Device and Account Security Basics - Checklist

Device Security Essentials

- Set a strong PIN, password, or biometric lock

- Enable auto-lock after a short period of inactivity

- Turn on full disk encryption

- Disable Bluetooth, location, and Wi-Fi when not in use

- Keep your OS and apps updated

Install Security Tools

- Use built-in or trusted antivirus/anti-malware tools

- Use a firewall or network monitor

- Back up data to encrypted drives or secure cloud storage

Account Protection Best Practices

- Use a password manager to generate unique passwords

- Avoid using personal info in passwords

- Never reuse passwords across services

- Enable two-factor authentication (2FA)

- Prefer app-based or hardware key 2FA over SMS

- Enable 2FA for email, banking, and cloud accounts

Review and Maintain Your Accounts

- Delete unused or duplicate accounts

- Revoke access for third-party apps you no longer use

- Update security questions and recovery options

Device Hygiene Tips

- Restart your phone weekly to clear background tracking

- Avoid unnecessary apps or browser extensions

- Only install apps from trusted sources

- Use browser privacy extensions (e.g., uBlock Origin)