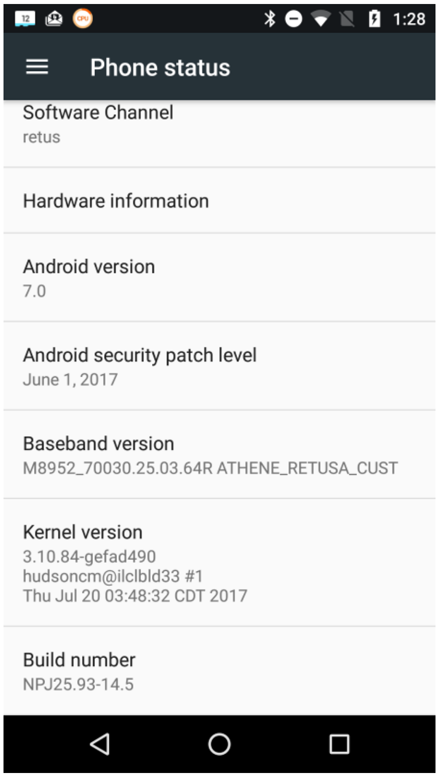
Securing Android

By Dick Maybach, Member, Brookdale Computer Users' Group, NJ

January 2018 issue, BUG Bytes

www.bcug.com
n2nd (at) att.net

Your PC remains at home behind locked doors, accesses the Internet through a firewall, and has its software updated regularly, but none of this is true of your Android device. If you haven't thought about its security, you are overdue to begin. We obtain PC software updates directly from the software vendors, e.g. Microsoft issues these for Windows. Google releases monthly security updates for Android, but the only end users that get them are owners of Google Nexus and Pixel devices. All others receive them through their device vendors and usually get them much later, if at all. To see the date of your last security update, go to Settings, then About phone (probably the last item). Figure 1 shows the lower part of the resulting screen. (This is for a Motorola G^4 using Android 7; screens on other configurations may differ.)



Phone status

Software Channel
retus

Hardware information

Android version
7.0

Android security patch level
June 1, 2017

Baseband version
M8952_70030.25.03.64R ATHENE_RETUSA_CUST

Kernel version
3.10.84-gefad490
hudsoncm@ilclbld33 #1
Thu Jul 20 03:48:32 CDT 2017

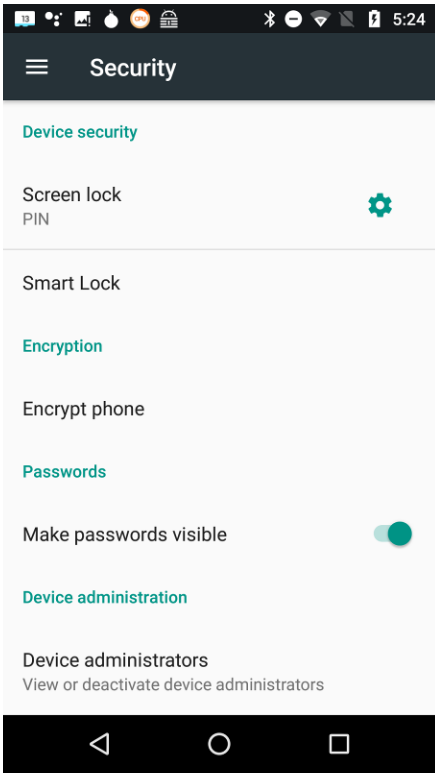
Build number
NPJ25.93-14.5

Figure 1. About Phone Screen

This shot was taken in November and shows that the latest security update had been made in June, which was not reassuring (although I did receive the September update later in November). Many security professionals believe that keeping software up to date is the most important security measure, more so than using anti-malware software.

That your Android phone is subject to damage and loss, probably runs on software with known vulnerabilities, and lacks protection from Internet aggressors are beyond your control, but there are things you can do to reduce your risk.

Be sure your phone is protected by going to Settings then Security and enabling screen lock; a password here is more secure but less convenient than a PIN. Don’t use None or Swipe, as these make your device fully accessible to anyone who picks it up. I don’t care for the Smart Lock features as they unlock your phone for extended periods. Making passwords visible isn’t as dangerous as it sounds, as it displays the only last character you enter and only for only a short time. I find it greatly reduces errors when entering passwords. I haven’t encrypted my entire device because all my sensitive data is encrypted separately. Figure 2 shows the upper portion of the security screen.



5:24

Security

Device security

Screen lock
PIN

Smart Lock

Encryption

Encrypt phone

Passwords

Make passwords visible ●

Device administration

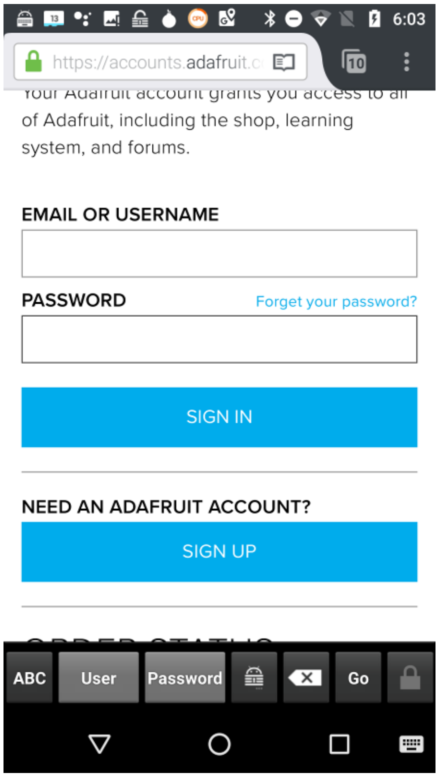
Device administrators
View or deactivate device administrators

Figure 2. Settings/Security Screen

Sanitize your browser favorites, especially if you sync them with your PC over the Internet. Review all your favorites. (With Firefox, open the menu, select Preferences, then Security, and finally Saved Logins…; for other browsers check the Internet.) Delete any, such as banks, that are sensitive, and the next time you log into one with a password, your browser will offer to save it. Select “Never for this site,” or the equivalent.

Use a password manager that stores its data in an encrypted database and use a non-trivial password for it. I like Keepass2Android Password Safe by Croco Apps, as it uses the same database as KeePass, KeePassX, and KeePassXC, which are available for Linux, OS X, and Windows. You can transfer the database file among all your devices.

Because it's encrypted, you could sync it using a cloud service, but I prefer not to so expose it. Keep all your sensitive information here, passwords, PINs, account numbers, passport numbers, etc. Figure 3 shows Firefox on a site's login page with KeePass2Android active.

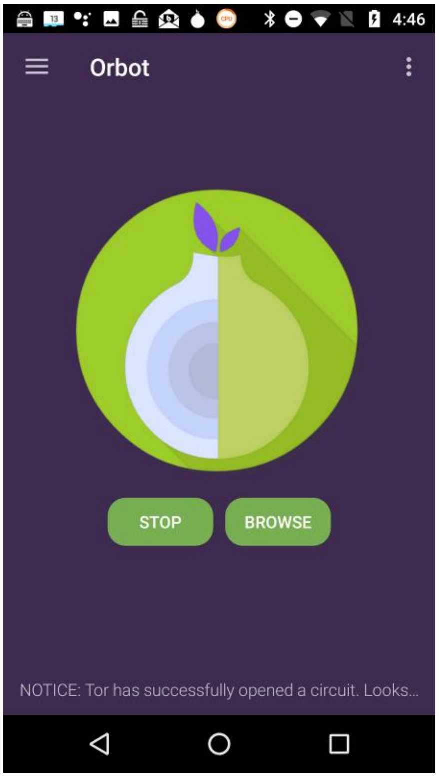


Your Adafruit account grants you access to all of Adafruit, including the shop, learning system, and forums.

Figure 3. Web Login Page with KeePass2Android Running.

To get to Figure 3, I opened KeePass2 and selected the Adafruit entry. Then when I launched Firefox and opened the Adafruit location, it displayed a keyboard icon in the bottom menu bar. I selected this and then selected the KeePass keyboard, which added a second lower-menu bar. Now placing the cursor in the Username box and tapping the User button (in the second lower-menu bar) causes KeePass to enter the name in that box. Then placing the cursor in the password box and tapping the Password button does the same for the password. (Of course, I had previously entered the Adafruit information, its URL, my username, and my password, in KeePass.) All this takes longer to describe than to do.

Be careful when using public wi-fi, as with readily-available software anyone on the same network can view every packet you send and receive. Fortunately, Tor is available for Android, and you should use it whenever you access the Internet using a public wi-fi hot spot. Install the app "Orbot: Proxy with Tor" from Everyone, which will ask that you install "Orfox; Tor Browser for Android, "also from Everyone. Orbot is a proxy that enables access to the Tor network, and Orfox a secure browser that uses Tor. When you use these, a wi-fi snoop will see only encrypted packets and won't know where they are going or from where they are coming. Figure 4 shows the opening Orbot screen. (While we’re considering networks, don’t ever set your device up as a portable hotspot, which makes it a server.)



NOTICE: Tor has successfully opened a circuit. Looks...

Figure 4. Orbot Opening Screen.

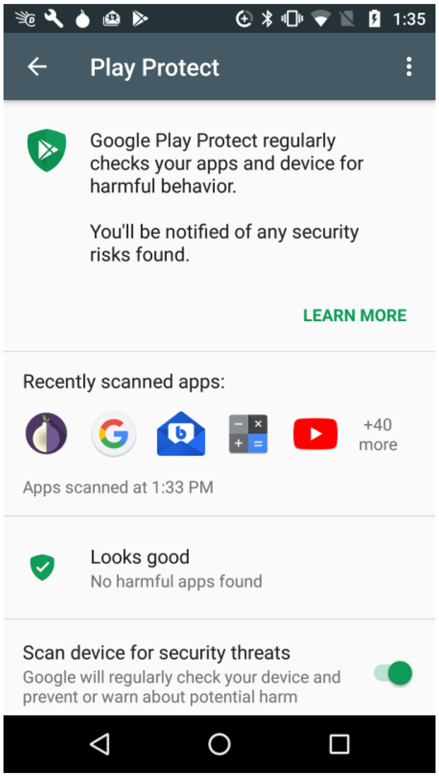
Because of its vulnerability, an Android device is not a safe place to store data. Don’t keep anything in it, unless its encrypted, that you wouldn’t write on a post-it stuck to the roof of your car. Encrypt anything sensitive, such as passwords and banking information, and as soon as it’s convenient, copy your new data to a PC. Although it’s not a security issue, be cautious about purchasing copyrighted items encumbered with Digital Rights Management (DRM) features. Some can be used only on a single device, which means if your phone is lost or damaged, you also lose these. See my December 2017 article (available at http://www.bcug.com) for sharing data among Android devices and computers.

Every app you install adds potential security vulnerabilities, and many consume resources even when they appear not to be running. Their icons clutter your screen, making it difficult to find other apps, and their files fill your storage space. Your device can become less usable with each visit to the Play Store. Google is a large, technically competent organization, with procedures that ensure that Android is a high-quality, secure product. However, this isn’t necessarily true of app developers, whose competence is unknown. Google performs security audits on all Playstore apps, and your risk of installing malware is just 0.05 per cent if download apps from only there, compared to an overall infection rate of 0.71 per cent. That an app is popular doesn’t mean it’s well-designed or safe. Take a disciplined look at your app collection and remove all you don’t use regularly. This is one of the most important security measures you can take.

Some apps add considerable risk. For example, some checkbook programs require linking to a bank account, and anyone now accessing your phone could potentially also access your bank account. If you really need this feature, you must secure your phone with a secure password, e.g. one that is long and difficult to guess, which of course will make using the device less convenient.

If you keep your Android data synced with your home computer, you can be casual about backing it up. Nevertheless, backing up may be good insurance if it also backs up your installed apps, since if you lose your phone, you could reinstall them on a new one.

Be sure Google Play Protect is operating by going to the Google Play Store app, selecting the menu (the icon at the left of the menu bar), and then Play Protect; the Scan device for security threats item should be turned on. See Figure 5.



Google Play Protect regularly checks your apps and device for harmful behavior.

You'll be notified of any security risks found.

Recently scanned apps:

Apps scanned at 1:33 PM

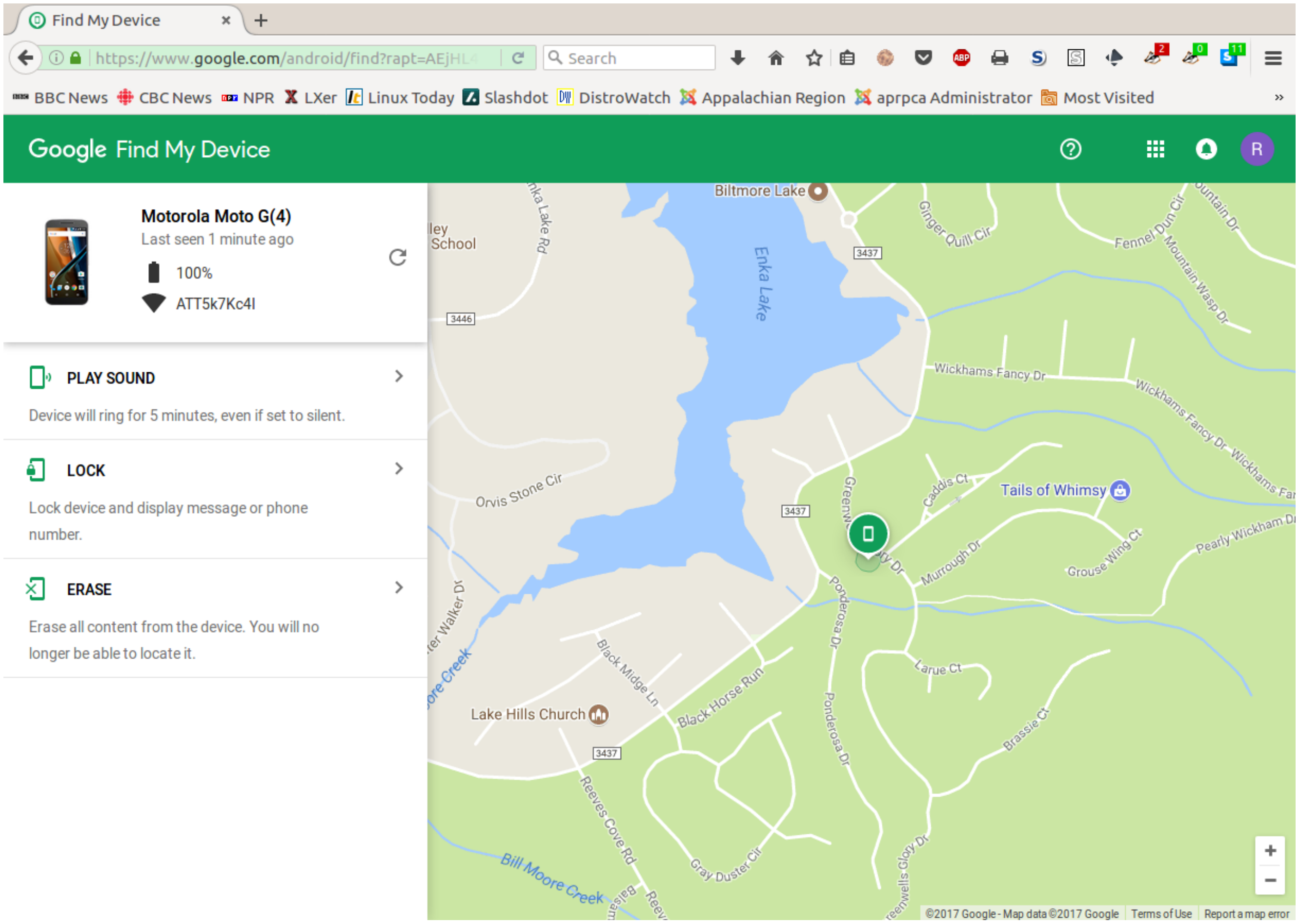
Looks good
No harmful apps found

Scan device for security threats
Google will regularly check your device and prevent or warn about potential harm

Figure 5. Google Play Protect Screen.

This checks apps as you download them and periodically scans your device for threats. I don’t think other anti-virus programs are needed. Android is less vulnerable than Windows, although “less vulnerable” is not the same as “invulnerable.” If you keep your device synced with your home PC, and protect any sensitive data with encryption, you haven’t much at risk. That an anti-virus vendor would like to sell you an app doesn’t mean you need one.

If your device is lost, you can use Google's Android Device Manager service to help you find it and to safeguard its data. Go to http://www.google.com/android/devicemanager and log in with your Google password. The eventual result will be the screen in Figure 6.



Motorola Moto G(4)
Last seen 1 minute ago
100%
ATT5k7Kc4l

PLAY SOUND

Device will ring for 5 minutes, even if set to silent.

LOCK

Lock device and display message or phone number.

ERASE

Erase all content from the device. You will no longer be able to locate it.

Figure 6. Google Android Device Manager.

This shows you the location of your lost device and gives you the options to have it make some noise (in case its misplaced), lock itself (if you expect to get it back), or wipe its memory (if you think it's gone forever), The last two won't get your phone back, but they will prevent whoever has it from using it or accessing your data. Note however, there is no way to undue the last.

With these few simple precautions you can significantly reduce the risks of using your Android device. For more information on Android security see http://source.android.com/security/.