To date, there's never been a major outbreak of mobile phone malware. Yet several security vendors - including Trend Micro, Norton and Kaspersky offer mobile solutions of their security packages. It's reasonable to question whether such software is really necessary in the absence of a visible virus threat.

In fact, virus in the traditional sense - programs that spread by making copies of themselves - are very rare these days even on PCs. By far the most common way to get infected is via a dodgy download from a seemingly innocuous website. Since all the major smartphones feature a web browser and support third party applications, that's a risk as applicable to mobile devices as it is to a iPad, Mac or PCs

In some ways, mobile phones are better defended than regular PCs. That's partly because they were designed in an age in which online threats are well understood. Mobile operating systems have security built in at a fundamental level: It would be impossible to give Windows that sort of security without breaking compatibility with software and ways of using the computer that dates back more than two decade.

Since mobile phones are used more casually than computers, they can also afford to place more restrictions on the user. Computer malware could be all but eliminated if Microsoft had to approve every application before it could be run on Windows, but if it tried to do this there would be uproar.

With Apple's iPhone, though, exactly such a system is in place - making it extremely difficult for rouge software to get onto the phone - and millions of satisfied users have no complaints at all.

Mobile threats

Although your smartphone maybe less vulnerable to malware than your windows PC, there are still dangers out there, Many online threats, for example, don't involve software at all: phishing scams in which fake banking websites steal your login details, run just as well on your locked down iPhone or Blackberry as on an unsecured PC

In fact, the scam works better on a mobile platform: the smaller screen makes it harder to spot telltale mistakes on fake websites. Web addresses may be truncated in the browser, concealing the incorrect URL's. Against threats such as his, your only defense is vigilance and perhaps, security software that can warn you when a website has a dodgy reputation. Webster Consulting recommends not using mobile and public places for online banking as prevention is better than cure.

Another danger is fake applications - programs that are disguised as games or tools but security monitor your secretly monitor your keyboard or run malicious processes at the same time. Although Apple, Microsoft and Google all have more or less strict approval process in place at their official application stores, these aren't guaranteed to be foolproof, and if you download from other sources you don't have even the wisp of reassurance. In cases such as this, your only hope is mobile security software that can identify the malevolent code before it strikes.

What happens if you do get caught out? Mobile phones are a great opportunity for criminals since they're directly linked to a payment system. For example, a rogue application could work by sending multiple text messages to a premium number, racking up huge costs over days and weeks. In fact just such a program, disguised as a music player and distributed for Android, was detected by Kaspersky in 2010.

Although mobile malware hasn't yet become a widespread problem, it's clearly possible and it's becoming a more attractive prospect for criminals by the day. So while you may not feel the need to install a security suite on your phone right now, it's important not to be complacent the first epidemic could strike at any time.

telefon dinleme