

Typically we associate birthdays as joyous occasions. Candles are blown out. Gifts are given. Fibs about our real age cause our friends and family members to chuckle with delight. Sometimes birthdays of beloved figures in human history are even commemorated decades or centuries after their deaths. However, one birthday that mobile phone users would like to forget, is the appearance of the first mobile phone virus. Fortunately, mobile phone security software can now be used to detect and destroy viruses before they harm our mobile phones.

Today's mobile phones resemble gadgets that we might expect to see in Dick Tracy comics or James Bond films. They can contain an array of features, including Internet access, radios, games, cameras, and even mobile phone security software. However, one drawback of using mobile phones that can send and receive electronic data is the chance that the phones can be infected with viruses.

The first mobile phone virus that could duplicate on its own was discovered on June 15, 2004. A Finnish and Russian anti-virus company jointly reported the mobile phone malware (software created to penetrate or harm a computer system without the owner's informed permission) used wireless technology to spread to other mobile phones. Nearing the first virus's second birthday, roughly 200 mobile phone viruses existed. Several of them are simply variations of the first virus.

The good news is that mobile phone security software is now available, and experts believe that it is improbable that the virus situation will become as troublesome as that of PCs. The difference is that when PC viruses were initially discovered in 1986, hardware and software producers were not creating solutions to viruses. Today, however, both manufacturers of cell phones and their operating systems are joining forces to attack the problem. One result has been mobile phone security software that can even recognize and destroy the newest mobile phone viruses.

On the other hand, cell phone malware is developing into an industry that could eventually become very profitable for "cybercriminals." In the typical life cycle of malware, amateurs create the first generation, to basically prove that it can be done. Later, the professional hackers typically enter the market, providing their devilish expertise. Fortunately for the mobile phone security software industry, this has not yet occurred in the world of cell phones.

For instance, the Redbrower is a Trojan horse that was created to illegally "earn" money on Java-activated cell phones. Redbrowser is advertised as a special Web browser that can provide instantaneous WAP (wireless application protocol) browsing. However, Redbrowser sends huge numbers of text messages to a first-class rate phone number located in Russia. This could add hundreds or even thousands of dollars to the victim's mobile phone bill. Luckily, mobile phone security software can now help to search and destroy such electronic bugs.

Additionally, spyware has expanded the scope of its influence from PCs, to mobile phones. Flexispy is a spying application that was created to record text messages, document calls and transmit recorded calls to a third party. Although it is officially legal, after Flexispy is installed, the user is not notified about the copious amount of information that is sent to a third party.

While cell phone viruses have infected thousands of phones in over 30 countries, the situation has not become an epidemic yet. Hopefully mobile phone security software will continue to wish cell phone viruses on their birthday: "Rest in peace!"

[telefon dinleme](#)