HBCS CW1

Portfolio of Research Papers

Student ID: 2136685

Table of Contents

Member Paper 1

""My Data Just Goes Everywhere:" User Mental Models of the Internet and Implications for Privacy and Security"

Our first question was, "Do you agree with the findings that lay people can be more likely to be practically secure?". As a discussion of the first question, we agreed that, in general, lay people have simpler mental models over technical people. However, we also agreed that the example group was not sufficient and the sample size was not large enough to show that lay people are not as secure as technical people, as if there was a larger sample size, the discrepancy between them would have been clearly visible (Kang et al., 2015).

As the paper concluded, people with prior knowledge can recognise threats much faster due to intuition, as prior knowledge is a big part in people recognising threats. Therefore, technical people have a higher risk appetite and are more likely to take risks if they know how to tread lightly (Kang et al., 2015).

All people wish for privacy, however they wish not to act as convenience always outweighs security. Even technical people, who understand encryption, still choose not to encrypt their devices. As shown in Table 3, page 46 in the article, lay people, when asked about security, talk more about clearing cookies as they are more likely to have seen ads about them before, for example the DuckDuckGo ads, therefore they have a visual incentive to clear cookies, caches and the history (Kang et al., 2015).

Our second question was, "Do you believe that people's perceptions of the internet can be inferred from demographic characteristics? ". We believe that surveys would have been useful in gathering data, more than interviews, but there must be incentive for people to do the surveys, otherwise the data might be erroneous. Perhaps the experts that made the tests could have had their mental models done and compared to the lay and technical people. Overall, we agreed that the sample size was nowhere near enough to infer people's perceptions (Kang et al., 2015).

Member Paper 2

“Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment?”

Our first question was, “Do you believe that there should be a clear disparity between the results from scenarios based on intuitive and rational judgements and do you believe that a large difference would be seen in more cyber security educated individuals?”. In the methodology used by the researchers of the article, the intuitive test answers do not have a time cap, therefore we asked “at what point does the intuitive thinking become rational thinking?” , as intuition is defined as “the power or faculty of attaining to direct knowledge or cognition without evident rational thought and inference” (Merriam Webster, 2019). Allowing participants to have unlimited thinking time, all the intuitive thinking done in the test becomes rational thinking (Yan et al., 2018).

In the case of cyber security professionals, we agreed that they would have a smaller disparity between the results as they would have much more experience with recognising threats, be it intuitive or rational (Yan et al., 2018).

Our second question was, “Do you think that scenarios q8 and s3 were answered so poorly (...) due to the scenarios taking place in a person's daily life or do you believe that the lack of education (...) causes the disparity?”. Q8 was focused on the environment, as some US cities have more car smash and grabs, therefore some people may be more weary of leaving valuables in their cars, whereas otherwise, the majority of people would be less aware of leaving important belongings in the car. S3 was focused on education, as a less cybersecurity educated person may not be aware of a record disappearing and just replace it instead of reporting it as a potential threat. Whereas a cybersecurity professional would immediately follow an incident response policy (Yan et al., 2018).

Member Paper 3

“Virtuous human hacking: The ethics of social engineering in penetration-testing”

Our first question was, “Should constraints be placed on white hat social engineering to cultivate virtuous hacking, or can a utilitarianist approach offer greater results that outweigh this?”. There is a dillema here, as the employees must get told if they are subject to social engineering attacks for testing, but if they are told, the test is compromised as they get unusually aware and vigilant (Hatfield, 2019).

Utilitarianism says that the ends justify the means, so as long as the system gets more secure, it doesn’t matter who gets manipulated. However, there are example where this goes horribly wrong, such as the NHS nurse who fell to a social engineering attack by some Australian radio hosts, which drove the nurse to suicide. Therefore, Kant suggests that penetration testing should miss social engineering altogether (Hatfield, 2019).

Otherwise, some compromises can be done to ensure that the employee’s dignity is not affected, such as intruding only on work life and not outside life, however utilitarianism will always offer more results and adding constrants doesn’t emulate a black-hat hacker (Hatfield, 2019).

Our second question was, “Do you believe that the phrase “as long as the ends justify the means within reasonable boundaries” has an effect on penetration-testers seeking consent, given the context of the ethical dilemma of social engineering in penetration-testing?”. There can be a clause in the contract where it states that when you sign, you can be subject to social engineering attacks for the purpose of testing, but that would be coerced on to the employees, as otherwise they would not get the job. Moreover, implicit consent from a contract may not be ethical, as they have not explicitly given consent, just like Google collects data without someone giving explicit consent, but they agreed to the terms and conditions. On-the-other-hand, consent can be opt-in, but this jeopardizes the test as it is not a faithful emulation of a real incident (Hatfield, 2019).

Leader Paper

"Security factors on the intention to use mobile banking applications in the UK older generation (55+). A mixed-method study using modified UTAUT and MTAM – with perceived cyber security, risk, and trust"

Mobile banking applications and have become increasingly preferred in the UK, especially among the younger generation, however the older generation is generally apprehensive in using mobile banking applications as they mention privacy and security concerns. The paper aims to research why the older generation is so apprehensive, in regards to cyber security. The researchers used the Unified theory of Acceptance and use of Technology (UTAUT) model, modified to include "perceived cyber security risk", "perceived cyber security trust" and "perceived overall cyber security" (Hanif and Lallie, 2021).

Approximately 32% of mobile banking users are between ages 55-64 and 16% are ages 65+. This number is very low as some customers cannot use mobile banking, or just prefer bank branches. Moreover, the customers that wish not to use mobile banking cite a lack of trust or security concerns with the platform. As the UK has increasingly adapted the use of mobile banking applications, more high street bank branches have been closed down, with over 3509 high street banks closed from January 2015 to February 2020. This can be a problem for customers that prefer to go to a local bank branch, leaving older users with fewer options and causing anxiety when using online or mobile banking. Therefore, this research looks into how the perceived cyber security risk affects the intention to use mobile banking applications in ages 55+ (Hanif and Lallie, 2021).

A problem the growing older generation faces when trying to adopt mobile technology is that technology advances very quickly and it is difficult for them to keep up, so they would rather not bother. Loss in motor function due to age or due to diseases such as Parkinson's disease limits an older person's ability to use a smartphone – Kuerbis et al. Believes that training and better design of mobile phones would help in overcoming this obstacle – however, the leading factor is the lack of knowledge which influences an older person's usage of mobile technology, because it leaves negative perceptions towards technology. Making mobile devices easier to use, or making the older customers aware of the benefits of using mobile devices would result into an uprise in the uptake of mobile technology in the older generation (Hanif and Lallie, 2021).

There have been previous studies into the intention to use mobile banking, but only recently and some have been more generalised towards the adoption of e-technology overall. Most of these tests have a relatively small sample size of the older generation, for example Kumar et al. wanted to determine the likelihood of users to adopt mobile banking but only 12 people were 56+ and security was recognised as a limiting factor but it was not considered in the survey. Moreover, Van et al. investigated the relationship between perceived risk, trust and intention to use mobile banking in Vietnam, however out of the 403 people, only 48 people were aged 40+. Van et al. did find out that perceived risk is negatively related to trust and intention to use and that trust is positively related to intention to use. The perceived risk is comprised of financial risk, social risk, time risk, privacy risk, security risk and performance risk, but unfortunately it doesn't focus on the security risk. Unlike Van et al., Alonso-Dos-Santos et al. determined, in ages 18-34, that trust does not impact intention to use, however it impacts bank loyalty. Other tests also concluded that trust does not impact intention to use, but the perceived security did, such as Akhter et al., however Merhi et al. found that trust did impact intention to use positively in a sample size of 901 people, where only 37 were aged 56+. Overall, there is a lack of representation for the older generation (Hanif and Lallie, 2021).

The paper uses the OWASP top 10 threats to mobile applications to show the risk of using them and how the older generation's fears are not unjustified. Some examples of risks are insecure data storage, where it is believed that 83% of the UK's and US' financial applications' data is stored insecurely, the older generation is also more prone to falling victim to malware, leading to a risk of the data stored on the smartphone to be compromised. Moreover, these applications may use insecure authentication methods which could allow threat actors to execute tasks within the mobile applications, or the application may be vulnerable due to weak password policies, storing passwords on the device or even using vulnerable biometrics such as Touch ID. These threats have a severe impact on the user (financial and psychological) and on the bank (reputational, loss of customers, heavy penalties due to breaching GDPR) (Hanif and Lallie, 2021).

The researchers have used UTAUT and Mobile echnology Acceptance Model (MTAM) in this study. UTAUT has been used in the past to assess the adoption of technologies by the older generation, such as smart homes, online banking and tablets. One advantage of UTAUT over any other model is that you can add determinants that the researcher thinks would impact the intention to use based on the case study to fit the analysis and to give a better conclusion. MTAM puts significantly more attention on cyber security than UTAUT and determinants such as mobile usefulness, mobile ease of use, mobile perceived security risk and mobile perceived trust can be added in tandem with UTAUT to create the research model (Hanif and Lallie, 2021).

The research model is made out the main dependent variable, which is the intention to use, and it is extended with several security determinant factors, each with a hypothesis. The researchers found that the strongest determinant factor was the performance expectancy, with the hypothesis being "Performance expectancy positively impacts the intention to use mobile banking applications in the UK 55+" (Hanif and Lallie, 2021). If the older generation believes they will benefit benefit from using the technology, then they will use it. A strong determinant factor was the effort expectancy, with the hypothesis being "Effort expectancy positively impacts the intention to use mobile banking applications in the UK 55+" (Hanif and Lallie, 2021). As people get older, their motor skills degrade, therefore the less effort it requires for them to use the application, the more likely they are to use it. An increase in perceived cyber security trust does lead to an increades intention to use, the hypothesis being "An increase in perceived cyber security trust positively impacts the intention to use mobile banking applications in the UK 55+" (Hanif and Lallie, 2021). Moreover, increased perceived overall cyber security also positively impacts the intention to use, as hypothesised "An increase in perceived overall cyber security positively impacts the intention to use mobile banking applications in the 55+". On the other hand, a negative perception of the cyber security privacy concern will lower the intention to use, as hypothesised "An increase in perceived cyber security privacy concern negatively impacts the intention to use mobile banking applications in the UK 55+" (Hanif and Lallie, 2021). Also, an increase in perceived cyber security risk causes uncertainty and anxiety in a customer, therefore lowering the intention to use, as hypothesised, "An increase in perceived cyber security risk negatively impacts intention to use Mobile Banking Applications in the UK 55+" (Hanif and Lallie, 2021).

The data above was collected using multiple methods such as surveys, quantitative data (closed-ended questions), qualitative data (open ended questions) such as how or why users felt a certain way. The participants were recruited from Facebook advertisements, the public library or through meet-up groups. Some of the participants carried the surveys online and some were given paper-based versions (Hanif and Lallie, 2021).

The participants are between ages 55 to 69 and they were broken down into groups of ages 65-69, 60-64 and 55-59. The qualitative analysis questions are as follows:

- Why is it unsafe to transmit confidential data?
- Why is it unsafe to pay bills?
- Why is it unsafe to view your balance?
- What can banks do to increase your trust in mobile banking applications?
- What would make you more likely to use a mobile banking application in the future?
- Describe any other thoughts or comments that you have regarding the security of mobile banking applications

The main theme to these questions was that “hackers” will affect their transmission of confidential data, with 25% of the participants believing so. The participants also are worried that their phone can be lost or it may be stolen and they will be left without control over their account. Some participants were worried that the money they would transfer would go to the wrong place (Hanif and Lallie, 2021).

The participants suggested improvements in order to increase the trust. Some participants would trust the platform more if the systems were secure but also easy to use, if there were more security questions and passwords and some suggested that the older generation may forget passwords and they would rather have fingerprint unlock, but not iris or pupil unlock because they could develop eye conditions such as cataracts (Hanif and Lallie, 2021).

Some participants suggested that providing cyber security assurance and remediations, and training and information would make them consider using mobile banking applications, as they are not brought up with computers therefore their knowledge is limited. Some suggested that online tutorials or in-branch demonstrations would be sufficient. However, when asked what would make the participants use a mobile banking application in the future, some replied that nothing can improve their trust to use it or that they would only as a last resort, whereas some would try it if the security was improved (Hanif and Lallie, 2021).

References

Hanif, Y. and Lallie, H.S. (2021). Security factors on the intention to use mobile banking applications in the UK older generation (55+). A mixed-method study using modified UTAUT and MTAM - with perceived cyber security, risk, and trust. *Technology in Society*, 67(0160-791X), p.101693.

Hatfield, J.M. (2019). Virtuous Human Hacking: The Ethics of Social Engineering in Cybersecurity. *Computers & Security*, 83(0167-4048), p.1477.

Kang, R., Dabbish, L., Fruchter, N. and Kiesler, S. (2015). '*My Data Just Goes Everywhere:' User Mental Models of the Internet and Implications for Privacy and Security*. [online] Available at: https://www.usenix.org/system/files/conference/soups2015/soups15-paper-kang.pdf [Accessed 23 Mar. 2023].

Merriam Webster (2019). *Definition of INTUITION*. [online] Merriam-webster.com. Available at: https://www.merriam-webster.com/dictionary/intuition [Accessed 25 Mar. 2023].

Yan, Z., Robertson, T., Yan, R., Park, S.Y., Bordoff, S., Chen, Q. and Sprissler, E. (2018). Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment? *Computers in Human Behavior*, 84(0747-5632), pp.375–382.

Appendix

Leader Discussion Overview

Good evening all,

Tomorrow we will be discussing the following two questions:

- The ownership of smartphones in the older generation has grown rapidly in the UK population, from only 28% in 2015 to 69% in 2021. Do you think that the amount of information available on the topic of security is readily available for someone who has just begun learning how to use a smartphone?
- The paper recognised that a recurring theme gathered from the questionnaire was making “improvements to security“ to mobile banking applications. Do you believe that mobile banking apps are secure enough? If yes, what do you think makes older users think of mobile banking apps as unsafe?

During the brief overview, we will be covering:

- The discrepancies related to smartphone usage between the younger generation and the older generation
- The UTAUT model, the variables used and the determinants of intention to use mobile banking applications
- The closure of high-street bank branches and its impact
- The mere-exposure effect and its prevalence in the survey demographic

Kind regards,
2136685