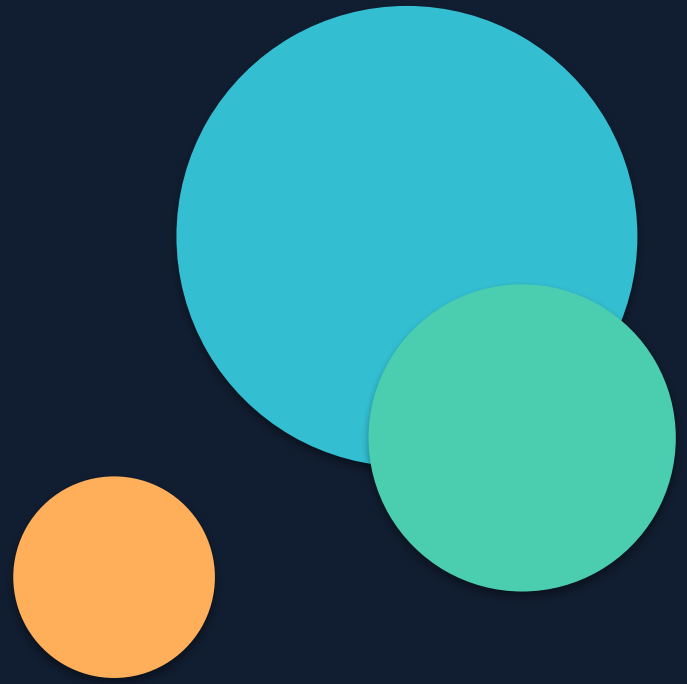
Melbpc Users Group 4 November 2026

Malvertising: when online ads become a threat

How ad blockers help — and why they are only one layer of defence



Some practical tips

How an advertisement becomes an attack

1. Malicious ad

A criminal buys, abuses or compromises ad inventory. A reputable site may unknowingly serve it.

2. The lure

Fake download buttons, security alerts, prize claims or redirects try to make people click.

3. The outcome

Scams, credential theft, unwanted software — or, in some cases, exploitation of a software flaw.

Key distinction

Seeing an ad is not the same as being infected. Risk rises when a person follows a deceptive link, downloads/runs something, grants permission, or when a vulnerability is exploited.

Term: malvertising = malicious activity delivered through online advertising.

What an ad blocker can — and cannot — do

Can help by...

- Blocking requests to known ad / tracking domains
- Applying filter rules to page elements and URLs
- Blocking some known malicious domains
- Reducing exposure to deceptive ad placements

Cannot guarantee...

- Blocking every new or compromised ad domain
- Detecting every phishing page
- Stopping every malicious download
- Preventing browser or OS vulnerabilities from being exploited

A blocker is a risk-reduction tool, not a substitute for browser security or careful decisions.

Three different checks

A. Ordinary webpage

Open the same ad-supported page in two Firefox profiles: blocker ON vs OFF.

Observe visible ads and the uBlock Origin panel.

B. Phishing test

Open the official AMTSO Security Features Check and choose its phishing test.

Also check on MS Defender Smartscreen test page.

Record whether a warning appears — and who issued it.

C. Download protection

AMTSO malware-download test. EICAR is another harmless test file for endpoint protection.

Do not use real malware.

What happened

Test	Safari + Ghostery	Firefox + uBO + MAB BG	Chrome+ uBO	Brave	MS Edge including ai scareware blocker
Ads visible	Mostly no	No	No	No	Yes
Phishing test (AMTSO/MS)	Fail/Fail	Fail/Fail	Fail/Fail	Fail/Fail	Fail/Pass
Download warning	security app	MAB BG blocked	security app	security app	MS Edge blocked
Drive by download	security app	MAB BG blocked	security app	security app	Browser + security app

Important: a phishing warning tests reputation protection; fewer visible ads tests ad filtering. They are different results, not one combined score.

Four browsers: overlapping, not identical, defences

Chrome

Google Safe Browsing checks known dangerous sites and downloads. Enhanced Protection offers more proactive checks.

Microsoft Edge

Microsoft Defender SmartScreen checks site and download reputation; Edge also offers tracking prevention.

Firefox

Deceptive-content and malware protection warns about reported phishing / malware sites and dangerous downloads.

Brave

Shields blocks many ads and trackers by default; separate Safe Browsing protections help identify dangerous sites.

Feature availability and defaults can vary by version, platform and settings. Check the browser's own security page.

Defence in depth: several chances to stop an attack

1 Reduce exposure — Ad / tracker blocking • malicious-domain filters

2 Recognise threats — Safe Browsing • SmartScreen • phishing / download warnings

3 Limit damage — Browser sandbox • OS protections • reputable endpoint security

4 Recover and contain — Updates • backups • password manager • MFA

If one layer misses a threat, another may still block it or limit the consequences.

Take-home message & useful links

Four habits worth keeping

- Use a reputable ad / malware blocker and keep its filter lists current.
- Leave browser phishing / malware protection enabled.
- Keep OS, browsers and apps updated.
- Pause at unexpected warnings; don't install “updates” from ads.

Demo & reference links

uBlock Origin & Browser Guard for Firefox

https://addons.mozilla.org/firefox/addon/ublock-origin/
https://addons.mozilla.org/en-GB/firefox/addon/malwarebytes/

AMTSO and MS Security Features Check

https://www.amtso.org/security-features-check/
https://demo.wd.microsoft.com/Page/UrlRep

EICAR test file (optional)

https://www.eicar.org/download-anti-malware-testfile/

uBlock Origin project / browser status

https://github.com/gorhill/uBlock/

No single extension guarantees safety. Layered protection reduces risk.