



CIRT.GY

Guyana National Computer Incident Response Team

T2025_22 Watch Out for Fake Download Links in Search Results (September 29, 2025)

Cybercriminals often manipulate search engine ads and results to make malicious download pages appear above legitimate ones. These sites may look identical to official vendor pages but instead deliver malware disguised as trusted applications. Victims who install these fake programs can unknowingly give attackers access to sensitive data, networks, and devices.

To stay safe, avoid clicking on sponsored ads when searching for software. Type the official vendor's address directly into your browser or bookmark the legitimate site for future use. Organizations should configure DNS filtering and browser security tools to block known malicious domains and train staff to recognize suspicious download links.

References

- AddictiveTips. (2023, June 15). How to identify real download links and buttons. AddictiveTips. Retrieved September 28, 2025, from <https://www.addictivetips.com/web/identify-real-download-links-and-buttons/>
- UMA Technology. (2024, February 7). How to avoid fake ads disguised as download links. UMA Technology. Retrieved September 28, 2025, from <https://umatechnology.org/how-to-avoid-fake-ads-disguised-as-fake-download-links/>