What Strategies could be employed to ensure the Security of Students using Social Networking Sites?

- What are the current ways of ensuring security on social networking sites?
- What are the most recent major breaches of students using social networking sites?
- What new innovations might be used to avoid such breaches in the future?
- Does the increase in the amount of users pose a threat to security, should we still be doing this?

School of Computing & Technology Declaration

DECLARATION

This Research Paper is a product of my own work and does not infringe the ethical principles set out in the University's Handbook for Research Ethics.

I agree that this research project may be available for reference via any and all media by any and all means now known or developed in the future at the discretion of the University.

(Student signature) 

(Typed student name): Martha Sewter

Date: 05/11/2016

Contents

Introduction

Social media, is defined as “a group of Internet-based applications that build on the ideological and technological foundations of Web 2.0, and that allow the creation and exchange of User Generated Content” (Kaplan & Haenlein,2010). Its usage has increasingly grown throughout the years, this being mainly with young people. It has become a global phenomenon, “as of the third quarter of 2016, Facebook had 1.79 billion monthly active users” (http://www.statista.com accessed 12/11/16). Students “form the category which is more exposed to SM” (Popesul & Georgescu,2015) with students often overlooking security risks such as identity theft, cybercrime, grooming and in extreme cases radicalisation, because “individuals are infrequently eager to forego some privacy for an adequate level of danger” (Kumar,2015).

The aim of this study is to access the current ways of ensuring security on social networking sites and investigate what new strategies can be put in place to protect students on SNS. In view of the previous comments, this subject is highly topical and extremely relevant to individuals, businesses and other institutions. The use of students as the focus group of this research reflects their status as prime users of social media and the fact that they go onto work in business for example, often taking their lack of awareness of security issues to their work place.

The objectives are to investigate a sample group of students from Gloucestershire University to enquire about their social media usage, if they have experienced any major breaches of security while using these sites and to enquire about their general level of awareness of protection strategies online. This study will hope to achieve a useful example of the extent of security risks and students’ awareness of them, and make suggestions on how students can be more secure online. It will include a comprehensive literature review of currently available materials on this subject, acquiring knowledge of current technical solutions; the main perspective of this study; along with background details. It will draw on any previous studies that have been done specifically on students, although most of these have been education or business orientated and a few have been from a technical view point. The final part of this research will speculate on the use that students make of social networking sites and whether it should continue

unchecked. I will produce guidelines for the University of Gloucestershire to post on their forum advising students how to be more secure on social media.

Literature Review

The literature reviewed here is taken mainly from journals. The few books on this subject are not readily available in libraries and are expensive purchases online. Most books in the library are about security in other areas of networking. This implies that social media and security is a new and ever-changing subject and an interdisciplinary one (Boyd and Ellison 2007), best researched and recorded by a variety of journals. These journals are international, with interest from the USA, (Lawler and Molluzzo, 2009), Korea (Kwon et al, 2013), and India, (Kumar, 2015). This is probably because these countries are noted for a high number of users of social media sites, together with expanding economies. The highly topical profile of this subject also legitimises the use of British newspapers, periodicals and radio programmes as sources for up to date information at the time of writing; British because this is the country in which this study is based.

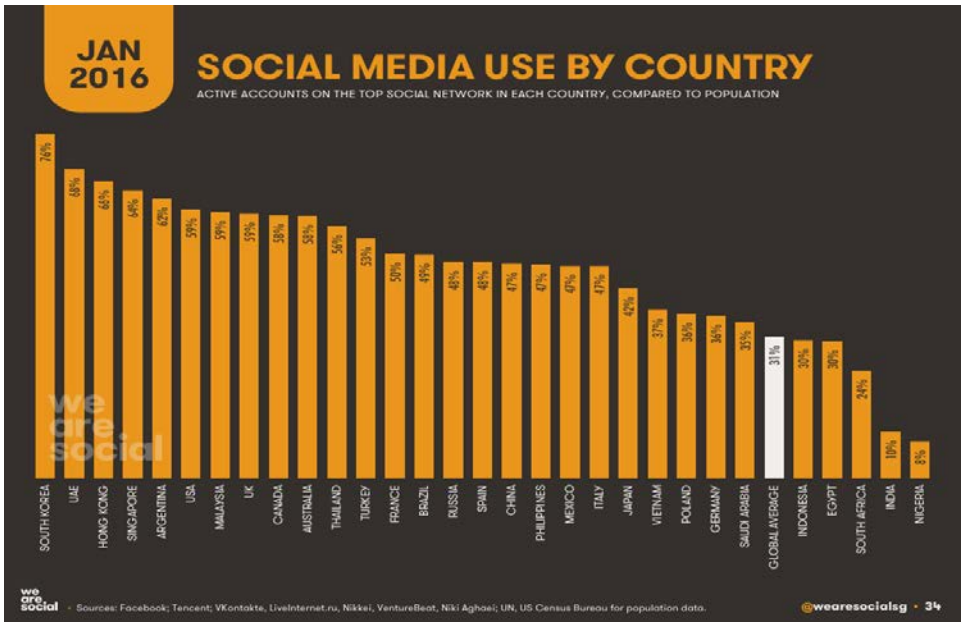


Figure 1: Shows social media use by Country in percentage, taken from http://wearesocial.com/uk/special-reports/digital-in-2016 accessed on 06/11/16.

Disciplines reviewed here include viewpoints from education, business, and IT. Educational journals stem from the concern that exists over the amount of young people who are addicted to social media, (Putnik and Boskovic, 2012), business interest comes from the ever-increasing recognition of the potential of social media for industry, particularly for marketing purposes, (Kwon et al, 2013) and technical papers which highlight security concerns and discuss mitigation techniques, revealing the degree of concern which exists over the ambiguity of social media: on the one hand an excellent means of information sharing but on the other something which demands a great deal of security and privacy (Kumar, 2015).

Consequently, this review is split into three sections, the first reviewing literature connected to students as users of social media with security issues a concern, useful because this paper is using students as the focus group. The second examines social media and security with employees in businesses as the focus users, relevant because such papers offer ideas on security problems and stress the fact that graduates go on to work using social media in such environments (Kwon et al, 2013). Thirdly, technical journals and books (Bahadur, Inasi, Carvalho, 2012), important because this dissertation has a technical perspective. However, it is to be noted that social media is not as technical as other areas of IT because, despite the fact that many people work on social media, the corresponding literature is not as technical as it is for other IT subjects. This is possibly because social media has so much potential that there is a reluctance to highlight the risks.

Student Users.

Lawler and Molluzzo (2009) aim to 'clarify the knowledge of students on issues of privacy and security on social networking sites', with the idea that 'learning the problems and risks of invasive technologies will help to protect the privacy of students'. This paper has strong similarities to my own research which makes the methodology described useful for comparison. A survey was conducted via a questionnaire, delivered mainly online, to undergraduate and postgraduate students in several disciplines at Pace University, New York. The questions contained a few essential demographic questions as well as those intending to gain information about what types of data students shared on their social networking sites and how their social networking sites handled their information.

The results indicated that whilst some data was freely shared (name, gender, school attended friends and photos), other information was less forthcoming (address and telephone number, political views and religion). Information about employment, relationship status and social activities was classed as indifferent. With regards to security awareness, the majority of respondents (55.6%) did not read the privacy policies of their social media sites.

The conclusion of this study is that social media sites need to make privacy more of a priority. Users need to be informed in easily accessible privacy statements which are shorter and easier to read. The authors blame these long and complex privacy statements together with difficult ways of customising privacy settings on Facebook for example, for being the reason for a lack of control when sharing of information. I think this paper is good but it is six years old, a long time by social media standards. For example, it mentions MySpace as the second most popular site, something which is almost obsolete in 2016. Consequently, it would be interesting to see if Facebook have made improvements to the privacy issues mentioned. The authors consider their study to have limitations, 'the sample size was small and had too many graduate students', and speak of the benefits of further similar studies.

Popescul and Georgescu, (2015) produced a more recent paper on a similar theme, aiming to 'learn about generation Y students' attitude to risks and security measures when using social networks', although it focuses mainly on Facebook. This paper likewise identifies students as in a category most exposed to social media, but it appears that the student users have developed to a more dangerous level. For example, the authors provide a more detailed profile of the student user: 'they are seen as well educated, internet savvy, and eager to learn on the one hand, but more shallow, sceptical, blunt, critical, cynical, narcissistic, difficult to wow and impatient, relative to predecessors'. Similarly, in *The Daily Telegraph*, in a short article dated Tuesday 15th November, Mark Zuckerberg declared 'everyone under 30 just shrugged and just got on with instagramming their boobs and bottoms... it is irredeemably middle aged to be mortally offended that someone is watching everything you do'.

Popescul and Georgescu saw students as multi-taskers, information consumers with high expectations, with social media being the means to achieve their aims. They identify both non-malicious and malicious uses of social media by students. Their research aims to analyse the degree in which the students from the Faculty of Economy and Business Administration are aware of the general dangers to which they expose themselves. The methodology employed

was again by questionnaire, and the results showed that the students agreed that Facebook was a dangerous source of viruses, but admit they don't have enough knowledge about the different types of attack. The authors also admit their methodology has limitations, namely a small sample size and the assessment of a single social networking site, specifically, Facebook. However, the authors justify Facebook because it originated as a student site and attracts many student aged people.

This paper is more precise than the previous paper because it names the technical dangers such as spoofing, clickjacking, tag jacking and phishing. It does appear that students have developed since the 2009 study because in 2015 it was found 'an overwhelming majority are careful not to expose themselves to hackers, viruses, spam and other attacks'. However, despite this awareness the authors concede that more modern technical dangers such as scareware, ransomware or rootkits are not mentioned. This paper concludes that universities need to establish a coherent security policy and set of procedures for students using social media, putting the onus more on the universities than the students or the media sites to ensure safety online. Some universities, such as Lancaster, have begun to provide information security advice pages.

Another study which involves students, social media and security is Putnik and Boskovic, (2012). This paper is Croatian and from an education journal and consequently takes a social perspective looking at cybercrime. They view young people as vulnerable to violation of personal privacy, cyberbullying and ideological manipulation. Unlike the two previous papers, the study concerns secondary school students as well as university students, but the purpose is similar: 'the extent to which students use social networking sites, and the way they perceive online security risks when using social networking'. Again, a questionnaire was used to obtain information.

Putnik and Boskovic's conclusion was that the majority of participants used social media for virtual contacts and association rather than promoting their knowledge and skills or making new contacts in the real world. A higher proportion of the participants felt that social networking can significantly compromise physical, moral or psychological integrity of a person, a figure that was higher for secondary school students but this does not stop them using it. The authors believe that continual education in the field of the safe use of the internet is highly justified as in the previous two papers.

The use of younger users alongside students is interesting because current evidence in the media points to the dangers of profiling by the younger group and but less for the older, possibly indicating that eighteen year olds are considered to be safer users of social media. For instance, *The Times* (Nov. 2016) suggested that 'sexting' and cyberbullying were responsible for the increase in mental health problems for school aged users of social media. The Government was reported to have said that 'social media giants should block children from sharing explicit images to help curb this crisis'. Technology was now able to achieve ways of identifying sexually explicit pictures and blocking them and tackling cyberbullying by using word-pattern recognition. This shows a development from Putnik and Boskovic in that it transfers the responsibility from education to the social media sites, indicating that the young user is too involved to appreciate the dangers and needs to be controlled.

However, the older user is likewise at risk. For example, the crime of sextortion, aimed at young men, is mentioned at the end of this article and also on the *Today Programme*. There have been over 900 reported cases this year and four suicides. It seems that the problems of social media have become more sinister, and although it is acknowledged that the technology does exist (Mark Skilton, University of Warwick), there is a lack of social responsibility when it comes to regulation.

To summarize this section. Young people, including students are over-exposing themselves to the dangers implicit in social media. Although students are savvier than school children, it is possible that they carry their bad habits from school to university. New ways of targeting young people are developing all the time. From the perspective of this study, current ways of ensuring safety are not enough, awareness raising needs to be met with help from university policy and technology put in place by the social media sites.

Benefits to Business.

Kwon et al, 2013 recognise the amount of time young people spend on social media but in relation to how business can use it as a tool for establishing relationships with citizens or consumers. Written for a marketing journal, they say that: 'brands may often find more traffic on their Facebook site/fan page on their corporate site', indicating how more and more

companies want to hire professionals to manage and utilise social media effectively for their projects.

Thus they suggest that universities should prepare a curriculum training young people for these jobs, and they conduct a survey of 400 students at a business school to enquire about current skills and to identify gaps in their knowledge. Unlike the other papers the questionnaire study was interested in the students' perception on the usage of social media, social media policy, technical issues, communication and personal qualifications for successful employment in social media jobs. Students are noted to spend approximately 30 minutes a day on Facebook which has over 500 million active users. However, the use of social media by future employees may pose serious implications through lack of productivity, improper communications and legal problems as well. The study concluded that again Facebook dominated social media use by students with 81% and that educating students in the fields of technology and communication are very important but in this paper, it is not the risk to the students or university which is emphasised but the benefits to business if these skills are mastered.

Turban et al (2011), also emphasised how many enterprises are using social media to exploit commercial opportunities for example Facebook is rapidly expanding its marketing and advertising activities with close to a million-businesses having a presence there. The success stories on the one hand and the potential risks on the other have however, led companies to wonder whether 'social networking is the next best thing or simply a time waster' (Steinhart 2009). This concept is best illustrated by the recent case of Kim Kardashian, who on the one hand lost millions of pounds' worth of jewels because of her high profile on social media, but reportedly lost3.6m in lost sponsorship deals since she reduced her postings. (Grazia, 2016) Even though this paper describes the potential risks of social networks and suggests ideas for their mitigation it is not readably transferable to student use and it offers no useful research methodology.

In contrast Wu He (2012), offers not only a business perspective but a much more thorough technical assessment of the risks that social media in the work place represents, providing useful security suggestions for my research. Wu He proposes developing a security policy to guide users in what is acceptable use of social media and what is not acceptable, notably the use of privacy settings and password policy. Security policies must be understandable for employees, they should use plain language and videos and examples. Lawler (2009) also

pointed to the importance of a readily accessible security policy. Wu He also advocates routine site monitoring, to check what employees are saying about their organisations via social media, for example 'tools such as google alerts and social mention can help organizations keep track of malicious activities and threats against organizations that attackers sometimes discuss publicly (Zeltser, 2011).

Wu He recommends a policy of both education and control. For example, he suggests monitoring employee's internet activity, and blocking access on social networking sites during certain hours through an administrator, but he also endorses training programs because the 'human link is felt to be the weakest one' (Curry, 2011; Vroom and von Solms, 2004). Training should provide an explanation of the security policy, examples of social media attacks and emphasise proper precautions against security threats. Wu He advises keeping software updated and performing regular scans on computers and any file that is downloaded in order to check for viruses and spyware. 'Updating both the operating system and associated applications like Flash or PDF applications is also needed' (Blue Ocean, 2011). Threats are real because social media sites are accessible anywhere and BYOD (bring your own device, such as mobiles, tablets and laptops) to work has increased the number of cyber-attacks from mobile devices, because mobile devices are increasingly targeted (McAfee, 2010).

Finally, he notes that despite effort, breaches can still occur in the work place with passwords being shared or easily guessed, information leakage, data breaches, viruses/malware and others. The best way to deal with this is through an incident notification and response plan. An article in *The Daily Mail* dated November 5th speaks of the most commonly used passwords which are easily guessed. Wu He concludes that to reduce the amount of risks from social media to business we need to focus on the usage behaviour of the employee, and the suggestions made here are highly transferable from employee to student.

The section differs from the previous one because the onus is on protecting businesses rather than the student user. Business appears to be a reluctant user of social media because it goes against traditional employment values, however the benefits are enormous and cannot be ignored. With this in mind, it is possible that new security measures will be developed with funding from business to make social media safer for all.

Technology.

This section concerns some of the technical issues raised by Wu He but the focus is not on students or business but technology itself. These papers come from Information Technology and Computer Science journals. Kumar et al (2016) appear to think it is social networking sites who need to take responsibility for security breaches as opposed to the human element forwarded by Wu He. Kumar et al provide a table stating the major attacks, the sub-attacks and solution to handle the attacks, for example Malware attacks, sub-attacks such as crime ware/spyware with the solution to use of anti-virus and not clicking on unknown links, friends, applications or email attachments. In comparison to the previous paper which provides solutions from company policy, this paper offers clear depictions of attacks and describes how to access privacy settings on Facebook for example.

Likewise, Kumar et al (2013), discusses some of the privacy and security concerns and their respective prevention techniques but also propose an architecture prevention for secure request response exchange of data between users. This paper gives the best definitions of privacy issues which are easily understandable and could be passed onto students who need to be made more aware of such new strategies of attack, such as watering hole, the purpose of which is to infect the system of developers not to steal information or funds. Kumar et al proposed architecture for secure communication between users, to improve the customization of the user profile and give the ability for the user to hide information from any unwanted friends/visitors. However, it is unable to protect from profile cloning if anyone gets information approval. He concluded that the only solution to social networking privacy is to have some knowledge in the ways in which one can get fooled.

Zhang and Gupta (2016), feel very strongly about security issues and social media, referring to the situation as urgent. They highlight the increased use of social media and state that available studies mainly aim at social media content and user security, including model, protocol, mechanism and algorithm. However, they feel that there is a lack of investigating on effective and efficient evaluations and measurements for security and trustworthiness of various social media tools, platforms and applications. Like Kumar et al (2013), Zhang and Gupta describe a list of possible threats and indicates the degree of danger to users and offer an alternative path from the perspective of information technology, information management and social behaviour.

Measure	Impact on User	Effectiveness of server side protection mechanism	Effectiveness of user side protection mechanism	Threat to Data Privacy	Threat to Data Integrity
Identify Theft	Average to High	Poor	Poor	Yes	Yes
Spam Attack	Small	Strong	Poor	No	No
Malware	High	Medium	Medium	Yes	Yes
Sybil Attack	Average	Strong	Poor	No	Yes
Social Phishing	High	Poor	Strong	Yes	Yes
Impersonation	High	Poor	Poor	Yes	Yes
Hijacking	High	Poor	Poor	Yes	Yes
Fake Requests	Small	Poor	Strong	Yes	No
Image Retrieval and Analysis	Average to High	Medium	Medium	Yes	No

Figure 2: Table of comparison of most popular attacks on online Social Networks taken from: Zhang.Z and Gupta.B.B, 'Social media security and trustworthiness: Overview and new direction, *Future Generation Computer Systems* (7th October 2016) http://dx.doi.org/10/1016/j.future.2016.10.007

In contrast to other researchers Zhang and Gupta examine the motivations for attacks on social media in some detail such as Revenge/Emotions or Financial Gains. They analyse the behaviour of social media users (individual or a group) and state that they need to be well informed of the threats they are faced with and behave securely and use reliable security measures. One factor they say that alters a user's experience on social media is whether they have experienced identity theft or cyberbullying. This point relates to my own research because I intend on asking my participants of their difficulties online (breaches). The authors advocate improving platform trust and security as well as establishing trust a security-preserving social media ecosystem. This paper is more forward thinking than others, suggesting that a new direction on social media and trustworthiness is paramount to our future.

From this review, it is apparent that all writers agree that social media usage is an essential part of modern life and is on the increase. Facebook is the most popular site.

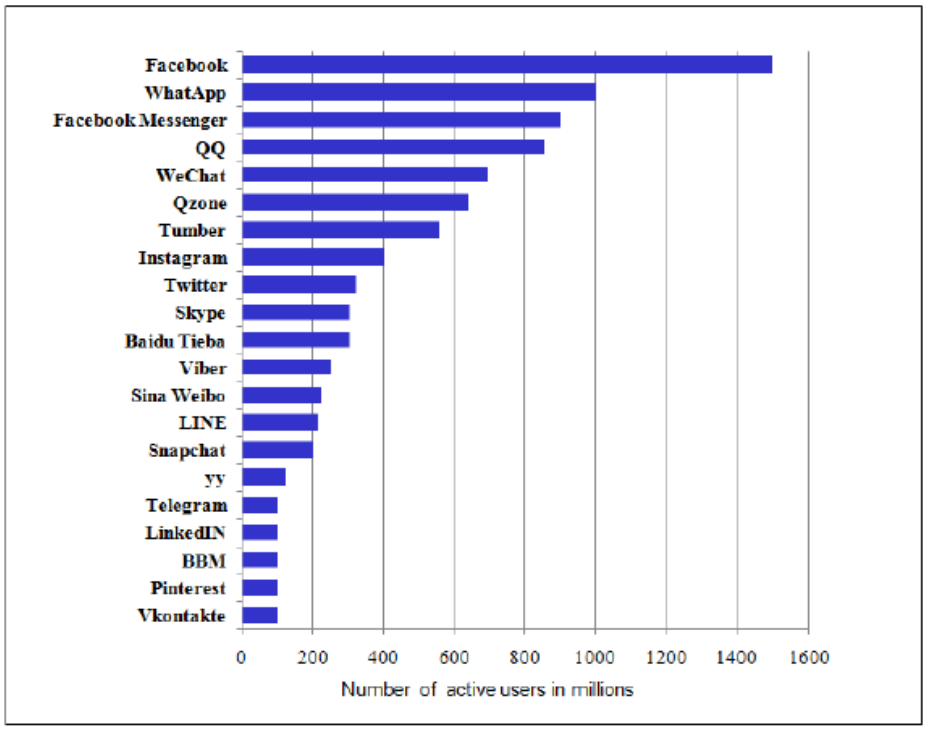


Figure 3: Leading Online Social Networks around the globe as of January 2016: taken from Zhang.Z and Gupta.B.B, 'Social media security and trustworthiness: Overview and new direction, *Future Generation Computer Systems (*7th October 2016) http://dx.doi.org/10/1016/j.future.2016.10.007

However, along with this is the observation that security threats are becoming an ever-increasing problem, which is felt to be urgent and in need of immediate attention. One factor that is continuously raised concerns the users of social media, who need to become more aware of the types of risks online and be informed of the latest threats. Social media sites also need to improve their privacy policies and settings, however since Lawler's study Facebooks privacy settings are now clearer. From this evidence my research appears to be both topical and necessary.

Methodology

To carry out my research and achieve my aims and objectives, I will conduct a survey with participants from the University of Gloucestershire as my primary research. This is because my focus group is students: the literature review has identified these as one of the main users of social media. The review has also noted a couple of comparative studies with transferable methodologies. My methodology is mixed, mainly quantitative, but with some qualitative interpretation being necessary. The Quantitative approach is needed to discover what current ways students' use to ensure security on social networking sites and how many have had major breaches while using these sites. Qualitative methods will be used to interpret the results and to think about what might be used to avoid these breaches in the future. In addition, this method will also be used to reflect upon whether the increase in the amount of users pose a threat to security that is "urgent" and whether we should still be doing this.

I will design a questionnaire with the aim of testing as many participants as possible, it will be distributed via Facebook, the most used social networking site (Appendix 1 fig 2). I will hopefully have a reasonable response to the survey, although response rates are always lower than anticipated. I believe having a response of a small group will be consistent with the size of this study, and being on a widely-used site I expect I will get a better response this way.

These participants I will aim my questionnaire at are undergraduates of mixed gender and studying a variety of disciplines from the University of Gloucestershire. The questionnaire will be in two parts, the first will ask questions on age, subject, ethnicity and gender, whilst the second will consist of yes/no questions and a Likert scale. A question will be asked on age as it is noted by The Daily Telegraph, people under the age of 30 are less security aware and it will be interesting to view whether students from the University of this age range have had serious breaches online. With gender, I can examine whether males or females have had more breaches online, and with subject whether people whom are doing a more technical course such as IT are more aware of the threats online whilst using social media. It will be interesting to have different ethnic groups as many studies are not carried out in the UK and views on the area may be different.

On the issue on breaches whilst using social networking sites, I will firstly ask a yes/no question: Have you ever had a major breach of security while using a social networking site? If yes is the response, I will provide a table for participants to tick a corresponding threat they have experienced online. This tabular method will also be used when enquiring about what social networking sites participants use, the type of information they share and the kind of threats they recognise.

To discover for example how safe people feel online I will use a scale. This scale will range from 0-10, 0 being not safe at all and 10 being very safe. The information received will be transferred into tables for example pie charts and bar charts to indicate differences in opinion on issues on privacy and security. From my results of my research I will endeavour to assess the extent of students' knowledge on security when using social networking sites, whether they appear to be taking unnecessary risks, whether experiencing a major breach of security effects their behaviour online and whether they are aware of the newer threats. These proposals have been listed via the literature as being significant. Finally, I will use this information to reflect on the level of threat posed to students using social media and to write guidelines for the University of Gloucestershire.

If distribution via social media does not achieve the feedback numbers I expect I will hand the questionnaires out myself to students within the University, online surveys are mostly looked over but in person it could be more effective. I have chosen a method however, which I believe will be successful due to the number of active users. I haven't chosen other primary methods such as interviews due to believing this is a more invasive experience and students may not want to discuss issues they have had online face to face as they may be personal. I have also done primary research over secondary as I wish to collect the data myself so I can make comparisons from the previous secondary sources. Secondary sources such as web information would be useful but, it is not always up to date and is not as focused as my question.

References

Bahadur, G., & Inasi, J., & Carvalho, A. (2011). *Securing the Clicks, Network science In the Age of Social Media*. New York: McGraw-Hill, pg 3-320

Boyd, D., & Ellison, N. (2007). Social Network Sites: Definition, History, and Scholarship, *Journal of Computer Mediated Communication*, 13 (1), 210-230. [online] Available from http://onlinelibrary.wiley.com/doi/10.1111/j.1083-6101.2007.00393.x/full (last accessed 03/11/16).

Blue Ocean. (2011). Social Media Security Policy. [online] Available from www.blueoceantechnologies.net/BlueOceanTechnologiesSocialMediaSecurityPolicy.pdf (last accessed 05/11/16)

Curry, S. (2011). The Weakest Link is the Human Link. [online] Available from www.securityweek.com/weakest-link-human-link (last accessed 05/11/16)

DAILY MAIL, (2016) The Secret Password we're still using? Password!, *The Daily Mail,* UK, November 5th.

DAILY TELEPGRAPH, (2016) Excuse me your age is showing, *The Daily Telegraph,* UK, November 15th, pg 15.

GRAZIA, Kendall's Fight To Break Free, November 28th 2016.

He, W. (2012). A review of social media security and risks and mitigation techniques, *Journal of Systems and Information Technology,* 14 (2), 171-18. [online] Available from http://www.emeraldinsight.com/doi/abs/10.1108/13287261211232180?journalCode=jsit (last accessed 02/11/16).

Kaplan, A., & Haenlein, M. (2010). Users of the world, unite! The challenges and the opportunities of social media. *Business Horizons.* 53. [online] Available from https://www.scribd.com/doc/63799736/Kaplan-and-Haenlein-2010-Social-Media (last accessed 10/11/16).

Kumar.A., & Subham, G., & Rai, A., & Sinha, S. (2013). Social Networking Sites and Their Security Issues, *Journal of Scientific and Research Publications,* 3 (4) [online] Available from http://www.ijsrp.org/research-paper-0413/ijsrp-p1666.pdf (last accessed (02/11/16).

Kumar.S., & K,S., K, Deepa. (2015). On Privacy and Security in Social Media - A Comprehensive Study, *International Conference on Information Security & Privacy*, 114-119. [online] Available from http://www.sciencedirect.com/science/article/pii/S1877050916000211 (last accessed 05/11/16)

Kwon, O. & Min, D. & Geringer, S. & Lim, S.K. (2013) Students Perception of Qualifications for Successful social media Coordinator*, Academy of Marketing Studies Journal*. 17 (1), 109-128. [online] Available from http://search.proquest.com/openview/12bf14d8951b24fac9412f3afebc1b03/1?pq-origsite=gscholar (last accessed 04/11/16).

Lancaster University, Information Security: Use of Social Networking tools. Available from http://www.lancaster.ac.uk/iss/security/ (last accessed 11/11/16).

Lawler, J.P., & Molluzzo, J.C. (2010). A Study of the Perceptions of Students on Privacy and Security on Social Networking Sites (SNS) on the Internet, *Journal of Information Systems Applied Research,* (3) (12). [online] Available from http://www.proc.conisar.org/2009/3732/CONISAR.2009.Lawler.pdf (last accessed 04/11/16)

McAfee (2010), 2011 Threat Predictions. [online] Available from http://161.69.13.40/us/resources/reports/rp-threat-predictions-2011.pdf (last accessed 05/11/16)

Popsecul, D., & Georgescu, M. (2015). Social Networks Security in Universities: Challenges and Solutions, *Scientific Annals of the "Alexandru Ioan Cuza" University of Iasi Economic Sciences,* 62 (SI) 53-63. [online] Available from https://www.degruyter.com/view/j/aicue.2015.62.issue-s1/aicue-2015-0036/aicue-2015-0036.xml (last accessed 05/11/16).

Putnick, N., and Boskovic, M. (2012). The Impact of Media on Students' Perception of the Security Risks Associated with Internet Social Networking – A Case Study', *Croatian Journal of Education,* 17 (2) 569-583. [online] Available from http://hrcak.srce.hr/index.php?show=clanak&id_clanak_jezik=208207 (last accessed 07/11/16).

The Statistics Portal. (2016). *Individual Analysis and Market research by Statista Research Analysis.* Available: https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/ (last accessed (10/11/16).

THE TIMES, 'Firms Must Stop Child Sexting', November 30th 2016.

TODAY PROGRAMME, RADIO 4, November 30TH 2016.

Turban, E., & Bolloju, N., & Liang, T-P. (2011). Enterprise Social Networking: Opportunities, Adoption, and Risk Mitigation, *Journal of Organizational Computing and Electronic Commerce*, 21 (3), 202-220. [online] Available from http://www.ecrc.nsysu.edu.tw/liang/paper/1/Enterprise%20Social%20Networking%20(JOCEC%202011).pdf (last accessed 03/11/16).

Steinhart, M. (2009). Web 2.0: Worth the risk? *Secure Computing.* [online] Available from http://www.securecomputing.com/webform.cfm?id=255&ref=pdtwp1657 (last accessed 05/11/16)

Vroom, C., & Von Solms, R. (2004). Towards information security behavioural Compliance. *Information Management and Computer Security,* 6 (4), pp. 167-73.

Zeltser, L. (2011). Monitoring social media for security references to your organization. [online] available from http://isc.sans.edu/diary.html?storyid=10921 (last accessed 05/11/16)

Zhang, Z. & Gupta, B.B. (2016). Social media security and trustworthiness: Overview and new direction, *Future Generation Computer Systems.* [online] Available from http://dx.doi.org/10.1016/j.future.2016.10.007 (last accessed 01/11/16).

What Strategies could be employed to ensure the Security of Students using Social Networking Sites?

- What are the current ways of ensuring security on social networking sites?
- What are the most recent major breaches of students using social networking sites?
- What new innovations might be used to avoid such breaches in the future?
- Does the increase in the amount of users pose a threat to security, should we still be doing this?

By Martha Sewter

School of Computing & Technology Declaration

DECLARATION

This Research Paper is a product of my own work and does not infringe the ethical principles set out in the University's Handbook for Research Ethics.

I agree that this research project may be available for reference via any and all media by any and all means now known or developed in the future at the discretion of the University.

(Student signature) 

(Typed student name): Martha Sewter

Date: 05/11/2016

Abstract

This research investigates the degree to which students at the University of Gloucestershire are safe using Social Networking Sites (SNS). It examines what experiences they have had of breaches, and to what extent these breaches have affected their usage of social media. Also important is if new technology can help or whether it is more important to provide training for students to ensure their safety online.

The research was carried out via a questionnaire to 60 students+ using google forms, emails and face to face contact. I discovered that students felt relatively safe online (91.6%) even though 78.33% had experienced a breach. I concluded that the best way to ensure student safety was to increase safety and technical awareness via training provided by universities.

Contents

List of Table and Figures

Introduction:

Assignment one identified students as high risk users of social media regarding security. Consequently, what strategies could be employed to ensure the safety of students online was made the subject of this study. The literature review confirmed that students were a high-risk group on social media, with suggestions ranging from a lack of awareness of safety issues to the idea that students were narcissistic and impatient. It was also proposed that students were not aware of the different types of threat, particularly the more recent technical attacks.

The methodology used to explore this research idea was quickly centred on a questionnaire. Consequently, other research options which might have been applicable were not explored. However, the literature contained examples of research with students which used questionnaires, and it appeared to be a successful and proven way to obtain data on this subject. The questionnaire was prepared for the students of the University of Gloucestershire with the aim of answering the four research questions, although other questions of a demographic nature were added to ensure a wide range of participants. Another fault was that it was too focused on what questions to ask rather than address the issue of why I was asking the questions in the first place. This I believe, led to some omissions, which will be identified in assignment 2 (see appendices 1 and 2).

The literature related to students advocated that universities needed to establish a coherent security policy for their students on SNS. Business journals also thought that universities should train students. This was security awareness for jobs using SNS, as businesses believe students bring their bad habits to the work place. Educational journals identified cyberbullying as a concern, but seemingly more for school age users. Such journals suggested continual education for the security of young users on SNS. In contrast, the Government believes that the responsibility lies with SNS. Papers from a technological perspective also favour the idea that SNS should ensure the safety of young people online. In addition, they say that students need to be made more aware of the type of threats they face.

All this information indicates the extent of the problem and a seemingly universal habit of universities, SNS, student users and businesses avoiding taking responsibility themselves for ensuring safety online.

Finally, the main body of assignment two consists of two central sections. The first is organised around each of the questions presented on the questionnaire in the order that they appear. Reasons are given for the selection of each question and the results are presented in tabular form where appropriate. The second part is organised around each of the four research questions. This allows for the results of the questionnaire to be applied directly to the research questions and cross referenced to the literature. It permits valid and thorough discussion and enables assessment of whether the aims and objectives have been achieved. This simple structure hopefully will make this work more readily accessible and cut out any unnecessary long sentences and paragraphs (see appendices 1 and 2).

Results/findings – Analysis & Presentation:

A questionnaire is the form of my analysis (Appendix 3). 60 responses from various courses from the University of Gloucestershire were obtained, providing sufficient data to analyse, interpret and discuss the 4 research questions. The questionnaire was designed using google docs, allowing for the data to be retrieved through a number of different resources. Facebook, despite being the most used SNS according to the literature, had a limited response, whereas the University email system proved more fruitful. However, to achieve my target of 60 it was necessary to approach 20 students directly. These are the results and findings.

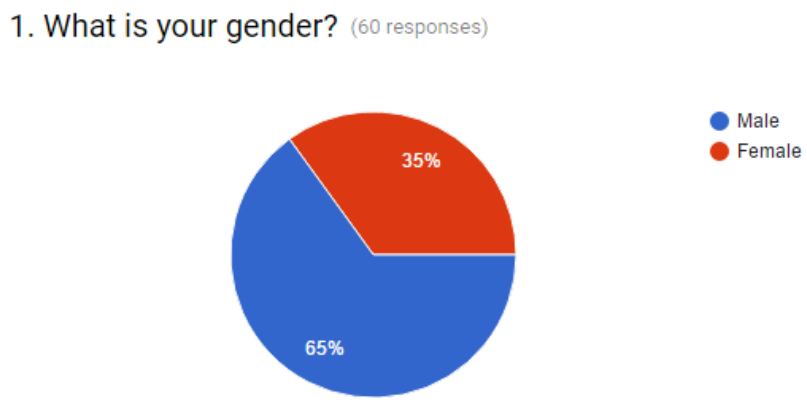


Figure 1: Pie chart showing the different percentage of gender respondents.

This question was included is to ensure the study is evenly distributed between genders. From the 60 students that responded, 65% were male and 35% female. This was a reasonable representation, although it would have been better to have more females. I did find that the technical students (for example computing) were mainly dominated by males.

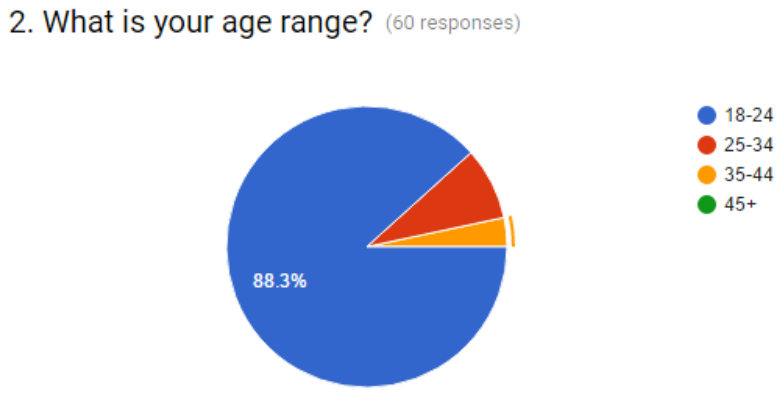


Figure 2: Pie Chart showing the different ages of respondents.

This question allowed me to verify that the majority of participants are within my target group (young people). Previous research has suggested that young people were at greater risk online.

88.3% were 18-24 who took part in the survey/ 53 people

8.3% were 25-34/ 5 people

3.3% were 35-44/ 2 participants

3. What subject are you taking at the University of Gloucestershire?

Subject	Participants
Forensic Computing	9
Popular music	7
Games design	7
Business and information technology	7
Computing	6
Film production	5
Business management	5
IT	3
Psychology	3
Journalism	2
Media production	2
Sports coaching	1
Computer science	1
Multimedia web design	1
Photography	1

Figure 3: Table showing the subject areas studied by participants.

This was an open question enquiring about the range of disciplines represented by the participants. Figure 3 shows the distribution of subject areas indicated via the questionnaire. This question was included in order to collect feedback from all subject areas both technical and non-technical to produce a study without bias to my subject area. Including subject ranges also allows for an investigation as to whether technical people e.g. computing students, have experienced breaches online similar

to those students in less technical subject areas. However, this is not one of my main research questions, so it is not a priority and could be the subject of further study.

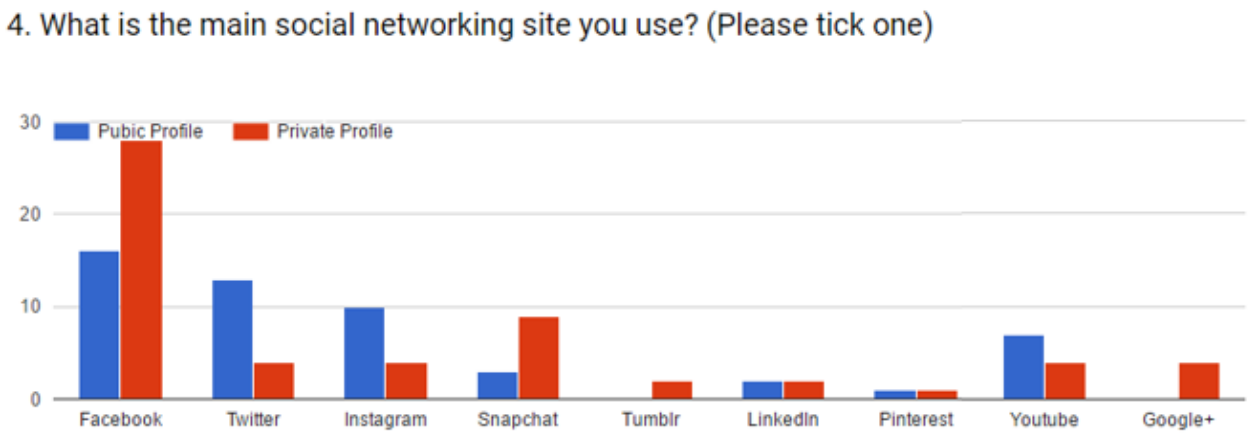


Figure 4: Bar chart showing the main SNS sites used and the public or private profile of the participants at a glance.

This question identifies which SNS students use the most and with what profile setting (either public or private). However, participants instead of just ticking one (as instructed) sometimes ticked more. Perhaps this was due to them using sites equally or possibly not reading the question. However it is clear that Facebook (44 users or 73.3%) is overall the most popular site, having a private profile on Facebook which has security measures in place is significantly more popular (see table below for numbers). The predominance of Facebook amongst participants is in agreeance with findings from the literature.

Site	Public profile	Private profile
Facebook	16	28
Twitter	13	4
Instagram	10	4
Snapchat	3	9
Tumblr	0	2
LinkedIn	2	2
Pinterest	1	1

YouTube	7	4
Google+	0	4

Figure 5: Table giving more accurate numbers of SNS and profile type.

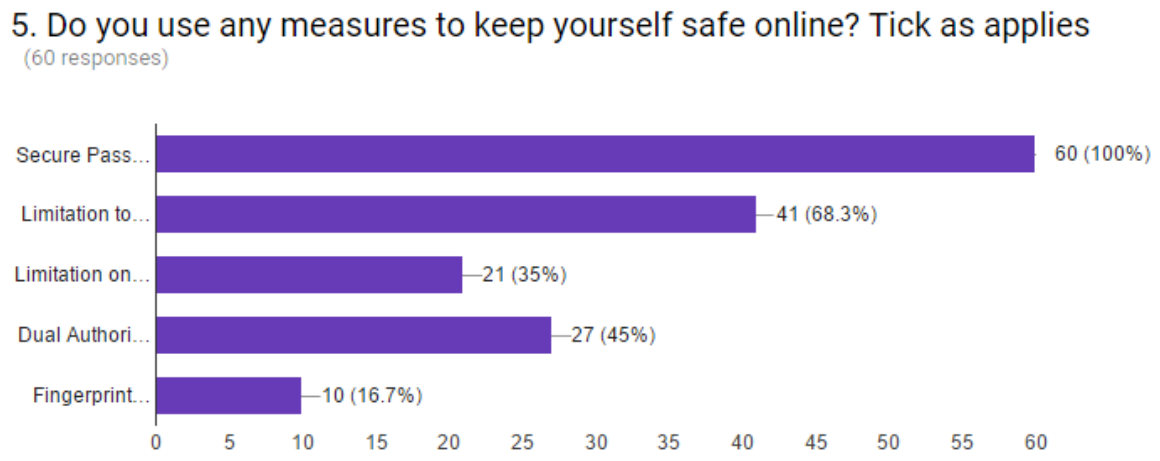


Figure 6: Bar chart showing the measures preferred by participants to ensure safety on SNS.

This question examines the ways in which students are currently keeping safe online, which is one of my main research objectives. The data shows:

- 100% of the students have a secure password
- 68.3% have a limitation to what people can see on their profile
- 35% have a limitation on who can send them friend requests
- 45% have dual authorisation
- 16.7% have Fingerprint recognition.

From this it can be deduced that standard security measures such as password and friend requests are well known and used. Students are also aware of the privacy settings offered by Facebook (represented by the first three in the list) and the two-step dual authorisation is used by 45% of the participants, something which is offered through the security and logins options (code from phone and password). However, more innovative security methods such as fingerprint recognition are not so well used. Only 10 participants (16.7%) used fingerprint recognition users, (90%) of whom were technical students.

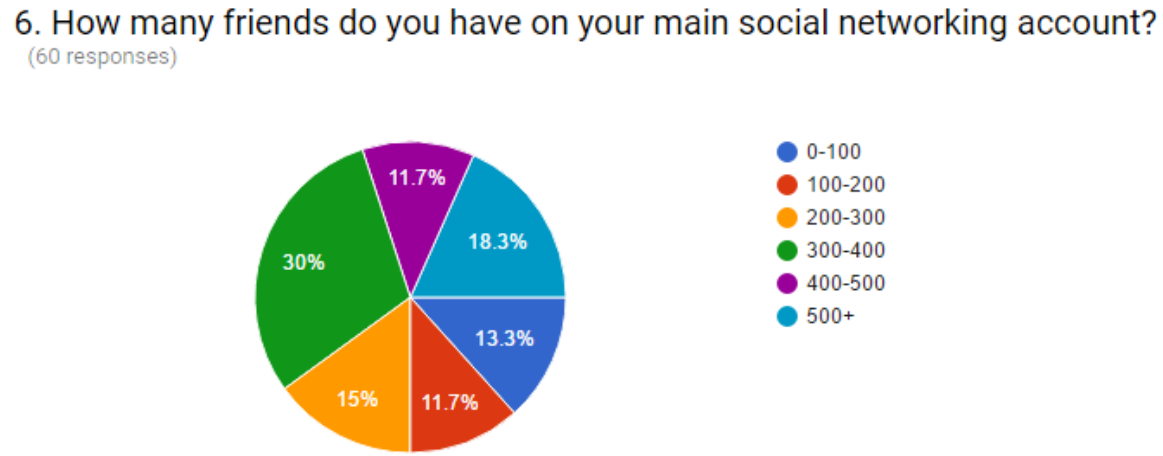


Figure 7: Pie chart showing the number of friend's students have on their main SNS.

This question was included to see how widely participants shared details of their lives. It also allows for investigation into whether people with the most friends have had more breaches. The results show that the amount of friend's students have on their main SNS varies from 0-500 plus, with most (30%) having 300-400 friends.

By using data gathered from question 9, it is possible to compare the 0-100 with the 500+ ranges of friends to see the amount breaches each has experienced. I found that students with 0-100 friends had a 75% incidence of breaches, whilst students with 500+ friends have experienced 90.9% of breaches. This suggests that the number of friends you have online does increase your security risk, but these figures are small and therefore inconclusive, indicating a larger study needs to be carried out. The amount of friends should not be confused with the amount of users online, so this question does not help with answering research question 4.

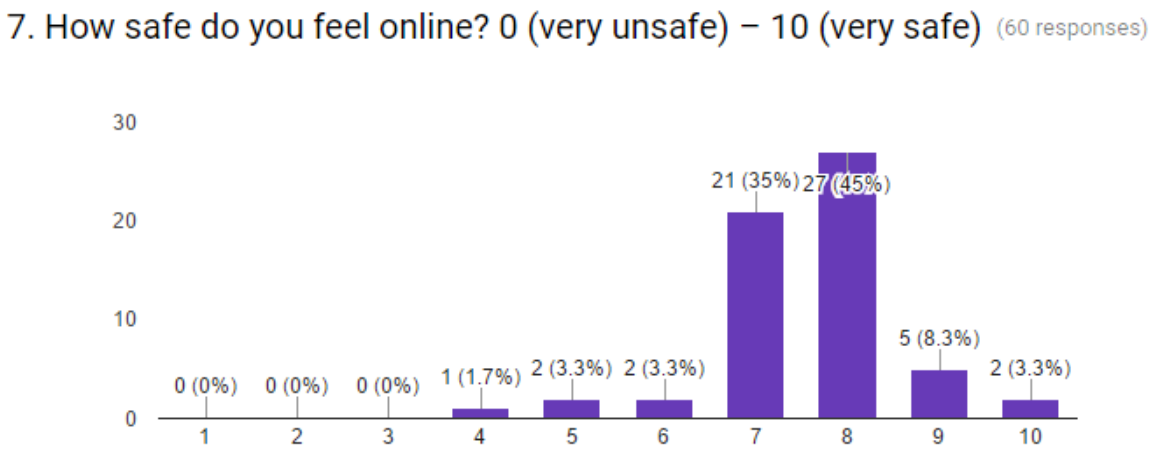
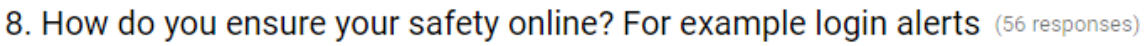


Figure 8: Bar chart indicating the degree to which students feel safe online.

91.6% (7-10 ranges) of students feel reasonably to very safe on line, an astonishing figure given the findings from the literature review which highlighted SNS security as a major issue. This result indicates that despite experiencing breaches in security (question 9) it hasn't affected how safe the students feel online, and therefore their use of social media.



This is an open question resulting in varied responses, some with more than one answer. This question was devised in order to gather more data on security measures, adding to question 5. This question directly relates to research question 1 and can be used to help answer research question 3. The results are presented via a table (Fig.9).

56 out of 60 students responded. 58.9% of participants identified login alerts as a further means of ensuring security on SNS. Login alert is described on Facebook Security as 'a means of letting you know if anyone logs in from a device or browser you don't usually use'. As this system notifies the user via email if any unfamiliar location or browser appears, it appears that this might be a highly effective way of ensuring that your account is secure.

How do you ensure your safety online?	Response
Login alerts	33
Strong passwords	11
Two step authentication	8
Private profile	7
Connected to mobile pin-codes	2
Checking account activity	1
Check security updates	1
Passphrase	1
Email alerts	1
Pay attention to account activity	1
Log out after use	1
Only accept people I know	1
Watch what I post	1
Not sure	1

Figure 9: Table showing the distribution of security measures adopted by participants.

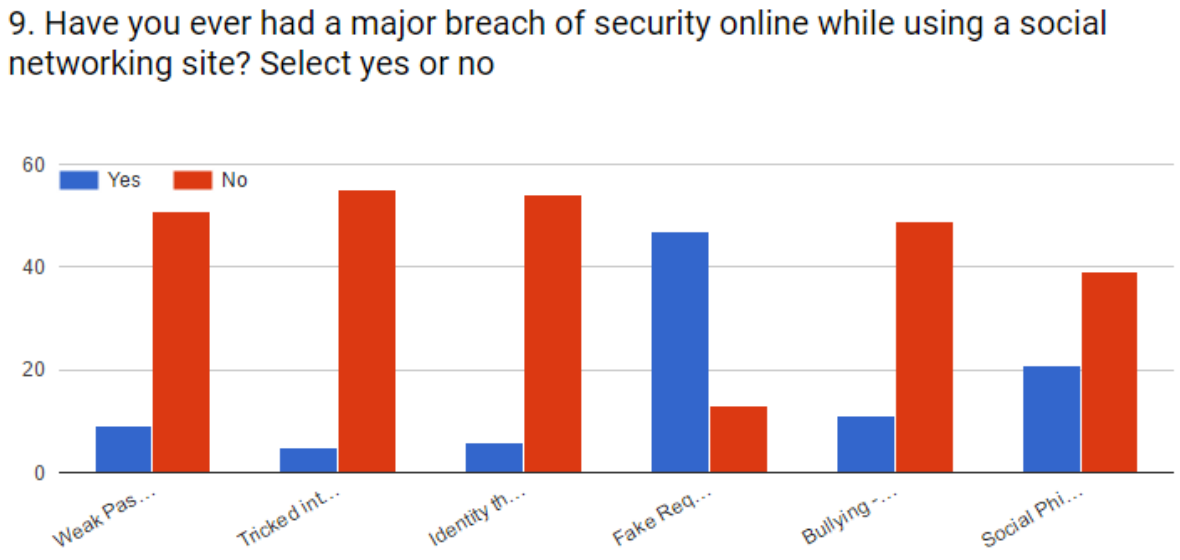


Figure 10: Bar chart indicating the amount of breaches encountered by participants and its type.

Breach	Percentage Yes	Percentage No
Weak password	15%	85%
Tricked into installing malicious hardware	8.33%	91.66%
Identity theft	10%	90%
Fake requests	78.33%	21.66%
Bullying	18.33%	81.66%
Social phishing	35%	65%

Figure 11: Table showing the percentages of the breaches encountered and its type.

This question asks the students about breaches and what types they have experienced whilst using a SNS. It relates directly to research question 2. Interestingly, 35% of students have experienced social phishing, identified as a high-level breach in the literature review (Zhang and Gupta, 2016). A significant amount of students have experienced fake requests. Security online needs to be a raised issue.

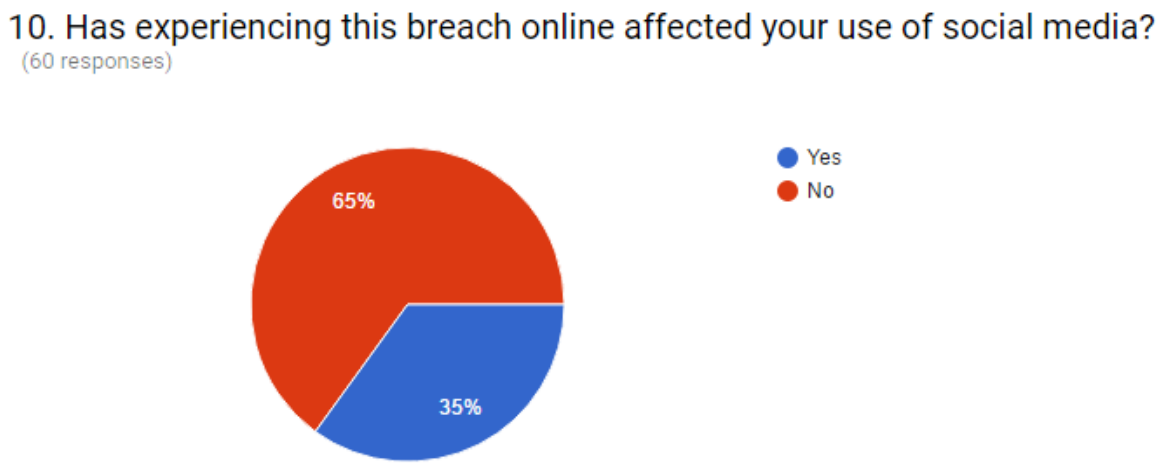


Figure 12: Pie chart showing whether this breach has affected their use of social media

Have they learnt anything from this breach? 65% of students said that experiencing a breach has not affected their use of social media. This was raised by the literature

whether somebody who'd experienced a breach became more aware about security issues.

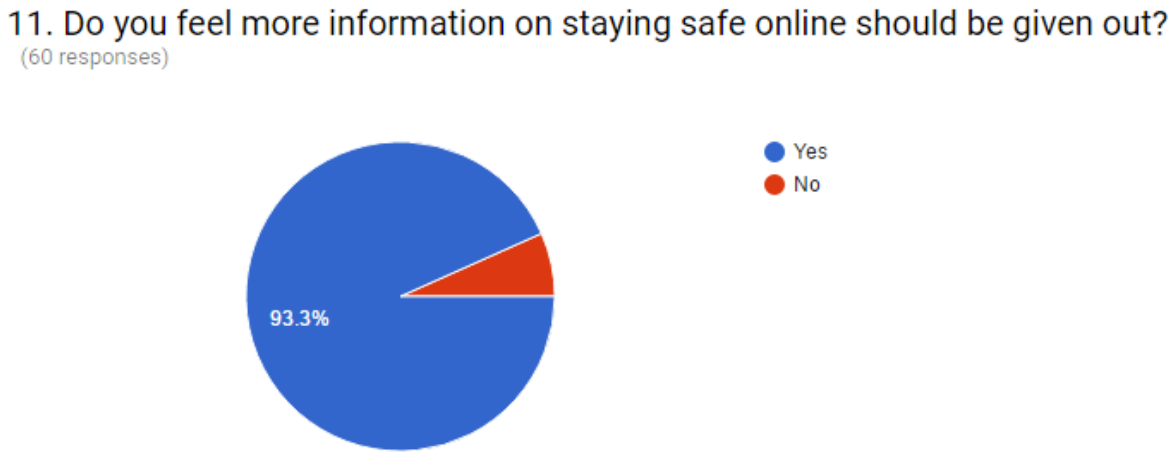


Figure 13: Pie chart showing the percentage of students who want more information on online safety.

Majority agreed (93.3%) that more information needs to be given out on how to be safe online. This high figure is indicative of the ambiguity surrounding social media use. On the one hand students recognise a great need for advice on the other they feel relatively safe online. (Question 7).

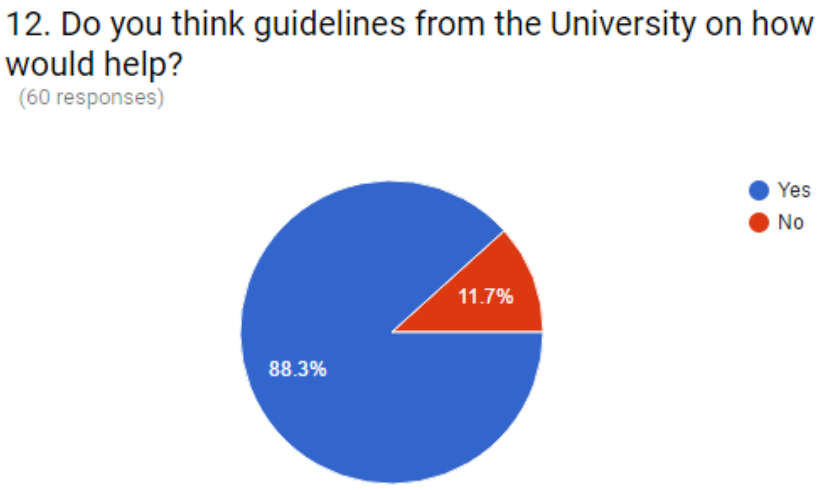


Figure 14: Pie chart showing whether participants believe guidelines from the University will help then be more secure online

88.3% agreed it would be beneficial to them for the University to give advice on how to be secure online. This guide should provide instruction on the current types of

threat (including most recent developments) and guidance into how to avert them and to stay vigil. The ever-changing face of technology requires this guide to be constantly updated.

Discussion:

What are the current ways of ensuring security on social networking sites?

From my research, it is apparent that students from the University of Gloucestershire use a number of ways to ensure their safety online. The top three ways they use are: with a secure password (100%), login alerts (58.9%) and thirdly limitation to what people can see on your profile (68.3%).

The literature however, is clear about the degree of threat that students face on SNS. Lawler and Molluzzo (2009) noted that 55.6% of students did not read the privacy policies of their SNS because they were long and difficult to read and also noted a problem with customising privacy settings. Putnik and Boskovic (2012) said that students were using SNS unwisely, and required educating in safe use of the internet because they lacked knowledge about the different types of attack they were exposing themselves to. In short, students need to develop ways of ensuring security online which keeps up with the developing skills of hackers etc. Popescul and Georgescu (2015) confirm that students, although able to protect themselves against hackers, viruses, spams, are not aware of the more modern technical dangers.

There is evidence from the data collected (they use login alerts, dual authorisation etc.) that suggests the students from the University of Gloucestershire now read privacy policies, although one oversight is that no specific question on this was included in the questionnaire. The participants also showed an awareness of needing extra security measures (question 8 on the questionnaire). Popescul and Georgescu's study identified current ways that students ensure their safety on Facebook via their specific policies. Their results showed that login alerts were a preferred way that their participants protected themselves online (71%).

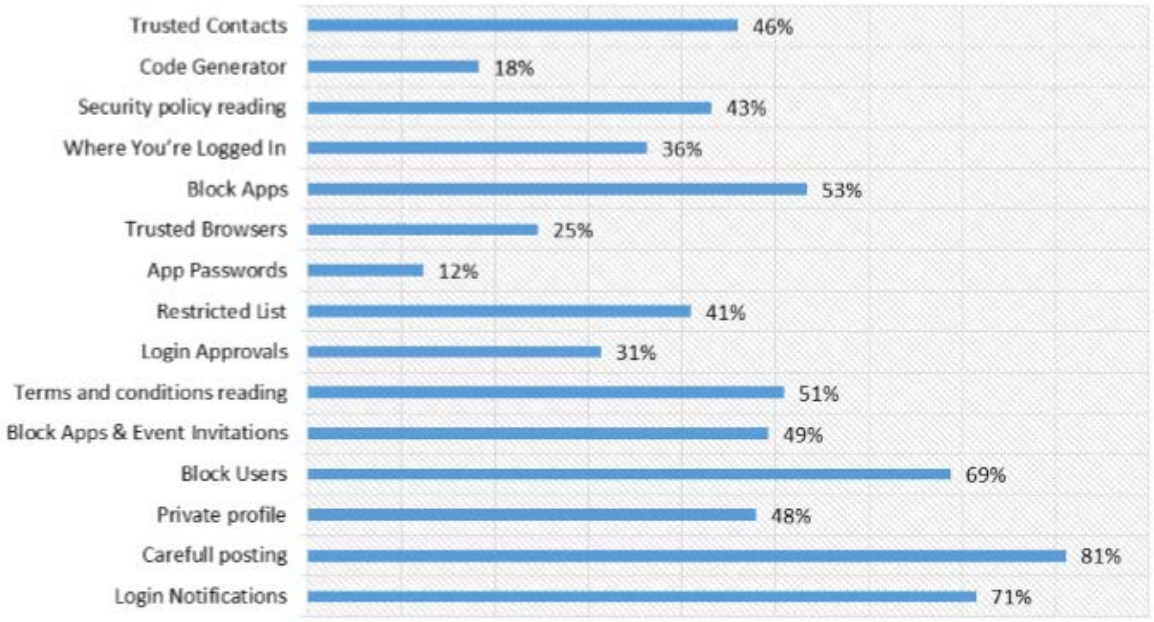


Figure 15: Students use of Facebook security settings taken from: Popsecul, D., & Georgescu, M. (2015).

For research question 1, the inclusion of a question specific to this has helped to achieve my aims and objectives. The fact that students were asked about security measures via an open-ended question might have prohibited them from including other measures that they simply failed to recall. Popescul and Georgescu's results were possibly gathered more effectively by suggesting more strategies. However, there security measures were related to Facebook specifically, whereas I did not restrict my research to this SNS.

<u>What are the most recent major breaches of students using social networking sites?</u>

The type of breaches experienced by the participants is important in order to identify current threats faced by students on SNS. The questionnaire allowed me to see what breaches are of most concern to students of the University of Gloucestershire and if this has affected their use on SNS.

From the data collected (question 9), 78.33% of students regularly have fake requests from suspicious accounts. Interestingly, when asked about having

measures of keeping safe (question 5) only 35% said they have a limitation on who can send them friend requests. Possibly, students are aware of this breach, but rather than use privacy settings decline the friend request. Zhang and Gupta (2016) say that the prevention of fake requests is not possible, requiring more responsible use of SNS.

Social phishing at 35% was the second highest breach and is regarded by Zhang and Gupta (2016) as a having a high impact on the user if successful. Zhang and Gupta say this can be significantly reduced if the users are aware and examine the data they receive carefully. After experiencing this breach, 47.6% of the participants who identified this directly, said that it had affected their use of social media. Generally, 35% of all the students said experiencing a breach affected their use of social media (question 10). There is a rise, but it is not significant enough to draw any conclusions. However, the fact that 65% felt that experiencing a breach was not enough to restrict their use of social media is indicative that the students enjoy using SNS too much to restrict their activity. Putnik and Boskovic's (2012) study states young people over expose themselves to dangers implicit in social media.

Popescul and Georgescu (2015) found from their respondents that 58% considered that the SNS are important gateways for malware. Data collected from my questionnaire revealed that this breach had the lowest concern (8.33%), despite the degree of threat involved. Interestingly only 18.33% of participants reported an incidence of cyberbullying, despite widespread media reporting of this. This finding complies with evidence from the literature review that this is more a concern to younger school -aged students (Putnik and Boskovic, 2012).

Conclusively for this research question I feel I have achieved my objectives in that I have found what breaches have affected the students of the University of Gloucestershire. Although, the sample group is small, I have noted trends similar to those identified in the literature review.

What new innovations might be used to avoid such breaches in the future?

Innovations in this context means new ideas in technology and methods. The study did not provide any specific evidence of emerging technologies but did reveal that students were using the main safety recommendations provided by their SNS. However, only 16.7% use more innovative strategies such as fingerprint recognition. In the open question about safety measures only a very small minority responded with answers about ‘paying attention to account activity’, ‘watching what was posted’, ‘checking security updates’ and only ‘accepting known people’. This is indicative that the users themselves might need to do more to ensure their own safety as well as becoming more aware of new technologies.

The theme of whether it is the responsibility of SNS or users to improve safety runs through the literature. Kumar and Gupta et al (2013) say that SNS offer security measures but it could be the user who does not know how to properly secure themselves online. They propose an architecture which ensures the secure exchange of data between SNS users, a method which involves the user taking responsibility for the passing of safe information.

The literature also suggests that SNS don’t do enough to ensure the security of their users. Kumar et al (2016) believe SNS should take responsibility for security breaches as opposed to the human element. Zhang and Gupta (2016), call for investigation into the effectiveness of social media tools, platforms and applications, implying that SNS need to update their traditional security techniques of cryptography and image processing methods. Kumar and Deepa (2016) call for enforced safety policies for SNS. Despite this, it is still felt that ‘users have become more addicted to sharing their personal ideas to a wider range of friends’. (Zhang and Gupta 2016). Evidence collected from this study reveals that in general the users do not consider restricting their use of SNS activity (the amount of friends for example) as an option for safer use.

The research did reveal that students thought more information should be given out on how to be safe online (93%), even though 91.6% said they felt safe on SNS. 88.3% thought that guidelines from the University of Gloucestershire would increase

security on SNS. The literature also proposes this: universities need to establish a coherent security policy and set of procedures for students using social media, with emphasis on education about the different types of attack they face. (Popsecul and Georgescu 2015). Business papers agree: curriculum training from universities in the fields of technology and communication would be of great benefits to business. Graduates should be able to 'utilise social media effectively for business projects'. (Kwon et al, 2013)

Lancaster University is one of the few universities to provide a security policy for students and staff on social media which recognises current threats. For example, they have a policy which deals with fake requests directly. Their solution appears to rely on user awareness rather than new technology, hence it educates on the proper use of social networks rather than rely on SNS. They regard SNS as valuable tools but it is important to avoid any breaches of data.

Conclusively, I believe the best way to ensure the security of students at the University of Gloucestershire on SNS is to create similar guidelines (see appendix 4).

These guidelines need to contain recommendations about the latest strategies for being safe online (taken from their breaches) and warn them of any new technical dangers. The University of Gloucestershire could develop a security policy which uses plain language and instructions on being safe on SNS. Knowledge, training and guidance from the University is essential because this study shows that students are not willing to cut their use of SNS.

<u>Does the increase in the amount of users pose a threat to security, should we still be doing this?</u>

This question is impossible to answer form the data that I have collected and it must remain speculative. From my survey, many students have a large number of friends on SNS (55% having 300+) but it was found that this does not affect the amount of

breaches they have experienced as participants with lower have had similar breaches. However, users must not be confused with friends.

The technological literature in particular is clear about the degree of threat that we all face because of the pace of growth of social media use. There were an estimated 2.13 billion users in 2016 worldwide and the situation about security is urgent. (Zhang and Gupta 2016). Threats are real because social media sites are accessible anywhere and BYOD to work has increased the number of cyber-attacks from mobile devices, because mobile devices are increasingly targeted (McAfee 2010). 'So much sharing allows hackers and thieves to find easy ways to steal personal information' (Kumar and Gupta 2013).

I believe that with this amount of users it is impossible for these sites to oversee all their users all the time. For example, after reporting an inappropriate image on Facebook it may take hours before it is taken down due to the sheer amount of complaints they have to go through daily. Facebook's community standards state that with explicit images "in order to treat people fairly and respond to reports quickly, it is essential that we have policies in place that our global teams can apply uniformly and easily when reviewing content". However, it seems that it cannot be done with immediate response. Despite this use of SNS grows. Students use them for sharing activities and interests with family, friends and the unknown, despite a threat to individual security.

Conclusion:

The primary aim of this research was to investigate the strategies that can be employed to ensure the security of students using SNS. My objectives were to answer this through 4 sub questions, namely what strategies were currently used, the type of breaches experienced and whether these breaches had affected use. I then assessed whether there were any new innovations which might help students be safer online. Finally, I tried to assess the degree of danger SNS represented generally.

My conclusions were that students were protecting themselves with security measures provided by the site. However, they were not aware of new technologies

which might not be covered by such measures. The breaches experienced by the participants were standard, and newer threat types as described by technical journals were not disclosed. These breaches did not appear to significantly affect use of the site, implying that users are willing to take risks for the degree of interaction they receive.

Student response suggested that written security policies for the students of UOG would be a good way to ensure their security online. Ideas from business and technology point to universities providing more information on how to be safe online, and to preparing students for work.

However, my study was small and much more work is needed considering the growth in social media use. Further work with more participants would be highly worthwhile. Another perspective would be to investigate whether technical students have had more or less breaches online compared to those courses less technical.

References

Bahadur, G., & Inasi, J., & Carvalho, A. (2011). *Securing the Clicks, Network science In the Age of Social Media*. New York: McGraw-Hill, pg 3-320

Boyd, D., & Ellison, N. (2007). Social Network Sites: Definition, History, and Scholarship, *Journal of Computer Mediated Communication*, 13 (1), 210-230. [online] Available from http://onlinelibrary.wiley.com/doi/10.1111/j.1083-6101.2007.00393.x/full (last accessed 03/11/16).

Blue Ocean. (2011). Social Media Security Policy. [online] Available from www.blueoceantechnologies.net/BlueOceanTechnologiesSocialMediaSecurityPolicy.pdf (last accessed 05/11/16)

Curry, S. (2011). The Weakest Link is the Human Link. [online] Available from www.securityweek.com/weakest-link-human-link (last accessed 05/11/16)

DAILY MAIL, (2016) The Secret Password we're still using? Password!, *The Daily Mail,* UK, November 5th.

DAILY TELEPGRAPH, (2016) Excuse me your age is showing, *The Daily Telegraph,* UK, November 15th, pg 15.

GRAZIA, Kendall's Fight To Break Free, November 28th 2016.

He, W. (2012). A review of social media security and risks and mitigation techniques, *Journal of Systems and Information Technology,* 14 (2), 171-18. [online] Available from http://www.emeraldinsight.com/doi/abs/10.1108/13287261211232180?journalCode=jsit (last accessed 02/11/16).

Kaplan, A., & Haenlein, M. (2010). Users of the world, unite! The challenges and the opportunities of social media. *Business Horizons.* 53. [online] Available from https://www.scribd.com/doc/63799736/Kaplan-and-Haenlein-2010-Social-Media (last accessed 10/11/16).

Kumar.A., & Gupta.S, & Rai, A., & Sinha, S. (2013). Social Networking Sites and Their Security Issues, *Journal of Scientific and Research Publications,* 3 (4) [online] Available from http://www.ijsrp.org/research-paper-0413/ijsrp-p1666.pdf (last accessed (02/11/16).

Kumar.S., & K,S., K, Deepa. (2015). On Privacy and Security in Social Media - A Comprehensive Study, *International Conference on Information Security & Privacy*, 114-119. [online] Available from http://www.sciencedirect.com/science/article/pii/S1877050916000211 (last accessed 05/11/16)

Kwon, O. & Min, D. & Geringer, S. & Lim, S.K. (2013) Students Perception of Qualifications for Successful social media Coordinator*, Academy of Marketing Studies Journal*. 17 (1), 109-128. [online] Available from http://search.proquest.com/openview/12bf14d8951b24fac9412f3afebc1b03/1?pq-origsite=gscholar (last accessed 04/11/16).

Lancaster University, Information Security: Use of Social Networking tools. Available from http://www.lancaster.ac.uk/iss/security/ *(last accessed 11/11/16).*

Lawler, J.P., & Molluzzo, J.C. (2010). A Study of the Perceptions of Students on Privacy and Security on Social Networking Sites (SNS) on the Internet, *Journal of Information Systems Applied Research,* (3) (12). [online] Available from http://www.proc.conisar.org/2009/3732/CONISAR.2009.Lawler.pdf (last accessed 04/11/16)

McAfee (2010), 2011 Threat Predictions. [online] Available from http://161.69.13.40/us/resources/reports/rp-threat-predictions-2011.pdf (last accessed 05/11/16)

Popsecul, D., & Georgescu, M. (2015). Social Networks Security in Universities: Challenges and Solutions, *Scientific Annals of the "Alexandru Ioan Cuza" University of Iasi Economic Sciences,* 62 (SI) 53-63. [online] Available from https://www.degruyter.com/view/j/aicue.2015.62.issue-s1/aicue-2015-0036/aicue-2015-0036.xml (last accessed 05/11/16).

Putnick, N., and Boskovic, M. (2012). The Impact of Media on Students' Perception of the Security Risks Associated with Internet Social Networking – A Case Study', *Croatian Journal of Education,* 17 (2) 569-583. [online] Available from http://hrcak.srce.hr/index.php?show=clanak&id_clanak_jezik=208207 (last accessed 07/11/16).

The Statistics Portal. (2016). *Individual Analysis and Market research by Statista Research Analysis.* Available: https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/ (last accessed (10/11/16).

THE TIMES, 'Firms Must Stop Child Sexting', November 30th 2016.

TODAY PROGRAMME, RADIO 4, November 30TH 2016.

Turban, E., & Bolloju, N., & Liang, T-P. (2011). Enterprise Social Networking: Opportunities, Adoption, and Risk Mitigation, *Journal of Organizational Computing and Electronic Commerce*, 21 (3), 202-220. [online] Available from http://www.ecrc.nsysu.edu.tw/liang/paper/1/Enterprise%20Social%20Networking%20(JOCEC%202011).pdf (last accessed 03/11/16).

Steinhart, M. (2009). Web 2.0: Worth the risk? *Secure Computing.* [online] Available from http://www.securecomputing.com/webform.cfm?id=255&ref=pdtwp1657 (last accessed 05/11/16)

Vroom, C., & Von Solms, R. (2004). Towards information security behavioural Compliance. *Information Management and Computer Security,* 6 (4), pp. 167-73.

Zeltser, L. (2011). Monitoring social media for security references to your organization. [online] available from http://isc.sans.edu/diary.html?storyid=10921 (last accessed 05/11/16)

Zhang, Z. & Gupta, B.B. (2016). Social media security and trustworthiness: Overview and new direction, *Future Generation Computer Systems.* [online] Available from http://dx.doi.org/10.1016/j.future.2016.10.007 (last accessed 01/11/16).

Appendices

Appendix 3: Final Questionnaire

Questionnaire

This questionnaire has been designed in order to view how safe students from the University of Gloucestershire feel online, the breaches they have had and what can be done to improve this.

1. What is your gender? Tick box.
- Male/Female

2. What is your age range?
- 18-24
- 25-34
- 35-44
- 45+

3. What subject are you taking at the University of Gloucestershire?
- Open question

4. What is the main social networking site you use and its profile type?

Site	**Public Profile**	**Private Profile**
Facebook		
Twitter		
Instagram		
Snapchat		
Tumbr		
LinkedIn		
Pinterest		
YouTube		

Google+		

5. Do you use any measures to keep yourself safe on this site? Tick/multiple
- Secure password
- Limitation to what people can see on your profile
- Limitation on who can send you friend requests
- Dual authorisation
- Fingerprint recognition

6. How many friends do you have on your main social networking site? – Tick box
- 0-100
- 100-200
- 200-300
- 300-400
- 400-500
- 500+

7. How safe do you feel online? Scale, 0 (very unsafe) – 10 (very safe).

8. How do you ensure your safety online? For example, login alerts. Open Question

9. Have you ever had a major breach of security online while using a social networking site? Please tick the boxes where you have experienced this

Breaches online

Breach	Description	Tick Box
Weak Password/hacked or revealed	Using a password which is weak, people can access your account(s) or you have revealed it.	
Tricked into installing malicious hardware	Opening links where there is hidden malware, leaving your computer vulnerable to infection.	
Identity theft	Someone has taken information and images from your profile and used them to create a fake account.	
Fake requests	Accounts which are clearly not who they say they are have requested a friend request.	
Bullying	Faced abuse online from people, either publicly or through private mail.	
Social Phishing	Someone has attempted to obtain information from you online, such as passwords, usernames or credit card details.	

10. Has experiencing this breach online affected your use of social media? Tick Box

- Yes/No

11. Do you feel more information on staying safe online should be given out? Tick Box

- Yes/No

12. Do you think guidelines from the university would help? Tick box

- Yes/No

Appendix 4 –Security measures for social networking sites.

UOG: Security policies for Social networking sites

1. Students should make sure they have a strong password, which they change regularly, do not use your University email address or password as your login.
2. Carefully read the privacy and security policies offered by your SNS, having a private profile will enable you to hide information from a fake account.
3. Set up extra security measures to make your account more secure – Login alerts and two-step authentication or fingerprint recognition to your devices.
4. Do not accept fake friend requests, this gives the attacker more privileges and information on their victims.
5. Only accept people you know, they can access your personal information and use this to impersonate you.
6. Do not share restricted information or personal data with anyone, such as passwords, credit card information online, be aware of posts that are phishing for personal information.
7. Watch what you post. Future employers may gain access to information which could affect your employability. Also, avoid details such as you are going away for a week.
8. Antivirus software should be installed on devices for protection against malicious hardware. Watch what links you are clicking on, it can lead to fake websites attempting to steal personal information from the target user.
9. Be careful what images you post online, they can reveal a lot about you.
10. If you feel threatened online and someone is sending you abusive messages, block and report the user.

What Strategies could be employed to ensure the Security of Students using Social Networking Sites?

By Martha Sewter

ABSTRACT

This research investigates the degree to which students at the University of Gloucestershire are safe using Social Networking Sites (SNS). It examines what experiences they have had of breaches, and to what extent these breaches have affected their usage of social media. Also important is if new technology can help or whether it is more important to provide training for students to ensure their safety online.

The research was carried out via a questionnaire to 60 students+ using google forms, emails and face to face contact. I discovered that students felt relatively safe online (91.6%) even though 78.33% had experienced a breach. I concluded that the best way to ensure student safety was to increase safety and technical awareness via training provided by universities.

INTRODUCTION

Assignment 1 identified students as high risk users of social media regarding security. Consequently, what strategies could be employed to ensure the safety of students online was made the subject of this study. The literature review confirmed that students were a high risk group on social media, with suggestions ranging from a lack of awareness of safety issues and knowledge of different types of technical threats, to narcissistic and impatient behaviour. It also revealed that universities needed to establish a coherent security policy for there students on SNS.

For my methodology I used a questionnaire. This was supported by the literature, which contained examples of research with students using questionnaires. This appeared to be a successful and proven way to obtain data on the subject.

OBJECTIVES

- What are the current ways of ensuring security on social networking sites?
- What are the most recent major breaches of students using social networking sites?
- What new innovations might be used to avoid such breaches in the future?
- Does the increase in users pose a threat to security, should we still be doing this?

References:

Lancaster University, Information Security: Use of Social Networking tools.

Popsecul, D., & Georgescu, M. (2015). Social Networks Security in Universities: Challenges and Solutions, *Scientific Annals of the "Alexandru Ioan Cuza" University of Iasi Economic Sciences,* 62 (SI) 53-63

Putnick, N., and Boskovic, M. (2012). The Impact of Media on Students' Perception of the Security Risks Associated with Internet Social Networking – A Case Study', *Croatian Journal of Education,* 17 (2) 569-583.

Zhang, Z. & Gupta, B.B. (2016). Social media security and trustworthiness: Overview and new direction, *Future Generation Computer Systems*

RESULTS

Participants from my questionnaire were 65% male and 35% female. 88.3% were between the ages of 18-24 (my target age range), the study group contained a mix of subject areas. It was found that Facebook was the most popular SNS, (44 users or 73.3%)

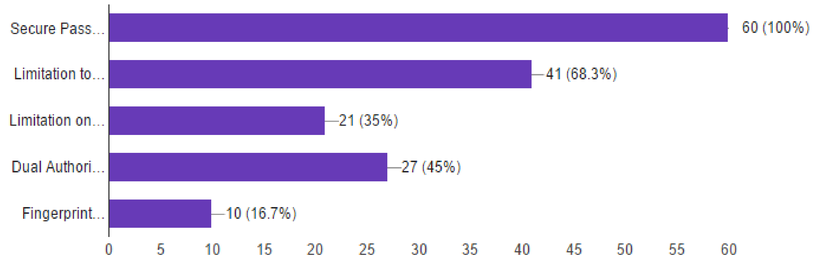
What are the current ways of ensuring security online?

Information was gathered to allow participants to select/comment on the ways they make sure they are safe online

Results revealed that students from the UOG use a number of ways to ensure their safety online. The top three ways they use are: with a secure password (100%), login alerts (58.9%) and thirdly limitation to what people can see on your profile (68.3%).

This agreed with the literature. Popescul and Georgescu's study identified current ways that students ensure their safety on Facebook via their specific policies. Their results showed that login alerts were a preferred way that their participants protected themselves online (71%).

Bar chart showing current ways students at UOG protect themselves on SNSs

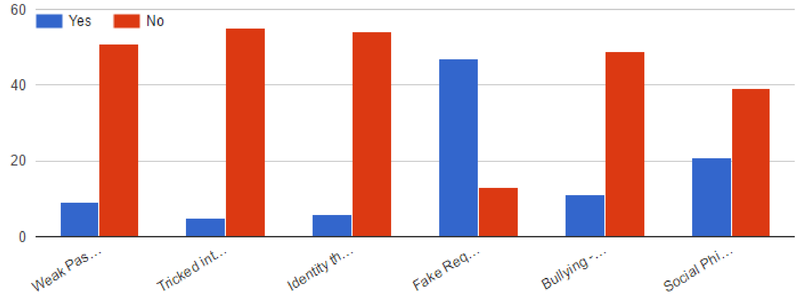


What are the most recent current breaches of students using social networking sites?

The highest breach was receiving fake friend requests online, 78.33% of students have experienced this. However, 35% of students have experienced social phishing, identified as a high-level breach (the second highest breach) and having a high impact on the user if successful in the literature review (Zhang and Gupta, 2016).

However, the fact that 65% felt that experiencing a breach was not enough to restrict their use of social media is indicative that the students enjoy using SNS too much to restrict their activity. Putnik and Boskovic's (2012) study states young people over expose themselves to dangers implicit in social media.

Bar chart showing security breaches of students from the UOG on SNS



What new innovations might be used to avoid such breaches in the future?

The study did not provide any specific evidence of emerging technologies but did reveal that students were using the main safety recommendations provided by their SNS.

However, it did reveal that students thought more information should be given out on how to be safe online (93%), even though 91.6% said they felt safe on SNS. 88.3% thought that guidelines from the University of Gloucestershire would increase security on SNS. The literature also proposes this: universities need to establish a coherent security policy and set of procedures for students using social media, with emphasis on education about the different types of attack they face. (Popsecul and Georgescu 2015).

Lancaster University is one of the few universities to provide a security policy for students and staff on social media which recognises current threats
Conclusively, I believe the best way to ensure the security of students at the University of Gloucestershire on SNS is to create similar guidelines

Does the amount of users pose a threat to security, should we still be doing this?

This question is impossible to answer from the data that I have collected and it must remain speculative. From my survey, many students have a large number of friends on SNS (55% having 300+) but it was found that this does not affect the amount of breaches they have experienced as participants with lower have had similar breaches. However, users must not be confused with friends.

There were an estimated 2.13 billion users in 2016 worldwide and the situation about security is urgent. (Zhang and Gupta 2016). I believe that with this amount of users it is impossible for these sites to oversee all their users all the time.

CONCLUSIONS

My conclusions were that students were protecting themselves with security measures provided by the site. However, they were not aware of the more technical options, for instance only 10 people (16.7%) used fingerprint recognition. The breaches they have experienced did not appear to significantly affect use of the site.

Student response suggested that written security policies for the students would be a good way to ensure their security online, 88.3% believed this would help.

However my study was small and much more work is needed considering the growth of social media use. Another measure could be to measure whether technical students have had more or less breaches online compared to those courses less technical.