everyday identity

10 Essential 'Be Safe' Personal Devices Checklist

1. Set a Strong Device Passcode ☐

Use a long, complex passcode to prevent unauthorized access.

2. Enable Device Encryption ☐

Encrypt your device to safeguard your data from physical breaches.

3. Keep Your Device Updated ☐

Regularly install software updates to patch security vulnerabilities.

4. Install Apps from Trusted Sources Only ☐

Download applications exclusively from official app stores to minimize malware risks.

5. Review App Permissions ☐

Regularly check and limit app permissions to ensure they access only necessary information., adjust as desired.

6. Enable Remote Wipe and Tracking Features ☐

Activate features like "Find My Device" to locate or erase your device if it's lost or stolen.

7. Use a Virtual Private Network (VPN) ☐

Utilize a VPN when connecting to public Wi-Fi networks to encrypt your internet traffic.

8. Disable Unused Connectivity Features ☐

Turn off Bluetooth, Wi-Fi, and NFC when not in use to reduce potential attack vectors.

9. Regularly Back Up Your Data ☐

Maintain backups of important data to recover information in case of device loss or failure.

10. Be Cautious with Public Charging Stations ☐

Avoid using public USB charging stations, as they can be compromised to steal data; use your own charger and plug into a power outlet instead.