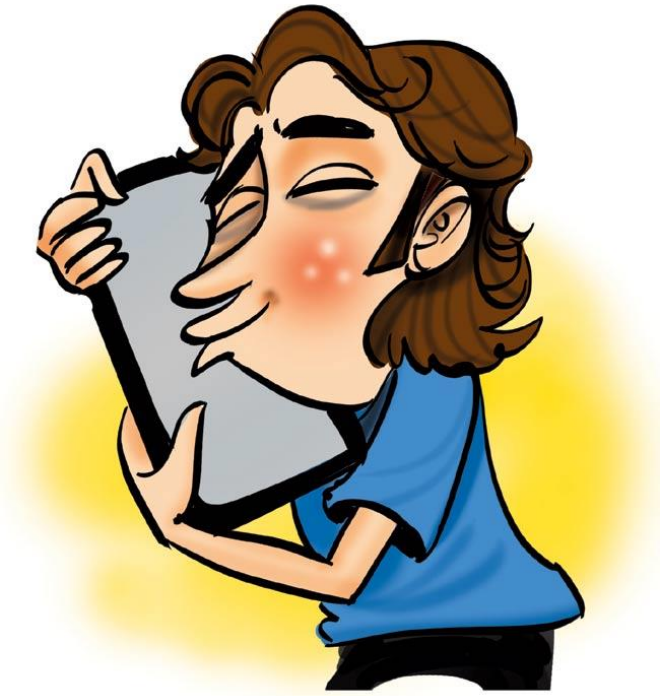
ARE YOU SAFE?



2017 is upon us and many people have probably received new mobile devices for the holidays. Great! You are now the owner of a Smartphone or tablet, joining the ranks of millions of consumers drawn into the 21st century's era of technology. Unbeknownst to many, every manufacturer has its way of making money that can affect our online activities. Major manufacturers such as ***Samsung, Apple, Microsoft, Huawei, LG*** and the rest all have agreements with App suppliers to provide them with Apps (e.g. "What's App", games, etc.); so software developers have vested interests in the deal they make with these manufacturers. Have you ever noticed the question that pops up when installing an App asking you to allow the installer to make changes to your device? The catch is that in order to **GET** the App, you must say "yes" thereby allowing the installer to gain access to your device. It's a case of "Damned if you do, damned if you don't" and we are all victim to it.

This kind of personal exposure can be mitigated somewhat if we practice some extra safety measures:

1. **Lock your device** using a PIN, password, complex swipe or fingerprint; enable auto-locking - yes, more to remember but worth the effort to have an extra deterrent.
2. **Keep your operating system up to date** – ignoring "system updates" can be costly as the newest patches tend to be all about security.

3. **Watch those Apps** – stay with official marketplaces; be aware of the permissions requested during installation…does a free game really need access to your camera? When in doubt, don't do it. Many mobile threats emanate from China, Russia, Kazakhstan, Belarus and the Ukraine but more than 50 countries are involved.
4. Get in the habit of periodically **backing up your device's data** – photos, notes, etc. How often depends on how much and how quickly you store material. Cloud storage is an inexpensive measure to pay for.
5. When possible, **NEVER use free Wi-Fi**. Trusted data connections (your home, office or personal mobile router) with personally created passwords are the safest way to conduct banking transactions, handling emails or online purchasing. "Free" can be very expensive and painful.
6. An old rule for computer users has been to **never click on links or unexpected attachments** – the same applies to mobile devices. Once you click, you have accepted the outcome and no anti-virus program will save you.
7. **TURN OFF location tracking, cookies, auto-fill** – do you really need them on at all times?
8. **TURN OFF your Wi-Fi and Bluetooth when not in use.** Simple but effective.
9. **Consider installing security and anti-virus software** that can lock, wipe, disable and protect you as much as possible.
10. Finally, when getting rid of your device, delete all apps and personal information – return to factory settings before you discard or pass it on.

Remember, your PC or MAC is still the safest way to connect to the internet and conduct most sensitive activities (banking, purchasing, etc.)

HAPPY AND SAFE 2017 TO ALL!