With the smartphone industry growing larger every day, there is a growing concern for the security of data on said mobile devices. The power of these devices is always increasing, as is the amount of software that can be installed on them. With the advent of these different types of software, including financial software and personal identification software, the need for more security is a must. Most of these types of devices come with some type of security built-in, but is this really enough for today's world?

For most people nowadays, their whole life is on their smartphone. It includes a plethora of personal information and data, such as:

- personal/work documents, notes, pictures, and emails that can contain sensitive information
- full access to Wi-Fi networks that you connect to at work or at home
- calendar appointments and contacts
- access to various sites/information through apps, such as social networking apps, bill paying apps, movie apps, shopping apps, and etcetera

With all this information on our smartphones, it makes it a goldmine for potential thieves. The risk of your phone being lost, stolen, or even being rummaged through by your IT guy is only the half of the security problem with them. Smartphones can also leak other kinds of data through sniffing of your internet traffic when connected to open Wi-Fi networks. Your passwords to unencrypted websites and services, such as Facebook, Twitter, web-based e-mail sites, POP3 e-mail services, etcetera could be easily be sniffed by someone else on the network. There is also the issue of viruses, malware, SMS/MMS exploits, and Bluetooth exploits; these exploits can manipulate your phone settings and prevent you from using certain features, send information to or call contacts in your phone, steal and/or destroy personal information on your phone, or render your phone completely unusable.

Though the biggest concerns for now should be more focused on protecting your phone from theft or loss or sniffing over Wi-Fi, the issues of malicious software and hacking are becoming more and more prevalent every day. These issues could become more of a concern in the not so distant future due to the lack of integrated active security systems, such as firewalls, anti-virus programs, and anti-malware programs into our phones.

To set a bit of background for the importance of securing your mobile phone, Juniper Networks

conducted a study of more than 6,000 smartphone and tablet users in 16 countries about mobile security threats. They found the following:

- 250% increase in the amount of mobile malware over the past year
- a Fortune 15 company discovered that 1,250 of its 25,000 devices were infected with malware
- 44% of respondents to the survey use their devices for both business and personal use
- 80% admit to using their devices to access their work network without the employer's knowledge or permission
- one out of every twenty apps in the Android marketplace requests permissions that could allow the app to place a call without the user knowing
- nine of ten mobile devices have little or no security protection
- more than 60% of reported smartphone infections are spyware and 17% are text message trojans that can rack up fees that are charged to the device owner's account

As clearly evidenced by Juniper's findings, there is an inherent need for more mobile phone security. Fortunately, there are several options to help secure your phone that are built-in to the operating system and several third-party programs as well. Even the most basic of security measures can help you protect your personal information. To begin, we will start with some of the simpler defense mechanisms.

While this first one may seem pretty obvious and straightforward, do not lose your phone! If you are in a public place, do not sit it down or put it in your pocket or an open bag, where it can be easily grabbed. This is actually the most common way that phones get lost or stolen.

You should also set your phone to lock or timeout after a certain period of time (recommend thirty second or less), especially if you happen to leave your phone out on your desk at work or in other public areas. All major smartphones come with this functionality built-in. You will want to make sure that you choose something that is not easy for anyone to guess, but easy for you to remember. It should not be something as simple as your address, name, phone number, etcetera. Here is how to easily set timeout settings and passwords on your phone:

Android:

Beginning with Android 2.2 (Froyo), users have the ability to set a pattern lock, PIN code, or

password on their device. Users of earlier versions of Android can only set a pattern lock. How to set the screen timeout and locks mentioned above can vary depending upon the manufacturer of the phone you have. The option is generally found by pressing the *Menu* button from the home screen, going to S
ettings
,
Location & security
,and
Set up screen lock
. From there, you should be able to easily setup the different types of screen locks. (
Word of caution
: Make sure that you have your Gmail account linked to your phone, so that you will be able to gain access to your phone in the event that you forget your password. I highly recommend this if you setup a pattern lock, as it can be very easy to forget your pattern). You may also want to be careful with setting a pattern lock, as unlocking your phone this way leaves oily residue on the screen that can remain even if you wipe it. A study conducted by researchers at the University of Pennsylvania on the Google Nexus One and HTC G1 showed that taking photos of the phone's screen with a standard camera and doing simple manipulations of the images within photo-editing software revealed the pattern more than 90% of the time.

BlackBerry:

Press the BlackBerry button, go to *Options* and*Password*. From there, select *Enable Password*
. Set the number of password attempts to what you consider a suitable amount (recommend four minutes). After the specified amount of attempts has been exceeded, it will completely lock you out of your phone for the time interval specified in the
Security Timeout
field. You can also set it to where it will lock upon placing your BlackBerry in a holster. This will only work with a magnetized holster. To set the screen timeout, go back into the
Options
screen and select
Screen/Keyboard
. From there, select the specified timeout period by
Backlight Timeout
.

iPhone:

Beginning with iOS 4, Apple introduced the ability to setup a password in addition to the standard 4-digit PIN code. To set a passcode, go to *Settings*, *General*, and *Passcode Lock*. From there, set the password or PIN code that you would like, as well as adjust the screen timeout through the
Auto-Lock
option. You may also select the
Erase Data
option to erase all data on the phone after 10 failed passcode attempts.

While password protecting your phone can greatly decrease the risk of your information being stolen, it is always good to take even more precautions. There are several different types of security suites out there from different vendors, as well as built-in software that can perform a "remote wipe" on your phone in the event that it is lost or stolen. Remote wipe means that you can completely remove all of your data from the phone, including e-mails, texts, documents, contacts, etcetera over the internet. For those corporate users who have a Microsoft Exchange e-mail account, this can easily be accomplished without any third-party software. You can either do it yourself through the *Options* panel in Outlook Web Access or have someone in the IT department initiate the wipe. For those who are personal users, or for those that do not have an Exchange account, there are several other options from third-party vendors.

Android/BlackBerry:

There are several different third-party applications that allow for you to remotely wipe your device, as well as provide several other security features. The most popular application out now is the Lookout Mobile Security suite. It not only allows you to remotely wipe your device, but also incorporates additional features that allow you to track your device via GPS, back up your contacts over the internet, and scan for viruses. The features mentioned above (minus remote wipe) are available through their free version of the program. The premium version of the program incorporates all of the above features, plus backup support for call history and pictures, remote locking, and includes a privacy advisor. The privacy advisor gives you insight into which apps can access private data on your phone, as well as scan every app that you download to see what data it accesses. The premium version is $2.99/month or $30/year. Some competitors to Lookout Mobile Security also offer protection from web threats by scanning apps before they are installed, scanning links for phishing URLs and other malware, and blocking unwanted calls and text messages. AVG Anti-Virus, McAfee WaveSecure, and Webroot Mobile Security are some of the other big name competitors.

iPhone:

The iPhone does not have quite as many options as other platforms. The only option available is to track your phone using MobileMe. If your iPhone has iOS 4.2 or higher, you can simply download the Find My Phone app from the App Store and enable it online through MobileMe. If you lose your phone, you can login through the MobileMe website and track your phone. If you have an older version of iOS, you will need to have a paid MobileMe account, which costs $99/year.

As far as anti-virus protection on the iPhone, there are none currently available on the consumer level. Apple relies strictly on the App Store's stringent review process to keep out any malicious software. While this sounds good in theory, it is not foolproof. With so many apps going through the approval process, there are bound to be some malicious ones that get through. The only other sort of protection available for the iPhone is Trend Smart Surfing, which blocks access to web pages with malicious content and helps circumvent phishing attacks.

However, Juniper Networks is currently working on the Juno Pulse Mobile Security suite that includes anti-virus, firewall, anti-spam, and remote monitoring/control services. It also remotely backs up and restores data and can locate lost devices. Juno Pulse is currently available to enterprise customers only, but they are looking to move into the consumer market.

Some other general security measures that you can take to protect yourself are to make sure that when installing third-party apps, you pay attention to the privileges that you are granting to them. Some of these privileges can include access to your GPS location, access to your contacts, access to your text messages, and other personal data. With BlackBerry App World and the Apple App Store, most of these problems are handled at the application store level before they are released to the masses. However, the Android Marketplace is a bit different, as Google does not screen all apps that come into it. It gives the end user more freedom, where the app asks you for specific permissions when installing and updating them. In short, it is best to use common sense and pay attention to what you are installing before you install it-read the reviews and make sure that it has a good number of users beforehand. Also, make sure that you only download apps from trusted sources. It is no different than the precautions you should use when installing programs on your computer.

Other aspects of securing your device that you should pay attention to are that when logging into a website, ensure that the connection is encrypted using SSL or HTTPS. You should also use secured Wi-Fi hotspots that will encrypt your traffic from others that utilize the hotspot. If you are unable to do this, you should opt into using the cellular data connection instead, as it is

typically encrypted by the network provider. You could also use VPN to secure all your internet traffic, as there are several free providers out there, including Hotspot Shield or WiTopia.

Device encryption is also a must for any mobile users, as it will secure your personal information and data from being recovered by a hacker or any other advanced user. Entire device encryption is currently supported on BlackBerry, iPhone, and Android 3.0 tablets.

BlackBerry:

Most of the newer BlackBerry devices support encryption on the entire device and on removable storage (microSD cards)-this will protect your pictures, documents, and other files in case you lose your BlackBerry or have someone take your card out when you are not looking. When encrypting your device, you may want to leave your contacts unencrypted, as encrypting them will cause caller names to not display when your phone is locked. To setup encryption on the device and/or removable storage, press the BlackBerry button, go to *Options*, *Security*, and *Encryption*
. From there you will able to specify what you would like to be encrypted.

iPhone:

Encryption on the iPhone is automatically turned on when you set a passcode on your device. However, it is only available on the iPhone 3GS and later-it is unavailable on earlier iPhone models. To ensure that encryption is enabled, verify that *Data protection is enabled* is displayed in the Passcode Lock screen in the
Settings
.

Android:

Unfortunately, Android does not currently support any device-level encryption for smartphones. If you would like to encrypt your emails, calendar, and contact info from your company's Exchange account, you may do so using a third-party Exchange client called Touchdown.

However, device-level encryption is currently available as part of Android 3.0 (Honeycomb), which is targeted for tablet devices. It should make its way onto their smartphone operating systems sometime in the near future.

After taking a look at some of these common smartphone security issues, you should have some sort of idea on how to best protect yourself from loss or theft of your device and loss of any personal information from your device. With smartphones becoming more and more popular, more security issues will be sure to arise and smartphone operating system manufacturers will continue to adapt their operating systems to best combat these issues. At some point, these mobile security suites may even be integrated into the operating system or pre-installed by your network provider.