Keep your information safe, wherever you are with an Android device.

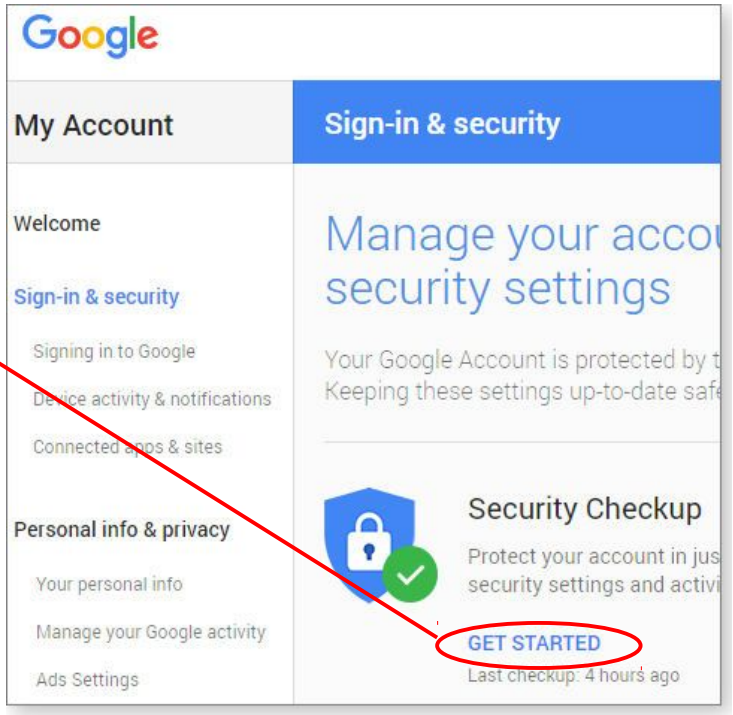
Step 1: *Run a basic Google-security audit*:
Google recently rolled out a revised, centralized site that makes it easier to:
- review, adjust, and control the security features of
- both Google accounts and Android devices.

In your browser (preferably Chrome), go to the **Sign-in & security** page , (https://myaccount.google.com/intro/security?utm_source=OGB&pli=1)

(My Account/Sign-in & security)
Sign in to your account, if requested.

Work through the "Sign-in & security" site step by step, top to bottom.

Begin by clicking the **Get Started** button under **Security Checkup.**



a) Follow the prompts to review or alter
- your account-recovery information,
- check the list of connected devices (ensuring that only authorized devices are accessing your account), and
- access to account permissions.

b) Next, run the **Find your phone** function, which lets you locate a misplaced or stolen Android phone (actually, a phone, tablet, or laptop); setups to:
- remotely trigger the phone's ringer to attract attention or to help find the phone,
- remotely sign out (enabling whatever sign-in lock you've previously set),
- and, as a last resort , remotely-erase the data on a lost or stolen phone.
- There's also a link that helps you contact your carrier and have the phone's SIM card deactivated, which will prevent the phone from connecting to the network.

c) Continue working through the "Sign-in & security" page. The **Signing in to Google** section lets you audit your Google account's security, including:
- its password strength,
- enable/disable two-step verification (aka two-factor authentication; more info (https://en.wikipedia.org/wiki/Two-factor_authentication)

(which can make it much harder for any unauthorized person to access your account details or use your phone).

d) The **Device activity & notifications** section shows:
- any recent security events that were logged;
- also shows devices that recently used your account;
- lets you alter security-alert settings.

Continue down the page, checking the "Connected apps & sites" section.
While you're at it, check others settings in the My Account section such as:
- "Personal info and privacy" and
- "Account preferences."

e) When you're sure everything's okay on the Google end of things, it's time to work directly on the phone itself. Whew!

Step 2. *Verify Android version and security-patch level*:
(usually under Settings/System/About device): You should always have the latest version available of Android and Security Patches for your specific model.

Android Operating System version:
a) As of this writing, the newest hardware runs Android **6.x** (aka Version "M" or "Marshmallow").
b) Older hardware might require earlier Android versions.
Check on your phone manufacturer's site or your carrier's support site to see what's been released for your specific hardware.
c) You can see the general versions available on the Wikipedia page https://en.wikipedia.org/wiki/Android_version_history, or "The Android Story." at https://www.android.com/history/#/marshmallow.

Android Security Patch Level (further down the "About device" page).
Much like Microsoft, Google now releases security patches monthly; Android-hardware makers and telecommunications carriers then process the patches and release custom versions (if required) for specific brands and models of phones.
a) Check the latest-available security-patch level for your phone on the Android Security Bulletin page:
https://source.android.com/security/bulletin/index.html
b) If your phone isn't running the latest level for your hardware, contact your carrier for an update.

Step3. *Check sign-on security*: especially when traveling:

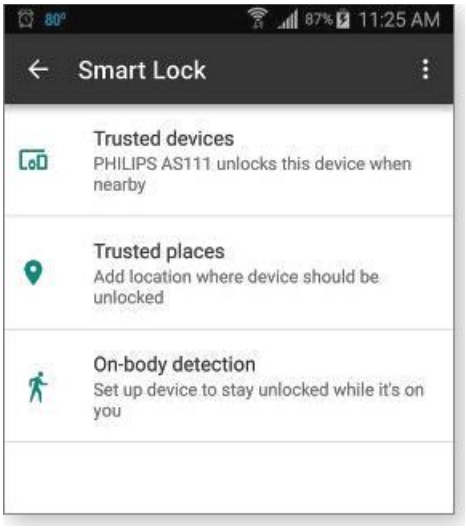
a) ensure your phone is set to lock itself quickly when not in use.

b) set it to display a lock screen;

c) require a PIN, pattern, password, fingerprint, or other form of authorized unlocking before it — and the data it contains — can be accessed.
(typically found under **Settings/Security/Lock screen,** though,
the exact words might vary slightly from phone to phone).

d) consider disabling Android's ***Smart Lock*** feature),
(automatically unlocks your phone if in a location
- you've designated safe,
- or if it's on your person such as in a pocket or purse).

Reason: to help prevent a phone-snatching thief from possibly bypassing the phone's lock — for example, by keeping the phone in motion.



Step 4. *Prepare for malware attacks*:

All mobile devices need to have anti-malware software installed and up to date.

For general information, there was a July 10, 2014 Windows Secrets article: Top Story, "Mobile security: Apps to protect Android devices." more articles:

Tom's Guide article, "Best antivirus software and apps 2016,"

Android Authority's review, "15 best antivirus Android apps and anti-malware Android apps."

Visit the Google Play online store (https://play.google.com/store) and search for "anti-malware" and/or "security."

Step 5. *Install a VPN*: Using a free virtual private network app/service can preserve your privacy and security when using public or hotel Wi-Fi networks. When you're connected to a VPN server, the rest of the Net sees only a temporary address for your system, hiding your real IP address.

For more information and an example, see the Dec. 10, 2015, Windows Secrets Field Notes column, "Taking a free VPN service for a drive."

For current product offerings, visit the Google Play store and search for "vpn."

Third-party product reviews and selection advice are available:

a) Android Authority's article "15 best Android VPN apps:" http://www.androidauthority.com/best-android-vpn-apps-577594/, and

b) Digital Trend's review "5 Best Android VPN apps for privacy and security:" http://www.digitaltrends.com/mobile/best-android-vpn-apps/.

Step 6. *Encrypt sign-in credentials — or the whole phone*:

Any of the many-available, better-rated password-manager apps can safely store your sign-in usernames and passwords in deeply encrypted forms (such as AES-256, generally considered uncrackable by today's hardware and software tools).

For current offerings, search for "password manager" in the Google Play store;

Guidance articles:

a) Tom's Guide article, "10 Best Mobile Password Managers,"

b) CNET's "Password Managers for Android" story.

With a password manager, even if someone steals or gains access to your phone, they still won't be able to do you much further harm because they won't be able to access sensitive information, such as through your banking app, shopping accounts, and so forth.

Step 7. *Attend to potentially sensitive tasks before you travel*:

a) Do as much financial, shopping, and other sensitive work or transactions from the relative safety of your home or office Wi-Fi.

b) Consider setting your bills to ***auto-pay*** while you're away, (instead of making payments from potentially unsafe public Wi-Fi on trip).

c) Use your VPN application to shop or do banking while on the road — and be sure to sign out of your session when you're done. (If you're not sure whether you're signed out, close your mobile browser and then reopen it.)

Step 8.1 *Plan for unreliable connectivity, possible roaming charges and data caps*:

a) review your carrier's coverage of the area you're traveling to;

b) set phone-data caps or permissions accordingly.

Typically, **Settings/data usage** lets you set warnings to alert you

- when you're roaming or are approaching your phone's data cap.
- settings might also be able to shut down non-Wi-Fi data use automatically when you switch to a high-priced network

or when your phone reaches the data limit you set.

These steps can help you avoid expensive roaming or data-cap charges.

Step 8.2 For GPS navigation while traveling, consider ***offline Navigation*** :

- lets you find your way using previously downloaded maps.
- you can navigate even in areas with no cell/data coverage at all.
- you might also save on roaming data charges.

a) Google Maps supports this mapping capability — https://support.google.com/maps/answer/6291838?hl=en

b) There are also over 100 offline navigation apps available in the Google Play store: https://play.google.com/store/search?q=offline%20navigation

For example, **HERE Maps** supports full voice-prompted, turn-by-turn GPS navigation, with no local data connection required. (https://play.google.com/store/apps/details?id=com.here.app.maps)

Step 9. *Back up everything just before you go*: Use:

a) a third-party app — or,
b) Android's free, built-in, cloud-based, backup function:
(typically accessed via "Settings/Backup and reset").

If enabled, Android's backup will automatically preserve:
- Wi-Fi-network passwords and settings,
- Google Calendar and Gmail settings,
- home-screen wallpapers
- apps installed through Google Play, photos, videos, and more.

(see the Android support page, "Back up or restore data on your device.")
(https://support.google.com/android-one/answer/2819582?hl=en)

c) you also can back up your phone's content to a PC:
As long as the phone's screen lock isn't engaged, Windows will usually recognize the phone as a media device and display its contents exactly as if the phone were an ordinary external drive.

Step 10. *Make sure your gear can be charged while traveling*:

a) Be sure you have at least one — preferably ***two*** — chargers and cords, and
b) Make certain they'll work with the electrical outlet shapes, voltages, and frequencies you'll encounter on your trip.

[This slide set is a paraphrase of the Windows Secrets Newsletter article by the same title, July 14, 2016. The article was written by Senior Editor Fred Langa.]