Mobile phone security, including virus control and protection from identity theft has become a core concern for government, business, personal users, and mobile equipment manufacturers. By the year 2014, the home PC may no longer be the primary means that the nation uses for surfing the Internet. This changeover promotes Antivirus software to the forefront of mobile communications.

The line that distinguishes between PC technology and mobile technology continues to shrink. More and more users are turning their purchasing power away from personal computers, including laptops. Tablet computers, iPads, and mobile phones are the new "choice" products. These portable devices are compact, easy to carry around, and more powerful than even fairly recent models of desktop and laptop computer equipment. Plus, more and more parents are dealing with the "Everyone has one and everyone is talking about one" argument.

A New Nest for Scammers and Identity Thieves

The Internet draws human flies. Wireless Internet breeds even more scammers and identity thieves. The advent of expanded capacity cell phones with easy to download apps, and the growing number of uneducated users, children included, opens up a great, new-horizon for hackers, malicious software applications, and deceitful contact practices.

The current barrage of compromised mobile phones is only the beginning. The more PC-like mobile equipment becomes, the easier it will be for scammers to phish personal information from mobile databases.

Some Common Scams

Subscriber Fraud: In this common form of identity theft, someone uses "smishing" to capture your personal information via SMS or text messages. The thief then opens a personal cell phone account under your name. In a very short time, your home mailbox will take in a mouthful of new and unexpected bills.

Bogus iPad Middleman: This scam takes lots of differ approaches, from a bogus blogger to a phony eBay seller.

Malware: This Internet based evil can rack up some really expensive premium phone calls, add a monthly payment to your bill, or harvest your personal information.

Basic Protection

Applied common sense is your primary line of defense. This means that you must establish some basic rules such as the following:

1. Do not leave your digital equipment lying around. People sometimes forget important items. Have you never had to go back into a restaurant to retrieve a forgotten cell phone? Whether dealing with an iPad, tablet computer, or a mobile phone a moment of carelessness can come upon any of us.

2. Keep your antivirus software up-to-date. Remember that modern devices are a mobile Internet resource, and not just for you alone.

3. Think before you provide any information in response to an unknown caller or text request.

4. Be careful what you download. Although effective and absolutely necessary, Antivirus software is not a perfect defense. Apply common sense to all your Internet activities.

5. Be aware of information risks that may affect your friends. Be careful with conversations that seek answers concerning other people.

6. Finally, remember the primary rule of wheeling and dealing: If it sounds too good to be true, it

is likely not true.

telefon dinleme