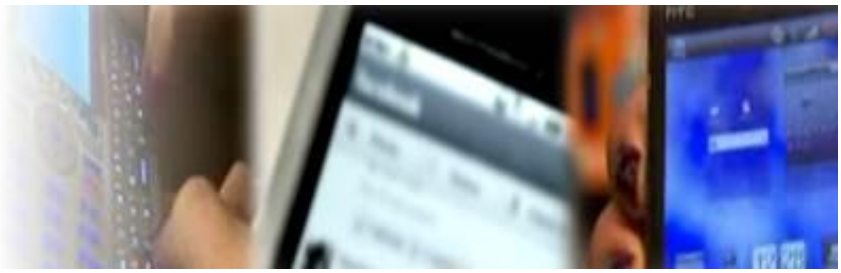
Business Vision
Real-World Results
AVISTAS



Mobile Device Security (Smart Phones, Tablets & iPads)

How can we protect ourselves?

Bill Morgan & Mart D. Nelson, P.E., CISSP

There is an exploding supply and demand of economical technology driving all of us toward the benefits and convenience of mobile devices. Today's pocket computers otherwise know as smart phones, tablets and iPads fit neatly in our hand and are often slid into our suit coat pockets or purses when done.

We carry these with us everywhere we go. To a great extent, they are replacing our Desktop or Notebook PCs for with the convergence of many daily personal and business functions. They are our electronic persona and consolidate our world into a sort of digital avatar.

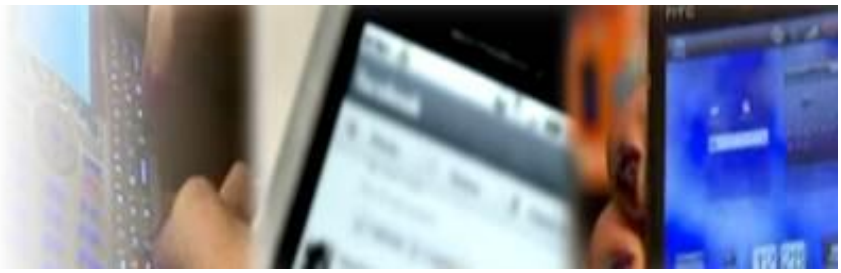
Our mobile devices, like our PCs, are subject to both technical and human behavior threats.

Unfortunately, nothing is really private or secure, and the bad guys can break into your mobile device if you lose it or they steal it. Assuming you have possession of the mobile device, the following steps should be accomplished with any Smart Phone, tablet or iPad to reduce the ability of others to gain access to your personal and financial information:

- On a new mobile device, immediately change default passwords for voice mail and for the device itself
- Activate the auto-locking feature for the device when the screen saver is invoked or when a few minutes has elapsed.
- If possible, set the device to erase all the data in the device after a series of unsuccessful log-in attempts. Be sure to perform periodic backups of the device.
- Encrypt data on the device (can be toggled on or is automatically encrypted upon password reset)
- Turn off Blue Tooth and Wi-Fi unless you are using it at that moment. Smart phones, tablets and iPads connected to wireless networks are exposed to hackers that can break into the mobile device just as they can with your PC.
- Turn off geo-location codes unless you need to use them for a specific application (most devices will let you authorize the various apps to use location services)

In terms of information on your smart phone, limit the information actually stored on the mobile device as much as possible. It may be a nuisance, but user IDs and passwords should be entered each time you access a service and not stored on the device.

Business Vision
Real-World Results
AVISTAS



Unfortunately, we are our own worst enemies and the bad guys know that. The easiest and most reliable way to gain access to information or to infect a computer or mobile device is to let you ask for it. A few rules will make it clear how easy it can be to get your information.

- Don't click on links that someone sends to you. E-mails, Facebook massages, tweets or other messages with links may look like they come from a friend, but may not. That new Angry Birds app may wind up making you angry! Instead, retype the link or wait for the friend to ask you about the material in the link.
- Delete suspicious emails immediately and don't open attachments, unless you are absolutely sure of the source of your message.
- Never respond to e-mails from your bank, the IRS, Social Security, or any other institutions. If they want information from you, they will send you a letter. Clicking on what you think is a link to your bank may take you to a very convincing replica of your Banks's web site and any data you enter is available to the bad guys.
- Load antivirus and antimalware protection programs on Android & Microsoft Windows mobile devices.
- There is also software available for the iPhone that will allow control of web access and maintain a list of known suspicious or criminal links.
- If you are accessing financial records or personal data, try to use the cellular 3G or 4G service for those tasks, rather than a Wi-Fi hot spot. It is possible for someone to collect your communications and discover passwords or personal information.
- Additionally, ordinary scams are abundant. If it looks too good to be true, it probably is.

These precautions apply to all mobile devices (smart phones, tablets, iPads, etc.) and your computers. With the increase in devices and technology, remember that they are all computers whose security and use should be treated the same.

Contact Avistas today for a
Complementary Executive Review of your current situation.
Bill Morgan, CEO & Consulting Principal – bmorgan@avistas.com
Mart D. Nelson, CTO & Consulting Principal - mnelson@avistas.com
Office - 214-544-0400