



Module 10

Safe Internet Browsing



Learning Objectives



RECOGNIZE THE RISKS OF
UNSAFE BROWSING.



USE SECURE WEB
BROWSING PRACTICES.



IDENTIFY SIGNS OF
MALICIOUS WEBSITES.



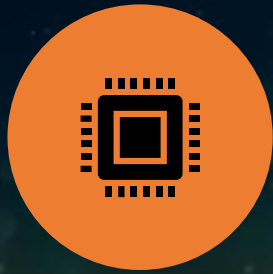
UNDERSTAND THE
IMPORTANCE OF BROWSER
UPDATES AND EXTENSIONS.



Why Safe Internet Browsing Matters



Risks of Unsafe Browsing



PHISHING WEBSITES: TRICKS
USERS INTO REVEALING
PERSONAL OR FINANCIAL
INFORMATION.



MALICIOUS POP-UPS: MAY
DOWNLOAD MALWARE WHEN
CLICKED.



UNSECURED WEBSITES: LACK
HTTPS ENCRYPTION.



EXCESSIVE TRACKING:
COMPROMISES PRIVACY
THROUGH COOKIES AND
TRACKERS.



Secure Web Browsing Practices

- ❖ Always check for HTTPS in the website URL.
- ❖ Avoid clicking on suspicious links or ads.
- ❖ Use private/incognito mode for sensitive activities.
- ❖ Log out from accounts after use on shared devices.



Recognizing Malicious Websites



Spelling errors in domain names (e.g., "goggle.com" instead of "google.com").



Unnecessary pop-ups or excessive advertisements.



Lack of contact information or privacy policy.



Warnings from your browser or antivirus software.





Browser Extensions for Safety

Ad Blockers: Prevent malicious ads (e.g., uBlock Origin).

Anti-Phishing Tools: Warn against suspicious sites (e.g., Norton Safe Web).

Password Managers: Generate and store secure passphrases.

VPN Plugins: Encrypt internet traffic for privacy.





Importance of Browser Updates

- Fixes security vulnerabilities.
- Improves browsing speed and functionality.
- Provides protection against new threats.
- Update all installed plugins and extensions regularly





References

- ❖ <https://www.kaspersky.com/resource-center/preemptive-safety/top-10-preemptive-safety-rules-and-what-not-to-do-online>

