



Safer Web Browsing in 5 Simple Steps

What don't we use the Internet for these days? We check email, read the latest news, stay in touch with friends, find sports scores and stats...and that's just before breakfast! Using the Internet is commonplace and comfortable — and in some cases, even necessary. Even so, surfing the Web has its dangers.

The fact is, the Internet is an ever-shifting landscape. More pages pop up daily, with new applications, new capabilities, and new information sources. While plenty of the sites and features we use are perfectly safe, scammers are working overtime to take advantage of unsuspecting surfers.

There are specific elements and behaviors you should watch out for online. Here are five pitfalls to avoid when browsing:

1. Prompts to run or download software.

Malicious websites can generate pop-ups that look like messages from your browser or computer. A random prompt to install or upgrade software is a warning sign. Don't click anything in an unexpected pop-up window; only install software from known, trusted sources.

2. Promises of free content, software, and products.

If someone online is offering you something for free, it's highly likely there is a catch. Free movies, music, and videos often include pirated — i.e., illegal — content, as well as hidden viruses and other malicious software. Plus, free products or downloads are often given in exchange for personal information, which criminals can use to access your home and business accounts. "Free" is tempting, as scammers know all too well. Don't get caught paying the price.

3. Doctored and shortened URLs.

URLs (or links) are essentially the addresses for websites. It's important to look closely before clicking because scammers can easily manipulate URLs to fool you. One common trick is to use known brands to create a sense of security. Even if you see a known name in a URL, check for other things like hyphens, symbols, and numbers, which can be warning signs. And be mindful of shortened URLs from services like Bitly and Tiny URL; these are often used in social media and can completely mask the true identity of a link. If you're at all concerned about a link, it's best to use a search engine to identify a legitimate URL for a site you want to visit.

4. Bogus search results.


When using a search engine, it's important to study your results before clicking. Hackers try to secure high-level search results and trick you into visiting their sites. Scrutinize URLs to ensure they are legitimate links, and be especially careful if you are searching for popular or trending topics. Scammers will act quickly to capitalize on celebrity news, recent deaths, and major disasters by creating fake web pages about these topics.

5. Convenience features like "Auto Complete" and "Remember Me."

Sure, it can make life easier to allow your browser to automatically complete web forms for you or to allow commonly visited websites to store your passwords. The problem is, it makes life easier for scammers as well. Dangerous websites can take advantage of auto-complete features and use hidden fields to steal the data from forms. And if a criminal should gain access to your computer, any sites with stored passwords would be easy pickings.

Bottom Line: Take Control

With old threats lingering and new threats emerging daily, it's more important ever than to practice safe browsing. It's critical to realize that you are in the driver's seat.



Because even with high security settings and anti-virus software in place, there's only so much your browser can do to protect you. Though you might get a warning about a dangerous site or dangerous content, your browser cannot stop you from visiting a risky site or downloading spyware.

So browse smart using the tips noted above. And don't stop there. Other online best practices will also keep you safe, like using strong passwords and varying them from site to site, and limiting all sensitive online activity (e.g., online banking, ecommerce, and accessing corporate email) to private computers and secure networks. Consider shared computers and open-access WiFi networks to be the public domain. Anything you wouldn't want to be shared should not be done on these systems.

You have the power to stay safe online if you take control. Browsing smart = browsing safe.

To learn more about how Machado can help secure your business from cyberthreats, **please contact 508.453.4700**

machado
be ready for the next.