



# DenverDA

Mitchell R. Morrissey, District Attorney - Second Judicial District  
201 W. Colfax Avenue, Dept. 801, Denver, CO 80202

Bus. Phone: 720-913-9000  
Fax: 720-913-9035



**Mitch Morrissey**  
Denver District Attorney

## Consumer Advisory

### Downloading Phone Apps Pose Possible Risks

More consumers are relying on the convenience of mobile phone apps to get quick information. Mobile phone apps are software programs that offer 'information-at-your-fingertips' and can be accessed directly from a smart phone or other mobile device. The use of phone apps is exploding in popularity and is expected to surpass computers as the information source most often used by consumers. As widely accepted as apps have become, there are important privacy and security risks that every user should know before downloading these products.

#### Privacy Concerns

App developers earn money by selling advertising space which allows them to offer the app for free, or at a reduced cost. It is an effective way for companies to market their product to more users and to promote new products. Before downloading an app, users are usually given a privacy policy that explains how their personal information will be used by the company. By agreeing, the user gives the company permission to access the information that is stored on the user's phone, such as phone and email lists, call logs, internet data, phone location and other information. App users may not be aware that such data is often used to explicitly target them for future advertising of select products. Consumers should read all privacy policies so they are aware of how this personal information is being used and why it is being stored.

#### Malware and Security Protection

Apps that don't include privacy policies should alert the user to the possible threat of a malware infection. Malware infections are introduced when the app is downloaded, therefore allowing criminals to retrieve personal information from the user's phone. Signs of a malware infection include any app that appears on the phone that the user didn't install. To avoid this risk, users should routinely upgrade their apps. Upgrades include the additional benefit of providing updated security patches that protect the phone from the latest malware. Security apps that detect and remove malware are also available. Mobile phones can also be hacked, and tell-tale signs include email or text messages that the user didn't write. Consumers should notify either their mobile phone carrier or the manufacturer of the mobile device to resolve a security breach.

**Denver DA's Fraud Line: 720-913-9179**

 **Follow us on Twitter @DenverScamAlert**

**December, 2012**