



# CYBERSECURITY AWARENESS DAY 15

Let's talk about  
**Safe browsing**

**Iwuchukwu Augusta Chioma**



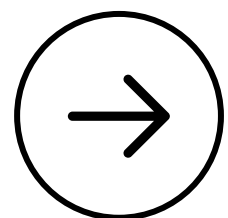
# Safe Browsing



The internet is like a city full of bright lights,  
but dark alleys too.

Safe browsing isn't paranoia.  
It's digital street-smartness.

**Iwuchukwu Augusta Chioma**



# What is Safe Browsing

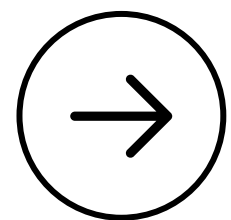


Safe browsing means using the web in a way that protects privacy, data, devices, and identity from threats like phishing, malware, tracking, malicious sites, and data leaks. It's not just about avoiding bad websites, it's about configuring browsers, networks, behavior, and tools so that the risk is minimized.

A few components include:

- Ensuring websites are secured (HTTPS)
- Configuring browser settings (blocking trackers, disabling risky features)
- Using protective tools (VPNs, ad blockers, anti-malware)
- Being cautious with links, downloads, and public Wi-Fi

**Iwuchukwu Augusta Chioma**

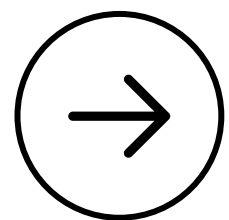


# Common Traps Online



- Fake download buttons
- Pop-ups asking for “urgent” updates
- Free movie or software sites
- Spoofed news links or clickbait headlines
- “You’ve won!” notifications
- The web is full of bait and the bait looks real.

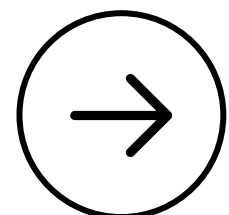
Iwuchukwu Augusta Chioma



# Why Safe Browsing Matters in 2025



- Attackers are smarter: AI-driven phishing, zero-day exploits in browsers, and stealthy malware are rising.
- Browsers are a central hub: Most web apps, emails, banking and much more runs through the browser, making it a high-value target.
- Default settings are weak: Many people never change default browser configurations, use weak settings, or install risky extensions.
- Public Wi-Fi & mobile browsing: More people browse on the go, public networks stay a major vulnerability.
- Tracking & privacy: Every site, ad, plugin, and cookie can collect data about behavior, preferences, and identity.

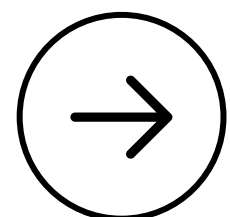


# Key Safe Browsing Practices



Practice	What to Do	Why / Benefit
Use HTTPS & check the padlock	Always look for “https://” and the lock symbol before entering sensitive info	Encrypts data in transit, protects against interception
Keep browser and extensions up to date	Enable automatic updates and review extensions frequently	Patches vulnerabilities, removes malicious extensions
Use privacy-first settings	Turn on “Do Not Track,” block third-party cookies, use stricter security modes	Reduces tracking, ad profiling, data collection

Iwuchukwu Augusta Chioma

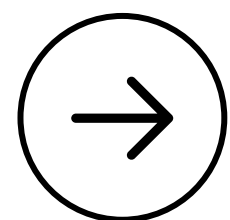


# Key Safe Browsing Practices



Practice	What to Do	Why / Benefit
Disable autofill of sensitive data	Turn off auto-save of card numbers, credentials	Prevents theft or misuse when the browser is compromised
Use a VPN on public Wi-Fi	Encrypt connection so others on same network can't snoop	Protects data from man-in-the-middle attacks

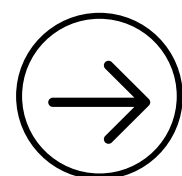
Iwuchukwu Augusta Chioma



# Key Safe Browsing Practices



Practice	What to Do	Why / Benefit
Be cautious with links & downloads	Don't click links from unknown sources; verify URLs before downloading	Prevents malware, phishing, drive-by downloads
Use a secure browser or privacy-focused browser	E.g. browsers built for privacy or with hardened security	Less exposure, better defaults
Clear cookies & cache regularly	Remove stored web data periodically to reduce tracking	Reduces persistent tracking and data footprint







**Share, like and  
follow for more  
Cybersecurity  
awareness tips**

**Iwuchukwu Augusta Chioma**