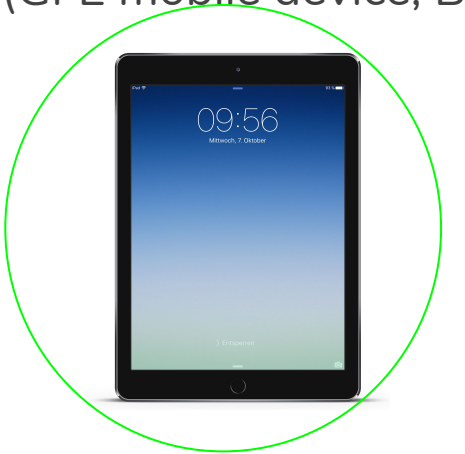
Mobile Device Security for the Home User

Are Your Mobile Devices Secure?

What is a mobile device?

Excludes Laptops - Includes tablets and mobile phones running a mobile operating system (GFE mobile device, BYOD, Personal)



Use of Personally Owned Mobile Devices with GSA's Data

Ways to use your personally owned mobile device securely:

Horizon - Virtual Desktop

Citrix - Access to many GSA applications (need SecureAuth installed first)

GSA Mail - Log into your GSA email with SecureAuth and a One Time Password

Use of GFE Mobile Devices and BYOD (Bring Your Own Device)

- GFE - Centrally Managed by GSA and is configured with the following applications added: MaaS360, Google, and Lookout
- BYOD - Bring Your Own Device
  - Submit a Service Catalog Request
  - Include a signed GSA Rules of Behavior for Personally Owned Mobile Devices form
  - Back up your personal data
  - MaaS360, Google Policies, Lookout will be installed

Cybersecurity for Mobile Devices

2017 was marked “the worst year ever” for security breaches according to Thales and The Online Trust Alliance.

Cybersecurity for your Mobile Device - What is at risk here?

Possible effects on our data:

- Loss of Confidentiality
- Loss of Integrity
- Loss of Availability

Cybersecurity for Mobile Devices - Why was 2017 the worst year for breaches?

- Stealthy Attackers
- Advanced Persistent Threats (APTs)
- Zero Day Threats

Applications on Mobile Devices - Did you know!?

The most **dangerous** types of malware often come from **infected applications!**

Applications on Mobile Devices

- Only install necessary applications
- Configure device to install apps only from trusted source
- Some applications request access to your device’s files/camera/location, etc. thus exposing your data.
- Remove unnecessary applications
- Keep applications up to date by enabling auto updates

Trusted Sources for your Mobile Device - iOS Devices

Download and Install only

apps from the trusted Apple

App Store

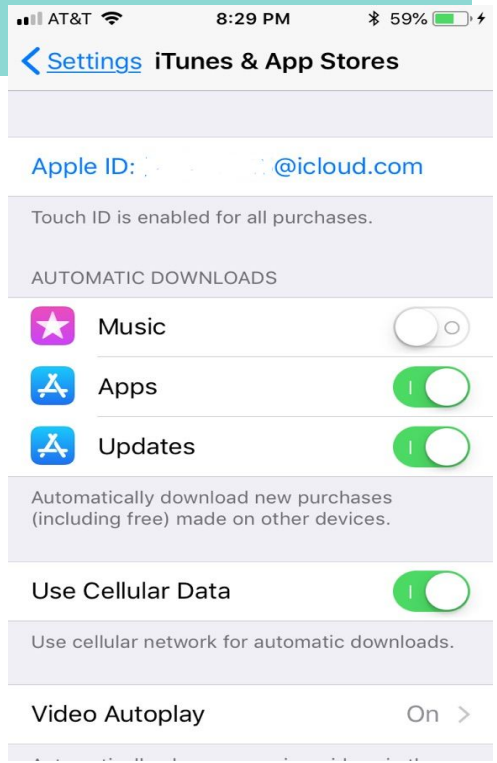
Trusted Sources for your Mobile Device - Android Devices

- With the default configuration on your Android smart devices, you can only install the apps that you have downloaded directly from the Google Play Store.
- After you tap the ‘Install’ button of any app that you have located on the Google Play Store, the app will automatically be downloaded on your Android smartphone/tablet, and installs without any further intervention except the ones that ask for your permission to access your information stored in your device.

Enabling app auto updates for your Mobile Devices - iOS

3 Easy Steps to enable auto-updates

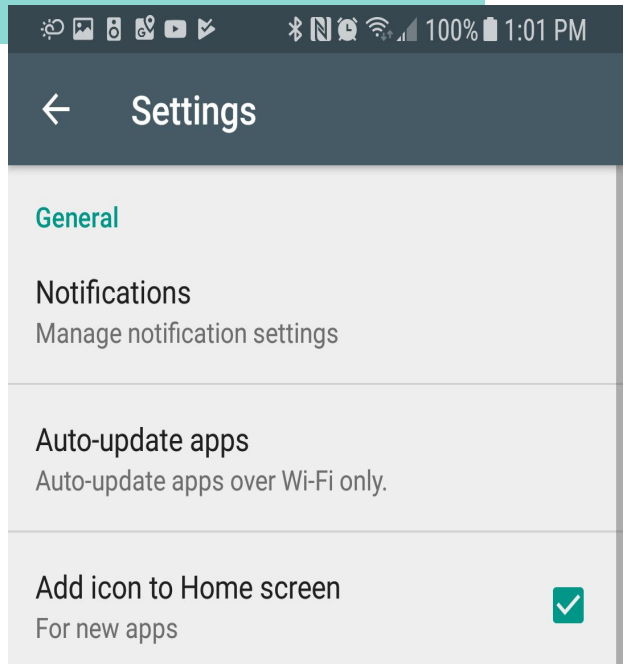
1. Tap on Settings
2. Swipe down and tap on *iTunes & App Store*
3. Tap the toggle next to *Updates* to turn it on/off



Enabling app auto updates for your Mobile Devices - Android

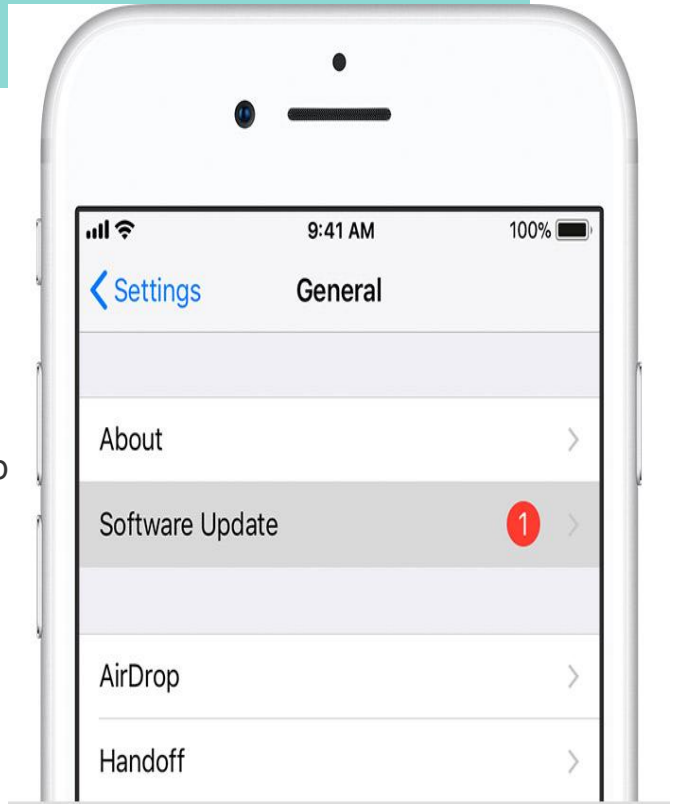
5 Easy Steps to enable auto-updates

1. Go to the Play Store
2. Tap the 3 bars icon in the upper left corner of screen
3. Tap on Settings
4. Tap auto updates apps
5. *Tap auto update apps over wi-fi only*



Operating System updates for Mobile Devices - iOS

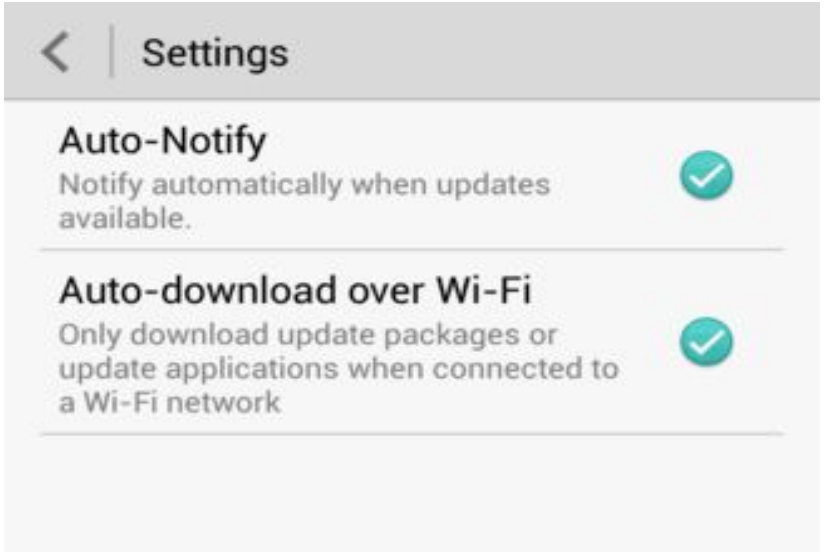
1. Plug your device into power and connect to the Internet with Wi-Fi.
2. Tap Settings > General > Software Update.
3. Tap Download and Install.
4. To update now, tap Install. Or you can tap Later and choose Install Tonight or Remind Me Later. If you tap Install Tonight, just plug your iOS device into power before you go to sleep. Your device will update automatically overnight.
5. If asked, enter your passcode



Operating System updates for Mobile Devices - Android

You can configure your Android smartphones to automatically download system updates and UI updates over Wi-Fi.

- Go to *Settings > About Phone > System Update*.
- Tap on the *Menu key > Settings*.
- Select "*Auto-download over Wi-Fi*".



AntiVirus Software on mobile devices - Continued

Antivirus software is one of the must haves on your mobile device if you hope to keep it secure!

- Scans and Detects Viruses
- Locates lost/stolen phones
- Scans downloaded apps for viruses
- Has backup options available

Avoid JailBreaking/Rooting your Mobile Device

What is Jailbreaking (for iPhones) and Rooting (for Androids) and why do we need to avoid it?

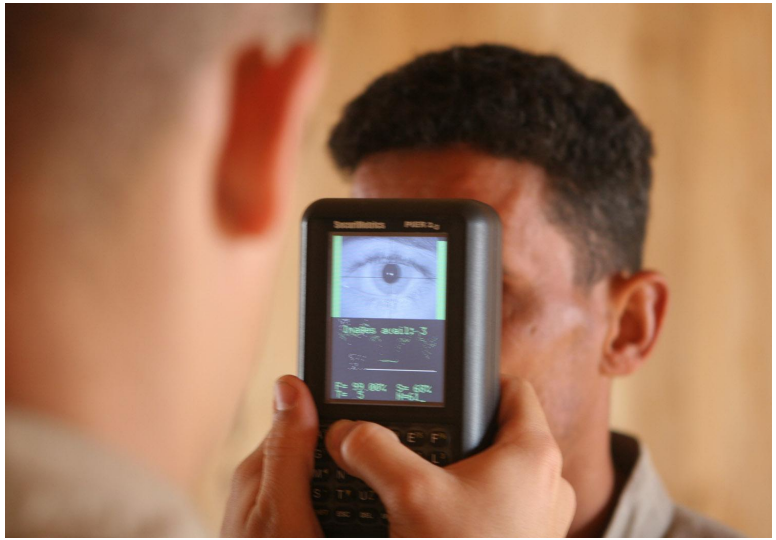
- Strips the device of built in programming that blocks certain actions from occurring
- Decreases Security - removes built in security
- Malicious apps can be installed
- Can turn your device into a “brick” if something goes wrong

Protection for your Mobile Devices- Lock your phone

Times sure have changed!

Just look at these keys, left right in the door! Everyone trusted everyone. Would you do that today!?

Screenlock your Mobile Device - Methods below

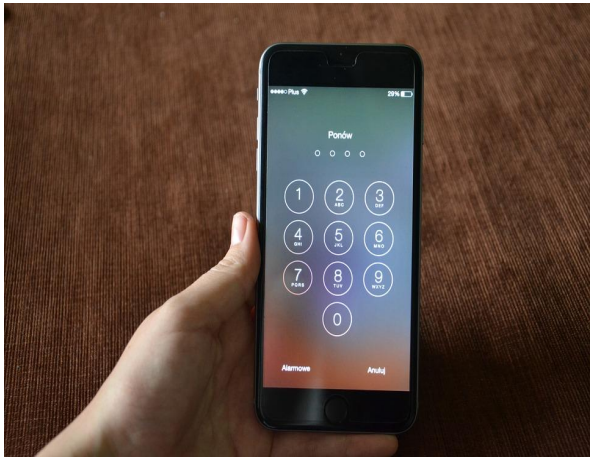


<u>Methods</u>:

- Strong password (can be used with encryption)
- Pin (can be used with encryption)
- Pattern
- Fingerprint
- Facial Scanner
- Iris Scanner

Encryption for your Mobile Device

One of the easiest methods any home user can take to increase the security of their mobile phone is to encrypt the files and data on their phone!



Encryption for your Mobile Device - Continued (iPhone Encryption)

For both types of devices (Apple and Android) start with a fully charged battery and backup your data prior to encryption.

1. Go to Settings on your iPhone
2. Go to touch ID & Passcode
3. Select turn passcode on.
4. Choose a strong passcode. The device will warn you if weak passcode is chosen.
5. Return to Settings menu - scroll down and you should see "Data protection is enabled."

Encryption for your Mobile Device - Continued (Android Encryption)

Ensure that a screen lock password or pin has been set for your device to ensure that your encryption is enabled.

1. In **Settings**, choose **Security** > **Encrypt Device**. (On some phones, you'll need to choose **Storage** > **Storage encryption** or **Storage** > **Lock screen and security** > **Other security settings** to find the "Encrypt" option).
2. Follow the onscreen instructions. During encryption, your device might restart several times.

Enable find my phone on your Mobile Device

Both iPhones and Androids can be located when lost or stolen through built in features.

On your iPhone

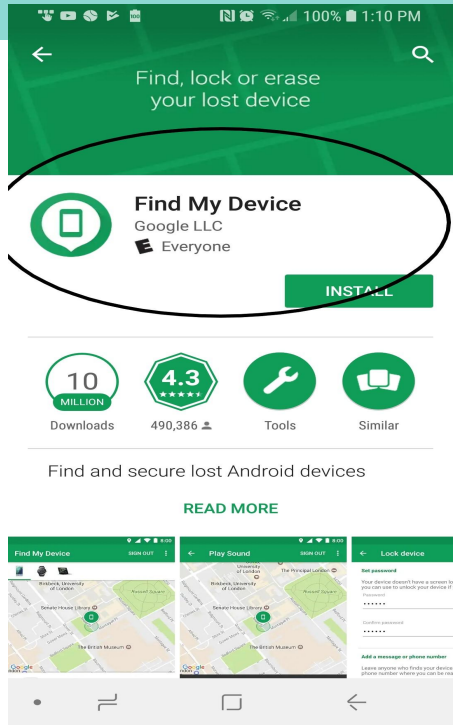
1. Start at your Home screen.
2. Tap Settings > [your name] > iCloud. If you're using iOS 10.2 or earlier, go to Settings > iCloud.
3. Scroll to the bottom and tap Find My iPhone.
4. Slide to turn on Find My iPhone and Send Last Location.

Install find my device on your Mobile Device - Android

How to locate and remotely wipe Androids

Setting it up

1. Go to the Play Store
2. Search “Find My Device”
3. Select Install on “Find My Device”
4. Open and follow prompts



Unsolicited Calls or messages on your Mobile Device

Unsolicited Calls and Messages:

- Illegal
- Attempt to steal something from you
- DO NOT ANSWER OR REPLY
- DO NOT CLICK ON LINKS

Summary - Securing your Mobile Device

Top easy cybersecurity tips for your mobile device to increase security immediately:

- Install Antivirus software
- Application management
- OS updates
- Avoid jailbreaking/rooting your device
- Encrypt your device
- Use secure screenlock - not easy password or easy pin
- Enable find my device
- Do not answer unsolicited calls/texts or download/click on links
- Last, but not least, do not forget - only connect over trusted and secure wireless connections, turn off bluetooth when not being used, and keep your personal devices safe and know where they are at all times.

End of Day Tasks for GFE, Personally Owned and BYOD Mobile Devices

- Check for updates!
  - Operating System
  - Applications
  - Antivirus
- Run Antivirus scan
- Log off of GSA applications

Question & Answer Time!

Please send any Questions to:

ACISSO@GSA.GOV

Helpful Resources

Visit Insite - Go to: Topics > Information Technology > Do It Yourself > Mobile Devices (Phones, Tablets)(Self Help): Tons of information on configuring your device for things we discussed today like auto updates for your mobile device, GSA commonly used Apps, Reporting a lost/stolen phone, BYOD, etc!

IT Service Desk can be reached at: Email - ITServiceDesk@gsa.gov or Call: 866-450-5250

Assessment and Compliance ISSO (ACISSO): ACISSO@gsa.gov

Mobile Device Management Team Email: mobile-device-support@gsa.gov