

BASIC DIGITAL SAFETY

Sagar Gai
ID:2416876
Date: 19/11/24



INTRODUCTION: This poster highlights things to keep your digital safety in the context of the growing usage of the Internet and other media.

USE STRONG PASSWORD

- Create complex passwords with a mix of letters, numbers, and symbols.
- Avoid easily guessable information, such as birthdays or simple sequences.
- Consider using a password manager for secure storage.



ENABLE 2-FACTOR AUTHENTICATION



- Add an extra layer of protection by enabling 2FA on all critical accounts.
- Use apps like Google Authenticator or Authy for generating secure codes.

BE AWARE OF PHISHING SCAMS

- Verify email senders and check for suspicious links before clicking.
- Avoid sharing personal or financial information over email.
- Look for red flags, like urgent language or unfamiliar attachments.



UPDATE SOFTWARE REGULARLY

- Keep operating systems, browsers, and applications up-to-date.
- Enable automatic updates to ensure you're protected against the latest threats.



SECURE YOUR WI-FI CONNECTION

- Regularly back up important files to secure locations.
- Consider using cloud services with robust security measures.



BACK UP YOUR DATA

- Use strong passwords for your Wi-Fi networks.
- Avoid using public Wi-Fi for sensitive transactions. Use a Virtual Private Network (VPN) if needed.

CONCLUSION: By implementing these practices, you can significantly reduce your risk of cyber threats and ensure a safer, more secure digital experience

