

## **Firefox 2 Phishing Protection Effectiveness Testing**

November 14, 2006

*Note: This document will be posted on Tuesday 11/14/06 to:*

*<http://www.mozilla.org/security/phishing-test>*

### **Overview**

We've been actively working to test the effectiveness of the Phishing Protection feature in Firefox 2 as part of Mozilla's ongoing commitment to security. As an addition to Mozilla's community development and testing process, we initiated a program to test the effectiveness of this feature in an open, transparent and unbiased way. We're doing this to better understand how well Phishing Protection performs in flagging potential phishing attacks in general and relative to Microsoft's phishing filter in Internet Explorer 7. More information will allow us, as a community, to make good product decisions. This document outlines the basic testing methodology we used and the final test results.

### **Summary**

- Firefox 2 Phishing Protection is more effective than the Microsoft Phishing Filter in Internet Explorer 7.
- Firefox 2 offers users a choice between local and remote protection modes.
- Firefox 2 Phishing Protection uses local mode by default, which protects user privacy.
- Even in local mode, Firefox 2 Phishing Protection is significantly more effective than the Microsoft Phishing Filter in Internet Explorer 7, operating in either mode.

### **Methodology**

#### **Source of Phishing URLs**

Test phishing URLs were received from PhishTank via their public XML feed of valid phishing URLs. PhishTank is a community-driven web service that allows for phishing URLs to be submitted and verified by their community participants. The PhishTank XML feed consisted of URLs verified by the PhishTank community as valid phishing URLs. The feed was downloaded once per hour, and any new phishing URLs found were added to a testing database.

#### **Browsers and Modes Tested**

Firefox 2 (RC3 and final release) and IE 7 (final release) were tested in this round, all using Windows XP machines. Additionally, two modes per browser were tested:

- Firefox 2 Check Local List
- Firefox 2 Ask Google
- Internet Explorer 7 Automatic Website Checking OFF
- Internet Explorer 7 Automatic Website Checking ON

## **Testing Company**

An independent, third party software services and testing company, SmartWare, was selected to perform the tests to ensure that testing was conducted in manner that was fair and unbiased. SmartWare testing extended over a period of two weeks, from 10/19/2006 to 11/06/2006.

## **Testing Application**

A web application was developed that allowed SmartWare testers to interface with the testing database, which served as the repository for the phishing URLs and test results. The testing application displayed a list of no more than 7 URLs at a time. Each URL linked to a reporting page that contained the actual test URL, and edit fields to report the results of the phishing test.

## **Testing Process**

Testers worked in teams of two, and would typically test one browser in both modes for up to 7 URLs at a time, then switch to the other browser to test both modes on those URLs. Testers had to report results on all four browser modes before a URL was considered complete. Once this occurred, the completed record dropped off the list and a new URL was added. Limiting the available test URLs ensures that all four modes were tested in as short of a time window as possible.

Since time favors the second browser tested (it gives the phishing features more time to update their lists), the testing order between Firefox 2 and IE 7 was rotated to ensure that no one browser had a testing advantage over another. It should be noted that Firefox was tested first more times than IE 7 to discourage any advantages for Firefox.

The available reporting fields were as follows:

- Not Blocked - the page loaded normally without notification to the user.
- Blocked - the page was blocked by a warning indicating that the current page was a suspected web forgery.
- Warned (IE 7 only) - This would warn the users of a suspicious page, but would not block or prevent the page from loading.

Each report was time stamped so that any results that exceeded a time limit could be disqualified.

## **Valid Phishing URLs**

Testers were instructed to report results only for URLs that were actively spoofing a legitimate site. Sites with 404 messages, server not found messages, or messages from an ISP stating that a site had been removed were tagged "site offline," and are not counted in the final results.

## Results Filtering

Once the test run was complete, test results were filtered to disqualify some records from the final results. The filters were as follows:

- Duplicate URLs were filtered. When records displayed the same test results, the record that had the smallest differential between timestamps across all four modes was kept. For duplicate records where the test results differed, both records were discarded.
- Any record with timestamps that exceeded a 15 minute window between the first and last results reported were filtered. This was to ensure that all four modes per URL were tested as close to one another as possible.

## Auditing

Our testing methodology and results were audited by iSEC Partners to validate the integrity of our findings.

## Results

### Total Reports

1040

Mode	Sites Blocked	% Blocked
Firefox 2 Local List	820	78.85%
Firefox 2 Ask Google	848	81.54%
IE7 Auto Check OFF	16	1.54%
IE7 Auto Check ON	690	66.35%

## Stats

- There were 243 instances where Firefox blocked but IE did not.
- There were 117 instances where IE blocked but Firefox did not.

## Data

The raw test results data, including phishing URLs, will be posted soon.

## Acknowledgments

Mozilla would like to acknowledge all of the hard work that everyone put into the Phishing Protection feature to make it such a great success. Google, for plugging their anti-phishing services into, and for contributing to, the Phishing Protection framework. PhishTank and the PhishTank community for their responsiveness and help in providing us with validated phishing data. SmartWare, for diligently running through such a large number of tests. And iSEC Partners, for auditing and reporting on our test methodology and results.