Imagine your closest friend standing next to you. Now imagine your closest friend betraying all of your secrets. And making a handsome profit whilst doing so. Now picture your smartphone inside your handbag or pocket. Picture your smartphone sending your passwords, banking information, e-mails, and private information to some stranger. And picture that stranger making a handsome profit. That is mobile malware.

What is mobile malware, really?

In more technical terms, mobile malware is the spread of malicious software (hence "mal-ware") among wireless devices. Mobile Malware is unpleasant stuff. It could compromise the information on a mobile device, and there have even been cases of compromised devices used to pull information from Personal computers (hijacking USB synchronization). Mobile malware is yet another growing fraud category which involves infecting mobile devices with viruses and Trojan horses that may force a mobile phone to do unauthorized activities,like making phone calls and deleting or stealing information.

Once installed on a device, mobile malware replicates itself and performs undesired activities, such as using network services like SMS or voice to make calls to PRS numbers or to subscribe to unwanted billing schemes; data theft, where the user's personal phone records such as contact lists and account details are stolen, sent to a third-party, and erased on the handset; and launching distributed DoS attacks intent on forcing a legitimate service to fail.

Not only is mobile malware a threat to individuals, it is also a huge security risk to businesses. It has the potential to commandeer a corrupted smartphone and use it as a proxy or gateway into an organization's central network. By commandeering a handheld device, cyber criminals can waltz past a standard firewall program and make their way onto a company's email server, client database, Customer relationship management tools, and other essential parts of the network. Damage of this magnitude can grow from something very small, such as a member of staff getting a message to download a free game or software update.

Mobile Malware is rapidly increasing

Mobile malware is on the rise for several reasons and it is following the Law of Computer Virus Evolution:

The Law of Computer Virus Evolution

In order for malicious programs targeting a particular operating system or platform to emerge, three conditions need to be fulfilled:
1. The platform must be popular
2. There must be well-documented development tools
3. The presence of vulnerabilities or coding errors

The widespread adoption of 3G (and soon 4G) and Wi-Fi connectivity and huge hard drives are other factors contributing to the increase of mobile malware infection. In fact, malware activity in 2010 increased 46 per cent over 2009.

The good news is that practically all mobile malware threats call for some type of effort on the part of the user. Malware can't magically appear on your phone. It usually happens after a user downloads a malicious app and the recent DroidDream incident reveals that mobile malware is more advanced than ever before.

How to stop mobile malware and protect yourself
Keeping a close eye on the app stores is a must, as Google proved. Google banished about 50 free applications from its app store immediately after it was found out that the titles hid a Trojan horse designed to steal users' information. The applications, which included pirated and copycat versions of legitimate Android titles, had been downloaded tens of thousands of times before Google took corrective action.

The best way to protect your mobile device (and yourself) is to take a layered approach to mobile security. Before you download that shiny new app, look at its permissions. An app shouldn't receive more permissions that what it needs. For example, a simple notepad app shouldn't need unrestricted access to the internet. Also, don't download apps from unauthorized or illegitimate app stores.

The second layer should be a very good antivirus app on your phone, and the third layer should be a firewall. If you choose wisely, the second and third security layers can be found wrapped up in a mobile security app.

How to choose an effective mobile security app
An typical mobile security solution will have capabilities that assist in operating the program and efficiently protecting the device. A very good mobile security application will include things like antivirus, antispam and firewall protection with realtime security. An exceptional mobile security

application will have all of the preceding, as well as sms protection, remote wipe (in case your smartphone is stolen), and gps location (again, in case your smartphone is stolen).

What is the best mobile security app?
Ask ten experts and you'll get ten different answers. This question is almost as hotly debated as "what's the best antivirus software for my computer?" In order to narrow down my choices, I used the criteria mentioned above to come up with a list of mobile security applications. As you can see, many of the desktop giants of antivirus software have developed mobile versions of their software. The list isn't comprehensive, but it will give you a good starting point.

AVG

AVG Mobile Security is specifically available for Android. It comes with anti-virus and SMS anti-spam features that give protection to your mobile against all unwanted messages and advertising. Price: $9.99

ESET

ESET Mobile Security brings a new level of protection to Symbian and Windows Mobile smartphones, so you can be confident in the safety of your device -- even if you lose it. Price: Free for thirty days.

Dr. Web

Dr Web Mobile Security Suite is an anti-virus security solution for Android, Symbian OS, and Windows Mobile. However, they aren't sold separately and are bundled with Dr. Web products for workstations.

Lookout

Lookout mobile security is also a multi-platform mobile device software that has a user-friendly, simple and in-depth virus scanning abilities. Lookout Mobile Security is currently available on Android, Blackberry and Windows Mobile.

Price: Free, with a Premium version at $29.99/yr.

F-Secure

F-Secure Mobile Security allows smartphone users to experience the full potential of their devices without the fear of mobile threats. F-Secure Mobile Security automatically retrieves the newest updates whenever any data connection is used. An additional SMS update mechanism patented by F-Secure ensures that critical malware fingerprints are received even when a data connection is not available.

Price: Subscriptions begin at $3.31/month (approximately).

Kaspersky

Kaspersky Mobile Security is currently available on Microsoft Windows Mobile 5.0, 6.0, 6.1, 6.5 and Symbian OS (Nokia smartphones only).

Price: $29.95/unit/yr.

BullGuard

BullGuard Mobile Security is one of the better mobile security applications. It is one of the very

few that supports all major mobile OSes like Android, Blackberry, Symbian and Windows Mobile.

Price: $29.99/license/yr

Mobile malware is a scary thought, and the problem is likely to get worse, especially since smartphone adoption is skyrocketing. Using the tips and advice in this article you can protect yourself (and your personal information) against the rising tide of mobile malware.

telefon dinleme