Hackers

Business

Mobile phone users are more vulnerable to hacking than computer users.

They are more likely to click on dangerous links or download malicious apps that expose them to hackers. A significant number of companies dealing with computer security recognize the need for enhancing security so as to avert the danger posed by mobile hackers. The need for protection has become paramount after the realization that hackers are able to acquire salacious photos, voice massages and credit card numbers, emails, as well as the addresses of their victims. Information about the victims used for a variety of purposes, many of which are illegal(Julie, 2004). This paper lays down the main points during its analysis and description of the main steps so as to facilitate the initial processes of protection. Ethical Issues Surrounding Hacking Hackers violate People’s rights by intruding into their privacy.

They use malware to hack Salacious celebrity photos, voice messages stored on their cell phones, steal one’s location information, add mobile bill, and steal credit card number. Computer security companies like McAfee, Symantec, Sophos, AVG, and Lookout have developed applications that protect people’s cell phones. These applications scan other applications that people try to download to their cell phones. Also, some these companies have introduced a security system for business mobile. These helps to keep peoples phone off the hackers’ malware (Miller, 2011). The pplications and security system developed by computer security companies prevent people from downloading malware.

They also alert user when they visit unsafe mobile website or click unsafe links. Mobile users are caused to incur extra cost in purchasing these apps.

Applications and system security developed by computer security companies help improve people privacy by preventing hackers from accessing their private information. Hackers pirate this software, add harmful code, and trick people into downloading them. People can back up photos and phone’ call history, allow them to lock or erase info from lost mobile devices.

These help to upheld peoples values. Mobile companies likeGoogleregularly scan apps in Android for malicious malware. This scanning removes this malware from people’s phone and market. Mobile companies also prevent Android applications accessing other apps and inform mobile users if a malicious application gains access to their contact list or location. Companies perform regular scanning to their apps in the market to remove malicious apps so as to prevent hackers from accessing people’s information.

This causes these companies to incur extra cost. Preventing hackers from accessing people private information improve their privacy. Regular scan of apps in the Android which remove malicious apps upheld people’s value. The scan prevents Android apps accessing other applications and preevents access of people private information. Evaluation The case explains two solutions to mobile hacking i. e.

regular scan by mobile company and the use of apps developed by computer security companies. Both the solution upholds people’s values by preventing malware from accessing people information. DecisionScanning of mobile phones applications is the better of the two solutions to mobile hacking. Hackers pirate applications developed by computer security companies, add malicious code, and trick people to download them, therefore, exposing

them to threat. Scanning of mobile applications by mobile company removes applications with malicious code (Diane & Thomas, 2011).

Regular scanning of mobile applications by mobile company helps to remove malicious apps from the people’s phone and the market. Conclusion Experts advices that prevention of hacking can be facilitated through passwords, switching off the phones when not in need of conversation, keeping the phone updated, as well as enhancing phone security (Roush, 1997). They indicate that users desire to avoid the use of the same password in more than one account. Password should be changed on a regular basis, and if possible, enable the remote locking of phones when necessary. Even though no system is perfectly secure, the best that users can do is to make the hackers attempts much more difficult (Jonathan, 2011).