

Computers, laptops and PC tablets are not the only devices that are targeted by malicious software developers but smartphones have now joined the list of the most threatened devices by intruders. There has been a steady rise on the number of attacks, which are targeted on smartphones and this means that people need to watch out for the malware. Apparently, the number of malware is so huge that people may not be able to identify them and it means that comprehensive information dissemination is required to educate smartphone users on the threats posed by malicious software.

Android in particular, tops the list of smartphones that are threatened by malware attackers. There are various reasons why android smartphones are being eyed by attackers. One of major reason is that there are many people using android devices. It is estimated that globally, android takes a commanding lead in smartphone market. Around 6 out of every 10 smartphone users own an android device.

This figure translates to around 52.3 percent of the smartphone market. These devices are owned by people who run businesses and this could mean that hackers and cybercriminals are looking for ways in which they can steal confidential business and personal details like bank account information.

Another reason is that smartphone users do not upgrade or update their operating systems. Those users who are running older versions of android OS are at higher risk of being attacked than those who update their operating system platforms regularly. Usually older versions of the operating systems are not protected of malicious codes and will most likely be attacked easily.

Moreover, lack of knowledge is another reason, which could be causing the increased attacks on android smartphones. Not every user is aware of the different malware threats found on the internet. There is a misconception by smartphone users that these devices are not susceptible to malware and virus attacks.

The term malware and virus has in the past been associated with personal computers and laptops but this is not the case today. There is a notion that smartphones run on different OS platforms, which are not vulnerable to hackers, phishers and cybercriminals and this has left many users suffering from ignorance. There is laxity among users in enhancing security measures to protect their devices and this substantiates the reasons why many do not even

bother to update their OS features.

Another reason is that these users do not know what to do about the security issues pertaining to their devices. Although PC and laptop users have gained more knowledge on how to prevent malware vulnerabilities, on the other hand, smartphone users seem to lag behind in observing ways to protect their devices. It is also argued that android software developers are not providing timely patches and updates to their consumers' devices.

It is estimated that more than 50 percent of android smartphones contain unpatched vulnerabilities. Various androids are released in the market with outdated software and more so, these programs are never updated once sold to consumers. This has created a loophole in protecting android devices and hackers have take advantage of such shortfalls. Android carriers and manufacturers should make sure that the software programs they release in the market are updated continuously to protect their consumers. In essence, the fight against android malware attacks is the responsibility of both developers and users.

[telefon dinleme](#)