

Sharing Photos without Revealing Too Much



mobilesecurity.com [San Francisco, CA] Antivirus vendors traditionally talk about security threats from malware and other viruses. A time will come when the mobile world won't be so different, but until now, cybercriminals simply haven't invested the amount of effort in creating malware for mobile operating systems that they've spent on Windows.

It's true to say when it comes to your smartphone, security concerns are better-focused on other aspects of the device. One area that you would be well-advised to pay particular attention to, is your smartphone's GPS features. This is an area where the hazards can be physical. The same technology that allows your parents, friends, and potential suitors to pinpoint your whereabouts might also be used by people whose intentions are less welcome. Let's take a look at how it works and what can be done to make sure you're protected from shady characters.

It's standard now for smartphones to contain a GPS chip, using satellite data to determine your exact location at any given time. Providing you have GPS enabled, it can help you plan your workout or morning run, you can keep abreast of your family's whereabouts, or finding new places in your neighborhood to hang out at. Sharing this information might also make it easy for you to be found by people who have no business finding you, so caution is advised.

Many apps leave it up to you to "check in," or pinpoint your whereabouts, others are voice-guided and active immediately. Some photo sharing sites make it possible for users to activate geotags, which also includes details such as latitudinal and longitudinal coordinates and altitude.

Adding your location to photos online might seem harmless and trivial, but it isn't beyond

the realms of belief that you might become vulnerable to being exploited by someone who could rob or assault you. The geolocation app "[Girls Around Me](#)," which applied data from social networking sites to track women in a given area (apparently without their consent or knowledge), was only recently removed from the app markets. The U.S. Army is now educating deployed soldiers about the substantial risks of geotagging their photos, or forgetting to deactivate GPS apps on their smartphones. In fact they're warned against using any kind of social media that features a location-based component. Carelessness in these areas could give enemy forces the tools to pinpoint an attack, and whilst this is an extreme situation, it's worth bearing these concerns in mind with your day-to-day use of social media.

Read Yvonne's piece on [mobilesecurity.com](#) for some simple tips on how to help your kids stay safe while enjoying the latest location-sharing services with social media apps.

References:

- 1) [Geolocation tips from PCWorld.com](#)
- 2) [Camera & phone GPS/Location Services article on digicamhelp.com](#)

Mobilesecurity