Anti-Phishing Certification

Kaspersky Internet Security

Language: English
July 2017
Last revision: 24th July 2017

www.av-comparatives.org

Introduction

What is Phishing?

Taken from Wikipedia[1]:

"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. https://www.consumer.ftc.gov/articles/0003-phishing

Tested product

The most recent product version of **Kaspersky Internet Security** available at time of testing has been used in this test. The test was performed with default settings:

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).

Test set

The test took place between the 7th and 11th July 2017. **510** 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. 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. The set of legitimate online banking websites for the false alarm test consisted of **500** clean URLs (all of them using HTTPS and showing a login form) from all over the world.

---

[1] http://en.wikipedia.org/wiki/Phishing

AV-Comparatives Approved Anti-Phishing Product

To be approved by AV-Comparatives for Anti-Phishing Protection, at least 90% of the phishing URLs used must be detected and blocked, without causing any false alarms with legitimate online banking sites.

Only products which were submitted for the Anti-Phishing Test, and which passed the test, are published. Eight vendors submitted their products for certification in 2017, of which only four reached the requirements (incl. Kaspersky Internet Security). Vendors can reapply for approval in 2018.

Test results

Below you can see the percentages of blocked phishing websites (size of test set: 510 phishing URLs). **No false alarms** were encountered on the tested 500 legitimate online banking sites.

	Detection Rate	FPs
Kaspersky Lab	**93%**	**0**

Anti-Phishing Detection Rate
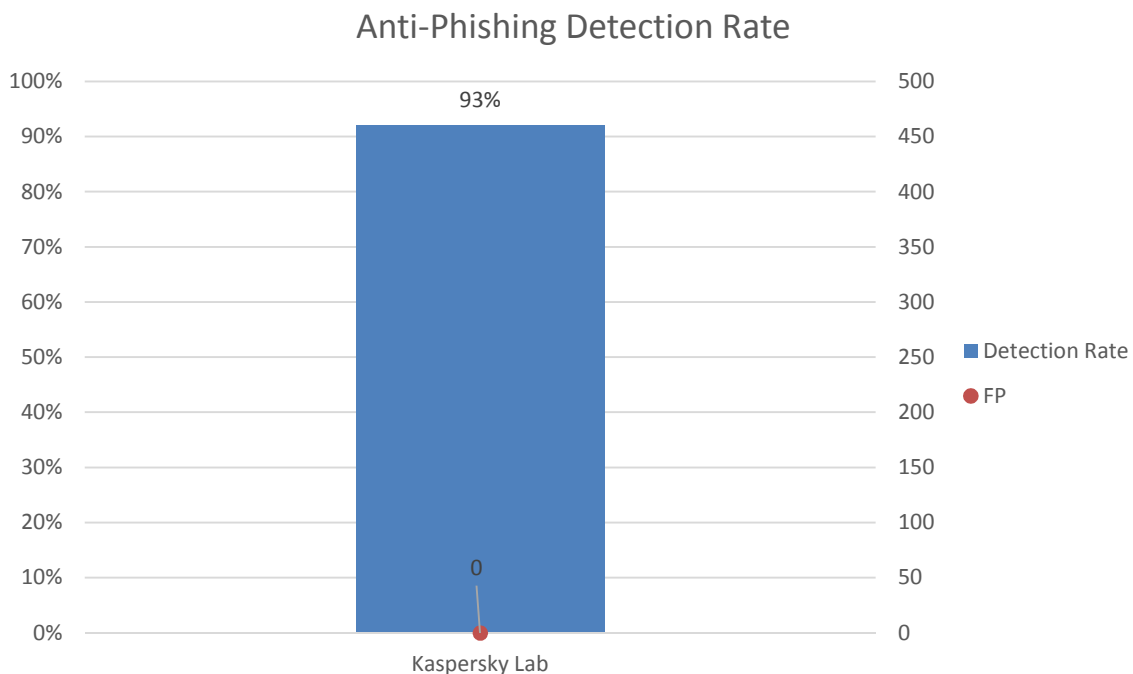
Copyright and Disclaimer

This publication is Copyright © 2017 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.

<div align="right">AV-Comparatives (July 2017)</div>