

Android mug shots have no lock and key

March 4 2012, by Nancy Owano



(PhysOrg.com) -- If Google loyalists will persist that this Internet Goliath can do no evil, they at least need to admit, based on new evidence this week, that Google can do a lot of mindless harm. A security door in Android smartphones is left open that can enable Android apps to nab your photos without your permission. In fact this has been an unsettling week in smartphone revelations. People have been informed that whether their smartphone of choice is from Apple with iOS or another vendor's phone with Android, they can never be certain who out there in cyberspace is able to view all their photos.

Apple's OS was the first platform to get nailed for photo insecurity. The

loophole is tied to the permission that apps seek to use location data, when access can be gained to the entire photo library.

Now *The New York Times* reports that because of a security loophole, Android apps can gain access to the photo libraries of users without permission and can copy the photographs to a remote server—with no impedance. According to experts, as long as an [app](#) has the right to go to the Internet, the user's [photos](#) can be copied to a remote server, with no notice to the user.

It is not clear whether any apps that are available for Android devices are actually doing this. What was confirmed by experts is that an app can read pictures without having to get any special permission.

As part of the NYT report, an Android developer put together a test application of a timer. When the app started and the timer was set, the app went into the photo library, retrieved the most recent image and was able to post it on a public photo-sharing site.

While the picture-scoffing app was only a test, the point was made that [Google](#) could do more to maintain people's confidence in Android as a safe mobile platform for their smartphones.

In response, Google confirmed that it's an issue, and is looking into the situation.

Interestingly, Lookout, a mobile security company, late last year prepared a report listing the firm's 2012 mobile threat predictions, In 2012, they said that they expected to see the mobile malware business turn profitable. "What took 15 years on the PC platform has only taken the mobile ecosystem two years."

They talked about vulnerabilities in smartphones, saying that "due to the

difficulty of updating software and patching vulnerabilities on [mobile](#) phones, malware writers will continue to exploit iOS and [Android](#) OS at a pace greater than vulnerabilities can be resolved.”

More information: [www.mylookout.com/news-mobile- ... -threat-predictions/](http://www.mylookout.com/news-mobile-...-threat-predictions/)
bits.blogs.nytimes.com/2012/03/01/android-photos

© 2011 PhysOrg.com

Citation: Android mug shots have no lock and key (2012, March 4) retrieved 19 April 2024 from <https://phys.org/news/2012-03-android-shots-key.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.