Smartphones and Identity Theft: The Risks and How You Can Protect Yourself

By: Sean Naron, Administrative and Advocacy Associate, Consumer Federation of America

According to a Javelin Strategy & Research survey , identity fraud (the actual misuse of illegally obtained personal information) in the U.S. increased by 13 percent in 2011, with more than 11.6 million adults becoming victims. What's even more frightening is that the personal information that you store on your smartphone is now a tempting target for ID thieves.

In fact, the survey found that smartphone owners were a third more likely than the general population to be victims of identity fraud. This may be due, at least in part, to consumer behavior: according to Javelin, 32 percent of smartphone owners don't update to a new operating system when it becomes available, 62 percent don't use a password on their home screens, and 32 percent save their login information right on their devices.

How should you protect yourself and your phone from identity thieves?

1) Lock it up:

Set up a password to open the home screen on your phone so that no one else can see your contacts, messages, accounts, or other personal information that's on it (like those embarrassing photos of you playing with your adorable cat). You should also lock your SIM card
– that's the memory chip in your phone that enables it to work with the phone network and stores all your account information and other sensitive data. An unlocked SIM card can be stolen and used with another handset, allowing the identity thief to access the information on it and to rack up charges under your account. The procedure for locking the SIM card varies depending on your phone's operating system (Android, iPhone, Windows, etc.) – it's easy to find instructions online.

2) Install anti-virus software. For my phone?

Yes! The fact is your smartphone is really a miniature computer, and it's just as susceptible to security and privacy threats as traditional PCs and laptops. There are many mobile security applications currently on the market. Which should you choose? PCmag.com recently released a list of the best mobile security apps. Most are either free or available at a very low cost.

3) Keep Current:

It's important to keep your phone's operating system and security software updated to fix any security problems that may have been discovered.

4) Erase the memory:

If you are disposing of your old phone or handing it down to someone else to use, wipe its memory first, just as you would erase the hard drive of your computer. Should you lose your smartphone, many of the privacy apps (and all iPhones) have a "remote wipe" feature that allows you to erase the private data on it.

5) Get the download before you download:

Did you know that there are fraudulent apps and other software programs out there that are specifically designed to steal financial account numbers and other personal information from your smartphone? Only download games, ringtones, apps and other programs from reputable, well-known sources, and use the same caution when clicking on links. The best place to get apps is directly from your phone's authorized application store (iTunes, GooglePlay, BlackBerry App World, etc). Before you download any apps, read reviews about them – if you're the first to use an app, you may be the first to discover that there is a security problem with it. You can get more tips about smartphone safety, privacy and security from the nonprofit Identity Theft Resource Center. For additional information about how to keep your identity, and your smartphone, safe go to the website for National Protect Your Identity Week and click on "ID Theft Protection on the Go."