There's no doubt about it - mobile devices have become man's new best friend. If you don't believe it, consider that there are currently over 4 billion mobile phones in use worldwide among 7 billion people, not to mention millions of tablets. People use their devices to stay in touch, take pictures, shop, bank, listen to music, and socialize. Additionally, they store personal and professional information on them, and because they use them for almost everything, they have both a high financial and emotional value.

Losing your smartphone or tablet, or the information on it, can be a hassle. If you lose your mobile device, you not only have to replace it, but you could also lose the sensitive information you had stored on it, including account numbers and confidential work information. So, why do so many of people leave their mobile devices unprotected?

Though most people do recognise the need to protect their computers from a myriad of digital threats, many don't realize that they face the same threats, as well as a host of new ones, with mobile devices. In fact, most mobile users don't even know that there is security software for mobile phones, even though it has become increasingly essential.

For one thing, the growing popularity of mobile devices has led cybercriminals to see them as a new avenue for attack. Mobile malware has grown significantly in recent years, becoming ever-more sophisticated and dangerous as it spreads. Furthermore, cybercriminals are not just designing malware for mobile, they are also taking advantage of the way you use these devices to trick you into opening risky emails and web pages, or accidentally downloading a malicious file.

So, as a mobile user, keep in mind that you need to learn how to how to protect yourself from a variety of threats. Some of the essentials for your mobile protection include: locking your device with a PIN number password that only you know, only installing applications from trusted sources, backing up your data, keeping your mobile software updated, remembering to log out of bank and shopping sites and making good use of Antivirus software.

It's also important to avoid sending personal information such as bank details or passwords via email, as such valuable information can be easily hacked by cybercriminals. It's also a good idea to turn off Wi-Fi, location services and Bluetooth when you are not using them. This will limit the chances of your important information being leaked in a shared digital environment.

Smartphone malware is not yet regarded as a big threat, but its coming. Malicious software is jumping from PCs to android mobile phones, malware makers target the smartphone platform in anticipation of making a quick buck. And if you can remember the infected Droid-Dream and Plankton Android apps, an infected app that was released into the Android Market with ability to infect several thousand android cellphone users' before anyone could detect the existence of the malware.

While taking note of the DroidDream incident, numerous phones that downloaded the software infected with a Trojan horse and rooted their phone and later on gave vital data like the user's location and cell phone numbers to a remote server. The very same day, Google destroyed the contaminated apps in the Android Market, and washed away the apps from phones remotely. It later issued an update to re-pair the damage which the DroidDream Trojan horse had done.

How to shield yourself

The safest way is of course to avoid unknown apps and if necessary, research apps and their publishers in detail before tapping the download button. Before you install an app, you should ensure that the apps avails a list of authorizations for services that the app should access on your phone. For example, if an app prompts to access an alarm clock, it doesn't need to access your phone's contacts list. And if something in the consent screen looks suspicious, ensure thorough precautions before you download the app.

Touch screen on android mobile phones can be very dangerous when you are surfing on the net, hence you should be on the look out of what you click while surfing the web. Some time in June, a mobile security company 'Lookout' exposed malicious advertisements aimed at android smartphone users and deliberate to swindle them into installing infected apps. A few types of mobile antivirus software, such as Lookout Mobile Security, have features aimed to protect you from malware such as these.

It is however advisable to install antivirus software on your android phone. Most big-household security companies such as McAfee, AVG, and Sy--mantec have a downloadable cellphone app for protecting your smartphone. Aside from guarding against malware, these apps include vital abilities such as to lock and wash your phone remotely. When you purchase a new phone; it's a better to install antivirus software before you add any other apps. And you'll tremendously reduce your phone's ability to get phished against malware activities.

telefon dinleme