HAPPY NEW YEAR and BEST WISHES TO ALL!

MOBILE SHIELD

A warm welcome to 2013 – may it be filled with peace, good health and an easing of some of the world's woes – improvements are certainly in order! Now for those of you who received a mobile device for Christmas, Congratulations on becoming part of the future in communication-ware….these range from a USB flash drive to a smartphone to a tablet like the iPad.

As we've written in past articles, PCs and mobile devices are vulnerable to hackers, viruses, and malware, with tech experts expecting a huge increase in these kinds of activities this year. Mobile devices only have minimal encryption protection built in, leaving you exposed to the majority of threats. But why the concern? Because more and more we use our smartphones and tablets to STORE personal information, do work, handle e-mails and conduct internet transactions like purchasing airline tickets. As we become more comfortable with our mobile "toys" we tend to use our PCs less –the wrongdoers have already noticed that. So how can you best protect yourself? Here are some tips:

1. **Lock your device and use your PIN.** Every unit has the option of your own unique PIN number as well as automatically being locked when finished using it. Change your PIN periodically – good practice for your emails and other sensitive sites too.
2. **Disable your GPS, Bluetooth and wireless when not using them**. Not only do they drain your battery, they're an open highway to potential hackers. It takes a few moments to re-enable your connection…in the end, it's time well spent. In airports and cafés be especially vigilant of those around you when turning on your connection.
3. **Get updates when notified**. Fabricators and software programmers are on your side, constantly improving or patching their equipment. It may be time-consuming or even a bother to do them (far too many people turn them off), but you must attend to these updates when they occur.
4. **Download Apps with caution.** We are inundated with thousands of Apps…some useful, some desired, and many frivolous…..but an inherent factor of these downloads is the access level to your data, allowing the App provider complete entry into your device. Research the app well and make sure it comes from a legitimate site before downloading it, free or purchased.
5. **Backup your data.** Just as it's a good habit to back up your PC files, the same applies to your mobile device. Use iTunes for an Apple device and a simple

"Document" file for any Android device…..it´s a simple task but extremely useful when needed.

6. **Install reputable security software** from legitimate companies who have developed the appropriate programs specifically for mobile devices….not all are created equal and free ones are ineffective.
7. **Last resort: install a remote wipe App**. This App allows you to remotely access your mobile device from your PC, erase all personal information and return the device to factory settings.

Statistically, 28% of data theft is from mobile phones, while 32% is from devices being controlled remotely. Taking a few precautions will allow you to enjoy your new "toy" the way it should be.