

10 Essential Tips for Seniors to Spot Fake Websites and Stay Safe Online

Programs @ The Blue Marble · 4 min read

The internet offers many benefits, but it also has risks, especially for seniors who may not be familiar with the tricks scammers use. Fake websites can look very real and try to steal your personal information or money. Learning how to recognize these suspicious sites before entering any details is key to staying safe online. This guide shares 10 practical tips to help seniors identify fake websites and protect themselves.



Checking a website URL carefully to avoid scams

1. Check the URL Carefully

One of the easiest ways to spot a fake website is by looking closely at the web address or URL. Scammers often create URLs that look very similar to real ones but have small differences. For example, instead of "www.bankofamerica.com," a fake site might use "www.bankofarnerica.com" or "www.bankofamerica-secure.com."

Look for:

- Misspellings or extra words
- Strange characters or numbers in the URL
- URLs that end with unusual domain extensions like ".xyz" or ".info" instead of ".com" or ".org"

Always type the website address yourself instead of clicking on links from emails or messages. This reduces the chance of landing on a fake site.

2. Look for HTTPS and the Lock Icon

Secure websites use HTTPS, which means the connection is encrypted. You can see this in the URL bar as "https://" and a small lock icon. This does not guarantee a site is safe, but the absence of HTTPS is a red flag. If a website asks for sensitive information like passwords or credit card numbers and does not have HTTPS, do not enter your details. Modern browsers often warn you when a site is not secure, so pay attention to those alerts.

3. Spot Fake Login Pages

Fake login pages are designed to steal your username and password. They often look identical to the real login pages of banks, email providers, or social media sites.

To avoid falling for these:

- Always access login pages by typing the official website address directly.
- Check the URL carefully to make sure it matches the official site.
- Be cautious if the login page appears after clicking a link in an email or message.
- Look for poor spelling, grammar mistakes, or unusual design elements on the page.

If you suspect a login page is fake, close the browser immediately and do not enter any information.

4. Avoid Pop-Up Download Scams

Pop-ups that ask you to download software or updates can be dangerous. Fake websites often use pop-ups to trick you into downloading malware or fake antivirus programs.

To stay safe:

- Never click on pop-ups asking you to download something unexpectedly.
- Use official websites or trusted app stores to download software.
- Keep your computer's security software updated to block malicious downloads.
- If a pop-up appears, close it using the "X" button on the window, not by clicking inside the pop-up.

5. Check for Contact Information and Website Details

Legitimate websites usually provide clear contact information, including phone numbers, email addresses, and physical addresses. Fake sites often lack this or provide vague details.

Look for:

- An "About Us" or "Contact" page with real information.
- Customer service phone numbers you can call.
- Privacy policies and terms of service.

If this information is missing or seems suspicious, avoid using the site.

6. Use a Search Engine to Verify the Website

Before entering any personal information, search for the website's name on a search engine like Google. Look for reviews, warnings, or news about scams related to that site. If many people report the site as fake or unsafe, do not trust it. Official websites usually appear at the top of search results and have consistent information across different sources.

7. Watch for Poor Design and Errors

Fake websites often have poor design quality, broken links, or spelling and grammar mistakes. While not always the case, these signs can indicate a scam site.

Check for:

- Low-quality images or logos
- Pages that do not load properly
- Text that looks unprofessional or contains errors

If the site looks rushed or untrustworthy, it is safer to leave.

8. Be Wary of Too-Good-To-Be-True Offers

Scammers use fake websites to lure victims with unbelievable deals, prizes, or discounts. If an offer seems too good to be true, it probably is.

Avoid sites that promise:

- Free money or prizes without any effort
- Extremely low prices on expensive items
- Urgent requests to act quickly or provide payment details

Take time to research and verify before trusting such offers.

9. Use Browser Security Features and Extensions

Modern web browsers have built-in security features that warn you about dangerous websites. Enable these features to get alerts about suspicious sites. You can also install trusted security extensions that block known scam sites and phishing attempts. These tools add an extra layer of protection when browsing.

10. Keep Your Software Updated

Keeping your web browser, operating system, and security software up to date helps protect you from fake websites and malware. Updates often include patches for security vulnerabilities that scammers try to exploit. Set your devices to update automatically or check regularly for updates to stay protected.