Get dialed in on how to safeguard your smartphones

September 2 2013, by Paresh Dave

Remember the sneaky trick played by software makers? Download a free program and somehow it would automatically install an unwanted "search toolbar" on your computer's Internet browser. That annoying ploy hasn't disappeared on mobile phones. At least 50 million Android smartphones have downloaded a free application from the Google Play store called Brightest Flashlight Free that installs an unnecessary search feature on phones.

The app activates a phone's camera light when launched - helpful. But it also has by default permission to display ads, track the phone's location and take photographs and video. That means the makers of the app could see what users are doing and where they are.

Besides not falling for the download-the-free-app trick, what other protections should you consider for your mobile device?

First, turn on the "screen lock" function on your device. It's in the phone's "settings" menu. It's annoying to constantly unlock a phone, but smartphone makers say they are working on making it more of a natural process in future devices.

Next, remember to turn off GPS and Wi-Fi when you don't need them because they could be used by location-tracking apps to figure out where you are. The switches to turn them on and off are also in the settings menu.

Now, to the big question: Is there a need for anti-virus programs for mobile devices?

With iPhones and iPads, users have to entrust their privacy and protection solely to Apple Inc.

But with the Google Inc.-developed Android operating system, Google's policy of "openness" means not everything goes through the company. Security and anti-virus apps can bring Android smartphone and tablet owners some extra peace of mind.

Many of the apps are ahead of the curve compared with Google in providing usable information about how apps affect your mobile device, what data they collect and what happens to that information.

Google says it's not aware of any security holes in Android-powered devices that result in a need for outside help. But some customers may feel more comfortable having another layer of protection or the user's employer might require it, said Adrian Ludwig, Android's lead security engineer.

"We're very conscious of that, and nothing in any way prevents a user from having a second security product," he said.

Because Android users in the U.S. are familiar with Google and use it for most of their activities, including downloading apps, few run into issues. Foreign users are more likely to download phone viruses or malicious software that's typically designed to steal money from users.

Still, it's a smart move for everyone to go to the device's security settings screen and check the box next to "Verify apps." This will turn on Google's anti-virus protection.

Google says the most common threat is apps that secretly bill a user's credit card by sending a "premium" text message to a hacker. The charge appears on cellphone bills but is often overlooked. The latest version of Android warns users several times that an app could be sending such text messages.

Another Android problem is that sometimes what seems like a scary request for permissions is actually legitimate. An app may need to access call logs to know not to disturb a user while he or she is on a call. Many security apps are now helping users learn more about these pesky permission requests. They can also block people from visiting fake websites or being scammed.

Although there are many apps that cost money, some free apps have nearly identical features. Free options include TrustGo Antivirus & Mobile Security, Sophos Free Antivirus and Security, and Avast.

Among paid apps, Lookout Mobile Security dominates the industry because it's automatically distributed on many Samsung and T-Mobile phones, according to the research firm MarketsandMarkets.

After Lookout are big names such as Trend Micro Mobile Security & Antivirus, Norton Security Antivirus and McAfee Antivirus & Security. They all charge about $30 a year.

Bitdefender costs $10 a year but doesn't include any privacy features. Bitdefender and F-Secure are good options for people who use the Google Chrome Internet browser on their mobile device.

Beware of fake security apps that appear to have the same name or same features as those listed above. They can allow hackers to control your device.

Analysts say the features packed in the security apps might eventually show up in Android, but Google may not yet have the security expertise to develop them. Ludwig says Android adds outside security features when there is demand for them.

Take, for example, the recovery of a lost device. Android recently copied that feature from security apps.

Go to the listing of apps on a phone. Look for and click on "Google Settings." Then, look for and click on "Android Device Manager." Check the two boxes. Finally, navigate to google.com/android /devicemanager" target="_blank">www.google.com/android/devicemanager. Check the boxes to enable the device to be rung, tracked, located and deleted if lost or stolen.

Be wary: If someone does a "factory reset" on the device, these features will no longer work. The Samsung Galaxy S4, through LoJack for Mobile Devices, has tracking that's reset-proof.