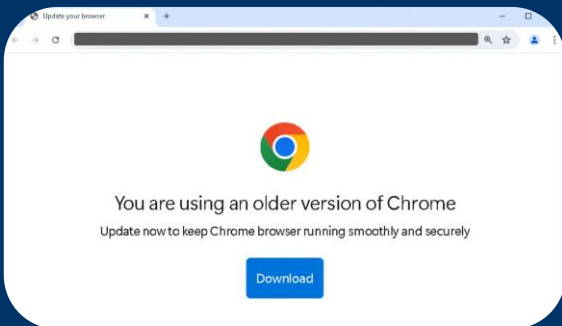


Safe Web Browsing

Real Example of Attackers Targeting Web Browsers

FakeUpdates is a malware family that uses fake browser-update messages on compromised websites to trick users into downloading malware. **Check Point** identified FakeUpdates as a leading malware family in 2023. Attacker tactics have evolved and can now appear as fake CAPTCHAs, software-download prompts, and malicious online advertisements.



Example from a **Google Cloud Security Community blog** of a fake browser-update message prompting users to download malware.

Additional Resources

CISA

[Tips to Stay Safe while Surfing the Web, Part 1: Web Browser Settings](#)

Better Business Journal

[BBB Tip: How to identify a fake website](#)

U.S. Department of Education

[Cybersecurity Best Practices for Schools and Districts | Protecting Student Privacy](#)

WHAT IS SAFE WEB BROWSING?

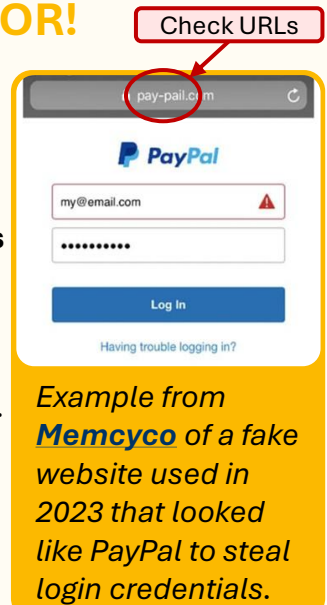
Safe Web Browsing means using the internet thoughtfully with caution to help protect yourself and your organization from online threats. Before clicking anything, verify the contents of what you are clicking and where it will take you.

WHAT TO WATCH OUT FOR!

1. **Fake Websites That Look Real**
2. **Unexpected Browser Pop-Ups**
3. **Browser Extension Risks**
4. **Credential Harvesting Attempts**

Local government and school staff frequently use the web to access cloud applications, educational resources, and government services.

Cybercriminals target **you** by creating convincing fake websites or malicious links designed to steal credentials or install malware.



WHAT SHOULD YOU DO?

1. **Check before you click.** Check website addresses carefully for misspellings or unexpected domains.
2. **Use trusted bookmarks.** Access your frequently used websites through saved bookmarks instead of going through a search engine.
3. **Keep your browser updated.** Browser updates provide fixes to known security vulnerabilities and help block malicious websites.
4. **Be cautious with pop-ups.** Close unexpected pop-ups and avoid allowing notifications from unfamiliar websites.
5. **Report suspicious websites.** If a website looks unusual or requests unexpected information, immediately report it to your IT or security team.



Report Suspicious Activity Through Your Organization's Established Reporting Channels