information

MDPI

Article

Security Awareness of the Digital Natives

Vasileios Gkioulos [1,†,*], Gaute Wangen [1,†], Sokratis K. Katsikas [1,2,†], George Kavallieratos [2,†] and Panayiotis Kotzanikolaou [3,†]

1 Department of Information Security and Communication Technology, Norwegian University of Science & Technology, 2802 Gjøvik, Norway; gaute.wangen@ntnu.no (G.W.), sokratis.katsikas@ntnu.no (S.K.K.)
2 Department of Digital Systems, University of Piraeus, 18532 Piraeus, Greece; georgekavallieratos0@gmail.com
3 Department of Informatics, University of Piraeus, 18532 Piraeus, Greece; pkotzani@unipi.gr
* Correspondence: vasileios.gkioulos@ntnu.no; Tel.: +47-61135162
† These authors contributed equally to this work.

Academic Editor: Rami J. Haddad
Received: 8 March 2017; Accepted: 5 April 2017; Published: 8 April 2017

Abstract: Young generations make extensive use of mobile devices, such as smartphones, tablets and laptops, while a plethora of security risks associated with such devices are induced by vulnerabilities related to user behavior. Furthermore, the number of security breaches on or via portable devices increases exponentially. Thus, deploying suitable risk treatments requires the investigation of how the digital natives (young people, born and bred in the digital era) use their mobile devices and their level of security awareness, in order to identify common usage patterns with negative security impact. In this article, we present the results of a survey performed across a multinational sample of digital natives with distinct backgrounds and levels of competence in terms of security, to identify divergences in user behavior due to regional, educational and other factors. Our results highlight significant influences on the behavior of digital natives, arising from user confidence, educational background, and parameters related to usability and accessibility. The outcomes of this study justify the need for further analysis of the topic, in order to identify the influence of fine-grained semantics, but also the consolidation of wide and robust user-models.

Keywords: security; mobile devices; digital natives; security awareness; user behavior; education

1. Introduction

Mobile devices (i.e., cellphones, laptops, tablets) have become an indispensable part of our everyday life, since they fulfill the increasing users' desire for Internet connectivity and access to information, social and private networks at any time and place. Owing to the proliferation of "smart" devices and the escalating dependency on them with respect to the execution of everyday tasks, they have evolved from a communication medium to a multifunctional equipment. The reduced cost, in combination with the increasing computational and storage capacity of mobile devices, allow them to accommodate critical functionalities with significant security and safety related impact such as e-banking, control systems and Internet of things architectures. Such devices do not simply store information related to their owners, but also receive data on people and infrastructure related in some way to them. As a result, they can retrieve, store and modify extensive quantities of diverse and potentially sensitive information.

Furthermore, the users are accustomed to the notion of continuous connectivity, even across networks with potentially unknown configurations. Such transmissions are likely to be vulnerable to unauthorized access and, consequently, they constitute a security risk. In many cases, these risks materialize as direct criminal attacks, such as privacy intrusions or unauthorized disruptions of

communication. Moreover, they can expose the users to more complex types of malicious activity, such as identity theft, blackmailing, active data collection, or defamation. In light of the increasing risks due to the aforementioned use of mobile devices, it is important that users are aware of the risks they are exposed to and, more importantly, that they are informed about how to protect themselves.

Therefore, the aim of this study is to investigate the user behavior of digital natives from distinct educational backgrounds and levels of security competence. We seek to identify how user confidence, security awareness and background affect their decisions, in aspects related to the use of their mobile devices that can inflict significant security related impact. More specifically, this study investigates how the background and technical competence influences the digital natives' security awareness within five focus areas: (i) Use of Mobile devices, (ii) Connectivity and Network Access, (iii) Management of Credentials, (iv) Knowledge and Fear of Risks, and (v) Self-evaluation of security awareness. With this study, we aim to understand how young people use their mobile devices, how well they know them, and what their concerns are, in order to help improve the secure and safe use of these devices. Our results outline the generic properties of the whole sample and the categorical differences across the groups (see Section 3) within the focus areas.

The results of this study are useful both for designing educational and awareness campaigns, but also for purposes of user behavior modeling. With this article, we aim to highlight areas in which current security related knowledge dissemination is sufficient, areas where there is a clear difference in behavior across the digital natives, and areas where they lack knowledge as a whole or they choose usability over security. The remaining of the paper is structured as follows: Section 2 discusses related work, while Section 3 presents the methodology used for this study. Subsequently, in Section 4, we present the results of the executed surveys, identifying categorical differences across the groups and discussing their origins. Finally, Section 5 summarizes the results extracted from our analysis, while we conclude with presenting the limitations of our study and potential paths for future work.

2. Related Work

Since 2014, mobile devices have been becoming the leading digital platform, displacing the desktop PC [1]. Prensky [2] writes that the digital natives have radically changed their way of thinking by being exposed to technology almost since birth, while other scholars [3] have contested such claims. However, there is no denying that the digital natives have a different view of technology than older generations.

The scope of this article is the digital natives and their security awareness, related in particular to mobile devices. A considerable number of studies concerning user behavior, with regards to selecting and installing applications on smartphones, have found that users do not consider security and privacy issues during app selection, as they tend to ignore privacy policies and EULAs (End-user license agreement) [4]. Furthermore, Android users were found not to pay attention, understand, and act on permission information during installation [5,6]. Mylonas et al. [7] have explored the security awareness metrics of smartphone users who download applications from official application repositories. The authors of that study applied these to measure how the security background affects the smartphone security awareness of their sample, concluding that security background has a slight impact on awareness. The key differences between the current study and Mylonas et al. is that the latter applied self-rating as the independent variable for determining skill level, did not explicitly target the digital natives and investigated different areas of smartphone security awareness.

Furthermore, Mylonas et al. [8] explore the security awareness of smartphone users who download applications from official application repositories. The findings from said study show that users are complacent in their smartphone security behavior and display high levels of trust towards smartphone application repositories. In addition, they rarely consider privacy and security when installing new applications, and do not install adequate protection mechanisms [9]. Additional research into users and protection mechanisms partially contradicts the idea that smartphone users are not security aware, and finds several correlations between security awareness and smartphone OS,

language, and gender [10]. However, the said study [10] does not specifically target the digital natives, despite them being the majority of users. More related to the topic are the studies conducted by Markel and Bernik [11] and Markel and Zgaga [12]. These papers report the findings of a survey carried out in 2011 among 281 students of Slovenian faculties, investigating threat perception on mobile devices [11] and in cyberspace [12]. The findings show that the sample student population had a low awareness of security threats and security measures, and the authors suggest that education and awareness levels must be increased in Slovenia to counter this development.

A common argument towards the reviewed studies is that, although they address a similar topic, they are geographically limited [11–13] or they investigate behaviors in relation to subsets of technologies [5,6,9] and problems [4,7–9] that are not specifically related to the digital natives. Ariu et al. [14] have worked on filling this gap by studying the level of awareness and perception of IT security amongst university students, paying particular attention to the world of mobile devices. Their report analyses the answers given by 1012 students from over 15 Italian universities to a multiple-choice questionnaire. The analysis shows that students' perception of their knowledge is generally wrong and that they are unaware of the risks arising from their behavior. This paper builds on the Ariu et al. results and supplements with two additional datasets, thus expanding the knowledge base. The second data set targeted generic computer science students, while the third dataset targeted information and cyber security students specifically.

3. Methodology

This article builds on a previous study [14] on the topic of security awareness of the digital natives, and was conducted to investigate the differences in risk perception across three distinct groups categorized by their technical background. This section has the following structure: the first sub-section addresses the choice of data collection method and instrument, followed by the sample description, and a brief overview of the statistical methods used for data analysis.

3.1. Data Collection and Instruments

The survey aimed to explore the security awareness of the digital natives addressed to students of the digital age, i.e., persons who were born in the years of the technological boom in Information Technology and Communications (ICT), between 1987–1997. Universities are ideal since they comprise a diverse population. Thus, the sample of this study comes from students born within range. We found the online questionnaire to be the best option for data gathering as it reaches a broad audience and provides a strong level of anonymity; therefore, the presented datasets were collected using Google Forms.

The original survey was developed by Ariu et al. and initially ran in multiple Italian universities [14]. The survey had 60 questions that investigated security awareness aspects within the five areas outlined in the introduction. As for the level of measurement, the questionnaire had categorical, ordinal, and continuous type questions. Category type questions are used here mainly for demographics, while the main bulk of the questionnaire was designed using several mandatory scale and ranking questions.

3.2. Sample and Analysis

This study utilises three distinct samples:

- The data set collected by Ariu et.al., which was targeted at the Italian digital natives, is included in this study and corresponds to our general security competence group (GSCG). The sample consists of 1012 respondents from various university departments (Including law, engineering, computer science, humanitarian, marketing, and multiple other faculties not directed to IT education), which are mapped for the purposes of this study to the general population of digital natives.
- Secondly, we collected data for the medium security competence group (MSCG) by targeting digital natives from Greece with education exclusively in computer science. This group is

expected to a have wider knowledge over the use of mobile technologies and increased awareness over security related aspects due to their educational background. The sample consists of 303 responders in total at the undergraduate (234), postgraduate (54), and doctoral (15) levels.

- Finally, the target population for the high security competence group (HSCG) was undergraduate, postgraduate and doctoral students of information security from Norway. These were expected to have a higher security awareness regarding the four main areas than the medium and generic groups, due to their specialized education. For this group, we had 35 respondents in total, of which 21 are undergraduate students, 10 postgraduate, and four doctoral students.

The difference in quantity of respondents for each survey reflects the scarcity of each group in the general population; for example, there are more respondents in GSCG than MSCG, and more in MSCG than HSCG, with the latter group was large enough for the central limit theorem to apply [15]. For the descriptive data analysis, we primarily consider differences in the frequency distributions, while we used the security competence groups as categorical data for bi-variate analysis. The questionnaire primarily asked categorical and ordinal multiple-choice questions, while, as a measure of central tendency for ordinal questions, we considered the median, variance, and range.

4. Analysis of Results and Discussion

The individuals participating in the survey, across all competence groups, were requested to self-evaluate their knowledge on aspects related to information security, both before and after participating in the survey (Table 1 and Figure 1). A degradation is noticeable at the "before" and "after" responses across the groups, with the exception of HSCG group participants that selected "Insufficient". In conjunction with the results presented in the following sections, this is attributed to the increased user confidence that characterizes the everyday use, when security threats are not prioritized or not directly visible. This contributes to the unjustified perception of being secure, hence intensifying the security risk, and necessitates increased effort towards educating and making the users aware of the risks.

Table 1. How do you assess your knowledge on information security?

		Excellent	Good	Sufficient	Insufficient	Minimal
Before	*GSCG*	*6.5%*	*36.6%*	*39.3%*	*16.0%*	*1.6%*
	MSCG	9.3%	38.5%	35.3%	15.4%	1.3%
	HSCG	14.3%	48.6%	28.6%	8.6%	0.0%
After	*GSCG*	*4.4%*	*27.4%*	*34.4%*	*30.7%*	*3.1%*
	MSCG	6.7%	36.5%	31.7%	21.2%	0.6%
	HSCG	11.4%	51.4%	34.3%	2.9%	0.0%

GSCG: general security competence group; MSCG: medium security competence group; HSCG: high security competence group.

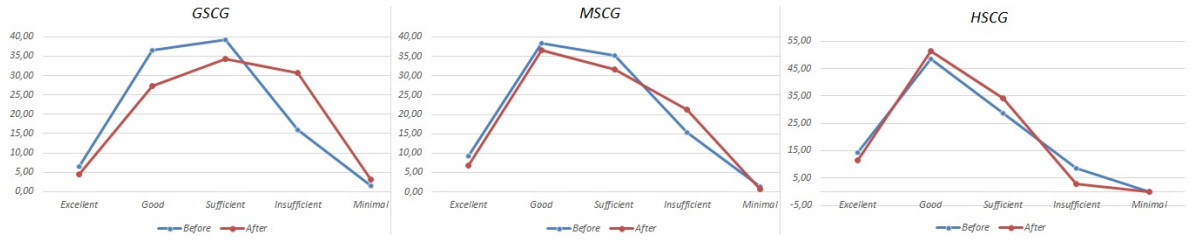

Figure 1. How do you assess your knowledge on information security?

4.1. Use of Mobile Devices

This section includes questions related to the use of mobile devices and applications, as well as questions related to user behavior when selling or losing a mobile device, and modifying its operating system.

We asked the digital natives what they store on their mobile devices, while a section of the question referred to personal passwords. As presented in Table 2, despite the frequent warnings, an average of 29.1% of the responders stores personal passwords in their mobile devices, regardless of their security related competence or background.

Table 2. Do you store personal passwords on your mobile device? (in plaintext)

	Yes	**No**
GSCG	*27.7%*	*72.3%*
MSCG	31.1%	68.9%
HSCG	28.6%	71.4%

Subsequently, we asked the digital natives if, in the case of loss/theft of their mobile device, they reported the event to the authorities. The results that are presented in Table 3 highlight the fact that the users are not widely aware of the ability to deny access to wireless networks based on the IMEI (International Mobile Equipment Identity) and other misuse countermeasures. Additionally, some of the differences in the responses between the GSCG and the MSCG/HSCG groups are likely caused due to regional variations in legislation, trust in the efficiency of the authorities, and the awareness of related countermeasures.

Table 3. Have you reported the loss/theft of your device to the authorities?

	Yes	**No**
GSCG	*68.5%*	*31.5%*
MSCG	33.5%	66.5%
HSCG	28.6%	71.4%

The next question focused on software updates on cellphones/tablets and laptops. The results for each category of mobile devices are presented in Table 4 and Figures 2 and 3. It is noticeable that 14.5% of the GSCG group state that they do not update anything in their laptops, while across all groups, updating only the applications ranks higher than updating only the operating system. Furthermore, comparing the results of the two categories, we observe that the GSCG and MSCG groups better maintain the software of their cellphones/tablets in comparison to their laptops.

Table 4. Do you regularly update the software on your mobile device?

		Apps and OS	**Apps**	**OS**	**Anything**
Cellphone/tablet	*GSCG*	*81.3%*	*8.8%*	*6.8%*	*3.1%*
	MSCG	79.5%	8.3%	5.1%	4.2%
	HSCG	88.6%	8.6%	0.0%	2.9%
Laptop	*GSCG*	*75.3%*	*5.1%*	*5.2%*	*14.5%*
	MSCG	73.1%	5.8%	7.1%	8.0%
	HSCG	94.1%	5.9%	0.0%	0.0%

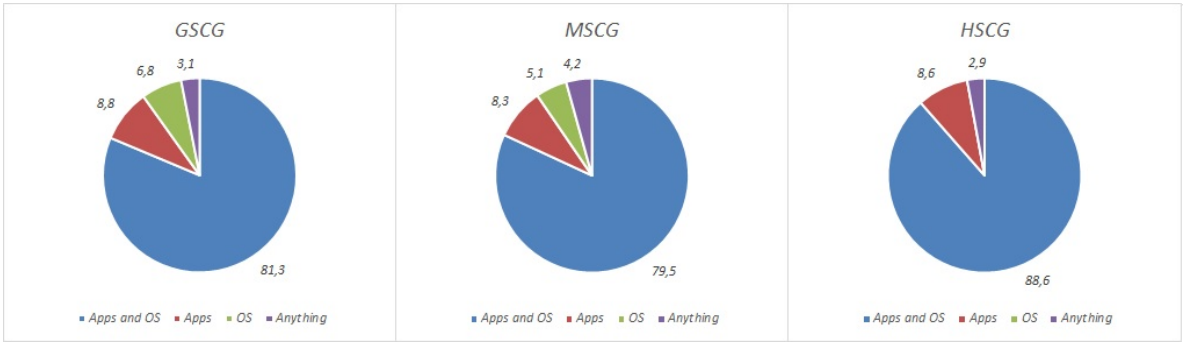

Figure 2. Do you regularly update the software on your mobile device? (cellphone/tablet)

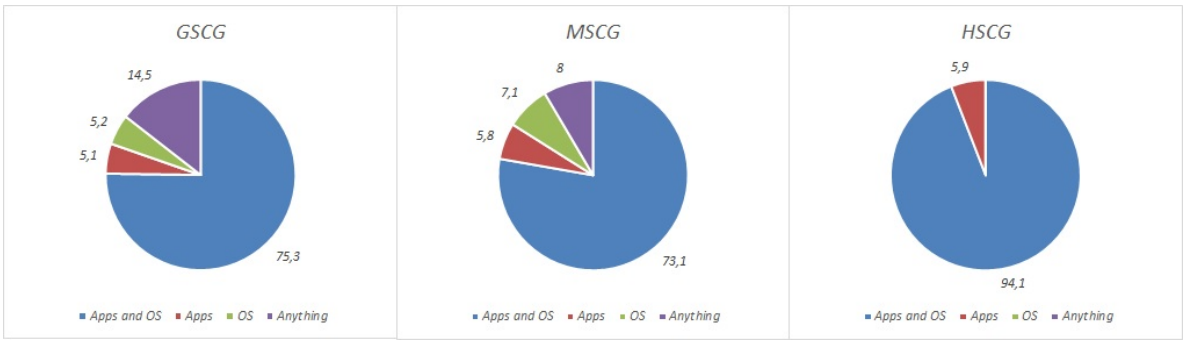

Figure 3. Do you regularly update the software on your mobile device? (laptop)

Regarding the use of applications, the next question focused on the sources that the digital natives use in order to download applications from, as presented in Table 5. Over 80% of the digital natives primarily use the official store, while an average of 12.3% across groups consciously uses non-official sources, regardless of the potential security threats. However, there is a positive correlation between security competence and application source.

Table 5. Where do you download applications from?

	Official Store	**Other Sources**
GSCG	*83.1%*	*16.9%*
MSCG	85.9%	11.5%
HSCG	91.4%	8.6%

Focusing on the behavior of the digital natives in terms of the application usage patterns, we asked how they manage their credentials when they have finished using an application. The results that are presented in Table 6 highlight that, regardless of knowledge on the potential privacy and other implications, they select usability over security, since only an average of 24.5% logs out. Furthermore, there is a notable difference between the MSCG and HSCG regarding saving the credentials, where the HSCG group more frequently chooses to save the credentials to stay logged in. Another notable finding is that a significant percentage of participants states that logging-out is "not important".

Table 6. As soon as you have finished using an application, you..?

	Save Credentials to Stay Logged in	Log out	Forget to Log out	Do Not Log out Because It Is Not Important	Do Not Log out Because I Do Not Know How
GSCG	*40.3%*	*24.1%*	*19.6%*	*10.3%*	*5.6%*
MSCG	30.8%	26.6%	16.7%	20.5%	1.9%
HSCG	48.6%	22.9%	14.3%	14.3%	0.0%

Another aspect of application usage patterns with significant security implications is the control of application access rights. Thus, we asked the digital natives how frequently they check the permissions that an application requires prior to accepting its installation. The results, in Table 7, show significant differences across the groups with a positive correlation between competence and security behavior. Analyzing these responses, in conjunction with the results of Table 6, highlights that expertise and knowledge can affect user behavior when security is not in conflict with usability.

Table 7. How frequently do you check the permissions (access rights) that the application requires before completing the installation?

	Never	Rarely	Often	Always
GSCG	*15.6%*	*38.2%*	*25.5%*	*20.7%*
MSCG	8.0%	26.3%	27.6%	34.9%
HSCG	5.7%	14.3%	40.0%	40.0%

A set of questions in this section focused on technical knowledge regarding mobile devices, in particular jailbreaking and rooting, as presented in Table 8 and Figure 4. The respondents across all groups seem to be familiar with these practices, and despite justifiably considering them potentially hazardous in terms of security, an average of 41.6% has used them in their mobile devices. The results show a difference between the groups where the competence level correlates positively with having a jailbroken or rooted mobile device, while the HSCG is slightly (8–10%) less likely to consider these practices as risky. It is evident, from the second data set presented in this table, that individuals with computer science/engineering background are less reluctant in applying such methods. This has also been traced across the GSCG group, when filtering the digital natives according to their academic background [14].

Table 8. Jailbreaking and rooting mobile devices

Do you know that smartphones and tablets might be jailbroken or rooted?		
	Yes	No
GSCG	*84.2%*	*15.8%*
MSCG	94.9%	5.1%
HSCG	94.3%	5.7%
Have you ever had your smarphone or tablet jailbroken?		
GSCG	*35.7%*	*64.3%*
MSCG	40.4%	59.6%
HSCG	48.6%	51.4%
Do you think these are risky practices?		
GSCG	*83.5%*	*16.5%*
MSCG	82.1%	17.9%
HSCG	74.3%	25.7%

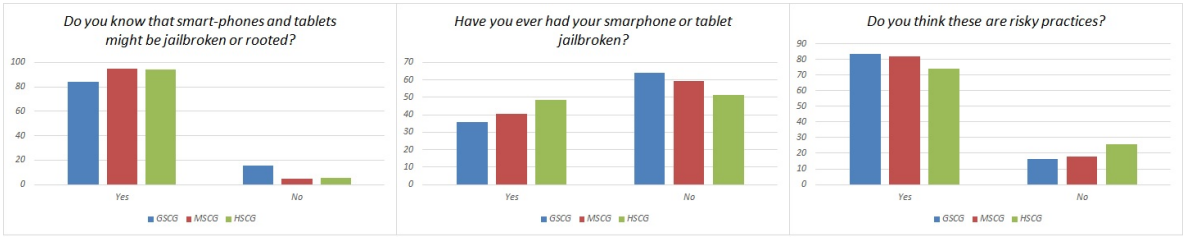

Figure 4. Visualization of Table 8 results.

Additionally to these results, the questionnaire included a number of propositions regarding the security of these techniques (jailbreaking, etc.), which the respondents had to evaluate as "True", "False", or "Unknown". An example of the investigated propositions is: *"Some Jailbreaking methods delete some operating systems' protections, which can be exploited by malicious code"*. In the majority of cases, these propositions have been answered incorrectly by all groups, suggesting that the digital natives are willing to apply such methods on their mobile devices, despite being aware of the involved security risks and without the required experience/knowledge.

4.2. Connectivity and Network Access

This section was focused on analyzing the behavior of digital natives towards connectivity and network access. The results show significant variations across the groups, while one of the most notable differences relates to user behavior when they have the opportunity to connect to an unsecured wireless network, as presented in Table 9.

Table 9. If you find free Wi-Fi, what do you do with your mobile device?

		I Connect and Use the Internet without Restrictions	I Connect but Only Do Activities That Do Not Require Credential Authentication	I Do Not Connect
Cellphone/tablet	*GSCG*	*43.6%*	*33.4%*	*23.0%*
	MSCG	26.0%	44.9%	21.8%
	HSCG	22.9%	34.3%	42.9%
Laptop	*GSCG*	*43.6%*	*33.4%*	*23.0%*
	MSCG	28.0%	46.9%	25.1%
	HSCG	25.7%	45.7%	28.6%

As presented in Figure 5, there exists a significant difference between the GSCG and the other two groups when it comes to connecting to free Wi-Fi, with both mobile devices and laptops, the former having the largest divergence. The MSCG are more likely to connect their mobile devices, but restrict the use of activities that require credential authentication. Moreover, the HSCG stands out with 42.9% opting not to connect with mobile devices at all, which represents a 20% difference from the two other groups. It is also noticeable that a larger portion of the HSCG (45.7%) opts to connect their laptops, rather than their mobile devices, to unsecured Wi-Fi with restricted activities.

Figure 5. If you find free Wi-Fi, what do you do with your mobile device?

The results across all types of mobile devices, show that user background and knowledge of the involved risks can affect their behavior, according to the significant differences across groups in response to the "I connect and use the Internet without restrictions" question. However, the results highlight that only with small exceptions across people with a security related background do users disregard or are unaware of the involved risks. Furthermore, users tend to be less reluctant when using their laptops in comparison to other mobile devices, potentially due to a falsely increased trust level in the security of such devices.

4.3. Management of Credentials

This section presents results in questions related to the management of credentials and the use of protection technologies. Initially, the digital natives have been asked about the solutions they use, in order to enforce access control to their mobile devices. The results revealed that 40.1% of the GSCG group, 19.9% of the MSCG group and 8.6% of the HSCG group choose to not use any access control mechanism in their mobile devices, while the pattern lock and PINs (Personal Identification Numbers) were the most popular solutions among the GSCG–MSCG groups and biometrics for the HSCG group. The results showed that the users' background can significantly affect related decisions regarding the overall use of access control mechanisms, while the exact choice of technologies can also be affected by financial or cultural agents.

Aiming to identify potential external influences on these results, we asked the digital natives to identify the reasons behind the decision to not utilize an access control mechanism. The results that are presented in Table 10 show that the usability of these mechanisms can significantly affect this decision. For the HSCG group, the use of access control was at 91.4%, with biometrics used in 54.3% of the sample, which highlights that users who are aware of the involved risks and provided with usable solutions (biometrics) will increasingly incorporate access control mechanisms.

Table 10. If you do not use a mechanism to protect access to your mobile device, why is that so?

	I Know Them but Never Thought About Using Them	I Know Them but I Am Not Interested in Using Them	I Know Them but They Make the Use of My Device Uncomfortable	I Do Not Know Them
GSCG	*13.6%*	*27.7%*	*52.5%*	*6.3%*
MSCG	3.0%	41.5%	51.0%	5.0%
HSCG	16.7%	33.3%	50.0%	0.0%

A further set of questions was dedicated to analyzing the use of passwords for authentication purposes. The results in Tables 11 and 12 show that a mixture of best and worst practices is implemented across the groups, with significant variations among the different password types.

Lasting and persistent awareness campaigns focused in the past several years on educating the public and raising awareness about best practices. However, these results show that, despite the visible positive influence, the system did not reach a stable state yet, while educating the users on security best practices requires sending a simple and clear message.

Table 11. For applications that require a password.

	I Always Use the Same Password for All the Applications	**I Use Small Variations of the Same Password for Different Applications**	**I Always Use Different Passwords**	**I Do Not Use Applications That Require Passwords**
GSCG	*20.6%*	*41.3%*	*31.7%*	*6.3%*
MSCG	8.7%	41.7%	39.1%	6.7%
HSCG	5.7%	51.4%	40.0%	2.9%

Table 12. What type of password are you most likely to use?

The passwords that I use are at least 8 characters long		
	Yes	No
GSCG	*87.0%*	*13.0%*
MSCG	83.7%	11.5%
HSCG	100.0%	0.0%
I use passwords that contain personal information		
GSCG	*36.5%*	*63.5%*
MSCG	36.8%	63.2%
HSCG	17.1%	82.9%
I use passwords that contain simple strings of characters (1234, qwerty, etc.)		
GSCG	*8.7%*	*91.3%*
MSCG	29.5%	80.5%
HSCG	0.0%	100.0%
I use passwords that contain meaningful words		
GSCG	*45.0%*	*55.0%*
MSCG	27.8%	72.2%
HSCG	34.3%	65.7%
I use passwords that contain numbers and special characters		
GSCG	*74.6%*	*25.4%*
MSCG	9.1%	90.9%
HSCG	97.1%	2.9%
If the system allows it, I do not use a password		
GSCG	*6.2%*	*93.8%*
MSCG	9.4%	90.6%
HSCG	14.3%	85.7%

4.4. Knowledge and Fear of Risks

This section included questions aiming to identify how the users perceive security related risks, their level of confidence in using their mobile device and their concerns. A summary of the results is presented in Figures 6 and 7, showing that the background affects the confidence of users in respect to security related risks, especially regarding laptop usage. However, a difference between the distributions corresponding to cellphones/tablets and laptops is noticeable. In correlation with the network access results presented in Section 4.2, this can be traced both to the maturity of the

technologies and the roles of the distinct devices in daily use. Additionally, it is evident that, despite their increased computational capacity, access to personal data, and incorporation into critical systems, the users, to a great extent, seem to still perceive smartphones and tablets in a more liberal fashion.

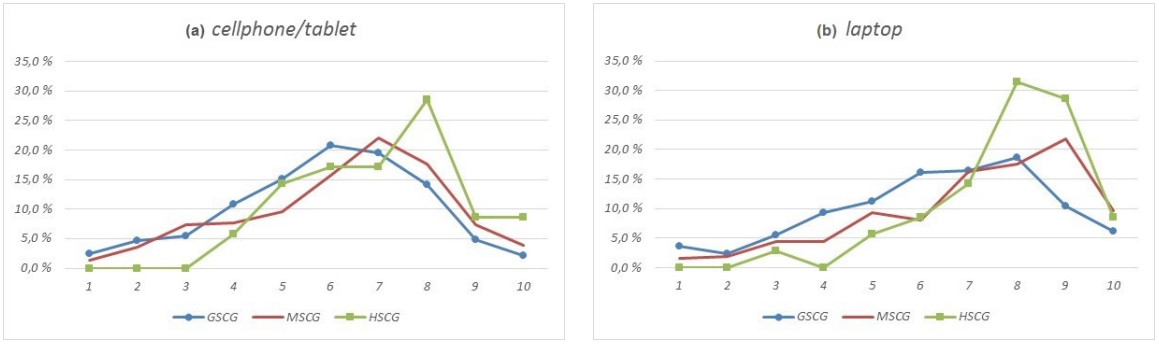

Figure 6. On a scale from 1 (none) to 10 (excellent), how do you assess your knowledge of issues and risks associated with the use of your—(**a**) cellphone/tablet, (**b**) laptop?

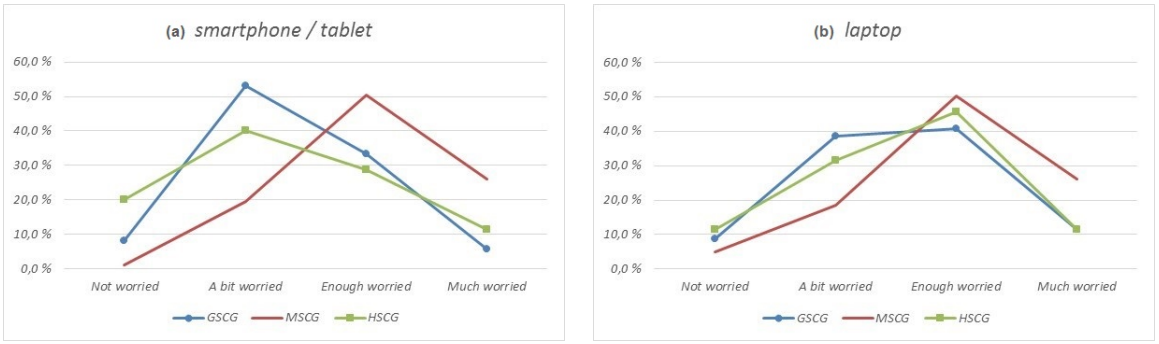

Figure 7. How concerned are you about the security of your—(**a**) cellphone/tablet, (**b**) laptop?

5. Summary of Results

The most significant findings of this study can be summarized as follows:

- Users tend to have increased confidence in the daily use of their mobile devices, leading them to negligent behavior towards actions with potential security related impact. However, the digital natives seem to adopt a more constrained stance when security threats become directly visible. It would be interesting to investigate the variations in user behavior prior and after a major security incident, along with analyzing the duration and extent of this phenomenon.
- Specific areas of user behavior (such as the storage of plaintext passwords in mobile devices) are not significantly affected by their security awareness or background, with a consistent percentage of digital natives remaining willing to accept the risk. Aiming to facilitate further security improvements in such areas would require not only informing the users about the potential threats, but also channeling those who persist in the practicality of such actions into more secure alternatives (e.g., password managers).
- The digital natives still remain unaware of some countermeasures that are available at their disposal and could improve their user experience while maintaining higher security standards.
- Variations in user behavior have been identified to originate not only from their level of security awareness, but also from regional, financial and cultural agents. Thus, regional studies and campaigns aiming to raise security awareness, must be scoped and adapted accordingly.
- Users tend to prioritize access to services and the usability of their mobile devices over the enforcement of security measures, without major differentiations based on their background.

However, the results of this study have shown that users who are aware of the security risks are willing to opt for security when usable solutions become available.

- Digital natives are willing to accept risks despite of their concerns about security (e.g., jailbreaking/rooting, unofficial application sources) in order to obtain access to additional services. This decision is not significantly affected by their overall knowledge about security, while users with backgrounds in engineering, computer science or information security are less reluctant due to their increased confidence.
- The users of mobile devices seem to feel more confident and less constrained in terms of security when using their laptops in comparison to smartphones and tablets. This is attributed to the maturity of the technologies, but also the lack of recognition of the increased computational capacity and criticality of tasks allocated to smartphones and tablets.
- In some aspects, such as the selection of secure passwords, the digital natives seem to be informed of the appropriate practices. However, the results highlight that, despite the noticeable improvement, a precise framework still needs to be consolidated across the users' mindsets.

6. Limitations

This study has been conducted under the limitation that the dataset referring to the GSCG was collected in a prior investigation. Therefore, access to the raw data was not possible, something that restricted the possibility for deeper statistical analysis. Inherently, expanding the samples' geographic distribution for this study carries interlacing cultural influences. Therefore, future work in this field should also consolidate an understanding of the influences arising from such fine-grained cultural divergences.

7. Conclusions

The purpose of this study was to investigate how the digital natives use their mobile devices, their level of security awareness, and how these relate to their background and educational influences. Our goal was to identify common usage patterns with negative security impact in order to facilitate the deployment of suitable risk treatments. To this end, an initial study of students across Italian Universities has been extended, totaling 1350 participants across three countries, mirroring distinct educational backgrounds and security related competence levels. Categorical differences have been identified between the groups within all five investigated areas, allowing the extraction of findings referring to the modeling of digital natives both across and within the investigated groups.

The results of this study open multiple paths for future work. Regarding risk understanding, the digital natives tend to have increased confidence in the daily use of their mobile devices, but seem to adopt a more constrained stance when security threats become directly visible. A path for future work would be to investigate the variations in user behavior prior and after a major security incident as stated earlier. Our results may also contribute to targeted user-modeling validation studies, specifically regarding the correctness of how developers and security experts perceive the user behavior of the digital natives.

Acknowledgments: We extend our thanks to Francesca Bosco for giving us access to the questionnaire used in [14]; to Elisavet-Maria Katsika for translating it from Italian to Greek; and to Marte Lunde for suggesting to extend the survey to Norwegian students.

Author Contributions: These authors contributed equally to this work.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Lella, A.; Lipsman, A. The US Mobile App Report. 2014. Available online: http://www.comscore.com/Insights/Presentationsand-Whitepapers/2014/The-US-Mobile-App-Report (accessed on 8 April 2015).
2. Prensky, M. Digital natives, digital immigrants part 1. *On the Horizon* **2001**, *9*, 1–6.

3. Bennett, S.; Maton, K.; Kervin, L. The 'digital natives' debate: A critical review of the evidence. *Br. J. Educ. Technol.* **2008**, *39*, 775–786.
4. Chin, E.; Felt, A.P.; Sekar, V.; Wagner, D. Measuring user confidence in smartphone security and privacy. In Proceedings of the Eighth Symposium on Usable Privacy and Security, Washington, DC, USA, 11–13 July 2012.
5. Felt, A.P.; Ha, E.; Egelman, S.; Haney, A.; Chin, E.; Wagner, D. Android permissions: User attention, comprehension, and behavior. In Proceedings of the Eighth Symposium on Usable Privacy and Security, Washington, DC, USA, 11–13 July 2012.
6. Kelley, P.G.; Consolvo, S.; Cranor, L.F.; Jung, J.; Sadeh, N.; Wetherall, D. A conundrum of permissions: Installing applications on an android smartphone. In Proceedings of the International Conference on Financial Cryptography and Data Security, Kralendijk, Bonaire, 27 February–2 March 2012; Springer: Berlin/Heidelberg, Germany, 2012; pp. 68–79.
7. Mylonas, A.; Gritzalis, D.; Tsoumas, B.; Apostolopoulos, T. A qualitative metrics vector for the awareness of smartphone security users. In Proceedings of the International Conference on Trust, Privacy and Security in Digital Business, Prague, Czech Republic, 28–29 August 2013; Springer: Berlin/Heidelberg, Germany, 2013, pp. 173–184.
8. Mylonas, A.; Kastania, A.; Gritzalis, D. Delegate the smartphone user? Security awareness in smartphone platforms. *Comput. Secur.* **2013**, *34*, 47–66.
9. Ophoff, J.; Robinson, M. Exploring end-user smartphone security awareness within a South African context. In Proceedings of the 2014 Information Security for South Africa, Johannesburg, South Africa, 13–14 August 2014.
10. Parker, F.; Ophoff, J.; Van Belle, J.P.; Karia, R. Security awareness and adoption of security controls by smartphone users. In Proceedings of the 2015 Second International Conference on Information Security and Cyber Forensics (InfoSec), Cape Town, South Africa, 15–17 November 2015.
11. Markelj, B.; Bernik, I. Safe use of mobile devices arises from knowing the threats. *J. Inf. Secur. Appl.* **2015**, *20*, 84–89.
12. Markelj, B.; Zgaga, S. Comprehension of cyber threats and their consequences in Slovenia. *Comput. Law Secur. Rev.* **2016**, *32*, 513–525.
13. Sheila, M.; Faizal, M.; Shahrin, S. Dimension of mobile security model: Mobile user security threats and awareness. *Int. J. Mob. Learn. Organ.* **2015**, *9*, 66–85.
14. Ariu, D.; Bosco, F.; Ferraris, V.; Perri, P.; Spolti, G.; Stirparo, P.; Vaciago, G.; Zanero, S. Security of the Digital Natives. 2014. Available online: https://ssrn.com/abstract=2442037 (accessed on 13 October 2016).
15. Norman, G. Likert scales, levels of measurement and the "laws" of statistics. *Adv. Health Sci. Educ.* **2010**, *15*, 625–632.