TOOL KIT

Student Cybersecurity Toolkit

Privacy on Public Networks

Avoid accessing sensitive accounts or sharing personal information when connected to public Wi-Fi networks. Consider using a Virtual Private Network (VPN)

2FA

Enable 2FA wherever possible. 2FA adds an extra layer of security by requiring a second form of verification (text message or University authenticator app).

Regular Software Updates

Keep operating systems, browsers, and all software updated to patch security vulnerabilities. Enable automatic updates to ensure you're always protected

Browsing Safety

Install a reputable ad blocker. Avoid clicking on suspicious links or downloading files from unknown sources. Use HTTPS-enabled websites for secure data transmission.

Cybersecurity

Empowering Students for a Safer Digital Journey: Your Essential Guide to Online Security

Email Security

Be cautious with email attachments and links if they're unexpected and avoid phishing attempts by verifying the sender's email address before clicking on any links.

Data Backup

Regularly back up important files and documents to an external hard drive or a secure cloud service and enable automatic backups to ensure your data is always up to date

Anti-Malware Software

Install a reputable antivirus program and keep it updated. Schedule regular scans of your computer to detect and remove malware.

Password Security

Use a mix of uppercase and lowercase letters, numbers, and symbols and avoid using easily guessable information like birthdays or names.