
## Essential steps for secure internet searches

BY DEBORAH DOTSON, DIRECTOR, GRF BOARD

The answer to whether you are on the internet is likely a resounding yes, and this year you've spent more time surfing than ever before. Can you count how many searches you've performed in the past year? Can you say with confidence that you feel safe searching the internet?

Numerous tools can help you safely search the internet. Hardware protection, antivirus software and browser security settings are an imperative start to a worry-free searching experience, but the first and last line of defense is still you.

**Protect Your Hardware**

No computer should be without antivirus/antimalware software. These vital tools erect a "firewall" between you and the outside world and filter email to protect your computer against viruses or malware in case you accidentally open a harmful attachment, click a malicious link or visit an infected website. Although many operating systems on Mac or Windows come with enough security to screen your email, adding third-party protection is essential today. These tools may not be perfect, but without them, you could lose all your data from your computer.

**How 'Cookies' Crumble**

Many antivirus software products include ad blocking, which can offer an extra layer of protection against unwanted ads or history tracking. Tracking "cookies"—the cyberworld's tasty personal insight treats—are small pieces of text that help a website remember information about your visit. Cookies can make it easier and more useful to revisit the same site, but consider the information passing back to that site, as well.

You may recall seeing popup messages to the effect of "We use cookies to give you the best experience. Some cookies are necessary for the technical

operation of our website. If you continue browsing, you agree to this site's use of cookies. We share information about your use of our site with social media, advertising and analytics partners." This is where you really should pay attention and not just click "OK." This information can be sold, but you have the right to "opt out," which is recommended. Many sites make it difficult to opt out, knowing you'll give up and just click OK. However, don't do that; take a minute and allow the technical cookies but opt out of marketing and other nonessential cookies. Often you can just close the cookie message without accepting.

A good antivirus program not only offers protection against viruses, malware, spyware and ransomware attacks, but also monitors privacy and identity. Install antivirus software when you set up your device. If this task seems daunting, hire a professional. A few dollars spent now can save you later. It's like wearing a seatbelt while you drive: You still must pay attention, but you are safer wearing it.

**Use Browser Security Settings**

A browser is a computer program with a user interface for displaying and navigating web pages. If you go to the empty bar and start to type a word into that field, that is part of your browser. The most common browsers are Google Chrome, Firefox, Safari or Microsoft Edge.

Each browser allows you to customize settings to help narrow your search, protect it and manage the history of the webpages you visit.

When "safe search" is activated in your browser, the filtering tool ensures safe search results for all keywords entered. While it isn't 100%, it helps filter explicit content in search results for all queries across images, videos and many websites. Google offers a robust search, which allows for multiple customizations. Most browsers have these features, so check yours and customize the settings to suit your needs. Time spent now will save you later!

The best protection for any computer user is the proper use of security settings and tools. Establishing the security settings on your browser is like wearing sunblock when you go outside—it can keep you from getting burned as long as you use it properly.

**Read Before You Click**

What happens when you see the hundreds of thousands of results of that search? You click on the first few listed, right? However, be aware that companies often pay extra to be listed on that first page, and their content may not represent the best quality of your search.

Also consider what the result says. If it has ".pdf" at the end, it is a document, not a website; if it ends in ".html," it might be a computer-coded item. If the country of origin of the site is different than the United States, it will often end in a country abbreviation. For example, sites from the United Kingdom end in "co.uk" or "org.uk."

Once you find what you want to explore further and click to open the page, if anything pops up other than a warning about "this site uses cookies," be sure to read that message before clicking on it—messages are one of the easiest ways for a virus to infiltrate your computer.

You can take many measures to search the internet safely, but you are your own best defense. Read before you click, err on the side of caution and create good habits when searching.

# PICK UP CRUMBS AND DELETE COOKIES

You probably know by now that Big Tech chases your every click. It's a great way for them to pinpoint your preferences so they can route personalized ads your way. But you may not know just how these companies are tracking you. That's all thanks to cookies—small bits of data that track your online activity as you move from site to site. Cookies can save your passwords and help you log on more easily, but they can also collect so much data it can feel stifling.

For step-by-step instructions on how to clear cookies from five popular web browsers, visit **https://nr.tn/3eJbftN**.