Avoiding Search Engine Ad Malware

Search engine advertising (SEA) is a form of paid online advertising that allows businesses to reach potential customers who are searching for products or services similar to their own. This marketing technique places the paid advertisement directly into your search engine results and on partner websites, with a small fee paid by those running the ad campaign each time someone clicks on their ad.

But these paid ads could serve malware to those who click on them. Recently there have been reports of consumers downloading malware delivered to them through search engine advertising, especially promoted search results on websites like Google.

It's a sophisticated phishing effort where scammers spoof legitimate websites (like Grammarly and Slack) and pay search engines for advertising. In return, the spoofed websites get pushed to the top of web search results for specific keywords. Once a person clicks on the link in the ad, they might download malware, ransomware, or become a victim of some other scheme.

WHAT SHOULD YOU DO?

- Be careful about clicking on sponsored search results, which are usually marked as an "Ad" next to the webpage title.
- Make sure any link you click on from a sponsored search result is a legitimate website; however, this can be difficult because cybercriminals try to spoof URLs very carefully
- To be safe, scroll down to relevant, unsponsored search results that link to web addresses you know are legitimate.
- As with all online activity, THINK before you click!

  Take 3-5 additional seconds to check the link out, then decide if it's worth the risk.

This additional awareness won't slow you down. Still, it could save countless hours recovering your computer from a virus or ransomware.