Mobile Device Usage

Do This	Not That
Use a strong password, pattern, or biometric authentication; enable the screen lock; and use a password manager.	Reuse passwords for multiple websites, write down passwords, or share passwords.
Regularly review and update security settings on all devices, social media, and cloud storage sites.	Have a “set it and forget it” attitude toward security settings.
Disable Bluetooth and Wi-Fi when not needed; use the device’s cellular network in public areas.	Connect to untrusted public Wi-Fi networks.
Install OS and app updates as soon as they’re available. Enable automatic updates when possible.	Avoid updates “because they may slow down my device.”
Disable app access to your camera, microphone, location, etc., when not needed.	Grant device admin rights to apps.
Remove apps you don’t use, install only from native app stores, and avoid apps that access personal information.	Download or install apps from unknown app stores or untrusted sources.
Protect data stored in the cloud. Set privacy restrictions on personal files and use two-factor authentication.	Use the default security settings for cloud storage.
Review privacy settings for all Internet-ready devices before connecting them to the web.	Use default passwords/security settings for Internet-ready devices or use the same password across devices.
Enable privacy settings on social media and GPS tracking apps, use enhanced security controls, and set up alerts.	Accept friend requests on social media from people you don’t know, automatically publish GPS location information, or use GPS in sensitive areas.
Limit posting personal information (e.g., birth date, home address, Social Security number) on social media.	Post sensitive information online (including location photos), share your travel itinerary, or “check in.”
Create a secure wireless home network with a strong password and encryption.	Leave default passwords on your home networks or devices.
Maintain physical control of your devices in public areas.	Leave your device in a public place out of reach.
Before clicking on a link, decide if it’s expected, valid, and trusted.	Click links in messages from unknown contacts.

Think privacy. Think protection. Think security.

For more information, visit https://cyber.mil