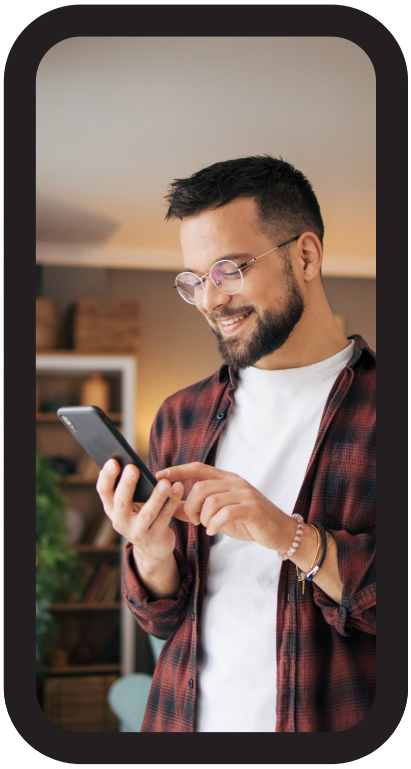
Practicing Good **Text Messaging** *and* **Mobile Device** *Security*

Office of Information Technology
Division of Information Security
APRIL 2025

Short Message Service (SMS), popularly called text messaging, is generally considered less secure than other forms of communication. SMS is transmitted over the cellular network and can be intercepted or eavesdropped on by unauthorized parties. Therefore, protecting your Government-Furnished Equipment (GFE) and personal cell phone from hacking is important, and involves a combination of good practices, using built-in security features, and staying vigilant. Here are key tips to help with keeping your mobile devices secure:



1. Use Strong Authentication and Authentication Apps

- Set a strong password or PIN: Avoid easy combinations like “123456” or “000000.”
- Enable biometric authentication: Use fingerprint or facial recognition if available.
- Enable Multi-Factor Authentication (MFA) if it is offered to secure accounts linked to your phone.
- For even more security, use Authenticator apps like Google Authenticator or Okta Verify, if available, to securely login to your accounts.

2. Keep Software Updated

- Update your devices and apps: Regular updates fix security vulnerabilities and ensure all apps are the latest version to avoid exploitation of old version vulnerabilities.

3. Download Apps Safely

- Use the official app platforms: On GFE, download only IHS-approved apps from the “Apps Catalog”. While using your personal cell phones, use Google Play and the Apple App Store.
- Avoid downloading apps from unknown sources, sometimes called “sideloading”. Downloading apps from unknown sources increases risk.
- Check app permissions: Only grant necessary permissions.

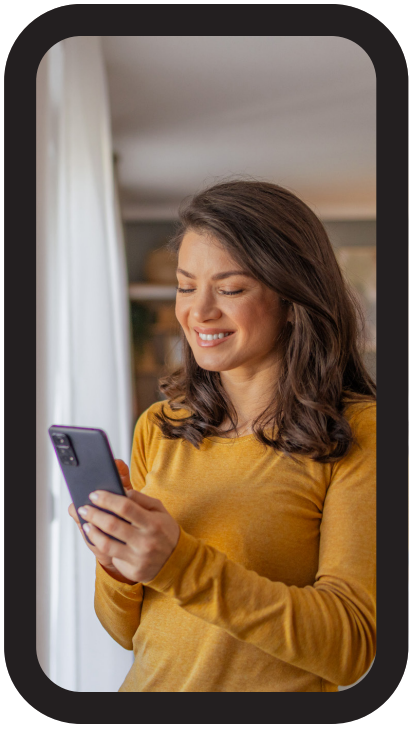
4. Secure Your Internet Connection

- Avoid public Wi-Fis: Instead, use your mobile data or a trusted network.
- Use a VPN: Encrypt your data when using public networks.
- Turn off Wi-Fi, Bluetooth, and Near-Field Communication: Disable them when not in use.

5. Beware of SMS Phishing, SMS Spoofing, and Malware

- Don’t click on suspicious links: Especially in emails, texts, or social media messages.
- Avoid downloading attachments from unknown senders, these can carry malware.

6. Encrypt and Backup Your Data



- Enable encryption: Most modern phones encrypt data by default.
- On your personal device regularly back up your data: Use a secure cloud service or external storage.
- On your GFE, 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 malfunctioned. This ensures that you can easily retrieve your information and minimize the impact of a security incident. Using 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.

7. Monitor Your Device

- Check for unusual behavior: Slow performance, apps you don't recognize, or high data usage might indicate hacking.
- Log out of accounts, especially on shared or public devices.

8. Secure Your Accounts

- Enable remote wipe: If your personal phone is stolen, you can erase its data remotely.
- Use "Find My Device": Tools like, Google Find My Device, or Apple Find My iPhone, help track and lock your personal phone.

9. Use Security Tools

- Install anti-malware apps: Apps like Norton, McAfee, or Bitdefender can help protect your personal phone.
- Mobile GFE devices are equipped with CrowdStrike for protection.

10. Stay Informed

- The following websites can help you stay updated on the latest hacking techniques and understand how to recognize social engineering and other scams:
  - Stay Safe Online
  - Cybersecurity and Infrastructure Security Agency
  - Federal Trade Commission

SMS is not end-to-end encrypted, so it can be intercepted and read by the network or other third parties. By combining these measures, you can significantly reduce the risk of hacking your cell phone. Official business should only be conducted and discussed over GFE. SMS should never be used to discuss official business as it is never secure.

NOTE: *The links and products in this document are for informational purposes only, and do not signify an endorsement.*

For questions or further information, please contact the IHS Office of Information Technology, Division of Information Security, at cybersecurity@ihs.gov.