iPhone/Android script

1. Use Screenlocks, Passcodes, and Biometrics

- iPhone
    - Settings > Face ID (or Touch ID) & Passcode
    - Will say 'Set up Face ID or Touch ID'
    - Require Attention
    - Turn on and set up passcode
    - Require Passcode
    - Erase data?
    - Settings > Display & Brightness > Auto-Lock
- Android
    - Settings > Security and privacy > Lock screen > Screen Lock
    - Go back - > Fingerprints
    - Settings > Lock Screen > Smart Lock

2. Activate Find My iPhone/Device

- iPhone
    - Settings > [your name] > Find My
    - Turn on 'Find My network' and 'Send Last Location'
    - Find Devices - Apple iCloud – Mark as Lost and Erase This Device
        1. Mark As Lost locks your screen with a passcode and lets you display a custom message with your phone number to help you get it back. You can also remotely erase your device if needed. Your custom message continues to display even after the device is erased.
    - Stolen Device Protection - Settings > Face ID (or Touch ID) & Passcode
        1. Turn on Stolen Device Protection
- Android
    - Settings > Google > Find My Device
    - www.android.com/find

3. Keep Device and Apps Updated

- iPhone
    - Settings > General > Software Update
        1. Turn on 'Automatic Updates'
        2. Automatically Install iOS and Security
    - Settings > App Store >App Updates
    - Or App Store > Click Profile picture > Manually update
- Android
    - Settings > Software update > System update preferences > Smart update
    - Google Play Store > Profile icon > Settings > Network preferences > Auto-update apps

4. Keep Your Identity Secure

- iPhone
  - Settings > [your name] > Sign-In & Security >Two-Factor Authentication
    1. Set Up Security Keys
  - Use Passkeys for other websites – PayPal on iPhone
- Android
  - Settings > Google > Manage your Google Account > Security (tab at top) > 2-Step Verification – also, Passkeys and security keys
  - Also, Settings > Accounts and backup > Manage accounts

5. Only Connect to Secure Wifi or use a VPN

- iPhone
  - Settings > Wi-Fi
    1. Look for lock icon
    2. Ask to Join Networks – Notify or Ask
    3. Click on connected network and turn off 'Auto-Join'
  - Settings > VPN
    1. Will have to install GlobalProtect or another VPN app
    2. Connect to GlobalProtect
- Android
  - Settings > Connections > Wi-Fi
    1. Look for lock icon
    2. Auto reconnect
  - Settings > Connections > More connection settings > VPN

6. Use Strong Passwords and Protect Them

- iPhone
  - Settings > [your name] > iCloud > Passwords & Keychain
  - Settings > Passwords> Security Recommendations > Detect Compromised Passwords
    1. Also 'Password Options'
  - Lastpass demo
- Android
  - Settings > General management > Passwords and autofill > Google > Password Manager
    1. Or Settings > Google > Manager Your Google Account > Security (tab) > Password Manager
  - Settings > Google > Manager Your Google Account > Security (tab) > See if your email address is on the dark web

7. Protect Your Privacy - Review App Permissions and Sharing

- iPhone
  - Settings > Privacy & Security > Safety Check > Manage Sharing & Access
- Android

        - Settings > Security and privacy > App Security
        - Settings > Security and privacy > Privacy > Permission manager

8. Encrypt Your Device/Data

- iPhone
    - Settings > Face ID (or Touch ID) & Passcode > scroll down to bottom – 'Data Protection is enabled'
    - 'Erase Data' – after 10 failed
    - Remotely erase – Find My
    - Settings > [your name] > iCloud > Advanced Data Protection
- Android
    - Same as iPhone – default encryption if passcode is set.
    - Settings > Security and privacy > Secure Folder
    - Settings > Security and privacy > Other security settings > Encrypt SD card
    - Remotely erase - https://www.google.com/android/find/

9. Backup Your Data

- iPhone
    - Settings > [your name] > iCloud > iCloud Backup
- Android
    - Settings > Accounts and backup > Back up data

10.Don't fall for Phishing or Smishing

- iPhone
- Android
    - Settings > Google > Manage your Google Account > Security (tab) > Enhanced Safe Browsing