Viruses can be disguised through sms or an email attachment as an enticing image, audio or video files or even a greeting card through the Bluetooth. This means that unless you are expecting an email attachment or you know the source of one, do not open any from an unknown source.

SYMPTOMS OF VIRUS INFECTION

- Your phone may go into re-starting frequently.
- Your phone may operate slower than usual.
- Your phone may stop obeying commands or locks up often.
- You may not be able to access some applications in your phone.
- Some applications on your phone may refuse to work properly.
- Unusual error messages may occur often and menus may appear unclear.
- Icons which you did not put may crop up and recently opened attachments may have dual extensions.
- Installed antivirus is likely to be disabled or the program may not start.
- New antivirus cannot be installed and even if it is installed, it will refuse to work until the phone is debugged.
- Battery depletion rate is likely to increase because the virus through its malicious operations will over labor the battery.

These are some common signs of assault by a virus although soft or hardware problems may present some of these symptoms.

My advice is that once your phone shows any of these signs; take the phone to a certified technician or your service provider. If you take action early enough, the damage may not be much. At the end of the exercise, you should have updated version of the necessary antivirus software installed on your phone. You must guard your phone against viruses and spy wares.

There are both simple and sophisticated ways to protect cell phones from attackers in the U.S. Since phones with Bluetooth connections and data capabilities are the main targets of malware, it is generally the Smartphone that must be secured against vulnerabilities. Cell-phone threats are primarily spread in three ways, Internet downloads, Bluetooth wireless connections, and multimedia messaging service (MMS).

Many protections are built into devices, such as allowing users to set a strong, five-digit PIN code for Bluetooth devices so that access is harder to crack, and most digital phones have encryption capabilities, which reduce the chance of someone latching onto a conversation. Mobile anti-virus software is also becoming more available, which is used for various device platforms.

Cell phone use varies around the world. In Japan, cell phones are used for financial transactions similar to a credit/debit card. Other uses include watching live TV, gaming, picture enhancement, and GPS navigation. On average, Japan is approximately five years ahead of the U.S. in regards to cell phone technology.

With the advanced use of cell phones in Japan, security capabilities are advanced as well. For example, NTT DoCoMo's P903i includes security features such as face recognition and password protection in order to make financial transactions. Another protection has the owner of a cell phone keep a security chip in their pocket or purse, and anytime the cell phone is out of range, it will lock and prevent usage. These methods, plus the protections mentioned for the U.S. above, can provide greater security, however, the risk of using the Internet and data being hacked during transmission is still high. Additional protection by cell phone service providers and manufacturers need continuous improvement because the wireless technology, and threats against it, is here to stay.

Cell-phone viruses downloaded from the Internet spread the same way as a computer virus. Infected files are downloaded using the phone's Internet connection, or downloaded to a computer and then synchronized or transferred to the phone. In order to protect a cell-phone from this type of exploit the user should verify the authenticity of downloads to make sure they are from trusted sources. In addition, users should consider using mobile antivirus software and synchronize files selectively since frequent synchronizing gives the maximum opportunity for transferring infected files.

Bluetooth wireless connection threats occur when a user receives a virus via Bluetooth while the phone is in discoverable mode, thus the user should turn off Bluetooth and discoverable mode until it is needed. In order for a virus to spread via an MMS message it must be included as an attachment. In order to stop a virus propagated in this manner, the user should not open unexpected attachments.

Users should be vigilant in keeping their software current by regularly checking for new versions of operating system and applications. In addition, they must exercise caution towards suspicious attachments, downloads, and activity.

Multiple levels of defense create the most effective protection. The first layer should secure the cellular infrastructure, including transmission towers and the mobile telecommunications switching office. The second level of protection resides with phone manufacturers and software developers. The third level of protection is the end user's responsibility.

A simple step end users can take is to monitor their battery usage, since one telltale sign of active malware is a quickly drained battery. Also, users should lock their keypad when not in use to prevent unauthorized access and change passwords frequently.

telefon dinleme