocking 92.3% of phishing URLs while providing the highest zero-hour protection rate (93.5%). Google Chrome provided the second-highest protection, blocking an average of 84.6%, followed by Mozilla Firefox at 83.2%.

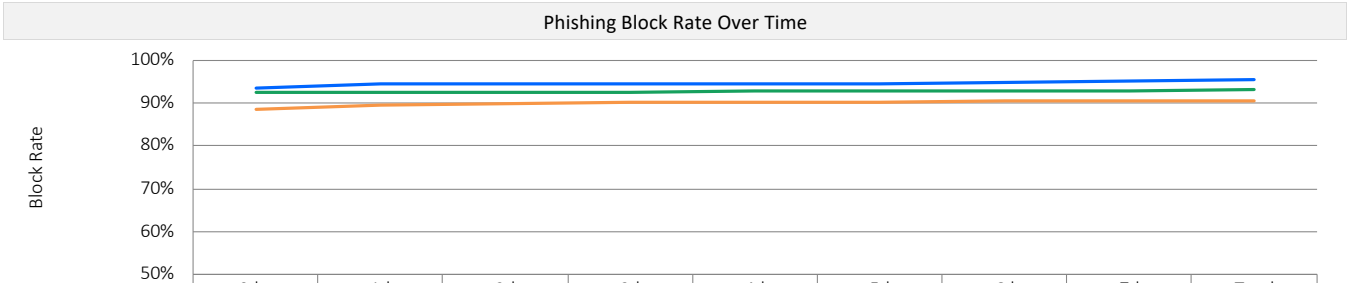


Summary of Results

URL reputation systems shorten the time attackers have to achieve their goals by preventing/warning users that a URL is a known phishing site. However, since users visit a wide range of websites, many of which are new, URL reputation systems cannot simply block all new URLs. Knowing this, attackers' phishing campaigns are constantly changing, with the bulk of new attacks occurring in the first few hours after an attack is launched.



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



	0-hr	1d	2d	3d	4d	5d	6d	7d	Total
Microsoft Edge	93.5%	94.4%	94.5%	94.5%	94.5%	94.7%	94.9%	95.1%	95.4%
Google Chrome	92.4%	92.6%	92.7%	92.7%	92.8%	92.8%	92.8%	92.9%	93.2%
Mozilla Firefox	88.7%	89.7%	90.0%	90.4%	90.4%	90.4%	90.5%	90.6%	90.6%

We measured the browsers' ability to block malicious URLs as quickly as we found them on the Internet. This continued every six hours to determine how long it would take a vendor to add protection. The figure above shows the response time for each browser to block a phishing site once the threat was introduced into the test cycle.

Phishing Attacks

Phishing is a type of social engineering attack that attempts to persuade a victim to provide sensitive personal information to the attacker. Some examples of sensitive information are credit card numbers, social security numbers, and login and passwords for bank accounts. Email, instant messages, SMS messages, and links on social networking sites are all vectors for phishing attacks. The landing page for a phishing website often attempts to silently exploit a visitor's computer and install malicious software (aka drive-by exploit).

Phishing attacks pose a significant risk to individuals and organizations by threatening to compromise or acquire sensitive personal and corporate information. The Anti-Phishing Working Group (APWG) reported a total of 396,688 unique email phishing campaigns in the fourth quarter of 2020.[1]

Web Browsers Protection Against Phishing

Phishing protection is provided by an application within a web browser that requests a URL's reputation from a cloud service that has been scouring the Internet to find phishing websites and adding them to a blocklist. That way, when a web browser attempts to visit a URL, the browser's phishing protection (i.e., Safe Browsing, SmartScreen, etc.) redirects the user to a warning message that explains the URL is malicious. Some reputation systems also include additional educational content. Conversely, if a website is determined to be "good," the web browser takes no action.

Google and Firefox use the Google Safe Browsing API for both URL reputation and to warn users about downloading certain types of files. Microsoft Edge uses Microsoft Defender SmartScreen, which provides URL-based protection from attacks via an integrated, cloud-based URL-reputation service, as well as application reputation for malicious file blocking.

Average Number of Malicious URLs Added Per Day

On average, 50 new validated URLs were added to the test set per day; numbers varied on some days as criminal activity levels fluctuated.

Test Environment

- Microsoft Windows 10 Pro, 21H1

Total Number of Malicious URLs In the Test

26,976 raw, unvalidated URLs were tested multiple times with each web browser over a total of 80 test cycles each, conducted without interruption over 480 hours (every 6 hours for 20 days). Our engineers removed samples that did not pass the validation criteria, including those tainted by exploits (not part of this test). Ultimately, 996 unique, valid phishing URLs were included in the final set of 61,605 discrete, valid phishing tests (20,535 tests per web browser), providing a margin of error of 3.1 percent (3.1%) at a confidence level of 95%.

How Test Composition – Phishing URLs

Data in this report spans a testing period of twenty (20) days between May 11 and May 31, 2021. During the test, our 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 emphasis was on freshness with new URLs constantly being added to the test and dead sites removed.

How We Assessed Results

We measured each browser's ability to block malicious URLs as quickly as they were discovered on the Internet. Engineers repeated these tests every six hours to determine how long it would take a vendor to add protection if they did at all.

Each browser's performance was measured continuously, and the overall block rate of all URLs tested with the browser was recorded. Each browser's overall block rate was calculated as the number of successful blocks divided by the total number of test cases. For example, with tests conducted every 6 hours, a URL that was online for 48 hours was tested eight (8) times. A browser blocking it on 6 (out of a maximum of 8) test runs achieved a block rate of 75%.

Tested Products

- Google Chrome: Version 90.0.4430.212 - 91.0.4472.19
- Microsoft Edge: Version: 91.0.864.19 - 91.0.864.37
- Mozilla Firefox: Version 88.0.1 - 88.0.1

[1] APWG Phishing Activity Trends Report

Authors

Thomas Skybakmoen, Vikram Phatak

Test Methodology

CyberRatings Web Browser Security Test Methodology v1.0 is available at www.cyberratings.org

Contact Information

CyberRatings.org
2303 Ranch Road 620 South
Suite 160, #501
Austin, TX 78734

info@cyberratings.org
www.cyberratings.org