OUR CONTINUOUSLY CONNECTED LIVES: WHAT'S YOUR "APPTITUDE"?

It seems like everything is connected to the Internet these days. While the number of "things" connected to the Internet has for several years been higher than the number of people, it is only recently that a massive increase in the number of things that can connect has occurred. From smart phones, which have been connected for a while now, to cars, to the light bulbs and thermostats in homes, almost everything is connecting to the network now and in many cases, can be contacted and interact with the Internet. Thanks to this "Internet of Things" (IoT), there are apps to control coffee makers, adjust the temperature in a room, change the channel on the television, start the car so it can warm up or cool off inside, and even to open the garage door. Where the phrase "There's an app for that" used to only refer to non-physical activities, now it can refer to a wide variety of activities that are "app enabled" by specialized sensors, devices, clothes, and connectivity.

With all of this power, it is easy to simplify even further and neglect the proper security setup for these apps, or choose poor passwords to protect them. Since most of them revolve around smart phones, properly securing and caring for these devices is more important that ever. Even when smart phones first came out, losing one would mean only that photos, texts, user content, and contact information would potentially be lost. Now, if a smart phone is lost, access to cars, houses, garages, confidential records, GPS coordinates, and other sensitive data is at risk. While for the most part users are at the mercy of device and app designers to build in proper security, the following guidelines should be considered when dealing with smart phones and IoT devices.

- Be sure that the security features on smart phones are enabled. Whether using a PIN, a thumb or finger print, facial recognition, or some other method, always make sure smart phones can be and are secured.
- Take special care to not lose smart phones or devices and be sure to enable the "find my device" features in case of a loss.
- Follow all security setup procedures when installing a new IoT device and connecting it to an app on a phone or tablet.
- Be aware that some of these devices and apps store potentially sensitive information, from location data, to health information, to financial assets. Treat the smart phone or device with care beyond the base cost of the device, as the data on it is far more valuable.

There are already billions of these devices in use, and the amount and sensitivity of data transmitted and collected from them is always increasing. While they make life easier and more informative, it is very important to be aware of the risks of IoT and adjust habits appropriately.