BCSI Investigations
www.picanada.ca

November 2014
Volume No. 6
Issue No. 16.1 of 16.4

THE INVESTIGATOR

In This Issue

About Us

Since 2000 BCSI has performed hundreds of successful investigations.

Our integrated team of investigators and support services ensure that the investigations are conducted in a timely fashion with leading edge techniques.

BCSI is considered the platinum standard of the industry based on the quality and the wide spectrum of its services as well as the expertise of the investigators.

Quick Links

Our Website
Services
Firm Profile
Contact Us

Social Media

Smartphones and Security

Are you one of thousands of people who download applications (apps) for your online banking or to upload your photos onto social media? If yes, then you need to know if your security and privacy is being compromised. Without considering it, a person might accept the terms and conditions for an app and not actually read the permissions that app is asking for, simply because they want the convenience that that app offers. These apps that we use on a daily basis might be gaining access to data we might not want to give up. If you were to instantly imagine your phone being stolen, what would that criminal have access to? Your Facebook account? Your emails? So far as to say your bank account? With technology nowadays, your smartphone acts as your computer and the way you treat your computer is how you should treat your phone. With technology in a constant evolutionary spin, keeping up to date with the strongest phone security is crucial. In a report taken from Consumer Reports Magazine, it was found that 5.6 million smart phone users had experienced unwanted activities occurring on or from their phone, this being an indication that a phone has harmful software or a/many virus/es on it.

Wireless

Most smartphones these days have the option of connecting to a wireless network. It should be noted to switch off your phones wireless connection when not in use which not only saves battery power but also lessens the risk of security breaches. It's beneficial to check up on your phone's network security settings as it may be programmed to connect automatically to a WiFi zone without your knowledge, especially if it is a new phone. The most common form of security risk when using public WiFi is called the "evil twin" attack and happens when a third party offering what seems like a legitimate wireless connection requests you to connect by using pre-set passwords or login details. Once these are programmed in, these details may be used at a later stage to access the user's account.