Independent Tests of
Anti-Virus Software

Evaluating the Effectiveness of Security Products Against Internet Fake Shops (Scams)

TEST PERIOD: NOVEMBER 2024

LAST REVISION: 25TH NOVEMBER 2024

WWW.AV-COMPARATIVES.ORG

Introduction

Online consumers face significant risk when inadvertently accessing fake web shops, which are often designed with a high degree of sophistication to closely mimic legitimate e-commerce platforms. Besides the critical threat of data theft, an equally concerning risk is the potential to make purchases under the pretence of genuine transactions, only to find that ordered goods are never delivered. These fraudulent sites aim to harvest sensitive data, such as credit card details and personal information, leading to financial loss and identity theft. Consequently, in the organisational context, a single breach can have cascading effects, jeopardising company data and customer trust.

As the holiday shopping season approaches, consumers should be extra cautious of fake shops offering deals that seem too good to be true. Scammers often target the surge in online purchases during this period. Shoppers should verify websites and avoid rushing into discounted offers, especially from unfamiliar sellers. Further details about fake shops and best practices for identifying them are provided at the end of this report.

We conducted our first *Fake-Shops Detection Test* in June 2024[1], with various cybersecurity solutions, including Internet security software, browser extensions, and specialised web filters under test. The aim was to assess their effectiveness in detecting threats posed by fake and untrustful web shops. With this precise and objective evaluation, consumers can make informed decisions that substantially mitigate the risk of fraud and data theft within their organisations, empowering them to take control of their cybersecurity. The cybersecurity solutions proactively identify and block access to potentially harmful online resources with advanced techniques such as heuristic analysis, web reputation services, and real-time fraud detection. This not only prevents data theft and financial loss but also provides users with a sense of reassurance in their online activities.

In this report, AV-Comparatives re-evaluated the previously tested cybersecurity products and two new ones using 500 new URLs as well as 189 URLs from June 2024, and compared the results with those of the earlier test. This emphasises the changes in the product's performance over time in detecting fraudulent websites. Additionally, we tested the products against newly acquired fakeshop URLs from official, publicly available sources.

[1] https://www.av-comparatives.org/fake-shops-detection-test-2024/

Test Procedure

AV-Comparatives tested the effectiveness of cybersecurity products against fake shops. A false alarm test with 100 popular legitimate online shopping sites was also performed – no false positives were observed with any of the tested products. Of the 500 fake shop testcases from the test in June, we reused 189 that remained online at the time of testing. Additionally, new fake shop websites were this time taken from publicly available sources between June 1st and October 10th, 2024. We randomly selected 500 URLs from those that were still online at the time of testing. All tests were performed on a fully patched Microsoft Windows 10 64-bit system using Google Chrome as the default browser.

Time of Testing:	November 2024
Collecting Testcases:	From June 1st 2024 to October 10th 2024
New Fake Shop Testcases:	500
Old Fake Shop Testcases (June):	189[2]
Legitimate Web Shop Testcases:	100
Operating System:	Microsoft Windows 10 64-bit
Browser:	Google Chrome

[2] 189 of 500 fake shop testcases from June were still online during testing in November.

Tested Products

To ensure a fair evaluation based on each product's intended focus and help users identify the solution that best aligns with their needs, we distinguished between dedicated and non-dedicated solutions in this test.

- *Dedicated solutions* are specialized tools designed specifically to detect scams and fake online shops. While they primarily target these types of threats, they might also detect phishing attempts.
- *Non-dedicated solutions*, such as Internet security products, primarily focus on protecting against malware and phishing. They may only partially detect fake online shops.

The products were tested using default settings. Where applicable, we installed all available browser extensions with relevant settings enabled in both the main product and extensions to optimize the detection of fraudulent websites. We used the latest product versions available at the time of testing (November 2024).

Dedicated Solutions:

1. Fake-Shop Detector[3]
2. Netcraft Extension
3. ScamAdviser[4]
4. Trusted Shops Extension
5. WOT: Website Security & Safety Checker

Non-dedicated Solutions:

6. Adaware Privacy Standard
7. Avast Premium Security
8. AVG Internet Security
9. Avira Internet Security
10. Bitdefender Total Security
11. Comodo Internet Security Pro
12. Dr.Web Security Space
13. Emsisoft Anti-Malware Home
14. eScan Total Security Suite
15. ESET Home Security Essential
16. F-Secure Total
17. G Data Total Security
18. Google Chrome
19. K7 Total Security
20. Kaspersky Standard
21. Malwarebytes Premium
22. McAfee Total Protection
23. MetaCert Internet Security
24. Microsoft Defender Browser Protection
25. NordVPN Threat Protection Pro
26. Norton 360 Deluxe
27. Norton Ultra VPN
28. Panda Dome Essential
29. Quick Heal Internet Security
30. SafeDNS Home
31. Sophos Home Premium
32. Total Defense Premium Internet Security
33. TotalAV Antivirus Pro
34. Trend Micro Internet Security
35. VIPRE Advanced Security
36. Webroot Internet Security Plus
37. ZoneAlarm Extreme Security NextGen

[3] Fake-Shop Detector is a research project by the Austrian Institute for Applied Telecommunications (ÖIAT), X-Net, and AIT Austrian Institute of Technology.

[4] Results of ScamAdviser are not included in the results table on the next page due to a product issue. Please refer to section *Analysis of Findings* for further details.

Test Results

We checked if the website was blocked or at least a warning or hint was shown to the user while visiting the website. The table below compares the detection rates of fake shop URLs by the tested products from tests conducted in June and November.

Cybersecurity Product	Detection Old Jun	Detection Old Nov	Detection New Nov	False Positive Check
Number of Testcases	500	189	500	100
Dedicated Solutions				
Fake-Shop Detector	>90%	>90%	71-80%	✓
Netcraft Extension	71-80%	>90%	51-60%	✓
Trusted Shops Extension	6-10%	6-10%	6-10%	✓
Non-dedicated Solutions				
Adaware Privacy Standard	<6%	<6%	<6%	✓
Avast Premium Security	41-50%	>90%	71-80%	✓
AVG Internet Security	41-50%	>90%	71-80%	✓
Avira Internet Security	41-50%	51-60%	31-40%	✓
Bitdefender Total Security	11-20%	11-20%	11-20%	✓
Comodo Internet Security Pro	<6%	<6%	<6%	✓
Dr.Web Security Space	<6%	<6%	<6%	✓
Emsisoft Anti-Malware Home	31-40%	31-40%	31-40%	✓
eScan Total Security Suite	6-10%	11-20%	6-10%	✓
ESET Home Security Essential	6-10%	41-50%	31-40%	✓
F-Secure Total	41-50%	71-80%	61-70%	✓
G Data Total Security	6-10%	6-10%	11-20%	✓
Google Chrome	<6%	<6%	<6%	✓
K7 Total Security	<6%	<6%	<6%	✓
Kaspersky Standard	11-20%	11-20%	11-20%	✓
Malwarebytes Premium	<6%	<6%	<6%	✓
McAfee Total Protection	41-50%	>90%	81-90%	✓
MetaCert Internet Security	<6%	<6%	<6%	✓
Microsoft Defender Browser Protection	<6%	<6%	<6%	✓
NordVPN Threat Protection Pro	61-70%	71-80%	81-90%	✓
Norton 360 Deluxe	31-40%	81-90%	81-90%	✓
Norton Ultra VPN	N/A	>90%	81-90%	✓
Panda Dome Essential	<6%	<6%	<6%	✓
Quick Heal Internet Security	11-20%	11-20%	11-20%	✓
SafeDNS Home	<6%	<6%	<6%	✓
Sophos Home Premium	6-10%	6-10%	11-20%	✓
TotalAV Antivirus Pro	31-40%	31-40%	31-40%	✓
Total Defense Premium Internet Security	11-20%	11-20%	11-20%	✓
Trend Micro Internet Security	31-40%	51-60%	31-40%	✓
VIPRE Advanced Security	6-10%	11-20%	11-20%	✓
Webroot Internet Security Plus	6-10%	>90%	81-90%	✓
WOT: Website Security & Safety Checker	21-30%	21-30%	21-30%	✓
ZoneAlarm Extreme Security NextGen	11-20%	11-20%	21-30%	✓

Analysis of Findings

The evaluation highlights the performance evolution of the tested cybersecurity products over time. It shows that only a small number of the tested products offer a good level of protection against fake shop websites or online scams, although detection rates might fluctuate depending on the age of the websites. Comparing dedicated and non-dedicated solutions is a valid approach, as their purposes and capabilities differ. If an Internet security product lacks robust fake shop detection, it would be advisable to install a dedicated solution alongside it which warns against such websites. However, users should not rely solely on cybersecurity products. A multi-layered security approach is essential which includes regular updates, awareness of common scam tactics, and cautious online behaviour. Further details about fake shops and best practices for identifying them can be found on the following pages. **Norton Ultra VPN** and **ScamAdviser** were included only in the November test and therefore did not have results from the June test. No false positives were recorded in either testing period.

"Detection Old Nov" includes all testcases from June that remained online during testing in November. In general, fake shops often have an online lifespan of only a few weeks or months. We noticed that more than half of the old fake shop URLs had gone offline since June. Comparing the results from June and November, we observed little improvement in most products' ability to detect the old testcases, despite these URLs remaining online for a considerable period. This might be an indication that these products may not focus on detecting fake shops.

Non-dedicated solutions that now detect many fake shops previously missed in June include **Avast**, **AVG**, **F-Secure**, **McAfee**, **Norton**, and **Webroot**. Additionally, when tested against the new fake shop testcases used in November, which were sourced from publicly available lists, **NordVPN** also achieved strong detection rates alongside the aforementioned products. **ESET** and **Trend Micro** improved as well though they have limited capabilities in detecting fake shops. **Avira**, **Emsisoft**, and **TotalAV** did not improve and also have limited detection capabilities.

Among *dedicated solutions* for detecting scams and fake shops, **Fake-Shop Detector** and **Netcraft** performed well, though they detected fewer new fake shop URLs in November than in June. The **ScamAdviser** browser extension detected <6% of the testcases. However, manual checks using the website tool showed that 81-90% of the testcases should have been flagged. This discrepancy suggests an issue with the browser extension, and its results will therefore not be included in the table.

Although the new fake shop URLs used in November were sourced from publicly available lists and had been listed for over a month, the products did not perform as well as initially expected. Most products appear to rely solely on blacklists to identify fake shops. The effectiveness of these products depends on the accuracy and maintenance of these blacklists, yet some seem not to use very up-to-date lists. We suggest vendors to proactively seek out these lists, collaborate closely with organizations managing these resources, and evaluate the integration into their products. In general, we encourage vendors of non-dedicated solutions to reconsider and improve this feature or keep improving. Enhancing the ability to identify and block fraudulent websites will greatly benefit users by providing better protection against online scams.

Vendors seeking for a **Fake-Shop Detection Certification** are encouraged to reach out to us at **contact@av-comparatives.org** for more details.

Understanding Fake Online Shops and Other Scams

Scammers often impersonate legitimate brands by stealing logos, copying website designs, and creating domain names with minor misspellings. They manipulate reviews, use phishing emails, and run fake ads to lure victims. Search engine manipulation, fake trust badges, and deceptive customer service are common tactics to create a sense of legitimacy. Recent research by SRLabs[5] revealed that these criminals frequently exploit previously expired domains with good Google reputations, enabling fraudulent websites to appear credible, trustworthy, and rank prominently in search engine results.

Examples of fake shops include websites based in China selling luxury goods at huge discounts, Eastern European sites offering cheap electronics, and Southeast Asian sites selling poor-quality clothing. Some shops even sell harmful health products from countries with lax regulations. However, not all suspicious signs guarantee a site is fake. Reasonable prices, customs delays, and foreign-based shops do not always indicate a scam. Even secure websites (HTTPS) can be fraudulent. Additionally, fake goods can sometimes be sold on major platforms like Amazon and eBay.

To minimise the risk of falling victim to these scams, we have compiled a list of some best practices for identifying fake shops:

- Be careful when shopping online on your mobile phone, as it is easier to accidentally click on fraudulent popups or ads.
- Verify website legitimacy by checking for misspelt domain names, valid SSL certificates (indicated by "https://" and padlock symbol), and domain registration information[6].
- Look for contact information, such as a physical address, phone number, and email address.
- Review the website for grammatical errors and unclear policies on returns, refunds, and shipping.
- Search for reviews or scams associated with the retailer's brand on various sites and social media.
- Report suspicious websites to relevant authorities.
- Avoid making payments outside the online shop and be cautious of foreign bank accounts (IBAN).
- Avoid advance payments.
- Ensure that you receive an order confirmation and invoice after purchase.
- Watch for hidden subscription traps in free offers.
- Monitor your financial accounts and report any suspicious activity to your bank or credit card company immediately.
- Use trusted and up-to-date security products with high detection rates.
- Avoid purchases from foreign shops, especially if legal action or refunds may be difficult.
- Keep up with the latest news on online scams and fraud tactics.
- Educate and share experience with your friends and family to help them stay safe online.

A more exhaustive list can be found in our previous report[7].

[5] https://www.srlabs.de/blog-post/bogusbazaar
[6] https://who.is/, https://lookup.icann.org/
[7] https://www.av-comparatives.org/fake-shops-detection-test-2024/

Copyright and Disclaimer

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

AV-Comparatives
(November 2024)