Q1: 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?

The **ENISA Threat Landscape 2023** report highlights several critical insights regarding the cybersecurity threat landscape. Let's delve into the specifics:

1. **Primary Threat**:
   - **Ransomware** emerges as the primary threat within cyberspace, constituting **34% of all threats** in the European Union.
   - Following closely behind are **Distributed Denial of Service (DDoS) attacks**, accounting for **28%** of the threats.
2. **Alarming Aspects of Ransomware**:
   - Ransomware is particularly alarming due to its **widespread impact** across various sectors.
   - Sectors most affected by ransomware include:
     - **Manufacturing** (14%)
     - **Health** (13%)
     - **Public administration** (11%)
     - **Services** (9%)
3. **Mitigation Strategies**:
   - To effectively mitigate the ransomware threat, consider the following strategies:
     - **Regular Backups**: Maintain frequent backups of critical data to minimize the impact of ransomware attacks.
     - **Security Awareness Training**: Educate employees about safe online practices and how to recognize phishing attempts.
     - **Network Segmentation**: Isolate critical systems from the rest of the network to limit lateral movement during an attack.
     - **Patch Management**: Keep software and systems up-to-date to address vulnerabilities that ransomware exploits.
     - **Incident Response Plan**: Develop and test an incident response plan to swiftly handle ransomware incidents when they occur.

Remember that proactive measures and a comprehensive approach are essential in safeguarding against ransomware threats in our increasingly interconnected digital world.

Q2: Visit the website www.csk.gov.in and outline some of the recommended best practices for securing personal computers.

Certainly! When it comes to securing personal computers, following best practices is crucial to protect against cyber threats. Here are some **recommended security measures** from the **Cyber Swachhta Kendra (CSK)**:

1. **Use Licensed and Genuine Software**:
   - Always use legitimate and licensed software to reduce the risk of vulnerabilities and malware.
   - Avoid downloading cracked or pirated software, as they may contain hidden threats.
2. **Keep Your System Updated**:
   - Regularly apply security patches and updates to your operating system and software.

    - These updates often address known vulnerabilities and enhance overall security.
3. **Install and Maintain Antimalware Solutions**:
    - Install reliable antivirus and antimalware software.
    - Keep it updated to detect and prevent malicious software from infecting your system.
4. **Disable Autoplay/Autorun for Removable Drives**:
    - Disable the automatic execution of files when you connect USB drives or other removable media.
    - This prevents potential malware from spreading through autorun features.

Remember that proactive security practices significantly reduce the risk of cyberattacks and help keep your personal computer safe and secure