Independent Tests of Cybersecurity Solutions



Fake-Shop Detection Certification

Avast Premium Security

TEST PERIOD: OCTOBER 2026

LAST REVISION: 13 OCTOBER 2026

WWW.AV-COMPARATIVES.ORG

Introduction

Online consumers face significant risk when inadvertently accessing fake webshops, which are often designed with a high degree of sophistication to closely mimic legitimate e-commerce websites.

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.

Fake-Shop Detection Test

AV-Comparatives verified the effectiveness of cybersecurity products in detecting fake online shops. The test set consisted of 500 fake-shop URLs, randomly selected from our pool of collected URLs that were still online at the time of testing. A false-alarm test with 100 popular legitimate shopping websites was also conducted. The test was performed from 1 to 7 October 2026.

All tests were carried out on a fully patched Microsoft Windows 11 (64-bit) system using Google Chrome as the default browser.

To be certified by AV-Comparatives for Fake-Shop Detection, a product must detect at least 80% of the fake-shop URLs used in the test without causing any false alarms on legitimate shopping sites. Only a few products on the market currently aim to warn users about fraudulent e-commerce websites, and recognising such scams remains technically challenging. Therefore, while the certification threshold may appear modest, achieving it is not easy, and only a small number of products are presently able to meet this standard.

Fake-Shop Detection Certification

Avast Premium Security received certification for its fake-shop detection capabilities, highlighting its commitment to user safety and security. This certification is a testament to the product's effectiveness in safeguarding users from financial loss caused by online scams.



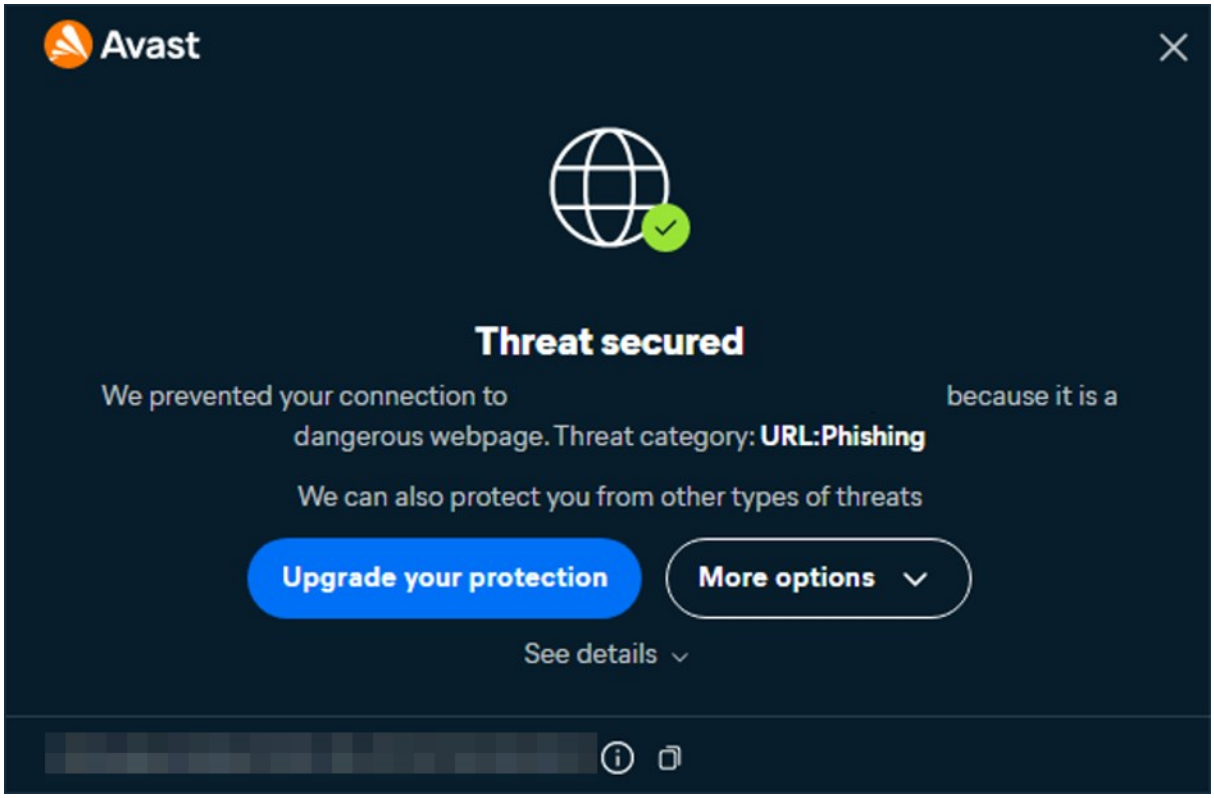
Avast Premium Security

We have included a short feature review in this report so that users can see how the product's fake-shop protection works in practice.

Avast Premium Security includes technologies intended to warn users when they visit fraudulent online shops. The feature analyses website characteristics and URLs to identify known or suspicious patterns commonly associated with fake online shops.

When a potential fake shop is detected, the website is blocked, and a warning message is displayed in a separate window. The warning informs the user about the risks of fake online shops and recommends not visiting the site. Additionally, the user can view more details about the detection.

An example screenshot of a detection message is shown below.



This feature was directly relevant to the Fake-Shop Detection Certification, as it determined whether the product could effectively recognise fraudulent e-commerce websites.

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. Research by SRLabs revealed that these criminals frequently exploit previously expired domains that still have a good reputation with Google, enabling fraudulent websites to appear credible, trustworthy, and rank prominently in search engine results.

Examples of fake shops include websites selling luxury goods at huge discounts, sites offering cheap electronics, or sites offering medications without a prescription. Some of these shops might never ship anything; others might ship cheap copies of legitimate products or even fake medication containing no active ingredients or the wrong ones. However, not every warning sign means that a site is fake. Large discounts, customs delays, and shops based abroad do not always indicate a scam. Even secure websites (HTTPS) can be fraudulent. Fake goods can also end up on major platforms such as Amazon or eBay.

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

- Be careful when shopping online on your mobile phone, as it is easier to accidentally click on fraudulent pop-ups or ads.
- Check for misspelt domain names and look up the domain registration information (https://who.is/, https://lookup.icann.org/). An encrypted connection ('https://' and a padlock symbol) is a basic requirement, but it does not prove that a shop is genuine.
- Be wary of offers that are 'too good to be true', such as discounts of more than 60 to 70%.
- 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 online and on social media for reviews of, or scam warnings about, the shop.
- Report suspicious websites to relevant authorities.
- Be careful when making payments and use payment providers that offer buyer protection. Be especially wary of foreign bank accounts (check the IBAN) and avoid advance payments.
- Ensure that you receive an order confirmation and invoice after purchase.
- Watch out 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.
- Be cautious with shops based abroad, especially where legal action or refunds may be difficult.
- Keep up with the latest news on online scams and fraud tactics.
- Share your experience with friends and family to help them stay safe online too.

Copyright and Disclaimer

This publication is Copyright © 2026 by AV-Comparatives®. Any use of the results, etc., in whole or in part, is ONLY permitted after 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 that 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 no representative of AV-Comparatives can accept liability for the correctness of the test results. 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
(October 2026)