M

Malvertising: How Malicious Ads Work and How to Stay Safe

Learn how malicious ads lead to fake software, phishing, scams, and exploit pages, why reputable sites can display them, and what to do after a click.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
3 min

CONTENTS

In this guide

01 What does malvertising mean?
02 How malvertising attacks work
03 Do you have to click the ad?
04 Common malvertising lures
05 How to recognize a risky ad destination
06 How users can reduce the risk
07 Organizational defenses
08 What to do after clicking a malicious ad
09 Ads, pop-ups, and browser hijackers

Malvertising is the use of online advertising to deliver malicious content or direct people to phishing, scam, fake-software, or malware pages. Attackers may buy legitimate-looking ads, compromise advertiser accounts, abuse ad redirects, or insert hostile code into the advertising supply chain.

A reputable website can display a malicious ad because advertising is often selected and delivered by third-party systems in real time. The site owner may not have reviewed that exact creative or destination.

01 What does malvertising mean?

Malvertising is short for malicious advertising. The advertisement may itself contain hostile code, or it may be a convincing lure whose link leads to a fake login, fraudulent support page, or malware download. It differs from adware: malvertising is an attack delivered through advertising, while adware is software that displays or injects advertisements on a device.

02 How malvertising attacks work

1. An attacker creates or compromises an advertiser account.
2. The ad imitates a known brand, download page, support service, or investment offer.
3. Targeting and redirect rules send selected users through intermediate domains.
4. The landing page steals credentials, promotes a fake installer, or attempts exploitation.
5. The campaign changes domains and content to avoid review and blocking.

03 Do you have to click the ad?

Many current campaigns require a click and further interaction, such as downloading and running a file or entering credentials. Historically, malicious ad content and exploit kits could also abuse browser vulnerabilities with little interaction. Keep browsers updated and treat both the ad and its destination as untrusted.

04 Common malvertising lures

- Sponsored results imitating popular software download pages.
- Fake browser, codec, antivirus, or operating-system updates.
- Tech-support warnings claiming the device is infected.
- Cryptocurrency, investment, giveaway, and celebrity-impersonation scams.
- Ads that redirect through multiple unrelated domains.
- CAPTCHA pages instructing the user to paste or run a command.

05 How to recognize a risky ad destination

Check the complete hostname instead of the visible brand name. Warning signs include misspellings, recently created look-alike domains, unexpected download types, requests to disable security, and “support” pages demanding remote access or payment. HTTPS only protects the connection; it does not make the advertiser honest.

06 How users can reduce the risk

1. Navigate to software vendors through a saved bookmark or independently typed address.
2. Keep the browser, extensions, and operating system updated.
3. Use browser reputation protection and approved DNS or web filtering.
4. Remove unnecessary extensions and notification permissions.
5. Do not install software or call a number from an alarming advertisement.
6. Use a password manager, which is less likely to fill credentials on a look-alike domain.

07 Organizational defenses

CISA and NSA guidance supports blocking unnecessary advertising content in higher-risk environments. Organizations can combine managed browsers, DNS filtering, web gateways, endpoint controls, and browser isolation. Test blocking against business needs, provide a false-positive path, and protect off-network devices as well as office users.

08 What to do after clicking a malicious ad

If nothing was entered or downloaded, close the page and report the ad and destination. If credentials were entered, change them from a clean device, revoke sessions, and review MFA and recovery settings. If a file ran or a command was pasted, isolate the device, preserve details, and start the approved incident-response process.

09 Ads, pop-ups, and browser hijackers

Seeing one bad ad does not prove the browser is infected. Persistent redirects, a search engine that changes back, or ads on sites that normally have none can indicate an unwanted extension or browser hijacker. Review extensions, notification permissions, installed applications, and managed-browser policies.

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com