Digital Natives and Mobile Phones: A Survey of Practices and Attitudes about Privacy and Security

Stan Kurkovsky, Ewa Syta
Central Connecticut State University
kurkovskysta@ccsu.edu

Abstract

The generation of young people who do not remember life before the Internet, who grew up surrounded by computing technology and mobile phones, are often referred to as 'digital natives'. This generation has a special affinity to mobile devices – young people often carry their mobile phones with them at all times to keep a constant connection with their friends while also consuming and creating digital media. This paper presents the results of a survey of over 330 young people aged 18 to 25, which attempts to evaluate their use of mobile technology, their attitudes about security and privacy as it relates to mobile phones, as well as their perceptions of different ways how security and privacy could be improved in future mobile devices. Despite a commonly held belief that digital natives are technologically savvy, their self-assessment does not appear to support this statement. Furthermore, despite the respondents' awareness of various threats to security and privacy, very few of them actually take any concrete steps to protect their devices from unauthorized access. This paper discusses these findings and analyzes the views of young people on different authentication technologies.

1. Introduction

Marc Prensky introduced the term 'digital natives' in 2001 [13] to describe the generation of young people born after 1980. This cohort has been given a wide range of names, including Millennials, NetGen, Homo Zappiens, etc., all of which emphasize that this generation has two distinctively new cognitive traits: they possess sophisticated knowledge of information technology and have the corresponding skills, and as a result of their innate experiences with technology, they have different preferences in learning styles.

A substantial amount of research work reflects a diverse range of opinions regarding the learning styles of digital natives. While the pedagogy-related aspects of the digital natives phenomenon are well outside of the scope of this paper, we will examine the other claim concerning the innate advanced technological skills possessed by the members of the digital native generation.

In particular, we were very interested to study how digital natives use mobile technology and what they think about potential threats to their security and privacy in this context. A large survey in the core of this work examines different patterns of using mobile phones exhibited by young people, as well as their perception of risks associated with private and sensitive information that they may have stored on their mobile devices. Since young people participating in our survey were in the 'digital native' age category, one of the underlying goals of this work was to verify the claim whether they indeed have advanced technical skills which they would exhibit through the use and understanding of mobile technology. We also aimed to compare our results with those published by Clarke and Furnell in 2005 [3], which examined the attitudes and practices of mobile phone users regarding security and authentication. Because Clarke and Furnell's work did not focus specifically on young people with presumably superior skills, we expected that our results would show at least the same level of user awareness and adoption of security practices.

This paper is organized as follows. Section 2 briefly reviews previous work studying technical skills of digital natives and the role that mobile technologies may have already played in their upbringing and is playing now in their everyday lives. Section 3 describes general traits of the surveyed young people, while Section 4 summarizes different ways in which they use mobile technology. Sections 5 and 6 discuss whether our survey participants are concerned about their security and privacy while using mobile phones and if they are willing to do anything to protect it. Section 7 provides a general discussion of our findings, and Section 8 concludes the paper with a summary.

2. Digital natives and mobile technologies

Many studies have examined how digital natives use information technology for educational purposes, as well as in their every day lives. For example, a large study of over 4000 college students in the US [11] indicated that they "have very basic office suite skills as well as e-mail and basic Web surfing skills, [but] moving beyond basic activities is problematic." Furthermore, the authors indicate that the students "do not recognize the enhanced functionality of the applications they own and use."

A survey of over 2500 Australian undergraduates examined how digital natives use emerging Web 2.0 tools [9]. The results of this survey indicate that the surveyed students were not using new technologies as frequently and intensively as has been previously suggested. A very large percentage of the surveyed students frequently used well-established web technologies, such as web search and email, as well as mobile telephony and texting. However, this study indicates that the newer technologies, such as blogs, wikis, and social bookmarking, "that allow students to collaborate and to produce and publish material online are used by a relatively small proportion of students."

Digital natives may have grown up surrounded by electronic gadgets and information technology and became "fluent in the digital language of computers, video games, and the Internet" [14]. However, the degree of this fluency is now widely disputed, especially in the aspects that go beyond computer games and email, and require a deeper understanding of the technology and its possible impacts. Proponents of this phenomenon originally suggested that digital natives would have a revolutionary impact on the field of education due to their unique learning styles and evolved forms of communication. Recent analysis of the research work in this field suggests that although "technology is embedded in their lives, young people's use and skills are not uniform," contrary to the common characterization of the digital natives [1]. While it is undisputed that the society evolves and becomes more saturated with technology, young people lack homogeneity "with regards to technology and a potential 'digital divide'" separating digital natives from the other generations [10].

One of the central points in the notion of digital natives is that they have grown up surrounded by the technology, they use it all the time and they cannot live their lives without computers, game consoles, and other electronic gadgets. Of all electronic devices that surround them, mobile phones have emerged as the forefront of young people's lives. Mobile phones of today serve as the nexus for many means of communication (voice calls, texting, emailing, staying in touch using social networks), as well as rich media features attractive to young people (taking pictures, making and watching videos, and gaming). Network connectivity enables these mobile devices to become a ubiquitous interface to many kinds of data-centric services, such as shopping and banking.

Due to their nature, mobile devices are more vulnerable to threats of accidental loss than their desktop counterparts. It is possible to argue that such risks can be downplayed because thieves are more likely to target devices themselves rather than the data stored on them [2]. However, since the role of mobile devices in our everyday lives increases exponentially, it will be impossible to ignore such threats in the near future. According to a recent survey by McAfee Mobile Security [12], 65% of mobile phone users in the UK, the US and Japan indicated that they are concerned about losing important or private information stored on their phones, while over 54% said that they worry about possible theft of information using a wireless channel. These concerns will become more prominent as more users adopt and switch to mobile platforms.

The importance of security on mobile devices is difficult to underestimate, especially in the context of young people. Much has been said about their affinity to mobile gadgets. But now we are witnessing an emerging trend showing that they may be making a complete switch from desktops to mobile computing platforms, including netbooks and internet-capable mobile phones. In fact, according to a recent study, over 50% of 15-30 year-olds in the US, UK and China indicated that they would choose a mobile device over a PC for Internet access [7]. Many young people making their own decision about technology purchases, especially those from lower income families, may prefer to forgo a desktop or a laptop in favor of a mobile phone with added features and Internet connectivity. As a result, with many web-based applications accessible via mobile phones, they are becoming a central hub for all modes of communication, social networking, and entertainment for young people.

Increased range of features, data services, the amount of information that users choose to store on their mobile devices requires a greater level of protection. Broad range of advanced functionality makes mobile devices more expensive and, in case of theft or loss, would lead to a substantial financial loss. However, as the users choose to store an increasing amount of sensitive information (such as e-commerce web site logins), misuse or theft of a mobile phone could easily lead to unauthorized purchases, banking transactions, or enable identity theft. In the event if a mobile phone is stolen, user authentication becomes the first line of defense against misuse of sensitive information that may be stored in it. Presently, the most widely used methods of authentication on mobile phones are PINs and passwords. Notwithstanding the fact that such knowledge-based methods do not offer the best protection features, a number of surveys indicate that many mobile users are either unaware or do not use these security features available on their mobile phones. For example, a survey of 297 mobile phone users reported by Clarke and Furnell [3] found that 34% of the respondents did not use any PIN or password security. This widely cited survey was conducted via an online questionnaire over a period of two years up to February 2004; 86% of the respondents were male, 71% of whom were 17 to 24 years old. This survey examined the attitudes of users towards security on mobile phones, their usage patterns, as well as attitudes using biometric technologies as security enablers on mobile phones. A survey described in the remainder of this paper was conducted, in part, to answer a set of similar questions, but with the focus on digital natives.

3. Survey participants

We surveyed over 330 undergraduate students enrolled in a broad range of general education Computer Science and Information Technology courses in 2009. All students enrolled in these courses were asked to complete a written questionnaire. Participation in the survey was strictly voluntary and survey participants were not screened in any way. Less than 2% of the students responding to the survey were Computer Science or Information Technology majors. Overall, survey respondents ranged from 18 to 47 years of age. 55% of the respondents were male and 45% female. Since this work focuses on mobile phone usage by young people, the rest of the discussion refers only to the answers collected from the 304 respondents who were between the ages of 18 and 25 with age distribution shown in Figure 1. The ratio between males and females was the same as in the complete data set.

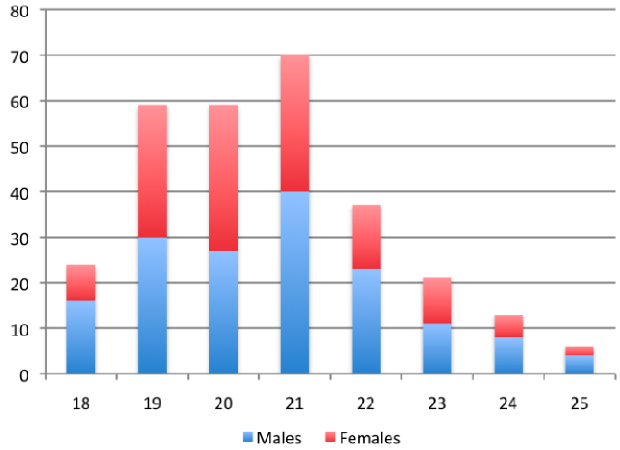

Figure 1. Age distribution of survey respondents.

According to some estimates, as of the middle of 2009, over 89% of all US residents had mobile phones [4]. Since the category of users between ages 15 and 24 has been reported to have the highest mobile phone penetration of all other age groups, it is not surprising that in our survey, all but four respondents had a mobile phone.

As a part of our survey, we asked the participants to identify themselves with one of five behavioral scenarios that directly corresponded to the technology adoption classes including innovators, early adopters, early majority, late majority, and laggards, as shown in Figure 2. This classification was popularized by Rogers [17]; it describes the process by which technological innovations propagate through different layers of society, as well as different categories of individuals and their roles in spreading these innovations. As expected, less than 3% of respondents classified themselves as innovators, while 63% identified themselves with either early or late majority. Males were disproportionately represented among the early adopters, while the laggards category included a higher percentage of females.

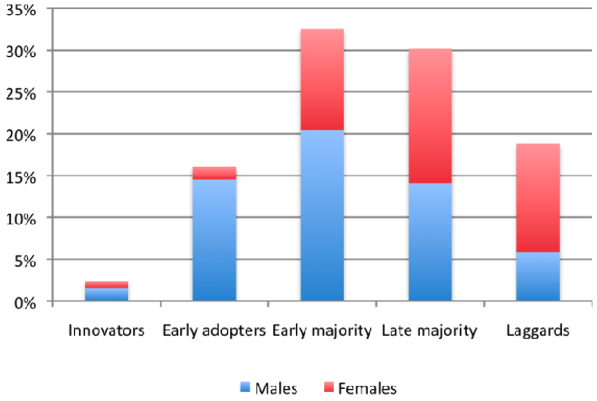

Figure 2. Technology adoption classes.

Survey participants were also asked to assess the level of their technical skills and general 'tech-savviness'. As shown in Figure 3, nearly 50% of all respondents indicated that they possess low to somewhat low technical skills, which directly contradicts the proposition that digital natives have advanced technological skills. Surprisingly, according to their own self-assessment, females indicated to have significantly higher technical skills than males.

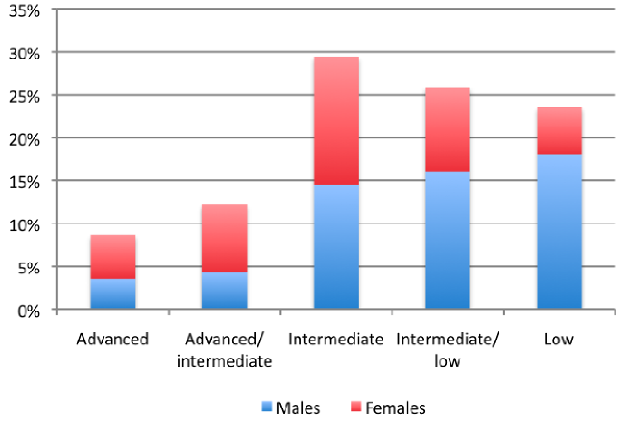

Figure 3. 'Tech-savviness' of survey participants.

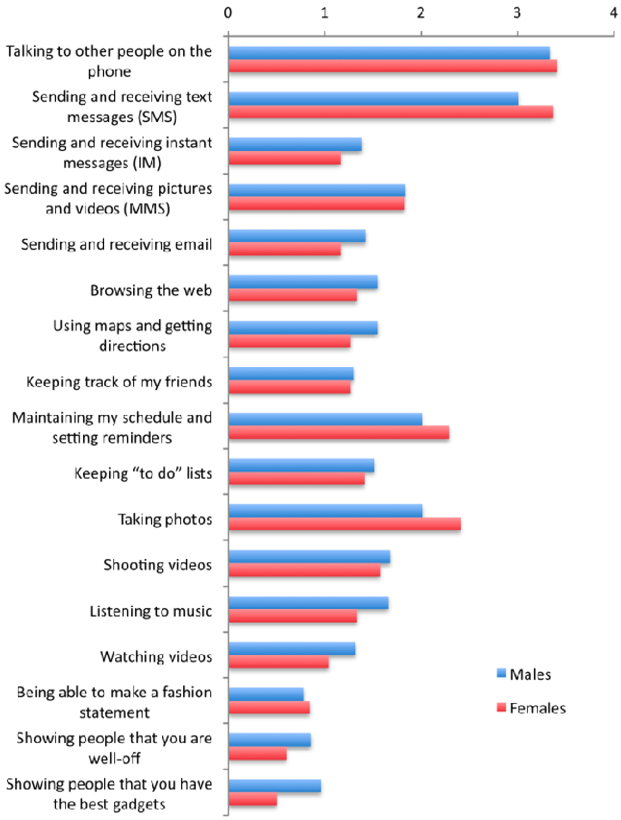

Figure 4. Relative importance of different mobile phone use cases.

4. Usage of mobile technologies

Our findings regarding the patterns of mobile phone usage by undergraduate students are largely in line with the data reported by EDUCAUSE in their 2009 Study of Undergraduate Students and Information Technology [5]. Our work aimed to identify students' perceived importance of different ways was how mobile technology is used in society. Students were asked to rank relative importance of mobile phone use cases, which comprised several categories:

- Basic communication: voice calls and text messaging;
- Advanced communication: IM, MMS, email, and web browsing;
- Productivity: using maps, schedules, reminders, and to-do lists;
- Entertainment: taking photos, listening to music, shooting and watching videos;
- Social status: making a fashion statement with a mobile phone, and impressing people with by owning expensive or advanced devices.

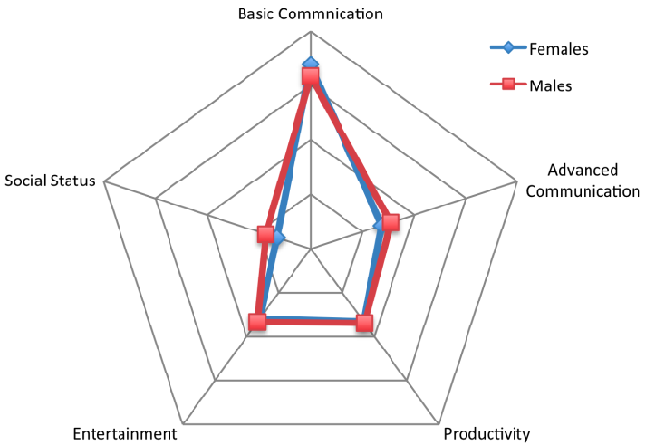

Figure 5. Categories of mobile technology usage.

As shown in Figure 5, relative importance of different categories of mobile technology use cases varies significantly. By far, basic communication is valued the most, although males give this category a very slight preference. Overall, there is little difference between the preferences of males and females. Contrary to the underlying premises of the 'digital natives' phenomenon, our group of respondents was more interested in basic communications and entertainment, than in advanced communication and productivity features of their mobile devices. As suggested by Prensky [13,14] and others, digital natives possess advanced technological skills and use technology in unprecedented ways to supplement many day-to-day and educational activities. Our survey results show the opposite trend: young people tell us that they use mobile technology almost exclusively for the most basic purposes, such as making phone calls and texting.

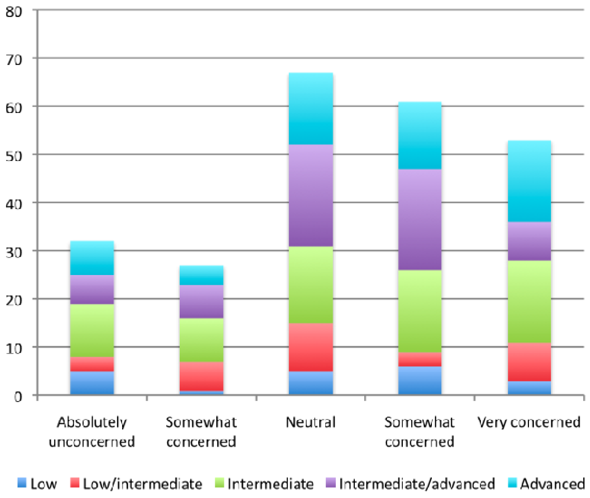

Figure 6. Security concerns of survey participants, by 'tech-savviness'.

5. Concerns about security

When asked whether they are concerned about the security of data stored on their mobile phones, 47.5% of the survey respondents were somewhat or very concerned, as shown in Figures 6 and 7. Not surprisingly, users who perceived themselves as ‘tech-savvy’ were generally more concerned about mobile data security. In terms of their self-reported technology adoption attitudes, innovators, early adopters and the early majority were significantly more concerned about mobile data security than the late majority and laggards.

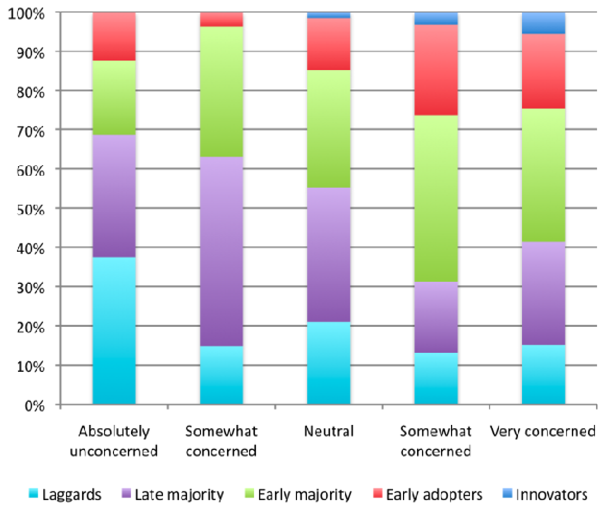

Figure 7. Security concerns of survey participants, by technology adoption class.

Emergence of different kinds of malware, including viruses, worms and Trojan horses, is a significantly increasing concern for many mobile computing platforms. If the experience with desktop computers is any indicator of the things to come, increased computing power and network connectivity will inevitably make many mobile devices widely susceptible to intrusion by malicious code. Recent news reports [8] indicate that a number of iPhones have been compromised by hackers who could remotely access the device left vulnerable after jailbreaking (a process that allows running unofficial code on iPod Touch and iPhone devices bypassing official distribution mechanisms provided by Apple). Current research indicates that capable viruses could spread relatively quickly on mobile phones utilizing open Bluetooth or WiFi channels, as well as via multimedia messaging services (MMS) [18]. Similarly to downloading desktop software from unknown sources, installing games and applications that have not been verified by a trustworthy agency (e.g. Apple App Store) could also help spreading mobile malware. It has been suggested that the only barrier that holds the potential flood of mobile viruses is a simple fact that it is difficult to make any money by spreading malware on mobile devices. In contrast, desktop worms and viruses are often used to create botnets out of infected computers that are used to send out spam messages. Today, nevertheless, malware on mobile platforms is a reality and it is important for mobile users to understand how malware could infect a mobile phone and its possible consequences.

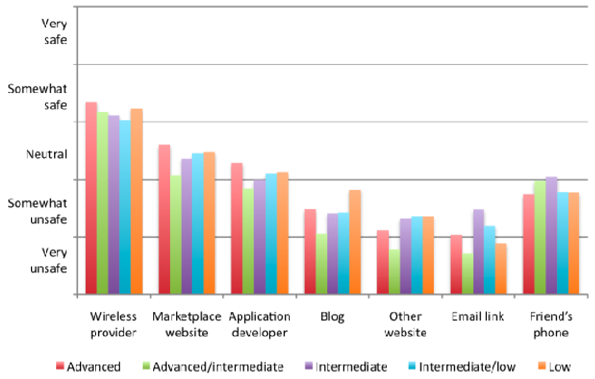

Figure 8. Perceived threats to mobile devices, by ‘tech-savviness’.

We asked our survey participants about their perceived safety of downloading games and applications from a number of sources, such as a wireless provider (e.g. AT&T or T-Mobile), a marketplace web site (e.g. Apple App Store, handango.com, pocketgear.com), an application developer’s website (e.g. eamobile.com), a blog covering mobile applications and games, some other website, a link in an email, or by copying from a friend’s mobile phone.

As shown in Figures 8 and 9, although our respondents indicated a relatively high confidence in the safety of software downloaded from a wireless provider, they are rather skeptical about the safety of software originating from an application marketplace. This is surprising because by their very definition, software offered by these marketplaces is as trustworthy as the offerings of wireless providers. Such a disparity of opinions could be due to the ignorance of our survey participants about the verification process that all applications must undergo when they are offered for sale or download via an application marketplace, such as Apple App Store or Android Market. Furthermore, survey respondents tend to trust their friends more than they trust experienced reviewers who publish their opinions on specialized blogs; they also trust their friends nearly as much as application developers. A number of interesting trends emerge according to the respondents’ self-assessment of their technical skills and ‘tech-savviness’. Users with low level of technical skills tend to trust wireless providers and blogs more than other users. At the same time, users who perceive themselves as 'tech-savvy' tend to give more trust to applications acquired from marketplaces and directly from application developers.

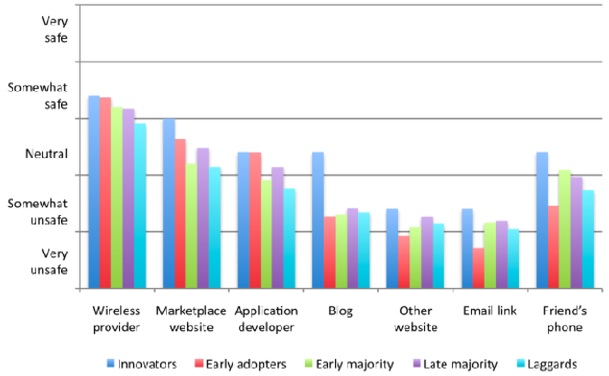

Figure 9. Perceived threats to mobile devices, by technology adoption classes.

Another trend emerges when the user's security confidence is plotted against their safe-assessed membership within the classes of technology adoption [17]. More than anybody, technology innovators would trust applications acquired from blogs and friends, which can be explained by their desire to try new things and willingness to pay for the possible consequences and compromising their security.

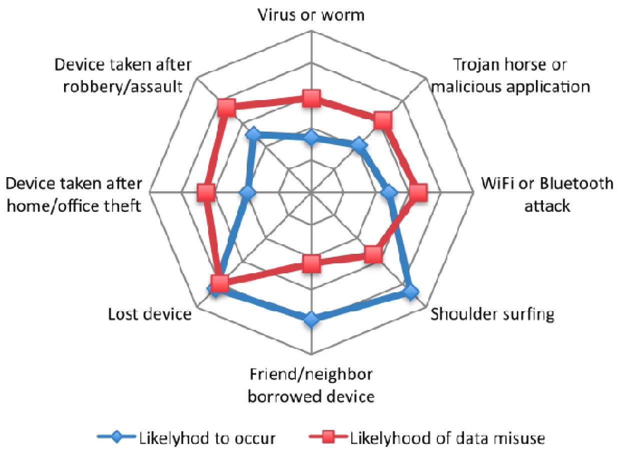

Figure 10. Sources of threats and severity of their consequences.

We asked the survey respondents to weigh the likelihood of different events that could potentially compromise the security of data stored on a mobile device, as well as the likelihood that any private or sensitive data will actually be misused as a result of such an event. Possible scenarios included a virus or worm somehow getting onto a mobile device; a Trojan horse (any game or other application that appears to work as promised, but may allow criminals to access the data on the device); a wireless attack using a Bluetooth or WiFi connection; shoulder surfing (which occurs when someone looks over the shoulder of a person using their mobile phone to see anything that may be displayed on the screen); allowing a friend/relative/neighbor/etc. to borrow a mobile device; accidentally losing a mobile device; losing a mobile device as a result of a home/office intrusion; and losing a mobile device as a result of a robbery. Figure 10 shows the likelihood of occurrence for a range of threats to security and privacy of mobile users along with the likelihood of adverse consequences, as our survey participants perceive them. The data clearly shows that young people in our survey simply believe that losing the device is the most likely cause for a possible data misuse. Our survey participants generally do not believe that the data on their mobile phones could be misused if the device is compromised by malware or by an attack via a wireless channel. Surprisingly enough, our survey participants believe that the chances of private or sensitive data misuse are higher if they accidentally lose a device than as a result of a deliberate theft. It is possible to observe a trend that our survey participants are much more concerned about the possibility and the consequences of adverse events in a social context (theft and loss) rather than those with a technical connotation (malware or wireless attacks).

6. PIN-based authentication

PIN-based methods are currently the predominant and often are the only available way to secure mobile devices and the data stored on them against a potential misuse. However, many users do not take a full advantage of this feature. Little has changed since Clarke and Furnell published their study in 2005 [3], which reported that 66% of the surveyed mobile users employed PIN-based authentication when switching on the device. 45% of users surveyed by Clarke and Furnell never changed their PIN code and 42% changed it only once after purchase. Since our work specifically targets digital natives that by definition are supposed to be more technically savvy, we expected our results to reflect their higher level of technical skills and understanding of technology.

Approximately 80% of our survey respondents were aware of their phones' capability to be locked using a PIN code, while 67% were aware of locking a SIM card with a PIN. Approximately 29% of all respondents indicated that they used phone lock PIN codes and 20% said that they secured their SIM card with a PIN. 14% of all respondents indicated that they actively use both kinds of PIN codes. However, as shown in Figure 11, many surveyed young people utilizing PIN-based authentication are actively undermining their efforts by keeping default values of PIN codes or changing them only once after acquiring the device: 59% of our survey participants had never changed their PIN codes and 35% changed them only once after purchase.

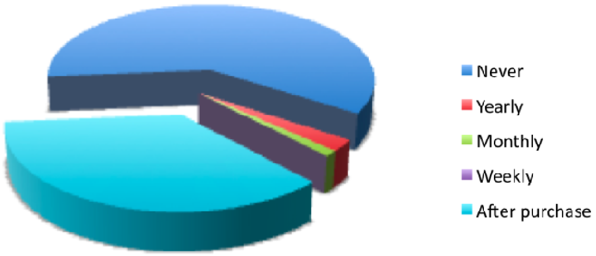

Figure 11. Survey participants changing their PINs.

Figures 12 and 13 summarize the survey respondents' attitudes regarding the use of mobile phone PIN codes. Less than 29% use PINs to lock their phones and only about 20% use PINs to lock SIM cards. This data provides a sharp contrast to the results reported by Clarke and Furnell who reported a significantly higher number of users (66%) taking advantage of PIN-based authentication. At the same time, over 80% of respondents are aware of phone-level PINs (67% are aware of SIM-level PINs), which clearly shows that the lack of knowledge is not the reason why young people choose to leave their mobile devices unprotected. The data indicates that 56% of survey respondents generally believe that PINs provide an adequate level of security and 63% agree that PIN codes are convenient to use.

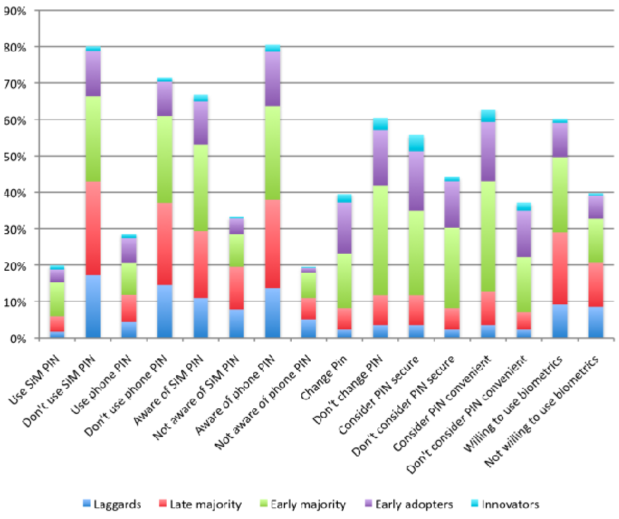

Figure 12. Attitudes about PIN-based and other forms of authentication based on technology acceptance classes.

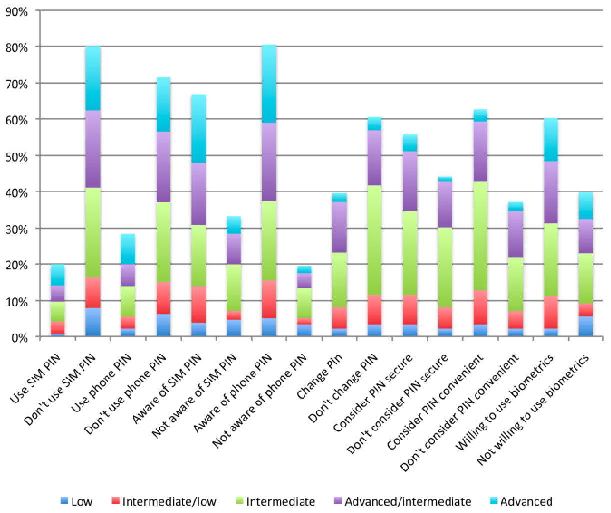

Figure 13. Attitudes about PIN-based and other forms of authentication based on 'tech-savviness'.

7. Discussion

Our survey results suggest that overall young people are concerned about the security of private or sensitive information stored on their mobile phones and are generally aware of the possible consequences of losing or compromising this information. Only 24% of the survey participants indicated that they had little or no concerns about privacy and security associated with using mobile phones. Generally, they are also aware that their phones can be locked by a simple PIN code. However, there seems to be a disconnect between this general awareness and the actions that young people take to protect themselves, their mobile devices and the private or sensitive data stored on them. Furthermore, although our survey participants are concerned about their privacy and security, they do not seem to understand the real sources of threats and the severity of possible consequences. According to our results, young people believe that losing their mobile phone is the most likely threat to the security of their private or sensitive data, yet 80% of them choose not to use PIN codes to lock their devices. Young people participating in our survey rank malware and wireless attacks as the least likely causes of compromising or losing private data stored on their mobile phones, but the vast majority admits that they do not understand the technology basics, which questions their ability to reasonably evaluate such threats.

When we started the work on this survey, we expected that our results would be in line or better than those reported by Clarke and Furnell [3] since their survey was aimed at the general population, while ours was specifically targeted at young people. Although we had a healthy dose of skepticism regarding innate superior technical skills possessed by 'digital natives,' we were expecting that their understanding of technology and their use of the very basic security methods will be at least as good as that of the average users. The survey results, however, largely contradict our expectations. The most basic benchmark for such a comparison of the two studies, the use of PIN codes for authentication, was more than twice lower among our digital natives than among those surveyed by Clarke and Furnell. We believe that there could be two possible reasons for such a disregard for the most basic and the simplest form of authentication.

Young people participating in our survey appear to *lack technical skills* that would help them understand the importance of authentication. As shown in Figure 10, they downplay the possibility that their phones could be compromised by a virus, a worm or a Trojan horse, or that their device could be penetrated through a wireless channel. Although such incidents have been reported in popular media on many occasions (e.g. [15,16]), over 50% of young people surveyed in this study admit that they have low or low to intermediate technical skills, and, therefore, they may not fully understand technical features and capabilities of the technology they use. Consequently, they may not fully comprehend how this technology, devices and the data stored on them can be exploited to their disadvantage.

Participants of this survey do not fully *understand and/or downplay the implications of losing private or sensitive information*. Today, young people are used to sharing many aspects of their lives using online social networks such as Facebook and Twitter. This includes posting up to the minute updates about many of their activities, pictures that they want to share with a circle of their friends, and disseminating various kinds of gossip. Many pieces of information that previous generation considered private, are posted for public view and enjoyment by the digital natives of today [6]. This could influence a degree of carelessness with which the participants of our survey view different threats that could compromise sensitive data on their mobile phones. Although identity theft has become a widely discussed topic, young people may not consider its consequences seriously or think that it can only happen to somebody else. In early days, perpetrators had to 'dumpster dive' or steal checks and credit card offers from the mail. Today, however, much of identity theft is enabled by technology. Despite the commonly held belief that digital natives have an innate affinity to technology and understanding of all things digital, our sampling of opinions appears to contradict this assumption.

8. Summary

This work was envisioned as an update to Clarke and Furnell's study of security-related attitudes and practices of mobile phone users, as well as an examination of the claim that the members of the 'digital native' generation possess advanced technical skills. We chose to focus on young people's use of mobile phones because this technology has truly become an indispensable part of their lives. Additionally, an ongoing debate concerning digital natives has been largely focused on the educational aspects of using the Internet and Web 2.0, with very few reports ever mentioning how digital natives use mobile technology.

Our findings generally contradict the assumption that digital natives are more technically advanced than the rest of us. It is true that they use technology in general and, in particular, mobile phones on a daily basis and for a broad variety of tasks. However, in the context of mobile phones, the most basic ones, such as calling and texting, overwhelmingly dominate the list these tasks. When it comes to security issues, our survey participants were mostly ignorant about the technical aspects of possible threats to their security and privacy. Consequently, they have largely downplayed the likelihood and possible severity of technology-enabled threats, such as malware or an intrusion via a wireless channel. Finally, four out of every five of our survey participants said that they are aware about PIN-based authentication, while only one out of every three reported actually using it. This rate is more than twice less than that reported by Clarke and Furnell. Such a disregard for the most basic and the simplest form of authentication could be a sign of a larger problem: digital natives may not be all that advanced in their technical skills and may lack a sufficient understanding of the implications that mobile technology has on many aspects of their lives.

9. References

[1] Bennett, S., Maton, K., Kervin, L. The 'Digital Natives' Debate: A Critical Review of the Evidence. *British Journal of Educational Technology*. 39(5), pp. 775-786, 2008.

[2] Botha, R.A, Furnell, S.M., Clarke, N.L. From Desktop to Mobile: Examining the Security Experience. Computers & Security, 28(3-4), pp. 130-137, May-June 2009.

[3] Clarke, N.L., Furnell, S.M. Authentication of Users on Mobile Telephones – A Survey of Attitudes and Practices. *Computers & Security,* 24(7), pp. 519-527, 2005.

[4] CTIA–The Wireless Association. *Wireless Quick Facts, Mid-year Figures*, Retrieved Nov 18, 2009 from http://ctia.org/media/industry_info/index.cfm/AID/10323.

[5] EDUCAUSE Center for Applied Research. *The ECAR Study of Undergraduate Students and Information Technology, 2009*. Chapter 6, Undergraduates and the Mobile Revolution. Retrieved Dec 7, 2009 from http://www.educause.edu/ers0906.

[6] Fortunati L. Reflections on Mediated Gossip. In: Kristof Nyiri (ed.). *Engagement and Exposure. Mobile Communication and the Ethics of Social Networking*. Pp. 45-58, Wien: Passagen Verlag, 2009.

[7] IBM. *IBM Study Finds Consumers Prefer a Mobile Device Over the PC*. Retrieved Dec 12, 2009 from http://www-03.ibm.com/press/us/en/ pressrelease/25737.wss

[8] Keizer, G. New iPhone Worm Steals Online Banking Codes, Builds Botnet. *Computerworld Security*. Retrieved on Mar 17, 2010 from http://www.computerworld.com/s/ article/9141354

[9] Kennedy, G., Dalgarno, B., Gray, K., Judd, T., Waycott, J., Bennett, S., Maton, K., Krause, K.-L., Bishop, A., Chang, R., & Churchward, A. The Net Generation Are Not Big Users of Web 2.0 Technologies: Preliminary Findings. Proc. of *ICT: Providing Choices for Learners and Learning Conference*, 2007.

[10] Kennedy, G., Judd, T., Churchward, A., Gray, K., Krause, K.-L. First Year Students' Experiences with Technology: Are They Really Digital Natives? *Australasian Journal of Educational Technology*, 24(1), pp. 108-122, 2008.

[11] Kvavik, R. Convenience, Communications, and Control: How Students Use Technology. In Oblinger, D., & Oblinger, J. (Eds.), *Educating the Net Generation*, Ch. 7. Retrieved Nov 16, 2009, from http://www.educause.edu/educatingthenetgen.

[12] McAfee. *Mobile Security Report 2008*. Retrieved on Dec 12, 2009 from http://www.mcafee.com/us/research/ mobile_security_report_2008.html

[13] Prenksy, M. Digital Natives, Digital Immigrants: Do they really think differently? *On the Horizon*, 9(6), pp. 1-6, 2001.

[14] Prensky, M. Listen to the Natives. *Educational Leadership*, 63(4), pp. 8–13, 2005.

[15] Reuters. *Experts warn mobile phones face hacking threat*. Retrieved Dec 12, 2009 from http://www.reuters.com/ article/idUSTRE5502RD20090601

[16] Reuters. *NY thieves want iPhones, victims are fighting back*. Retrieved Dec 12, 2009 from http://www.reuters.com/ article/idUSN1734775920090702

[17] Rogers, E.M. *Diffusion of Innovations*, 5th Ed., Free Press, 2003.

[18] Wang, P., González, M.C., Hidalgo, C.A., Barabási, A.-L. Understanding the Spreading Patterns of Mobile Phones Viruses, *Science*, 324, pp. 1071-1076, 2009.