5. SEO POISONING

SEO poisoning is a technique where attackers intentionally manipulate search engine rankings so their malicious websites appear at the top of Google results.
They use trending keywords, fake articles, and SEO tricks to make these harmful sites look legitimate.
When users click the top search results without checking carefully, they may be taken to malware-infected pages, fake login portals, or scam sites designed to steal information.

Google
keyword
Malicious Website
malicious-site.com
Check out this amazing offer!

Scenario: Maryam Searches “Adobe Reader Download”

Maryam searches “Adobe Reader” on Google and clicks the top result, not noticing it’s a sponsored ad placed by attackers.

The site looks legitimate, so she downloads “AdobeSetup.exe,” unaware it’s a malware-infected fake installer.

Lesson: Always download software directly from official websites, not from ads or unfamiliar links in search results.

AdobeSetup.exe
Download
Google
Adobe Reader
Ad
Adobe Reader Download
www.example.com
Adobe Reader - Free Download

Why Employees Fall for It?

- Trust top search results
- Don’t check domain
- Click ads assuming they’re official

Red Flags

- Domain unrelated to the product
- Too many pop-ups
- “Download accelerator” pages
- Fake reviews on website

Prevention Tips

- Only download software from official links
- Avoid sponsored search results
- Use company-approved software stores