Safe internet browsing includes the following best practices:

- **Keep your browser software up-to-date: This is crucial, as new patches are often released to fix existing vulnerabilities in browser software.**
- **Scan files before downloading: It is important to avoid downloading anything until you're confident that it is secure. If you have any suspicion that a file may not be legitimate or may be infected, scan it with antivirus software before downloading.**
- **Don't reuse passwords: Using the same password for multiple sites only makes it easier for attackers to compromise your sensitive information. Instead, keep track of your different passwords with a handwritten list that you keep in a safe place or come up with your own algorithm for creating unique passwords that only you would know. It is also recommended that you change your passwords every 90 days.**
- **Disable stored passwords: Nearly all browsers and many websites in general offer to remember your passwords for future use. Enabling this feature stores your passwords in one location on your computer, making them easier for an attacker to discover if your system gets compromised. If you have this feature enabled, disable it and clear your stored passwords.**
- **Use HTTPS: The "s" in "https" stands for secure, meaning that the website is employing SSL encryption. Check for an "https:" or a padlock icon in your browser's URL bar to verify that a site is secure before entering any personal information. Visit only trusted sites with valid security certificates.**
- **Read privacy policies: Websites' privacy policies and user agreements should provide details as to how your information is being collected and protected as well as how that site tracks your online activity. Websites that don't provide this information in their policies should generally be avoided.**
- **Turn on your browser's popup blocker: Popup blocking is now a standard browser feature and should be enabled any time you are surfing the web. If it must be disabled for a specific program, turn it back on as soon as that activity is complete.**
- **Avoid public or free Wi-Fi: Attackers often use wireless sniffers to steal users' information as it is sent over unprotected networks. The best way to protect yourself from this is to avoid using these networks altogether.**