 **Understanding Cybersecurity and Safe Internet Browsing**

 In today’s digital age, the internet has become an integral part of our lives. From social networking to online shopping and remote work, the web offers unparalleled convenience. However, with great convenience comes significant risk. Cybersecurity has become more critical than ever, as malicious actors continually develop new ways to exploit vulnerabilities and access sensitive information. Understanding how to protect yourself online is no longer optional—it’s a necessity. Understanding cybersecurity and practicing safe internet browsing are essential steps to protect your personal information and digital assets.

**What is Cybersecurity?**

 Cybersecurity refers to the practice of protecting systems, networks, and data from digital attacks, theft, or damage. These attacks come in various forms, including malware, phishing, ransomware, and hacking. The primary goal of cybersecurity is to ensure the confidentiality, integrity, and availability of information.

**Key Components of Cybersecurity**

**1. Confidentiality**: Ensuring that sensitive information is accessible only to authorized individuals.

**2. Integrity:** Safeguarding information from being modified or changed by unauthorized parties.

**3. Availability:** Ensuring that information and systems are available when needed.

**Common Cyber Threats**
Understanding the common types of cyber threats can help you know them and avoid them:
 **Phishing:**

Cybercriminals use fake emails, messages, or websites to deceive people into providing sensitive information such as passwords or credit card details.
**Malware:**

A malicious code, such as viruses, worms, and trojans that is developed to cause harm or destroy systems.
**Ransomware:**

A category of malware that encrypts a victim's data to demand payment for the decryption key.
**Man-in-the-Middle (MITM) Attacks:**

The interception of communications between two parties with the aim of stealing data.

**Social Engineering:**

Using psychological manipulations to get individuals to compromise their confidential information.

**Browser Extensions and Add-ons**:

Malicious browser extensions may introduce vulnerabilities or engage in unauthorised data collection.

**Cross-Site Scripting (XSS)**:

Attackers inject malicious scripts into webpages, exploiting vulnerabilities to steal sensitive information from unsuspecting users.

**Browser Hijacking**:

 Unauthorised changes to browser settings can redirect users to malicious websites or inundate them with unwanted ads.

**Guidelines for Safe Internet Surfing**
To stay safe online, one must be vigilant and practice best practices. Here are some tips to improve your online security:

**1. Use Strong Passwords**: Create unique, complex passwords for each account. Use a combination of uppercase and lowercase letters, numbers, and special characters.
**2. Disable Browser Password Saving**: Avoid relying on browser-based password saving features to prevent unauthorised access to your credentials.

**3. Enable Two-Factor Authentication (2FA):** Two-Factor authentication is an additional security measure

that requires a second step of verification, like a text message code or a biometric scan.

**4. Avoid Clicking on Suspicious Links and Downloading Attachments:** Do not click on suspicious links or download attachments from unknown sources. Confirm the identity of the sender before acting.
 **5. Update Software Regularly:** Update your operating system, browser, and other software regularly to patch vulnerabilities that cybercriminals could exploit.

**6. Use Secure Wi-Fi Networks:** Avoid using public Wi-Fi for sensitive activities, such as online banking. If you must use public Wi-Fi, use a VPN to encrypt your connection.

**7. Install Antivirus and Anti-Malware Software:** Use reputable antivirus software to detect and remove malware. Keep it updated to ensure optimal protection.

**8. Understand Privacy Settings:** Review the privacy settings of your social media accounts and online services to control who sees what information.

**9. Identify Phishing Scams:** Be wary of unsolicited emails or messages asking for your personal details. Look out for phishing by means of generic greetings, misspelled words, or strange URLs.

**10. Back Up Your Files:** Always back up essential files on an external drive or in cloud storage. This will ensure that your data can be recovered if a ransomware attack or system failure occurs.

**11. Learn and Teach Others:** Stay updated on the latest cyber threats and safe browsing practices. Share this information with family and friends to promote a culture of cybersecurity awareness.
 **Conclusion:**
 At Athena Global School, we frequently organize workshops, seminars, and interactive sessions to educate students about safe internet practices and the latest cyber threats, encouraging our students to apply these lessons in their daily digital activities.

 The internet is a powerful tool, but it also presents numerous risks. Understanding cybersecurity and having safe browsing habits can reduce one's vulnerability to cyber threats.

**Prepared by :** Sarannya.R