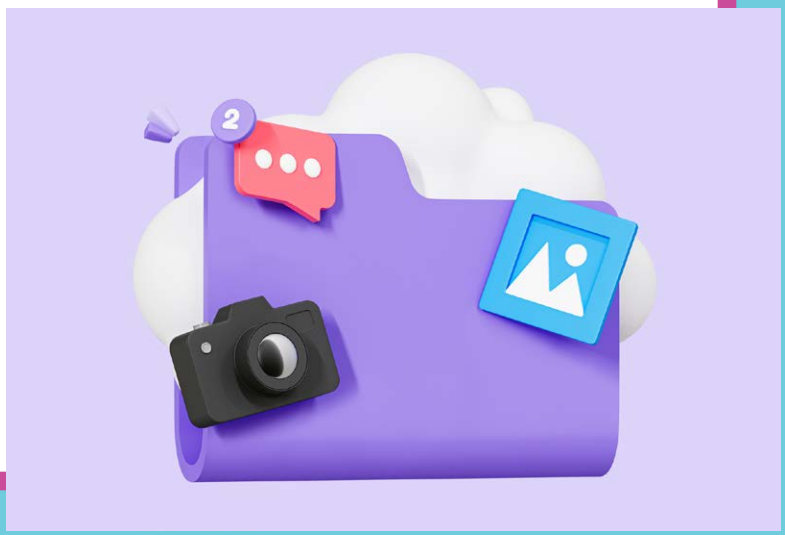
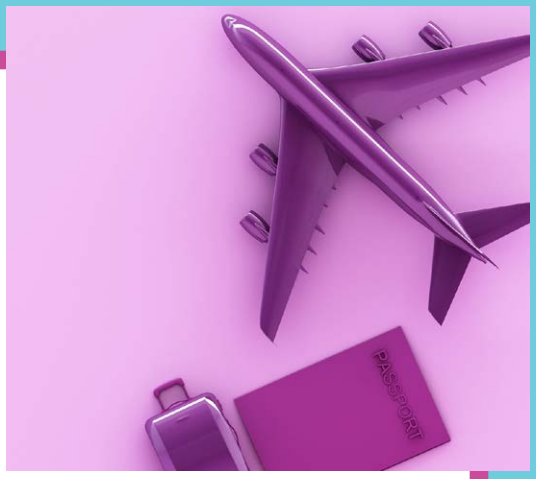
Keep Your **Government-Furnished Devices** Secure

Office of Information Technology
Division of Information Security
MARCH 2024

As spam, phishing, smishing, vishing, malicious apps, and ransomware increase mobile threats, our increasing reliance on mobile devices for both personal and professional use means that it is now more important than ever to prioritize mobile device security. Use the following essential tips to enhance the security of your mobile devices (e.g., laptops, smartphones, tablets):

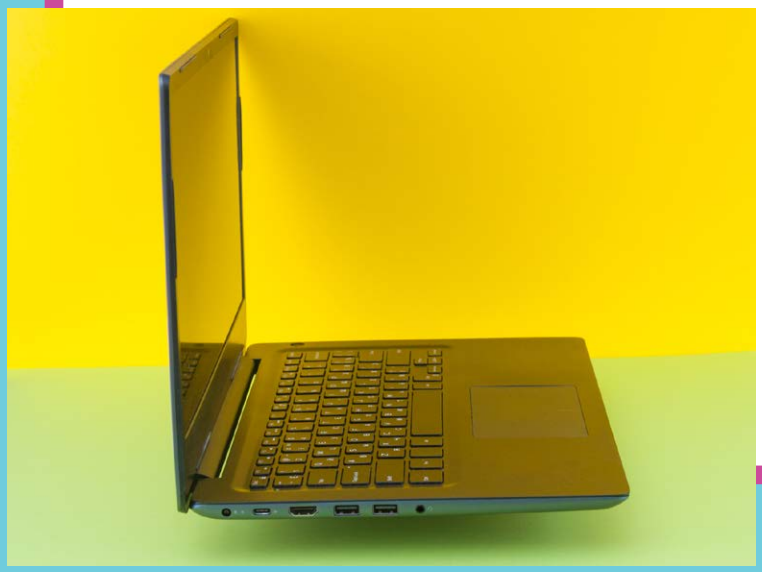
- **Take Physical Security Measures:** Set up a strong passcode/personal identification number on your government-furnished equipment (GFE) device to prevent unauthorized access. This serves as the first line of defense in case your device is lost or stolen. Never share your device passcode/personal identification number.
- **Update Your Software:** Update your GFE device's operating system, apps, and security patches as soon as possible or when the Indian Health Service (IHS) Information Technology personnel informs you an update is available. These updates often contain crucial security fixes that address vulnerabilities exploited by cyber attackers.
- **Use Secure Connections:** Use only secure Wi-Fi connections to minimize security risks and keep malicious actors from intercepting your data. When not directly connected to the IHS network, use the IHS virtual private network (VPN) for IHS business, as it encrypts your internet connection and protects your data during transmission.
- **Secure Your Apps:** In order to maintain a strong security posture with your mobile devices, download only IHS-approved apps from the "Apps Catalog" on your GFE. Before installing an app, review its permissions and grant access to only the necessary functions and data. Never download apps from any third-party source. Please be advised that TikTok is not allowed on GFE devices. Be aware that the app may silently install in the background if you open a TikTok link on your GFE device. For additional information see the following Memorandum: Memorandum M-23-13 "No TikTok on Government Devices" Implementation.
- **Back Up Your Data:** Regularly backup any data on your mobile device to the IHS network to protect your data in case you lose your device or if it is stolen or malfunctions. This ensures that you can easily retrieve your information and minimize the impact of a security incident. If you use an Apple ID on your GFE device, create one specifically for your GFE device using your IHS.GOV email address. Do not use the same Apple ID for personal iOS devices and GFE devices. For additional information, see the following Knowledge Base Article: How to Activate a New iPhone.





All IHS mobile device users must:

- Follow the IHS Rules of Behavior regarding limited personal use of their GFE mobile device.
- Read and understand the Mobile Device Justification and User Agreement and the consequences for violating the agreement.
- Not carry permanently-issued GFE devices during foreign travel, which the IHS specifically prohibits. See the HHS Memorandum – USE of GFE During Foreign Travel for further information.
- Encrypt all federal data and use a virtual private network for all information transferred to or from their mobile devices. The IHS prohibits the transfer of federal information over unencrypted networks.
- Agree to not display any IHS-issued mobile device passwords in public or attach passwords to any device.
- Minimize their downloading and storing of authorized sensitive information to the least amount of information needed to perform IHS official business.
- Not transmit unencrypted federal information or sensitive information (e.g., Personally Identifiable Information, Protected Health Information, and Controlled Unclassified Information) over guest wireless networks, including the IHS and HHS guest wireless networks.
- Manually deactivate Wi-Fi when not using their GFE to prevent automatic connections.
- Keep devices within sight or place them in a secure container (e.g., purse, backpack, carryon bag) under your personal control and within sight at all times. Do not leave them unattended at any time or ask others to attend to them for you.
- Store devices in a secure location such as a locked office or private home, locked desk drawer or file cabinet, tethered to furniture using a cable lock, etc.
- Do not leave devices in automobiles in plain sight; store them in a locked trunk that is not visible from outside.
- During air or train travel, do not place devices in checked baggage unless required by the Transportation Security Administration (TSA) or other air travel security authorities.



By following these tips, you can significantly enhance the security of your mobile devices and safeguard your sensitive information from potential threats. Stay aware, vigilant, and proactive in protecting your devices to maintain security, your privacy, and your peace of mind in an increasingly connected world. You must immediately report all lost, stolen, or compromised GFE mobile devices to your Area ISSO or the IHS Cybersecurity Incident Response Team at Incident@ihs.gov. If immediate contact is not possible, users should contact the IHS IT Service Desk (888-830-7280) within 24 hours of the reported loss.

Please note: Some of the links in this newsletter can only be accessed while logged in to the IHS network. If you are unable to open a link or have any other questions, please contact Cybersecurity@ihs.gov.