1. According to the ENISA Threat Landscape report for 2023, what emerges as the primary threat within cyberspace? Why is this particular threat deemed particularly alarming? Furthermore, based on the insights provided in the document, what strategies are recommended to effectively mitigate this threat?
   Answer:

The ENISA Threat Landscape report for 2023 identifies two main threats: **Ransomware and Denial-of-Service (DoS) attacks**. While the report doesn't definitively rank one above the other, ransomware appears to be a growing concern. Here's why:

- **Prevalence:** The report indicates ransomware accounts for a significant portion (around 34%) of cyber threats within the EU.
- **Increased Sophistication:** Attackers are employing more advanced tactics like "double extortion" (stealing data before encryption) and targeting supply chains to gain wider access.
- **Rising Impact:** These factors combine to make ransomware attacks more disruptive and costly for organizations.

Here's how the ENISA report suggests mitigating ransomware threats:

- **Regular Backups:** Having up-to-date backups allows restoring data without succumbing to extortion demands.
- **Software Updates:** Keeping systems and applications patched with the latest security updates eliminates vulnerabilities attackers exploit.
- **Employee Training:** Educating staff on identifying phishing attempts and social engineering tactics can significantly reduce the risk of infection.
- **Incident Response Plan:** Having a predefined plan for responding to ransomware attacks minimizes downtime and damage.

2. outline some of the Cyber Swachhta Kendra recommended best practices for securing personal computers.

   Answer:

The Cyber Swachhta Kendra emphasizes several best practices for securing your personal computer:

- **Think Before You Click:** Don't rush into clicking on links or opening attachments in emails or messages, even if they seem to come from familiar sources. Take a moment to verify their legitimacy.
- **Beware Security Warnings:** Don't ignore alerts and warnings from your security software or operating system. These might flag suspicious activity that needs attention.
- **Strong Passwords:** Create strong, unique passwords for all your accounts and enable two-factor authentication where available.
- **Software Updates:** Keep your operating system, applications, and security software updated with the latest patches to address vulnerabilities.
- **Antivirus Protection:** Install a reputable antivirus program and schedule regular scans to detect and remove malware.
- **Backups:** Regularly back up your important data to a secure external drive to avoid permanent loss in case of ransomware attacks.
- **Disable AutoPlay:** This prevents automatic execution of files from removable drives or network shares, potentially containing malware.
- **USB Security:** Be cautious when inserting USB drives and only use them from trusted sources. Consider using tools like "USB Pratirodh" to control access and scan for malware.