

Anti-Phishing Test



August 2015

Language: English

August 2015

Last revision: 10th August 2015

www.av-comparatives.org

Introduction

What is Phishing?

Taken from Wikipedia¹:

“Phishing is a way of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. This is similar to Fishing, where the fisherman puts a bait at the hook, thus, pretending to be a genuine food for fish. But the hook inside it takes the complete fish out of the lake. Communications purporting to be from popular social web sites, auction sites, online payment processors or IT administrators are commonly used to lure the unsuspecting public. Phishing is typically carried out by e-mail spoofing or instant messaging and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Phishing is an example of social engineering techniques used to deceive users, and exploits the poor usability of current web security technologies.”

For more information about how not to get hooked by a phishing scam, please have a look at e.g. <http://www.onguardonline.gov/phishing> (provided by the United States' Homeland Security).

Test procedure

In our test scenario, we simulate the common situation where users rely on the anti-phishing protection provided by their security products while browsing the web (and/or checking their webmail accounts; anti-spam features are not considered, as they are not within the scope of this test). The test was done using Windows 7 Professional 64-Bit and Internet Explorer 11 (without its built-in phishing blocker, in order to get browser-independent results). All security products were tested with default settings and in parallel, at the same time and on the same URLs.

Test set

The test took place between the 29th July and 3rd August 2015. Phishing URLs were tested as soon as we discovered them. All phishing URLs had to be active/online at time of testing and attempt to get personal information. After removing all invalid, offline and duplicate (sites hosted on same server/IP) test-cases, 245 valid phishing URLs remained. The phishing campaigns targeted various types of personal data, including login credentials etc. for PayPal, online banking & credit cards, e-mail accounts, Dropbox, eBay, social networks, online games and other online services.

¹ <http://en.wikipedia.org/wiki/Phishing>

Tested products

The tested product versions are the ones that were available at the time of testing. The following ten vendors chose to have their anti-phishing protection publicly tested:

- **Baidu** Antivirus 5.4.3 (English)
- **Bitdefender** Internet Security 2015
- **BullGuard** Internet Security 15.1
- **Emsisoft** Anti-Malware 10.0
- **ESET** Smart Security 8.0
- **Fortinet** FortiClient 5.2.3
- **F-Secure** Internet Security 2015
- **Kaspersky** Internet Security 2016
- **Lavasoft** Ad-Aware Pro 17.6
- **Trend Micro** Internet Security 2015

Anti-Phishing “False Alarm” Test

For the Anti-Phishing False-Alarm Test we selected 500 popular banking sites (all of them using HTTPS and showing a login form) from all over the world, and checked if any of the various security products blocked these legitimate online banking sites. Wrongly blocking such sites is a serious mistake. Of the products tested, only **F-Secure had 1 false alarm** on the tested 500 legitimate online banking sites.

Ranking system

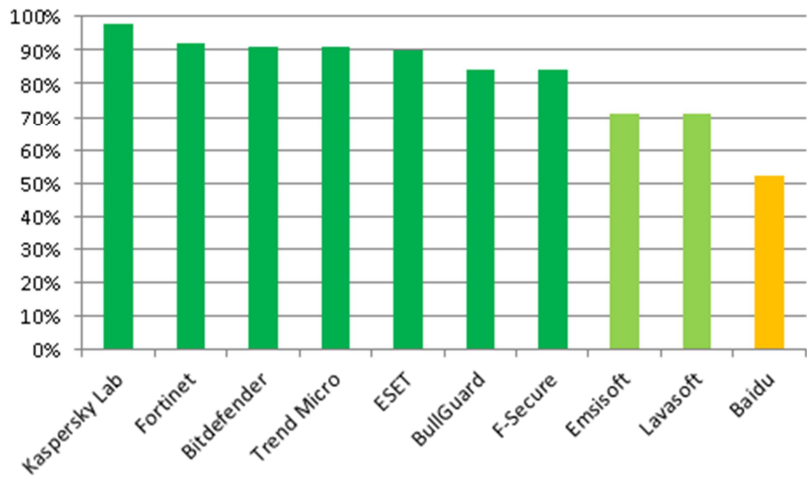
The awards are decided and given by the testers based on the observed test results (after consulting statistical models). The ranking system for this year’s Anti-Phishing Test is as follows:

<i>Ranking system</i>	Anti-Phishing Protection under 50%	Anti-Phishing Protection Cluster 3	Anti-Phishing Protection Cluster 2	Anti-Phishing Protection Cluster 1
Zero FPs	Tested	Standard	Advanced	Advanced+
1 to 2 FPs	Tested	Tested	Standard	Advanced
3 to 4 FPs	Tested	Tested	Tested	Standard
More than 4 FPs	Tested	Tested	Tested	Tested

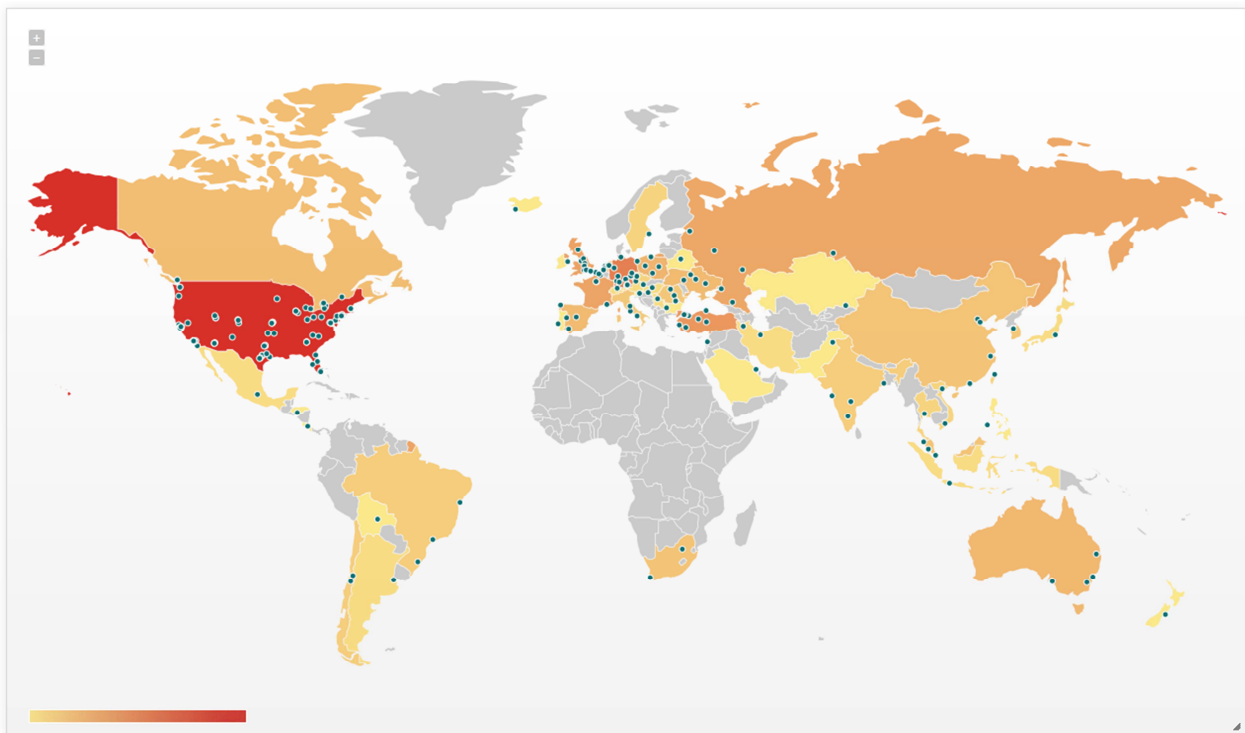
Test results

Below you can see the percentages of blocked phishing websites (size of test set: 245 phishing URLs).

- 1. Kaspersky Lab 98%
- 2. Fortinet 92%
- 3. Bitdefender, Trend Micro 91%
- 4. ESET 90%
- 5. BullGuard, F-Secure 84%
- 6. Emsisoft, Lavasoft 71%
- 7. Baidu 52%



The map below shows where the phishing websites used were hosted, based on their IP addresses.



Award levels reached in this test

The following awards² are for the results reached in this Anti-Phishing Test:

AWARD LEVELS	PRODUCTS
	<p>Kaspersky Lab Fortinet Bitdefender Trend Micro ESET BullGuard</p>
	<p>F-Secure* Emsisoft Lavasoft</p>
	<p>Baidu</p>
	<p>-</p>

* downgraded by one rank due to a false alarm; see page 3

² Please note that although we have used our usual awards scheme for this test, the results will *not* be included in the ratings for Product of the Year Award.

Copyright and Disclaimer

This publication is Copyright © 2015 by AV-Comparatives®. Any use of the results, etc. in whole or in part, is ONLY permitted with the explicit written agreement of the management board of AV-Comparatives, prior to any publication. AV-Comparatives and its testers cannot be held liable for any damage or loss, which might occur as a result of, or in connection with, the use of the information provided in this paper. We take every possible care to ensure the correctness of the basic data, but liability for the correctness of the test results cannot be taken by any representative of AV-Comparatives. We do not give any guarantee of the correctness, completeness, or suitability for a specific purpose of any of the information/content provided at any given time. No-one else involved in creating, producing or delivering test results shall be liable for any indirect, special or consequential damage, or loss of profits, arising out of, or related to, the use (or inability to use), the services provided by the website, test documents or any related data.

For more information about AV-Comparatives and the testing methodologies please visit our website.

AV-Comparatives (August 2015)