

Anti-Phishing Test



August 2011

Language: English

August 2011

Last revision: 19th October 2011

www.av-comparatives.org

Introduction

This test report is only a short summary for a test which was commissioned by a magazine and which has been recently published by German “PC Magazin”. As with all results in printed magazines, results are from several months ago, in this case from August 2011. We have been allowed to publish this short summary after the commissioning party published its own report in its magazine¹.

The Anti-Phishing test is not (yet) part of our regular yearly main test-series and can be considered as a first Anti-Phishing testing attempt. Due to that, there is (at least this time) no awarding for this test.

What is Phishing?

Taken from Wikipedia²:

“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.”

For more information about how to avoid phishing scams, please have a look at the Consumer Advice of the Anti-Phishing Working Group: http://www.antiphishing.org/consumer_rec.html

Test procedure

In our common test scenario we simulate a user which relies on the Anti-Phishing protection provided by its security product while browsing the web (and/or checking his webmail e-mail account, i.e. anti-spam features are not considered as they are not the scope of this test). The test was done using Windows XP SP3 and Internet Explorer 7 (without the build-in phishing blocker in order to get browser-independent results) under VMware. All security products were tested using default settings. All products were tested in parallel at the same time on the same URLs.

¹ PC Magazin 11/2011: <http://www.pc-magazin.de>

² <http://en.wikipedia.org/wiki/Phishing>

Tested products

The products to be tested were chosen by the magazine which ordered the test. The tested product versions are the ones which were available at time of testing (August 2011). The following 19 products were included in the Anti-Phishing test:

- **AVG** Internet Security 2011
- **Avira** Premium Security Suite 10.1
- **Bitdefender** Internet Security 2012
- **Bullguard** Internet Security 10.0
- **eScan** Internet Security 11.0
- **ESET** Smart Security 4.2
- **F-Secure** Internet Security 2011
- **G DATA** Internet Security 2012
- **K7** Total Security 11.1
- **Kaspersky** Internet Security 2012
- **McAfee** Total Protection 2011
- **Panda** Internet Security 2012
- **PC Tools** Internet Security 2011
- **Qihoo** 360 Internet Security 2.0
- **Quick Heal** Internet Security 2011
- **Symantec** Norton Internet Security 2011
- **Trend Micro** Titanium Internet Security 2012
- **Trustport** Internet Security 2012
- **Webroot** Internet Security Complete 7.0

We were asked to test also **Avast**, **Microsoft** (Security Essentials) and **Sophos**. But Avast and Sophos do not have any Anti-Phishing feature, except blocking phishing mails with their spam filter. Microsoft does block phishing websites in its browser (Microsoft Internet Explorer) and its spam filter (e.g. Microsoft Outlook); Security Essentials is not designed for this task.

Notes:

ESET doesn't have a dedicated module for anti-phishing protection yet. However, phishing sites are currently blocked along with other potentially harmful sites (like in most other products), employing various technologies such as webfilter, parental control and detection of suspicious content aimed at the phishing landing pages themselves.

Qihoo is mainly targeted to block Chinese phishing sites.

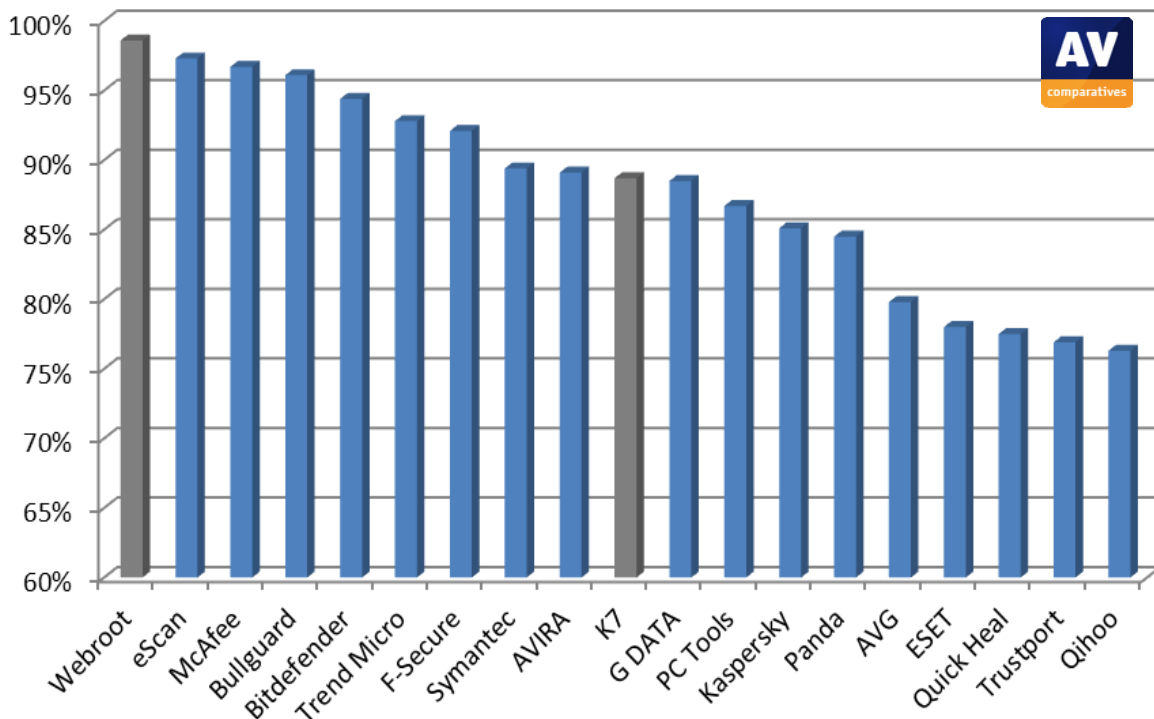
Test Set

Phishing URLs taken out from spammed prevalent phishing mails and/or collected by our crawler and researchers. All phishing URLs had to be active/online and attempt to get personal information. Duplicate phishing URLs, as well as phishing campaigns hosted on same server/IP were removed. All test cases were manually re-verified after the test. At the end, only 697 different and valid Phishing URLs remained. The phishing campaigns targeted various types of personal data. Among those were (in the following order) phishing attempts to gather e.g. login credentials etc. for: PayPal, eBay, Online Banking & Credit cards, Social networks, Online Games, E-mail accounts and other online services.

Test Results

Below you see the percentages of blocked phishing websites (size of test set: 697 phishing URLs). Please take into consideration the false alarm rates (on next pages) when looking at the below results (products with false alarms are marked with an asterisk).

1. Webroot	98.6%*
2. eScan	97.3%
3. McAfee	96.7%
4. Bullguard	96.1%
5. Bitdefender	94.4%
6. Trend Micro	92.8%
7. F-Secure	92.1%
8. Symantec	89.4%
9. AVIRA	89.1%
10. K7	88.7%*
11. G DATA	88.5%
12. PC Tools	86.7%
13. Kaspersky	85.1%
14. Panda	84.5%
15. AVG	79.8%
16. ESET	78.0%
17. Quick Heal	77.5%
18. Trustport	76.9%
19. Qihoo	76.3%



Anti-Phishing “False Alarm” Test

For the Anti-Phishing False Alarm Test we selected 1000 legitimate banking sites (all of them using HTTPS) from all over the world and checked if those legitimate online banking sites were blocked by the various security products. Wrongly blocking such sites is a serious mistake. From the tested 19 products, only two (K7 and Webroot) had false alarms on the tested 1000 legitimate online banking sites:

K7 (1 false alarm):

- Bank Islam from Malaysia

Webroot (12 false alarms):

- AB Finance Bank from Russia
- Bank of Kenya from Kenya
- BLC Bank from Lebanon
- Dawia Next Bank from Japan
- Dhanlaxmi Bank from India
- Habib Bank Zurich from UAE
- ING NL from Netherlands
- Marfin Laiki Bank from Cyprus
- Refah Bank from Israel
- Saxo eBank from Sweden
- ScotiaBank from Mexico
- UCO Bank from India

The discovered false alarms have been reported to the respective vendors and are now no longer blocked.

Which products support which browser?

Most browsers already include their own Anti-Phishing technologies. Nevertheless, due to the complexity and amount of social engineered scams and phishing attempts, it is recommended to make use of the Anti-Phishing features provided by security products too. Practically all security products support the main stream browsers (i.e. Internet Explorer and Firefox), while not all products support also other browsers. Due to that, it may be safer to make use of a supported browser for e.g. online banking.

	Microsoft Internet Explorer	Mozilla Firefox	Google Chrome	Opera	Apple Safari
AVG Internet Security	YES	YES	YES	NO	NO
AVIRA Premium Security Suite	YES	YES	YES	YES	YES
Bitdefender Internet Security	YES	YES	YES	YES	YES
Bullguard Internet Security	YES	YES	NO	NO	NO
eScan Internet Security	YES	YES	NO	NO	NO
ESET Smart Security	YES	YES	YES	YES	YES
F-Secure Internet Security	YES	YES	NO	NO	NO
G DATA Internet Security	YES	YES	YES	YES	YES
K7 Total Security	YES	YES	NO	NO	NO
Kaspersky Internet Security	YES	YES	YES	YES	YES
McAfee Total Protection	YES	YES	NO	NO	NO
Panda Internet Security	YES	YES	YES	YES	YES
PC Tools Internet Security	YES	YES	YES	NO	NO
Qihoo 360 Internet Security	YES	NO	NO	NO	NO
Quick Heal Internet Security	YES	YES	NO	NO	NO
Symantec Norton Internet Security	YES	YES	YES	NO	NO
Trend Micro Titanium Internet Security	YES	YES	YES	YES	YES
Trustport Internet Security	YES	YES	YES	YES	YES
Webroot Internet Security	YES	YES	NO	NO	NO

Copyright and Disclaimer

This publication is Copyright © 2011 by AV-Comparatives e.V. ®. 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 e.V., prior to any publication. AV-Comparatives e.V. 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 e.V. 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. AV-Comparatives e.V. is a registered Austrian Non-Profit-Organization.

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

AV-Comparatives e.V. (October 2011)