

4. RIVE-BY DOWNLOAD / MALVERTISING

A drive-by download occurs when simply visiting a malicious or compromised website causes your device to become infected, even if you don't click anything.

Attackers often inject harmful scripts into ads or webpages that automatically exploit browser or plugin vulnerabilities, silently installing malware in the background.

DRIVE-BY DOWNLOAD / MALVERTISING



Scenario: Arham Browses a News Site

Arham opens a well-known, legitimate news website to read the latest updates.

However, one of the ads displayed on the page has been compromised by an attacker.

As soon as the ad loads, it silently runs malicious scripts in the background, exploiting a vulnerability in Arham's browser.

He doesn't click anything, yet the malware installs automatically without his knowledge.

Lesson: Keep your browser, extensions, and antivirus fully updated, as attackers often rely on outdated software to execute drive-by downloads.

DRIVE-BY DOWNLOAD / MALVERTISING



Arham browses a news site

A compromised ad
silently loads malware
in the background

How Malvertising Works?

- Attackers buy ad slots
- Serve malware through banner ads
- Target employees with specific IPs
- Often appear on real sites

Warning Signs

- Browser suddenly slows
- Pop-ups appear
- Unexpected downloads
- Antivirus alerts

Prevention Tips

- Use ad-blockers
- Keep browser updated
- Avoid pirated/free movie sites
- Enable real-time protection