

Safety Measures in Using Information Technology

In today's digital world, IT security is of paramount importance to protect sensitive data and information. Let's explore the key safety measures we can adopt.

Presented By: Meenu Pathak
Faculty e-Governance, CGG,
DRSTUAoA



Why is IT Security Important?

1 Data Protection

IT security safeguards against unauthorized access, ensuring the confidentiality, integrity, and availability of data.

2 Identity Theft Prevention

By protecting personal information, IT security helps prevent identity theft and financial fraud.

3 Business Continuity

Robust IT security measures minimize the risk of cyber incidents and ensure continuous operations.

Types of IT Security Threats

Malware Attacks

Viruses, worms, and ransomware pose significant threats to IT systems and can cause data loss or financial damage.

Phishing Scams

Fraudulent emails or messages trick unsuspecting users into revealing sensitive information or installing malware.

Social Engineering

Manipulative techniques used by hackers to deceive individuals into sharing confidential data or performing unauthorized actions.



Common Safety Measures

2. Two-Factor Authentication (2FA)

Add an extra layer of security by requiring a verification code in addition to your password.

4. Firewalls and Antivirus Software

Install and maintain firewalls and antivirus software to detect and prevent unauthorized access and malicious software.

1

2

3

4

1. Strong and Unique Passwords

Create complex passwords and avoid using the same password for multiple accounts.

3. Regular Software Updates

Keep your operating systems, applications, and security patches up to date to fix vulnerabilities.

Best Practices for Safe Browsing and Email Usage

- Use secure, encrypted connections (HTTPS) when accessing websites or email servers.
- Avoid clicking on suspicious links or downloading attachments from unknown sources.
- Be cautious with sharing personal information on social media or public platforms.
- Regularly review privacy settings in browsers and email clients to enhance security.



Importance of Backing Up Data

1

Protection Against
Data Loss 

Regularly back up your important files to an external hard drive, cloud storage, or network-attached storage (NAS).

2

Recovery from
Cyber Attacks 

Having backups enables faster recovery in case of ransomware attacks or data breaches.

3

Accidental Deletion
Prevention 

Ensure you can easily restore files that were unintentionally deleted or modified.

Conclusion and Key Takeaways

Protecting ourselves and our digital assets requires a proactive approach. By implementing these safety measures, we can mitigate IT security risks and safeguard our online experiences.