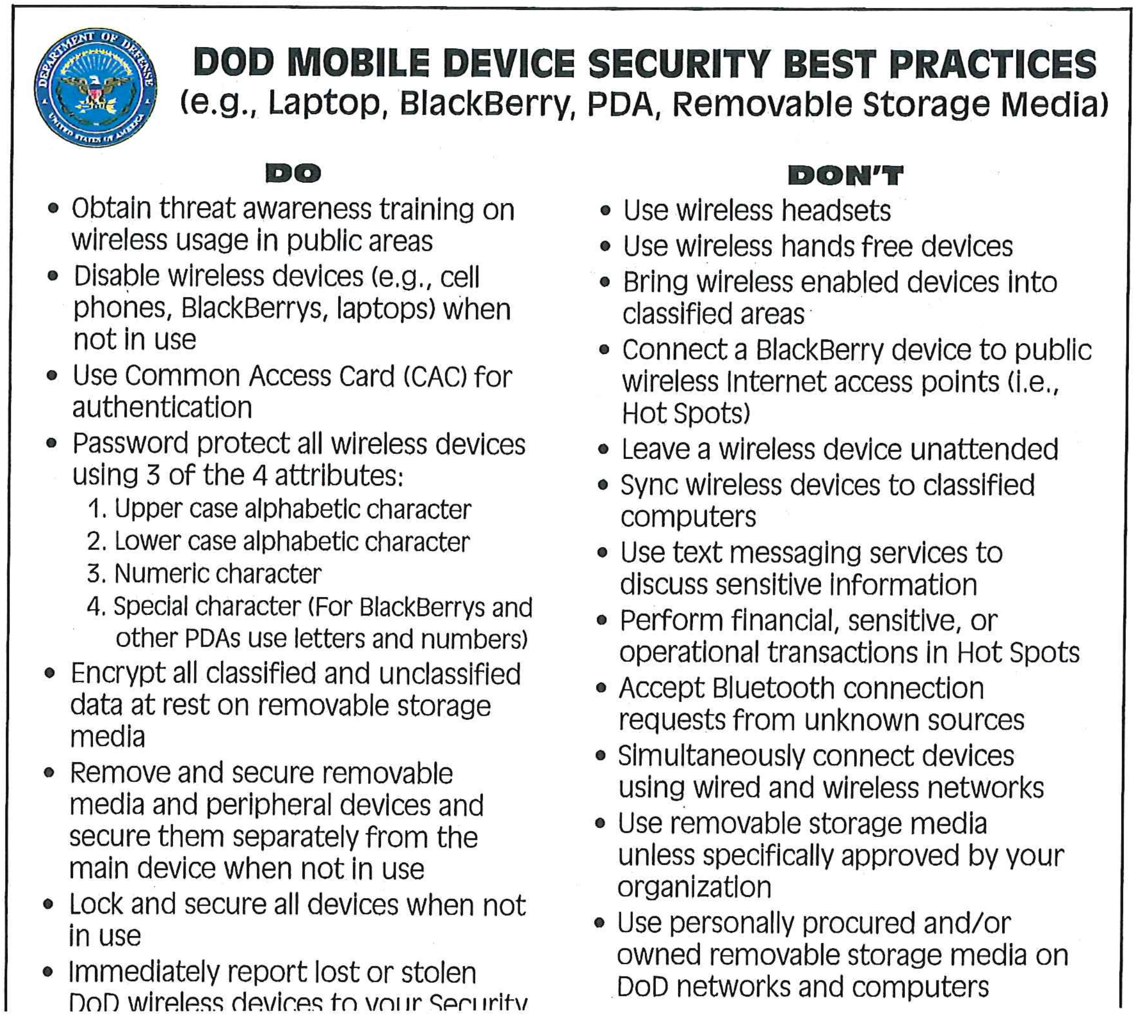
DOD COMPUTING SECURITY BEST PRACTICES

DO

- Take the DoD IA Awareness Training which details best security practices and current threats (https://osdportal.osd.mil/rs/training09/iaa/launchpage.htm)
- Use digital signatures for DoD email
- Use encryption for performing financial sensitive/operational transactions and when transferring Personal Identification Information (PII) (e.g., SSN, DOB)
- Notify your Security Manager when traveling OCONUS to ensure all electronic devices have the latest security updates
- Obtain threat brief before traveling OCONUS
- Consider taking a back up or loaner electronic device on OCONUS travel
- Clear electronic devices of unneeded data before travel
- Remove battery and media cards from electronic devices when going through security check points
- Have electronic devices checked by Security Manager after OCONUS travel
- Remove your CAC from devices when you are not physically present
- Report suspicious emails and/or activities

DON'T

- Transfer data using commercial web email (e.g., GMail, Yahoo)
- Download files from commercial web email or entertainment sharing sites to DoD computers
- Open emails from unknown users
- Open suspicious email
- Assume security is enabled on public wireless Internet access points (ie., Hot Spots)
- Discuss sensitive information in public spaces
- Place electronic devices in checked bags
- Use unknown computers for charging DoD devices (e.g., USB chargers)
- Have DoD devices serviced by unauthorized personnel
- Use DoD procured and/or owned removable storage media on non-government networks and computers
- Move data between unclassified and classified computing devices using removable media
- Use the preview mode in your email viewer
- Click on pop-up messages or unknown links



DOD MOBILE DEVICE SECURITY BEST PRACTICES

(e.g., Laptop, BlackBerry, PDA, Removable Storage Media)

DO

- Obtain threat awareness training on wireless usage in public areas
- Disable wireless devices (e.g., cell phones, BlackBerrys, laptops) when not in use
- Use Common Access Card (CAC) for authentication
- Password protect all wireless devices using 3 of the 4 attributes:
  1. Upper case alphabetic character
  2. Lower case alphabetic character
  3. Numeric character
  4. Special character (For BlackBerrys and other PDAs use letters and numbers)
- Encrypt all classified and unclassified data at rest on removable storage media
- Remove and secure removable media and peripheral devices and secure them separately from the main device when not in use
- Lock and secure all devices when not in use
- Immediately report lost or stolen DoD wireless devices to your Security

DON'T

- Use wireless headsets
- Use wireless hands free devices
- Bring wireless enabled devices into classified areas
- Connect a BlackBerry device to public wireless Internet access points (i.e., Hot Spots)
- Leave a wireless device unattended
- Sync wireless devices to classified computers
- Use text messaging services to discuss sensitive information
- Perform financial, sensitive, or operational transactions in Hot Spots
- Accept Bluetooth connection requests from unknown sources
- Simultaneously connect devices using wired and wireless networks
- Use removable storage media unless specifically approved by your organization
- Use personally procured and/or owned removable storage media on DoD networks and computers