Modern technology advances and so are the viruses for smart phones and mobile phones with internet connectivity. Mobile viruses are like human viruses. It can spread by close contact to a specific host. It can also spread in the same way as computer viruses. Mobile viruses can be transferred through infected files or programs.

Some mobile device has Bluetooth. It is a product of modern technology that transfers data. This is done between different devices through photo sending from cell phone to printer and or address transferring from your Windows mobile phone to computers.

Mobile phones evolve. Their purpose was originally to make people talk to each other while moving. Now they are considered as multi-media devices. It can replace items in the future like:

o game console
o messaging terminals
o credit cards
o digital cameras
o TV and others

Cell phones that are merely enabled for talking and SMS are not at risk with viruses. Those that are enabled to handle data or have Bluetooth are susceptible to viruses. Bluetooth technology has few risks so it needs to be manipulated properly. Once virus is installed or received, it will start to look for other Bluetooth devices to infect. Within a 30 feet radius, an enabled Bluetooth mobile device can be infected by another.

How do viruses multiply?

Infected MMS messages will be sent by a virus. It will then proliferate to every listed numbers in your phone memory.

What harm virus can do to your phone?

o The virus can delete or alter all the contact details and calendar entries in your mobile phone.

o It can crash, delete or lock up your phone applications.
o The virus will appear as pornographic item, free download, or mobile games.
o The virus will appear as text messages disguised as friend message's subject line.

Knowingly or unknowingly, the user installs the virus through transferring. Sometimes the virus disguise as a desirable application. It installs the bug without your knowing. It can cause trouble and cash losses, too.

How to avoid mobile viruses?

o Do not enable Bluetooth when not needed.
o Accept only file that you know when your Bluetooth is on.
o Say "No" for unknown file.
o Download materials that are not scanned from sharing network must be avoided.
o Delete the infected application program.
o Avoid installing unknown applications.
o Download only from official websites.

Ways to avoid mobile viruses

1. Network Security

There are mobile versions of anti-virus products that can be used. These are from industry leaders. It includes:

o Norton Smartphone Security for Pocket PC

o F-Secure Mobile Antivirus and
o Trend Micro Mobile Security-It can protect Windows mobile, Pocket PC, Symbian and Smart phone users
o Airscanner Anti-virus-It can protect mobile devices and Pocket PC from Trojans
o Commander Mobile Anti-virus- protects Symbian smart phones

2. Blocking Thieves

An important defense to block thieves of data is to enable the password lock. It can be found in the native system setting of PDA.

3. Privacy and Data Protection

To keep your files confidential, password managers and data encryption can help you. Encryption applications are:

o Ilium Software's eWallet Professional for Windows Mobile
o Smartphone and
o Palm with 256-bit RC4 encryption

A password for lockbox program will be required each time information is to be accessed. It includes bank account, car details, credit cards, and the like. Well-known viruses are:

o Cabir
o Duts
o Skull
o Kaspersky

Viruses and Malware will remain as long as 3G phones are here. Improvement of the

productivity levels of mobile devices will expose them more to virus infections. The solution is to implement security measures inside the device such as data encryption and anti-virus software applications.

telefon dinleme