According to Pew Research Center, in 2016 more than 77% of the U.S. population owned a smartphone. One can only assume this number has and will continue to increase. Additionally, up to 28% of owners don't use a screen lock password or routinely update the system or apps. Considering a smartphone is nothing less than a handheld computer, they should be treated just like our desktop or laptop when it comes to using a password and regular updates.

The iPhone has built-in security benefits over other systems, provided you don't have a jailbroken phone. If you don't know what that means, you should be fine. Since all iPhone apps come from the Apple App Store, each of these apps have gone through a great deal of scrutiny by Apple before being released for download and as a rule can be considered reasonably safe. But while they may not contain anything malicious, they can possibly be affected by external sources. For example, that web browser you installed can be a conduit for malicious software to get into the phone. Email apps are just as susceptible.

Android phones have a similar system to the Apple App Store called Google Play, and likewise these programs are reviewed by Google prior to being released and can be considered safe to install. However, android phones are not limited to installing apps only from the Play store. Even a non-jailbroken phone can install an app from other sources. This can greatly increase the risk of installing a malicious program. Be very selective of what apps you install from alternate resources.

Since most of us take our phones with us wherever we go, the security risk and chance of theft is greater. The first layer of defense for our phones should be a good password that others won't guess. If available, use the manufacturers security settings to allow you to trace your phone location when lost or stolen. Many of these mechanisms also allow a remote wipe or reset to prevent access to the phone's data.

Just like a computer, your phone should have good backups and antivirus software. Again, use the manufacturers backup systems or an alternate. Make sure it is configured to automatically backup your phone daily or weekly as needed. For antivirus, many antivirus PC subscriptions include a license for your phone as well. If not, search Google Play or Apple Store for a good antivirus app. Keep in mind that some antivirus apps must be manually run to scan the system for viruses.

Keep your apps and phone system updated with the most current release. Most phones will automatically update or notify you of available updates if the option is turned on. This is an important step since one of the main reasons software updates are release is specifically to resolve security issues and risks. You also benefit by getting new features and functionality with the software updates.

Finally, purchase a phone insurance plan that will replace your phone if something should happen. Most plans available are relatively inexpensive and have various options available. Read the details on the coverage provided, as some don't replace your phone if stolen or lost.

Take good care of your smartphone and it will take good care of you.