Security and Accessibility

Cristian Lopez

George Mason University

IT 103

Professor Kammy Sanghera

October 5, 2014

Security and Accessibility

Cellular phones have the potential to revolutionize the technological age in today's world. People can now access almost any form of information from anywhere on the planet. Although, at first this may seem as a convenience, it soon becomes a hazardous age in which everyone's personal information is potentially at risk. Every month, there are new cellular phones being released with new features, new designs, and increased functionality. These new phones are being sold out on their first day of release. Cellular phones and mobile devices have become an integral part of everyday life. Consumers can do their homework, answer work emails, call a friend, post a blog, and do their banking and almost anything else that can be done on a computer. However, the focus needs to shift from the convenience of mobile access towards the balance between accessibility and mobile security. If not addressed, it will lead to a malfunctioning structure with a broken legal, social, ethical, and security system. Consumers and professionals both need to understand the magnitude of the issues concerning Mobile security; this will allow cellular phones to produce accessible information and a web of mass globalization.

In the year 2013, 1.2 billion cellular phones were to be sold (Patten and Harris, 2013). This number surpasses the previous year's sale and this provides evidence for the inclination in people's choice to use mobile devices as it provides accessible information and more convenient day to day use. People can access their banking information, manage their social media, and do so much more from anywhere. The technological revolution is at their fingertips. However, consumers fail to realize that mobile security is even a major concern for the companies who produce these devices (Courter 2012). This effect is displayed in a survey conducted amongst IT security professionals in which sixty eight perfect reveal that they cannot identify the vulnerabilities of mobile devices (Patten and Harris, 2013). The issue does not only stem from a consumer perspective as it is also cultivated by the professionals who specialize in IT security aspects. Consequently, experts argue that the lack of awareness in mobile security from IT professionals and consumers opens the gates for hackers to gain the upper hand (Courter, 2012). It is always a constant battle between security and hacking. Information technology currently concentrates on computer security as it is seen as the most vulnerable, but mobile devices are in constant usage and leaves everyone the most vulnerable.

The major security concern in mobile security is mobile banking. According to the American Banker, forty eight percent of mobile device users have made use of their mobile banking features in the year 2013(Crosman, 2013). The attack locked user's screens with a fake FBI letter demanding for a payment of two hundred dollars (Crosman, 2013). The banks had no control over the situation and left their consumers vulnerable to the attack. Consumers are left vulnerable because they do not have a security system set in place on their phones beforehand. Banks cannot respond to some of these forms of attacks. Cellular phones need to contain a higher level of security, especially when dealing with consumer's sensitive information. The best form of defense for these scenarios would be prevention. Banks and other consumer services that rely on mobile accessibility need to focus on the prevention of attacks in order to keep their consumers safe. Secure applications are one of the methods in which vendors are making it safer for their customers to enjoy accessible and both safe services. However, president of Gartner, a technological research firm, Avivah Litan states that "This is surely a sign that mobile malware is on the increase and will become much more prevalent in the next year or two (Crosman, 2013)." Although people are always working on security aspects of cellular phones and mobile devices, there is also someone else trying to hack into these devices.

Security and Accessibility

Cellular phones contribute positively to social growth as they possess the ability to transform the world socially into a small place. The features they contain allow for mass social media and globalization at an increasingly growing rate (Harris, 2013). For example, Facebook contains 900 billion user's (almost one sixth of the world's population) and 340 million tweets are produced on twitter on a daily basis (Harris, 2013). This intricate web allows users to connect from around the whole world. Family members are able to connect with relatives who live far away, people in developing countries can use social media as a form of cultural change, and this allows countries to mix their cultures and lead to globalization (Harris, 2013). For instance the government revolution in Turkey was ignited through the social media. People were allowed to connect and execute their ideas as one. Globalization and cultural revolutions are becoming technologically dependent; and with mobile access this form of globalization takes seconds and is at the fingertip of consumers on a daily basis and at any second of the day.

There are also issues that surround mobile devices which question the ethical use of mobile devices. People can now record anything at any time without permission. This leads to the ethical questions which are raised in the workplace, public places, schools, etc. How can people use their mobile devices? According to a survey conducted by Express Computer, sixty five percent of employers view mobile devices as a threat in the work place (Express Computer, 2013). Companies fear that their sensitive information is at risk. Companies are therefore increasing their security and even banning cellular devices in the work place (Express Computer, 2013). Also in the news, almost on a daily basis, there are phone recordings of brutality or someone performing a good deed. These devices can be used to record a crime or to even steal information. It is the consumers choice how they used their products, but laws should be passed to restrict these uses and to punish people who trespass the boundaries of privacy. This issue ties back to the security of mobile banking. The people's privacy is equally as valuable as bank information and can be stolen by the snap of picture. Cellular phones can be used ethically in both good and bad ways, but laws should be passed to punish those who exploit it. The legal aspects will continue to expand, as technology will continue to grow at a rapid rate (Harris, 2013). Cellular phones have transformed from large bulky blocks to small computers capable of processing information at incredible speeds. Laws should continue to adapt to these changes and protect the privacy and rights of the people.

The legal aspect of cellular phones concludes in one word – security. It should be everyone's goal to provide a more secure use of a mobile device. The producers should enable more security systems and features to protect consumers. Consumers should be cautious as they use their devices and follow the protocol of the producers. The government needs to pass more rigorous laws to prosecute those who break these laws and also to pressure the producers to meet stricter guidelines (Express Computer, 2013). Ultimately mobile devices have the potential and currently are revolutionizing our social environment. People are allowed to connect, information is readily accessible, and shopping is at the click of a button. Mobile security needs to become a collaborative effort between all parties. If security is made a priority people will continue to explore this technological advance and will be able to feel safe and secure about it. Consequently, if security comes before convenience, mobile devices will continue to transform our technological age.

Security and Accessibility

Works Cited

Courter, E. (2012). Mobile security still a race between bad guys and good guys. *Credit Union Times*, , 8. Retrieved from http://search.proquest.com/docview/1031055877?accountid=14541

Crosman, P. (2014, Jun 16). First major mobile banking security threat hits the U.S. *American Banker* Retrieved from http://search.proquest.com/docview/1536077858?accountid=14541

Harris, T. (2013). MOBILE SOCIAL MEDIA & MASS MOBILIZATION. *Scitech Lawyer*, *9*(3), 14-15. Retrieved from http://search.proquest.com/docview/1318021661?accountid=14541

Patten, K. P., & Harris, M. A. (2013). The need to address mobile device security in the higher education IT curriculum. Journal of Information Systems Education, 24(1), 41-52. Retrieved from http://search.proquest.com/docview/1438693253?accountid=14541

Sixty five percent of global companies see personal mobile devices used at work as a threat: Report. (2013). Express Computer, Retrieved from http://search.proquest.com/docview/1466166874?accountid=14541