SMARTPHONE SECURITY AWARENESS, PERCEPTIONS AND PRACTICES: A WELSH HIGHER EDUCATION CASE STUDY

D.J. Cranfield[1], I.M. Venter[2], R.J. Blignaut[2], K. V. Renaud[3]

[1]University of Swansea (UNITED KINGDOM)
[2]University of the Western Cape (SOUTH AFRICA)
[3]Abertay University (UNITED KINGDOM)

Abstract

Higher Education students are purported to be heavy users of technology; specifically, smartphones, which are "Internet of Things" devices. These have revolutionized every sector of public and personal life, including teaching and learning within Higher Education. The way students engage with each other, with institutions of higher learning, and with their own education, has changed dramatically. The smartphone pervades all areas of their lives with a plethora of security issues accompanying its use. Cybersecurity perceptions are said to inform security practices and precautionary-related behaviours. If perceptions are skewed, the necessary security behaviours might be inadequate. The main objective of this quantitative study was to investigate the level of smartphone security awareness of Higher Education students undertaking a Business degree at a Welsh University during the 2016-17 and 2018-19 academic years. Understanding whether students have acquired prior cybersecurity knowledge through formal means was key to understanding whether there was a link between security education, security awareness, smartphone security behaviours, perceptions and practices. This research therefore aimed to investigate: 1) The level of smartphone security awareness depicted in the attitudes, behaviours, knowledge and competences of these university students; 2) Any gender differences in terms of attitudes, behaviours, knowledge and competences regarding smartphone security awareness; and 3) The importance of cybersecurity awareness & training. Participants in this study were largely male, with half of the participants having undertaken a prior information communication technology course. Almost all participants recognised that there were issues with social networking applications and location sharing. The majority did not deploy measures to prevent viruses, this being the case for significantly more females. More than half of the participants used mechanisms to protect their data. However, significantly more of the 2018-19 participant group, as compared to the 2016-17 participant group, did not do this. This study suggests that formal information communication technology training improved awareness of the security risks and more secure behaviours. Even so, smartphone security awareness is not as high as hoped. This study suggests that as technology and digital literacy gain importance, smartphone security literacy training should not be left to chance. It is clear that education and training should occur early in the education life cycle, and be a lifelong learning activity.

Keywords: Smartphone, cybersecurity, life-long learning, higher education, mobile phone.

1 INTRODUCTION

1.1 Nature and scope of problem

Technological advances have always impacted societies. However, it is expected that in the next decade its growth will be exponential and will have a transformational impact on the way people work and play, affecting all areas of our lives [1]. Klaus Schwab, the founder and executive chair of the World Economic Forum (WEF), based in Geneva, coined the term "The Fourth Industrial Revolution" (4IR) at the WEF meeting in Davos in 2016, and published a book with the same title. Schwab contends "we stand on the brink of a technological revolution that will fundamentally alter the way we live, work, and relate to one another" [2, p. 1].

This "revolution" promises to transform the ways in which goods are used and services rendered and many of these will be facilitate by smartphones, creating an "on-demand economy" [2]. Xu et al. [3] suggests that our core industries and sectors, such as health and education, are being positively impacted by this "disruptive innovation". It is clear that this digital "explosion" will present opportunities but also introduce a range of challenges [3].

The term "Internet of Things" (IoT), coined in 1999 by Kevin Ashton [4], refers to the "network of physical objects" [5, p. 41]. Advances in circuits and software have added a level of digital or artificial intelligence

to devices enabling real time data to be communicated without a human being involved, linking digital and physical worlds [6]. There has been a rapid increase in the deployment of IoT devices (see [7]); demonstrating the evolution of a hyper connected world.

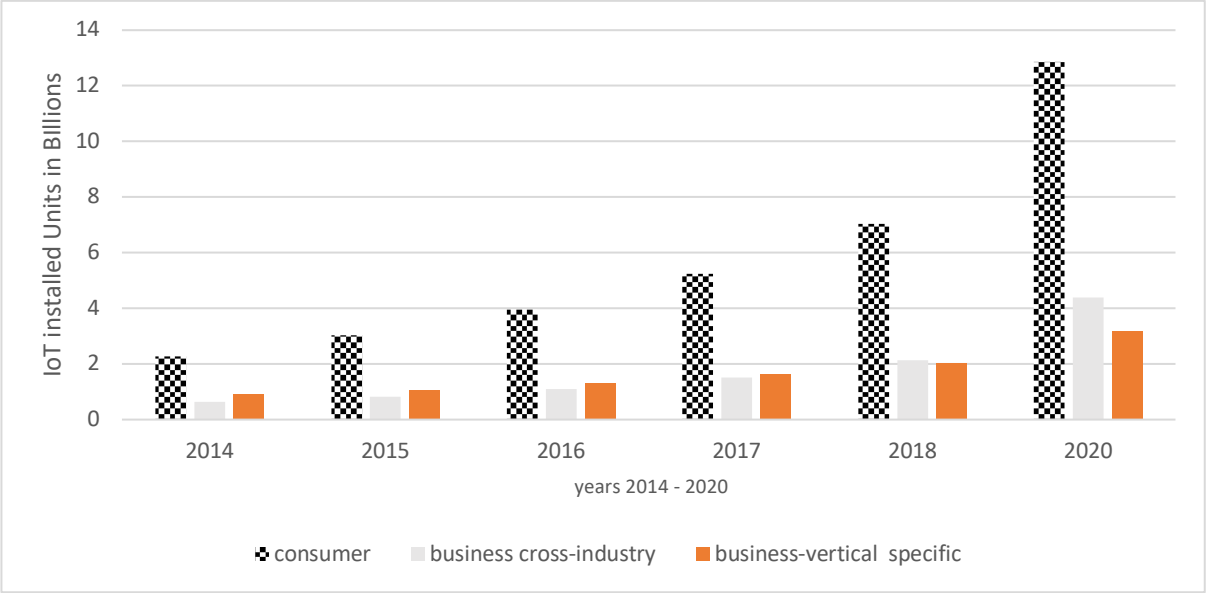

Figure 1. The Internet of Things (IoT) units installed base by category from 2014-2020) [7]

These small and relatively cheap intelligent devices are embedded in everyday objects and can send and receive information via the Internet, enabling data to be aggregated to monitor and control other devices [6]. Access to these IoT devices, and their data, needs to be secured to prevent sensitive data from being used without permission for illegal or unethical purposes. Rayome [8] argues that the smartphone, too, is an IoT device. Smartphones are essentially personal computers which give their owners easy access to the Internet, a functionality not afforded by older feature phones.

This research investigating the vulnerabilities caused by this rapid diffusion of IoT devices. In particular, we examine the awareness of Higher Education students, and their smartphone use, in particular whether prior IT related education impacts security behaviours and awareness, and whether there are any gender-related differences.

1.2 Vulnerabilities and Security threats

IoT devices increase the vulnerabilities present in any given network [3]. Hypponen's [9, p. 5] law: "*whenever an appliance is being described as being 'smart', its vulnerable*", is a fitting portrayal of this situation. Statistics show that there has been a dramatic increase in the volume and complexity of new mobile security threats [1], emphasizing the importance of mobile security awareness. A higher level of alertness is being required as lives become extensively connected to various devices, from mobile phones, cars, and light switches to home security cameras, and smart speakers [3]. Access to these devices and the information made available from these devices via the Internet; pose a new kind of threat. In particular, owners face the risk of data loss, degraded functionality, financial loss, and the invasion of privacy, risks that become real when exploitation of these vulnerabilities occur [10]. Furthermore, Watson and Zheng [10] contend that data on the mobile device can be stolen, tampered with, held for ransom, or outright deleted, the impact of which can be significant.

Smartphones are usually privately owned and most universities and organisations allow these to be used within the university—referred to as "bring your own device" (BYOD) [11]. BYOD security, in particular smartphone security, poses a greater risk, because according to a study conducted by McGill and Thompson [12], people are much more likely to actively protect their home computer or laptop than their smartphone or tablet.

The lack of user security awareness is a critical factor influencing mobile security behaviours [13, 11, 12]. Core industries and sectors, such as education, need to reshape how they operate [3]. The 4IR therefore requires educational institutions to redefine the conventional ways in which educational

content is being delivered to students, as well as the actual content, to keep abreast of the changing technological developments and the opportunities and threats these present.

1.3 The Educational Context

Penphrase [14] suggests that unlike previous industrial revolutions, the rapidity of advance of the divisive technologies of the 4IR share the capacity for rapid increases in scale and cost efficiencies, which demands a more proactive response from the educational sector than the more "gradual societal evolution and subsequent response from educational institutions in earlier industrial revolutions" [14, p. 224].

At a relatively large university in Wales, where this study was conducted, the majority (61%) of its students are from Britain (England, Scotland, Northern Ireland and Wales), with Asia being the second largest source of students (28.1%). Education for pupils from the ages of 5 to 16 years is compulsory in the UK.

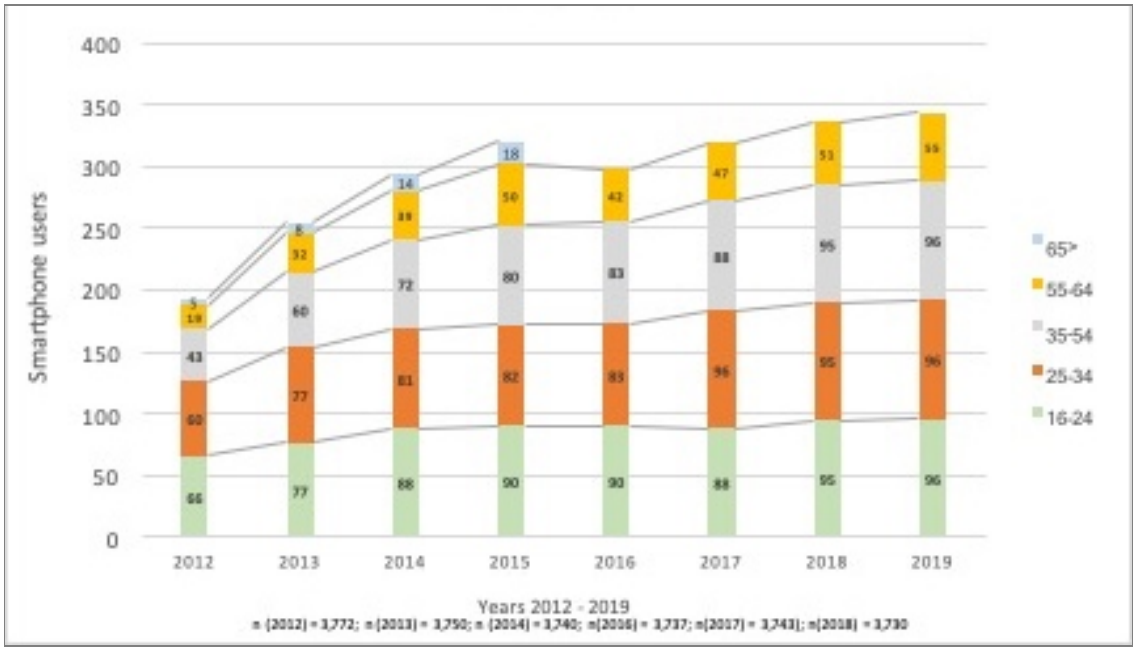

Figure 2. UK smartphone users by age: 2012 – 2019 [16]

Education is a devolved policy area in the United Kingdom with schools in Scotland, Northern Ireland and Wales following their own curricula [32]. The Welsh government curriculum includes a Digital Competence Framework, a cross-curricular responsibility applied for all children aged 3 to 16. It encapsulates the skills that will help children thrive in an increasingly digital world. According to the report, the framework has four strands of equal importance—Citizenship, Interacting & collaborating, Producing, and Data & computational thinking, the latter addressing data and information literacy [14].

1.4 UK Mobile phone usage

According to research conducted by O'Dea, 38% of households in the United Kingdom (UK) have two mobile phones and just four percent of households are without a mobile phone, while one in five have a single mobile phone in the house [15]. Most phones are smartphones (with the iPhone being the most popular device) and the smartphone penetration rate expected to be around 77% by 2020. The use of smartphones has increased significantly from 2013 to 2019 (see Fig. 2). Most smartphone users use their phones to search for information (using search engines), visit social networks and read e-mail. Messaging applications are used more frequently than other applications [15].

1.5 Main aim of the research

Once students enter university, how security literate are they? Is there a difference in behaviours of those with prior ICT education, and those without? Where do students gain their cybersecurity knowledge and skills? These are some of the questions that this study aims to investigate. To investigate

the level of smartphone security awareness of a selected group of Business students at a Welsh University the following questions were posed:

RQ1 The level of cybersecurity awareness depicted in the attitudes, behaviours, knowledge and competences of university students regarding smartphone security.

RQ2 Gender differences, in terms of attitudes, behaviours, knowledge and competences of university students regarding smartphone security.

RQ3 The impact of cybersecurity awareness education

2 METHODOLOGY

2.1 Context and participants

Two sets of data were collected from students enrolled for a Business degree in the School of Management. In the 2016/2017 academic year, it was collected from first-year students, enrolled for a core first-year module; and in the 2018/2019 academic year, from students enrolled for a second-year elective module. The aim was to compare smartphone security awareness of students exposed to prior formal Information and Communication Technology (ICT) education and those who were not. It should be noted that entry into the first-year Business degree does not require any formal ICT training, and no formal ICT training is offered during the first-year of the Business degree.

2.2 Data collection

Qualtrics was used to administer a pre-designed questionnaire of 65 open-ended and closed questions to the two student cohorts. The questionnaire addressed the cyber security awareness of smartphone users. Ethical clearance was obtained from the university's research committee.

The questionnaire was administered to the 2016/2017 cohort at the end of the term. One hundred and thirty students completed the questionnaire of which only 79 (n=79) could be used. Several questionnaires were incomplete, and thus excluded. Two hundred and ten students from the 2018/2019 cohort completed the questionnaire at the start of the second term but only 82 (n=82) were retained, because incomplete questionnaires were excluded. The data were combined to answer the research questions. For the rest of this report, participants will be referred to as *non-Information Communication Technology* (N-ICT) or *Information Communication Technology* (ICT) participants.

Quantitative analysis using SAS® [17] was carried out on the data set and on the following groupings: gender and ICT background, ICT and Non-ICT former education. The open-ended questions provided additional information that was coded and analysed quantitatively.

3 RESULTS

3.1 Participants

A total of 161 (n=161) students participated in this study. The majority (60%) being male. Most of the participants completed their school-leaving certificates in towns or in rural areas (56%) with fewer participants (44%) completing their schooling in cities. The majority were between the ages of 18-22, with the minimum age being 18 and the maximum 50. On average, the participants had been using smartphones for 6.9 years.

3.2 Descriptive statistics

Several questions aimed to investigate the usage of smartphones, which provided some interesting descriptive statistics. In particular, the Apple iPhone was listed as the most popular smartphone (73%), with Androids listed as the second most popular (24%). The study suggests that most participants (76%) always kept their mobile phones within reach, while 17% of the participants indicated that this depended on their current activities.

3.2.1 User behaviours and perceptions

Perceptions of mobile applications

Most participants (93%) felt that there were issues related to social networking and location based applications (such as WhatsApp, Facebook, Google Maps) (see Fig. 3). Significantly more females (13%) compared to 2% of males, were unsure about whether Google presented security issues (Chi-sq.=8.9040, P=0.0117). Significantly more of the 2018/2019 cohort (85%) compared to the 2016/2017 cohort (61%) were of the opinion that search engines like Google (Chi-sq.=11.21, P=0.0037) posed a security or privacy threat. A large number of participants were unsure whether Bit Torrent (41%) and Bitcoin (44%) presented security or privacy issues. More of the 2016/2017 cohort (57%) compared to the 2018/2019 cohort (46%) indicated that they are unsure whether it is possible to protect one's privacy on a smartphone (Chi-sq.=5.8548, P=0.0054).

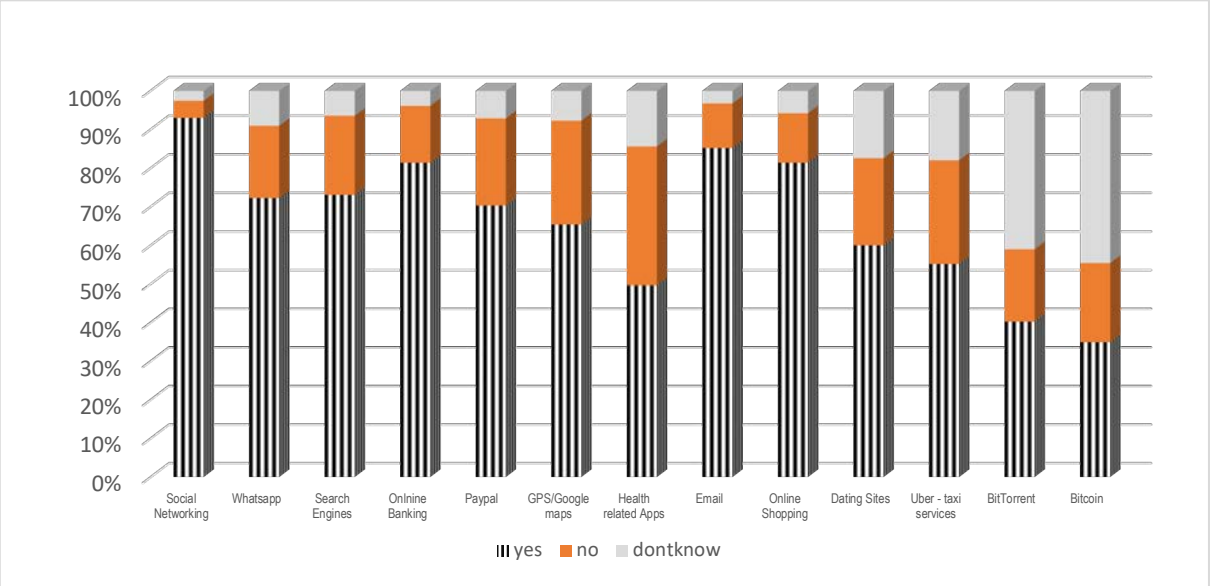

Figure 3. Perception of the security / privacy issues using mobile applications

As with search engines, 71% of the 2018/2019 cohort felt that using dating sites presented privacy/ security issues compared to the 2016/2017 cohort (49%) (Chi-sq.=7.4845, P=0.0237), with more males (64%) compared to females (55%), holding this view (Chi-sq.=1.1572, P=0.5602). Sixty-six percent of the 2018/2019 cohort compared to the 2016/2017 (44%) felt that Uber and taxi type services (Chi-sq.=7.5526, P=0.0229) presented security risks. Fifty-six percent of the 2018/2019 cohort indicated that there was definitely security and privacy issues with using Bit torrent (Chi-sq.=17.7935, P=0.0001), compared to the 2016 group (24%). Most of the 2016 participants indicated that they did not know (58%) if Bitcoin posed a security risk, compared to 32% of the 2019 group (Chi-sq.=11.4629, P=0.0032).

3.2.2 Protecting Mobile devices and stored data

Most of the participants (71%) indicated that they shared their passwords with their partners however, it is interesting to note that significantly more females (81%) compared to males (64%) shared their passwords with their partners (Chi-sq.=5.5988, P=0.0180) and more of the 2016/2017 cohort (79%) compared to the 2018/2019 cohort (63%) indicated that they shared their password (Chi-sq.=5.0557, P=0.02450). Only 12% of all the participants regretted sharing it. Seventy-five percent of all participants take action before selling their mobile phones, and 57% regularly backup their phones. Significantly more of the 2018/2019 cohort (51%) compared to the 2016/2017 (35%) indicated that they do not backup their phones regularly (Chi-sq.=4.3378, P=0.0373).

Very few participants (15%) shielded their access codes when they unlocked their phones when with family or friends. Only a third (32%) of the participants were of the opinion that it is possible to protect one's privacy when using a mobile phone. Most (58%) did not offer security advice to other smartphone users. However, significantly more of the 2018/2019 cohort (40%) compared to the 2016/2017 cohort (14%) offered advice to other smartphone users (Chi-sq. =12.6844, P=0.0018).

3.2.3 Handling of software updates and application installation

Forty-four percent would install an application when they liked it, 15% would look at ratings first, with 19% indicating that they would only install an application if it was useful or effective, and 7% only if it was from a reputable source. The remaining 15% used a combination of the previously mentioned reasons to influence their decision to install an application, or not. Seventy-six percent deleted apps from their phones and regularly installed updates (84%).

3.3 Security Awareness

3.3.1 Awareness of technical countermeasures

Half of the participants understood what encryption meant. Most (65%)—significantly more females (76%) than males (56%)—did not have an anti-virus software installed on their phones (Chi-sq=4.9378, P=0.0263). Most participants (69%) did not record the International Mobile Equipment Identity (IMEI) number of their phones.

Sixty-sic percent agreed that social media should not include personal information such as a mobile phone number. However, 31% indicated that it should not reveal their year of birth, with more of the 2016/2017 cohort (50%) compared to the 2018/2019 cohort (30%) disagreeing (Chi-sq.=6.5516, P=0.0378). Only 40% were of the opinion that if you tweet, retweet, or like a tweet, you can be held liable for its content. Most (53%) said that they had made a friend online.

3.3.2 Awareness of security rules

Most participants (54%) were unsure whether social media was governed by the same laws as normal publications. However, significantly more females (68%) compared to males (44%) were unsure of this (Chi-sq.=10.0410, P=0.0066), and significantly more of the 2016/2017 cohort (65%) compared to the 2018/2019 cohort (43%) were unsure (Chi-sq.=10.047.4872, P=0.00237).

Table1. Prior ICT education and security and safety behaviours

Question posed	***ICT (%) (n=79)***	***N-ICT (%) (n=68)***	***Differences in CS/NCS Chi-sq., p-value***	
Those that encrypt data on their mobile phone?	21%	14%	Chi-sq. 1.0	p=0.3267
Those with a PIN/password/passcode/fingerprint to control access their mobile phone	52%	44%	Chi-sq. 0.4	p=0.5246
Those that never share smartphone access control information	13%	11%	Chi-sq. 4.1	p=0.5310
Those who install system updates and upgrades on your mobile phone	44%	40%	Chi-sq. 2.7	p=0.2544
Those that hide the PIN/password entry when unlocking their phone when with friends?	8%	7%	Chi-sq. 0.1	p=0.9489
Those that have a record of the phone's IMEI number	19%	12%	Chi-sq. 1.3	p=0.2591
Have used passport style photo as profile picture	34%	14%	Chi-sq. 8.9	p=0.0029
Those that regularly back-up the data on their phone	31%	26%	Chi-sq. 0.01	p=0.9330

3.3.3 Prior education and security behaviours

The majority of the participants (55%) formally studied an ICT related course before undertaking this study. Table 1 presents their security and safety behaviours.

Significantly more participants with prior ICT education were confident enough to offer security advice to others, and slightly more of this group also displayed a more trusting attitude towards making friends online (see Table 2). More of this group were also aware that they were accountable for retweeting, liking or sharing posts.

*Table 2. Prior ICT education and security behaviours-confidence and trust (*Significant at a 5% level of significance)*

	ICT (%) (n=79)	N-ICT (%) (n=68)	Differences in CS/NCS Chi-sq, p-value	
Those that offer security advice to other smartphone users	19%	8%	Chi-sq.=8.0,	p=0.0182*
Those that made a friend online	32%	21%	Chi-sq.=7.16	p=0.0696

Although not significant, more of the participants who had prior ICT education understood the concept of encryption, with a similar number from both groups being of the view that divulging of personal details like a birth date on social media is unwise (see Table 3).

Table 3. Prior ICT education and security perceptions and understanding.

	ICT (%) (n=79)	N-ICT (%) (n=68)	Differences in CS/NCS Chi-sq, p-value	
Those who understand what encryption means	32%	18%	Chi-sq. 2.5	p=0.2922
Those who believe social media should not include personal details like a person's year of birth	18%	13%	Chi-sq. 0.3	p=0.8603

Most of the participants indicated that they found security advice on the Internet (see Fig. 4). However, more of the N-ICT group used the Internet whereas more of the ICT students received security information by speaking to others.

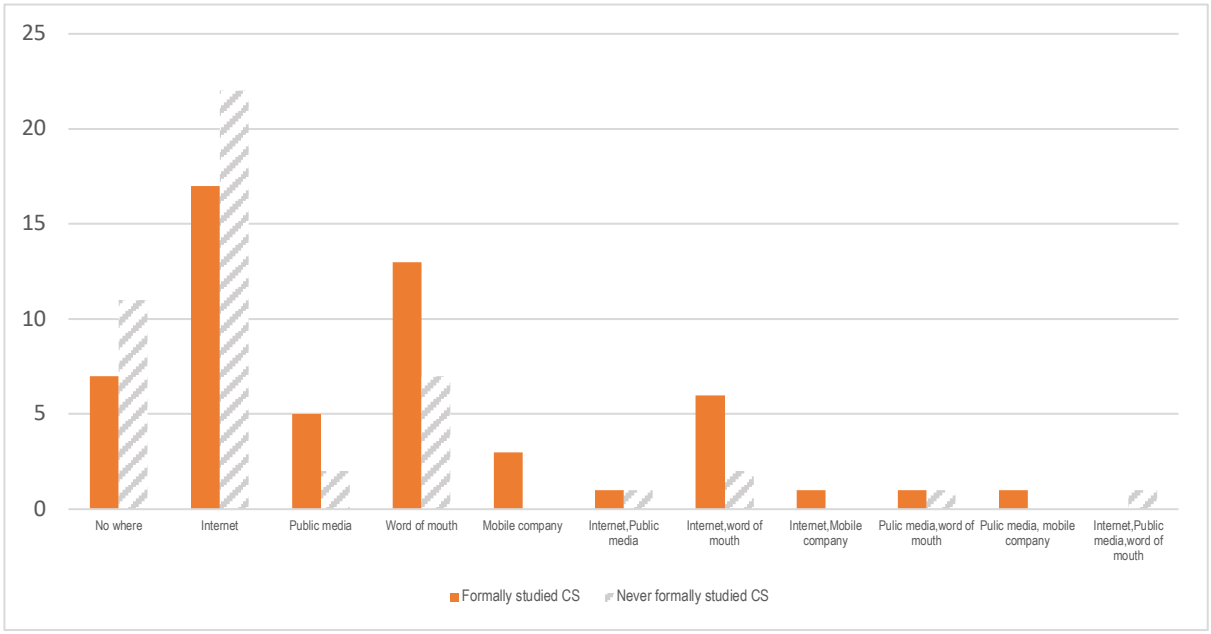

Figure 4. Prior ICT training and security behaviours: source for security advice

3.3.4 Software applications

Most participants (75%) were of the opinion that social media is beneficial for their future career and promotion, and that it can assist them in promoting themselves as experts in their fields (70%). Ninety-one percent considered social media important for keeping in touch with friends and family. Most indicated (75%) that other people's posts could taint their social media profile and could harm future careers, opportunities and promotions (61%). However, significantly more females (36%) than males (16%) were unsure about this (Chi-sq.=8.1075, P=0.0174).

It was interesting to note the different types of applications participants indicated they would install even if they mandated location sharing. Sixty-seven percent did not know how to identify a phishing attempt, with most participants using the Internet to find mobile security advice. However, 39% used the Internet as their only source for mobile security advice. Twenty percent found mobile security advice via word of mouth. Most (97%) used an access code to control access to their phones.

4 CONCLUSIONS

4.1 Revisiting the research questions

This study aimed to investigate the security awareness of university smartphone users from different perspectives: prior ICT versus non-ICT education, gender; and behaviour. The smartphone security awareness levels were measured. The conclusions of the study can be summarized as follows:

- **Level of cybersecurity awareness:** In general, the level of cybersecurity awareness could be improved. It is clear that some important indicators of secure behaviour and awareness were limited. User security awareness is a critical factor for smartphone security behaviours [1]. Mylonas, Kastania and Gritzalis [18] contend that users are not adequately prepared to make appropriate security decisions when downloading applications. There was a perception that the iPhone is more secure than Android phones [19]. The fact that the 2019 group did not backup their phones regularly as compared to the 2017 group, might indicate that they are benefitting from iCloud backups.
- **In terms of gender:** Females were generally more unsure about certain security issues, and in some cases significantly more so.
- **Formal education improves cyber security awareness:** Students with prior ICT training influenced chosen sources of security advice. A study conducted by Koyuncu and Pusatli [1] to investigate the security awareness level of smartphone users, emphasises the importance of education and training for cybersecurity. They found that those with a higher education degree have better awareness levels, and those having ICT security training represented the group with the highest awareness level, both of these being indicators of how important cybersecurity education is. Previous studies suggest that users with excellent ICT skills tend to be more aware of smartphone security issues [18] and those not exhibiting strong information technology familiarity tend to ignore or be unaware of many critical security options [10]. We confirmed the findings of these prior studies suggesting a direct link between technology training and familiarity and awareness of security issues and security behaviours [21].

4.2 Theoretical implication

The theoretical contribution this study makes is to:

1 Emphasize the importance of cybersecurity education, and the link between security awareness and behaviours of Welsh university students;

2 Highlight the suboptimal level of awareness of all participants;

3 Reveal gender differences in smartphone security awareness and behaviours of Welsh university students.

4.3 Practical implications

This study has important practical implications:

1 Smartphone awareness and learning should occur at an early stage of the educational journey. This study supports Koyuncu's [1] research which suggests that there needs to be a collective effort supported by governments, nongovernmental organizations, and others to ensure cybersecurity safety and security is adequately introduced at an early age. Security literacy and awareness and in particular smartphone security literacy and awareness programmes should be offered [20] throughout the curriculum.

2 Smartphone education and smart device safety and security threat awareness raising should be continuous, and continue as a lifelong learning skill required in the digital age, introduced at primary school, and continuing throughout young and older adulthood. Lifelong learning is

required to stay abreast of the impact of technological changes addressing the challenges and risks associated with these life-changing opportunities.

In a press release from the Welsh government, dated 7 November 2019, the Finance minister, Rebecca Evans, commented that “Cybercrime is growing, and we need to do all we can to ensure businesses and people, whatever their age, are equipped with the knowledge and skills they need to recognise the signs of cybercrime; and provide them with the tools they need to stay safe online” [22].

Smartphone device owners face a number of safety and security threats that put owners and their data at risk, with the options to select security and safety options left to the person who often is not fully aware of the mobile security options to protect their smartphones [10]. The results found in this study confirm previous studies that suggest that the lack of security awareness training and has an impact on the subsequent mobile security behaviours.

ACKNOWLEDGEMENTS

The research team would like to thank the School of Management, Swansea University for funding and Professor Paul Jones for his support.

REFERENCES

[1] M. Koyuncu and T. Pusatli, “Security Awareness Level of Smartphone Users: An Exploratory,” Hindawi Mobile Information Systems, Vols. 2019, no. Article ID 2786913, p. 11, 2019.

[2] K. Schwab, “The fourth Industrial Revolution: What it means and how to respond,” Foreign Affairs, 12 December 2015.

[3] M. Xu, J. M. David and S. H. Kim, “The Fourth Industrial Revolution: Opportunities and Challenges,” International Journal of Financial Research, vol. 9, no. 2, pp. p90-95, 2018.

[4] S. Ranger, “What is the IoT? Everything you need to know about the Internet of Things right now:Updated: The Internet of Things explained. What the IoT is, and where it's going next.,” 2018.

[5] P. Gokhale, O. Bhat and S. Bhat, “Introduction to IOT,” International Advanced Research Journal in Science, Engineering and Technology, vol. Vol. 5, no. Issue 1, January 2018.

[6] N. Gershenfeld and J. Vasseur, “As Objects Go Online:The Promise (and Pitfalls) of the Internet of Things,” Foreign Affairs, March/April 2014.

[7] Statista, “The Internet of Things (IoT) units installed base by category from 2014 to 2020 (in billions),” 2019. [Online]. Available: https://www.statista.com/statistics/370350/internet-of-things-installed-base-by-category/.

[8] A. D. Rayome, “How the term 'Internet of Things' was invented,” 27 July 2018. [Online]. Available: https://www.techrepublic.com/article/how-the-term-internet-of-things-was-invented/.

[9] M. &. N. L. Hypponen, “The Internet of (Vulnerable) Things: On Hypponen’s Law, Security Engineering, and IoT Legislation.,” Technology Innovation Management Review, vol. 5–11, no. 4, pp. 5-11, 2017.

[10] B. Watson and J. Zheng, “On the User Awareness of Mobile Security Recommendations,” ACM SE, 13-15 April 2017.

[11] P. Baillette, Y. Barlette and A. Leclercq-Vandelannoitte, “Bring your own device in organizations: extending the reversed IT adoption logic to security paradoxes for CEOs and end users,” International Journal of Information Management, vol. vol. 43, pp. 76–84, 2018.

[12] T. McGill and N. Thompson, “Old risks, new challenges: exploring differences in security between home computer and mobile device use,” Behviour and Information Technology, vol. Volume 36, no. Issue 11, 2017.

[13] F. Parker, J. Ophoff, J. Van Belle and R. Karia, “Security awareness and adoption of security controls by smartphone users,” Proceedings of Second International Conference on Information Security and Cyber Forensics (InfoSec), November 2015.

[14] B. E. Penphrase, “The Fourth Industrial Revolution and Higher Education,” in Higher Education in the Era of the Fourth Industrial, N. Gleason, Ed., 2018, pp. 207-229.

[15] Welsh Government, “How was school today? Parents’ and carers’ guide to primary school for children aged 7 to 11,” 05 January 2019b. [Online]. Available: https://gov.wales/sites/default/files/publications/2019-07/how-was-school-today-parents-and-carers-guide-to-primary-school-ages-7-11.pdf. [Accessed 2020].

[16] S. O'Dea, “The number of mobile phones per household in the United Kingdom (UK) in 2019,” 18 11 2019. [Online]. Available: https://bestterracedecking.com/statistics/387184/number-of-mobile-phones-per-household-in-the-uk/.

[17] Statista, “Smartphone ownership penetration in the United Kingdom (UK) in 2012-2019, by age.,” Statista, 2019. [Online]. Available: https://www.statista.com/statistics/271851/smartphone-owners-in-the-united-kingdom-uk-by-age/. [Accessed November 2019].

[18] SAS Institute Inc., SAS/STAT 14.3 User's Guide, Cary, NC, USA: SAS Institute Inc., 2017.

[19] A. Mylonas, A. Kastania and D. Gritzalis, “Delegate the smartphone user? Security awareness in smartphone platforms.,” Computers & Security, vol. 34, p. 47–66, 2013.

[20] J. Vermeulen, “iOS is generally more secure than Android,” 27 June 2018. [Online]. Available: https://mybroadband.co.za/news/security/265809-ios-is-generally-more-secure-than-android.html.

[21] S. Furnell and L. Moore, “Security Literacy: The missing link in today’s online society,” Computer Security and Fraud, pp. 12-18, 2014.

[22] I. M. Venter, R. J. Blignaut, K. Renaud and M. A. venter, “Cyber Security Education is as Essential as “The Three R’s”, Heliyon, vol. 5, no. 12, 2019.

[23] Welsh Government, “Educating the next generation,” 2019. [Online]. Available: https://gov.wales/educating-next-generation.

[24] A. McCormac, T. Zwaans, K. Parsons and D. Calic, “Individual differences and Information Security Awareness,” Computers in Human Behavior, pp. 151-156, 2017.

[25] H. Rosoff, J. Cui and R. John, “Heuristics and biases in cyber security dilemmas,” Envron Systems Decisions, pp. 517-529, 2013.

[26] J. Wacjman, “Feminist theories of technology,” Cambridge Journal of Economics, vol. 34, no. 1, pp. 143-152, 2010.

[27] M. Wolf, “Same as it ever was,” Foreign Affairs, vol. 94, no. 4, 2015.

[28] A. Ndagi and A. Salihu, “Fourth industrial revolution: prospects and challenges for Africa,” DUTSE Journal of Economics and Development Studies (DUJEDS), December 2018 ISSN.

[29] D. Wang, Z. Xiang and D. R. Fesenmaier, “Smartphone Use in Everyday Life and,” Journal of Travel Research, vol. Vol. 55, no. Issue 1, p. 52–63, 2016.

[30] L. Goode, “Everything is connected: no going back,” 17 January 2018. [Online]. Available: https://www.theverge.com/2018/1/17/16898728/ces-2018-tech-trade-shows-gadgets-iot. [Accessed 2019].

[31] B. E. Penprase, “The Fourth Industrial Revolution and Higher Education.,” Higher Education in the Era of the Fourth Industrial Revolution, pp. 207-229, 2018.

[32] N. Roberts, “The School Curriculum in England”, House of Commons briefing paper, Number 06798, 19 December 2019, pp 1-12