PROTECT YOUR PHONE

PROTECT YOUR DATA

IMPACT MAKING WOMEN

QUICK GUIDE:

Protecting Your Data on Your Phone

1. Set a Strong Lock Screen

- Use a PIN, password, or biometric authentication (fingerprint or face recognition).
- Avoid simple PINs like 1234 or birth dates.

2. Enable Two-Factor Authentication (2FA)

- Add an extra layer of security for your accounts.
- Use apps like Google Authenticator or Authy.

3. Keep Your Software Updated

- Always update your operating system and apps to patch security vulnerabilities.

4. Avoid Public Wi-Fi for Sensitive Transactions

- Use VPN when connecting to public networks.
- Do not log in to banking or sensitive apps on public Wi-Fi.

5. Download Apps from Trusted Sources

- Use Google Play Store or Apple App Store only.
- Avoid third-party or unverified app stores.

6. Regularly Backup Your Data

- Enable cloud backups or use external drives.
- In case of loss, you can restore your data.

7. Turn Off Bluetooth and Location When Not in Use

- Prevent unauthorized tracking or pairing with your device.

8. Watch Out for Phishing Links and SMS

- Do not click on suspicious links.
- Verify messages before responding or entering sensitive details.

9. Use Strong, Unique Passwords

- Avoid reusing passwords across multiple accounts.
- Use a password manager for better security.

10. Install a Trusted Security App

- Use antivirus or mobile security apps to detect threats.