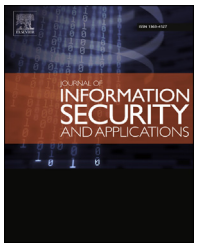
Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/jisa



Safe use of mobile devices arises from knowing the threats

Blaž Markelj[*], *Igor Bernik*

University of Maribor, Faculty of Criminal Justice and Security, Information Security Department, Kotnikova 8, 1000 Ljubljana, Slovenia

ARTICLE INFO

Article history:
Available online 7 December 2014

Keywords:
Mobile devices
Cybersecurity
Threats
Users

ABSTRACT

Today, the safe use of mobile devices is a prerequisite for successful and transparent work, both on a personal and business level. The study presented in this paper shows that work safety in cyberspace depends on the users' knowledge of threats and their appropriate response to them. Based on the results, it has been established that user awareness should be raised, users should be informed of threats and undergo suitable education on work safety in cyberspace.

1. Introduction

The information technology is an important factor in the way an individual works and lives. Due to the fast development of information technology, information is becoming increasingly accessible to each individual and plays an ever more important role in the decision making process. Non-stop access (unlimited and uninterrupted) to information is important. This is made possible by the information technology – to be precise, by the advanced mobile networks and mobile devices.[1] The latter enable individual users to have an unforgettable user experience by means of mobile networks and diverse software. People use mobile devices, among which smart phones have been on the rise over the last period, for gaining mobile access to cyberspace. According to research conducted by IDC (2011), the global sales of smart mobile phones have been increasing by 55 percent on an annual basis. The IDC report (2014) showing the sales of smart mobile phones (as part of the mobile devices' group) indicates that the sales of such devices exceeded one billion items in 2013 alone. The sales of other mobile devices (pads, e-watches, etc.) follow the same trend.

Mobile devices represent an increasingly important factor in the world of communications. They provide a faster and more efficient access to information. They are consequently making the decision process quicker by providing greater access to current information on any given problem. Mobile devices are not popular only among people in the business world, but rather among the entire population. As in the real world, communication is required in order to maintain contact and it is carried out through social portals, including via mobile devices. Due to the lack of users' knowledge, tools

* *Corresponding author.*
E-mail addresses: blaz.markelj@fvv.uni-mb.si (B. Markelj), igor.bernik@fvv.uni-mb.si (I. Bernik).

[1] Mobile devices mostly include devices with an adapted operational system, such as iOS, Android, BlackBerry OS, Windows mobile; and are portable (mobile phones, tablets, etc.). This category can include all portable devices with a wireless Internet access (including laptops, portable gaming consoles, industrial readers, etc.). On the other hand, the mobile phone group includes both mobiles phones intended solely for phone calls and sending short messages and smart mobile phones representing a modern communication device, which offers a whole range of additional functions, similar to those of a personal computer, in addition to calls through mobile networks.

http://dx.doi.org/10.1016/j.jisa.2014.11.001
2214-2126/

providing them with additional protection are currently more of a hindrance than a benefit.

The study, published by the Ponemon (2011) organisation in 2011, was carried out to determine the level of awareness regarding safety and privacy among users (American citizens) of smart phones. It showed that individuals mainly use smart phones for various data transmissions from the Internet (in addition to making phone calls). The equivalent numbers related to the intended use are interesting (most people have smart phones for personal as well as business use). On average, an American citizen spends 2.7 h a day participating in social networks and socialising through mobile devices, respectively (Microsoft Tag, 2011). Young people find the continuous connectivity to the Internet interesting, as it enables access to messaging and the opportunity to use numerous advanced social network services (Facebook, Google Chat, Twitter, etc.).

Mobile device software is developing at the speed of light, above all with the intention of attracting users and increasing sales. Young people forget the traps that are present with the use of mobile devices, as well the need for additional protection in order to avoid these pitfalls too often.

A mobile device can also be under threat by software fragments, installed on the device unsupervised, such as malware and other threats (e.g. spyware, botnets, Bluetooth connection and social network viruses (Leavitt, 2011)). Research carried out by Lookout (2011) shows that the number of malware application-based threats has increased considerably in the second half of 2011, especially compared to spyware threats, by as much as 14 percent. According to the Lookout report from 2011, the probability of malware infection ranges from 1 to 4 percent. The report published by Juniper Networks (2011) states that the number of Android mobile devices, infected with malware, increased by 400 percent since the summer of 2010. The report also found that 85 percent of protection tools on the users' mobile devices is useless, since (certain) mobile device software manufacturers take it upon themselves to install "back doors", enabling them to manage software settings on the mobile device without the users' knowledge, have the device automatically send information on where it is located (e.g. GPS location), or even take control of the mobile device, etc. According to reports published by F-Secure (2013), Juniper Networks (2013) and McAfee (2013, 2014), the trend of growing threats for mobile devices continues to rise. Insufficient knowledge of software and of all features enabled by a mobile device software can get people in trouble and make them targets of cybercrime. Users of mobile devices must be conscious of threats and consequences that they are exposed to, also in order to become aware of the need for adequate cybersecurity. Users should be able to take some level of security for granted (e.g. PIN code for the SIM card, locking of the Bluetooth connection and locking of mobile devices).

In December 2011, a survey was conducted among students of Slovenian faculties, entitled "Mobile device threat awareness". The purpose of the survey was to determine the extent to which young people are aware of dangers/threats they are exposed to and what security solutions they have implemented. The goal of the research is to obtain data on the purpose, manner and type of the use of mobile devices, and consequently acquire knowledge about the manner of use, threats and protection. Conclusions about the users' susceptibility and knowledge of cybercrime can be drawn on the basis of their knowledge of threats and the safe management of mobile devices.

2. Method

The survey was carried out using an online questionnaire, which was published on the "1ka" portal (www.1ka.si) and was active for 21 days. Students were informed of the survey/questionnaire via e-mail, Facebook profiles and in person. The questionnaire was structured in a way that made it possible to determine how the mobile device is used and with what purpose, as well as what types of mobile devices and software solutions are being used. A section of the questionnaire was structured so as to provide results, which offer an insight into the knowledge and use of security solutions, as well as the knowledge and awareness of threats associated with the use of mobile devices. Data analysis was performed using the SPSS software. 281 completed questionnaires were analysed.

The majority of respondents were between 21 and 25 years old, followed by the group aged 20 or younger; 61.5 percent of respondents were women; 63.2 percent completed secondary school education and 36.8 percent were postgraduate students.

We were trying to determine the knowledge of the use of mobile devices. In order to achieve that the questionnaire aimed at establishing what types of mobile devices are used by the respondents. Fig. 1 shows the numbers and percentages of respondents that use different types of mobile devices.

As shown in Fig. 1, the group that uses a classic mobile phone (today, many of them also provide a connection to the Internet) and a laptop computer simultaneously, is the largest. Almost 27 percent of them already use a smart phone, followed by 20 percent of respondents that use a smart phone, as well as a laptop computer. On the basis of these results, it is possible to deduce that respondents use multiple mobile devices.

Sample, ΣN = 282	N	%
Classic mobile phone and laptop computer	79	28.01
Smart phone	76	26.95
Smart phone and laptop computer	56	19.86
Classic mobile phone	48	17.02
Classic mobile phone, tablet and laptop computer	9	3.19
Smart phone, tablet and laptop computer	7	2.48
Classic mobile phone and smart phone	4	1.42
Classic mobile phone, smart phone, tablet and laptop computer	1	0.35
Smart phone and tablet	1	0.35
Tablet	1	0.35

Fig. 1 – Types of mobile devices used.