Safe Browsing & Downloads Guide

The web is full of threats — from malicious advertisements (malvertising) to drive-by downloads and fake software updates. Practicing safe browsing habits drastically reduces your exposure to malware, ransomware, and credential theft.

Key Points

- ✓ Always verify HTTPS (padlock icon) before entering credentials or sensitive data
- ✓ Be wary of pop-ups claiming your computer is infected — these are almost always scams
- ✓ Only download software from official sources and verified publishers
- ✓ Keep your browser and extensions up to date — enable auto-updates
- ✓ Use an ad blocker to reduce exposure to malvertising
- ✓ Avoid clicking shortened URLs (bit.ly, tinyurl) from untrusted sources
- ✓ Clear browsing data regularly and review installed extensions

Action Items

1. Install a reputable ad blocker (uBlock Origin) on all browsers
2. Review and remove unused browser extensions now
3. Enable "Ask where to save" for downloads to avoid accidental execution
4. Bookmark frequently visited sites instead of searching each time
5. Configure your browser to block third-party cookies

Quick Reference

Safe Download Checklist: Official site? HTTPS? Known publisher? File hash verified? Scanned by antivirus?
Red Flags: "You must update Flash Player", unexpected file downloads, sites asking to disable antivirus, pop-ups with countdown timers.
File Types to Treat with Caution: .exe, .msi, .bat, .ps1, .js, .vbs, .scr, .cmd