It's Cyber Security Awareness Month: Do you know the dangers of digital apps?

Posted October 11, 2016

October is National Cyber Security Awareness Month, and with two-thirds of Canadians owning a smartphone*, relying on the convenience of digital apps for daily tasks has become the norm. Apps use, store and share personal information for a variety of purposes, but BBB says it's important to be aware of the risks that come with some of these apps when it comes to protecting your digital information.

"Using digital apps has become a regular part of every day life, so people think nothing of giving their personal information to an app," says Mary O'Sullivan-Andersen, president and CEO of BBB Serving Southern Alberta and East Kootenay. "It is crucial for consumers to understand the responsibility that comes with using such apps and educate themselves about the risks of misuse."

Take a look at the types of popular apps that provide everyday convenience, but can create a potential threat to your personal information:

- Social media: Did you know that some social media apps share information with each other? Instagram and Facebook share their respective user data with each other to better detect spam and build better features, but that means your info could be shared with numerous other third-party "affiliate partners and service providers"...be sure you understand individual app privacy policies before handing over your info.
- Coffee maker: Coffee apps that are connected to your home Wi-Fi network are able to alert your smartphone when your coffee is ready in the morning, remind you to set the machine in the evening and allows you to remotely change the brewing time. Your habitual information becomes property of the coffee maker company or app developer, and it's a possible indicator of when you're home and when you're awake.
- Door lock: Having the ability to provide one-time, short-term, or scheduled access to your home can be a wonderful benefit. Being able to unlock a door remotely through a home Wi-Fi network is also a luxury some users have when using a connected lock program. A lot of times these lock programs are linked with home-automation systems, which will consolidate a lot of home's data on to a single server.
- Activity tracker: These apps allow you track how many steps you've taken, what your heart rate is, and in some instances allow you to track your runs through GPS. If this

data is sent from the tracker to the app un-encrypted, it's possible that information including your username, address, password and potential GPS data is at risk.

- Baby monitor: These types of monitors use your home Wi-Fi network and certain models can communicate directly with your phone using Bluetooth. If using these types of models, it's important to have a strong password on both your network and camera to ensure hackers are kept out.

So, how do you protect yourself?

- Know the privacy policies. Be sure you understand what information each app requires, if that information will be shared, and who it will be shared with. Remember convenient doesn't always mean safe.
- Only use secure WiFi networks. Stick to using apps while on a secure Wi-Fi connection, like at home or at your place of work. Using free, public Wi-Fi hot-spots aren't always secure, and could mean a greater chance of your information being accessed by others.
- Use strong passwords and change them regularly. It's easier to keep the same password for all of your apps and accounts, but if one of those accounts becomes compromised, chances are your other accounts will be too. Keep hackers at bay with different and strong passwords for each account.

*CRTC report shows more Canadians going mobile