WEB BROWSING
Road Trip

BROWSER ON BOARD

The basics of browsing safely

Most online resources offer you reliable, safe, and secure travel through the World Wide Web. However, you need to keep your eyes peeled for cyberattackers who are ready to steer you down a dark road by creating fake social media profiles, look-alike websites, and dangerous file shares.

One wrong turn, and attackers could steal your passwords, money, or personal info. They could even launch a cyberattack on your organization.

The defenses developers put in place to keep you and your accounts safe and secure aren't foolproof. However, your awareness can help you outmaneuver cybercriminals.

Being smart about your browsing and social connections will help make your trip through the internet a lot smoother.

Roadblocks, Detours, and Dangerous Curves

Anyone can host digital content. And when we say "anyone," that includes cybercriminals. After all, there aren't many restrictions. It's not like anyone needs to pass a test to get behind the wheel of a website.

Nobody verifies that a domain is being purchased for legitimate reasons. Nobody checks to make sure websites are safe before they're allowed online.

Warning signs to help you avoid "dangerous drivers" include:

- A domain name that is close to that of a known, trusted domain, but not quite right. Like, a misspelling of the name.
- Web addresses that don't include the domain name you'd expect to see.
- An invalid security certificate.
- Sites mimicking well-known brands but with misspelled words or blurry images.
- A lack of functionality you'd expect a legitimate site to have.

Simple safe-browsing tips include:

- Always examine domains closely. Even an extra number, letter, or hyphen is a big concern.
- Don't interact with a website if there's any sign it isn't safe or secure.
- Avoid clicking links in emails, social media posts, and other communications. Instead, type in known, familiar web addresses yourself, directly into your browser. You can also use addresses you've already bookmarked.

Recognize the hazards when on the information superhighway.

THE INTERSECTION OF TWO TERMS

Know the difference between "domain" and "URL"

Domain

- The "core" name of the website (e.g., "google.com" for Google)
- Takes you only to the website's main landing page

URL (Universal Resource Locator)

- Commonly known as a "web address"
- Includes a domain as well as other identifying info
- Takes you to specific content within a website
- Tells you if a website transmits data securely (seeing "HTTPS" in a URL is a common indicator)

Safety Comes Standard

Learn about some browser security features

Just like a car, a browser has built-in features that will warn you if something is not right. Here are just two examples of security alerts your browser may display:

- A warning that a site is not secure or can't be authenticated. This is a serious risk if the site is asking you for sensitive data, like passwords or financial info.
- An alert that indicates a site is suspicious or deceptive. It may be suspected of being a phishing website or having malicious software. It may also try to trick you into downloading dangerous programs.

Now, these warnings themselves won't stop you from unsafe browsing behavior. Just like when you're driving, it's up to you to heed road signs.

So, when you see signs or warnings that a site is not safe, don't go there!
Stick with known, trusted destinations.

Also, a good way to stay on top of known security issues is by keeping your browser up to date. Check your security settings regularly to make sure you're using the latest software version of the browser. Think of it as regular tune-ups before you go browsing.