May 2015

Want more information about frauds, scams or ID theft including ways to protect yourself against these crimes?

I provide presentations to your Office, Faith Organization, Club or Association at no charge.

For information contact:
Maro Casparian
Dir. Consumer Fraud
720.913.9036
amc@denverda.org

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

What's Your App-titude?

If you have a smart phone or other mobile device, you probably use apps to play games, get navigation assistance, weather info etc. Apps (short for Applications) are easy to download and are often free. They are also fun and so easy that you may download them without thinking about some key considerations, such as how they are paid for, what personal information they may be gathering from your device and who gets that information.

People who would never dream of downloading an email attachment from a stranger buy apps without considering the possible consequences. Some apps are malicious -- they contain viruses, worms, malware or some other way of harming your device. They can be programed to access things like your personal information, your contacts, or passwords and share them with others. Many apps are free because of advertising, and many ad-based games use your location information for the advertiser. Interestingly, app developers often aren't aware of the privacy-intrusive behaviors of their own apps.

Luckily, there are steps you can take to avoid downloading a malicious app:

- ✓ Double check what permissions an app uses. For Android phones, you can see what permissions it uses before installation. For iOS, apps request for permission right before sensitive data is used the first time.
- ✓ Put your mobile device in airplane mode, which makes it so that apps can't access the network or location data. This is obviously pretty inconvenient because you can't receive or make phone calls in airplane mode, but some apps still work perfectly fine in airplane mode.
- ✓ Look for info such as the upload date on app stores or the number of downloads. These are good signals for differentiating between legitimate apps and fake apps. Meaning, the older the app, and the more downloads, the higher the odds that the app is safe.
- ✓ Check out privacygrade.org before you download an app. This site "grades" apps on what data it may or may not be sharing and best of all, it's free!
- ✓ Research apps to determine if they are safe before downloading. If the app is new, or not well known, do a quick Google search to see if there are any reviews of the app. A Google search for "app name – problems" may be the best idea.
- ✓ How will you know if you're a victim of a malicious app? Just as your PC slows down when infected with malware, a smartphone will do the same. Problems with slow operation and decreased functionality can mean that malware is present on a phone's operation system. Another way to tell that your phone has been compromised is if it seems as though your phone has a mind of its own. If applications open on their own, the phone powers on or off by itself or items are downloaded without permission, it may mean that software allowing outside access has been installed.

Make sure you are APP-plying the same caution with your smartphone as you are about your financial or medical identity.

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