

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

- **Ransomware:** These attacks encrypt a victim's files, making them inaccessible. Criminals then demand a ransom payment to decrypt the data. ENISA reports a significant rise in 2023, with ransomware accounting for over half of reported incidents. The potential for data loss and disruption to critical services makes them highly damaging.
- **DoS Attacks:** These attacks overwhelm a system with traffic, making it unavailable to legitimate users. DoS attacks can disrupt critical operations and cause significant financial losses.

The ENISA report highlights several strategies to mitigate these threats:

- **Software Updates:** Keeping operating systems and applications updated with the latest security patches is crucial to address vulnerabilities exploited by attackers.
- **Backups:** Regularly backing up data provides a safety net in case of ransomware attacks. Storing backups securely, offline, prevents them from being encrypted alongside the original files.
- **Network Segmentation:** Dividing networks into smaller segments can limit the impact of a DoS attack by preventing it from overwhelming the entire system.
- **Security Awareness Training:** Educating users on how to identify and avoid phishing scams can significantly reduce the risk of ransomware infections.
- **Incident Response Plans:** Having a plan in place for how to respond to a cyberattack can minimize damage and downtime.

By implementing a layered approach that combines technical measures and user awareness training, organizations can significantly improve their resilience against these prevalent cyber threats.

2. Visit the website [www.csk.gov.in](http://www.csk.gov.in) and outline some of the recommended best practices for securing personal computers.

1. Keep Software Updated:

- Regularly update the operating system, applications, and antivirus software to patch security vulnerabilities.

2. Use Strong Passwords:

- Create strong, unique passwords for each account and use a password manager to store them securely.

3. Enable Firewall Protection:

- Activate the built-in firewall or use a reputable third-party firewall to monitor and control incoming and outgoing network traffic.

4. Install Antivirus/Anti-Malware Software:

- Install reputable antivirus and anti-malware software and keep it up to date to protect against viruses, spyware, and other malicious software.

5. Enable Automatic Updates:

- Turn on automatic updates for both the operating system and installed applications to ensure you receive the latest security patches.

## 6. Use Secure Browsing Practices:

- Avoid clicking on suspicious links or downloading files from unknown sources.
- Use HTTPS-enabled websites for secure browsing, especially when entering sensitive information.

## 7. Enable Encryption:

- Encrypt sensitive data stored on your computer, especially if it contains personal or financial information, using tools like BitLocker (Windows) or File Vault (macOS).