60. Smartphone Owners Need Security Advice. How Can We Ensure They Get It?

Karen Renaud
University of Glasgow
karen.renaud@glasgow.ac.uk

Rénette Blignaut & Isabella Venter
University of the Western Cape

Abstract

Computer users often behave insecurely, and do not take the precautions they ought to. One reads almost daily about people not protecting their devices, not making backups and falling for phishing messages. This impacts all of society since people increasingly carry a computer in their pockets: their smartphones. It could be that smartphone owners simply do not know enough about security threats or precautions. To address this, many official bodies publish advice online. For such a broadcast-type educational approach to work, two assumptions must be satisfied. The first is that people will deliberately seek out security-related information and the second is that they will consult official sources to satisfy their information needs. Assumptions such as these ought to be verified, especially with the numbers of cyber attacks on the rise.

It was decided to explore the validity of these assumptions by surveying students at a South African university, including both Computer Science and Non-Computer Science students. The intention was to explore levels of awareness of Smartphone security practice, the sources of advice the students used, and the impact of a Computer Science education on awareness and information seeking behaviours. Awareness, it was found, was variable across the board but poorer amongst students without a formal computing education. Moreover, it became clear that students often found Facebook more helpful than public media, in terms of obtaining security advice.

The implications of these findings are that the broadcast strategy needs rethinking. If people prefer to learn from their peers it is necessary to focus on empowering those within the community who can act as advisors, and not to expect people automatically to seek out information from official sources. Published guidelines are unlikely to reach the man and woman in the street with the required level of efficacy. Our study makes it clear that only by satisfying the community needs at the social level can society at large be made more resilient to cyber attack.

Keywords

Security, Smartphone, Society, Precautions, Awareness, Mobile phone

1. Introduction

The man and woman in the street increasingly uses online services: to obtain information, read and send emails, use social networks, and buy products and services. This personal use, by so-called home users (The European Network and Information Security Agency (ENISA), 2010), is reinforced by the growing adoption of the Internet as communication infrastructure. The most commonly used device these days is the smartphone, a handheld computer in everyone's pocket.

Whereas organisations spend a great deal of time and effort ensuring that their employees know how to behave securely, personal security has not received as much attention (Alghamdi, Flechais & Jirotka, 2015; Li, 2011). According to Kritzinger & Von Solms (2010), 95% of Internet attacks target humans, not technical systems. Smartphone owners thus need to be aware of, and know how to use, security tools and precautionary measures to protect their devices and data from unauthorized access.

Much research has been conducted into how to improve awareness and knowledge in this area. Research into assisting people to resist phishing attacks is a good example (Alnajim & Munro, 2009; Jansson & Von Solms, 2011; Kirlappos & Sasse, 2012; Kumaraguru, Rhee, Acquisti, et al., 2007; Maurer, De Luca, & Kempe, 2011). All of the aforementioned research has been reported in the academic literature but there is no evidence that it has reached smartphone owners. People still seem to be taken in by phishing messages (Ford, 2015; BBC, 2015) and since email is now mostly read on smartphones (O'Dell, 2014) this is also a smartphone issue. Many governmental and other official bodies have attempted to help smartphone owners to protect themselves against threats by publishing advice online[1]. Yet Kaspersky (2015) report that 45% of people have encountered malware and 25% have personally been hacked. It does seem that, despite advice being freely available, something is amiss in terms of reaching and empowering computer users.

The current broadcasting approach of publishing guidelines and advice on websites, in academic literature and in the media is not effective enough. This might be because it relies on two implicit assumptions:

Assumption 1. People experience an information need, realise they lack information, and seek to satisfy their information need.

Assumption 2. People will consult official sources (government sources, security body websites and educational institutions) in order to satisfy their information needs.

These assumptions are not necessarily founded. The first assumes that people know that they have an information need: that they know there is something that they do not know. It also assumes that, having become aware of such an information need, they will act to satisfy the need (Wilson, 1999). This belief is, unfortunately, overly optimistic. Case (2012) explains that information seeking behaviour varies widely across people, situations and objects of interest and that it is difficult to predict how, or whether, a particular person will go about seeking information. Derr (1983) explains that information is only sought when it contributes towards satisfaction of a purpose. Even if people become aware of the fact that they do not know how to secure their devices, this does not mean that they will act to find out how to remedy the situation – unless there is some purpose they are trying to satisfy.

If the person *does* have a purpose, and acts deliberately to satisfy an information need, the second assumption is that they will seek the information from authoritative sources such as

[1] For example:
http://cybercrime.org.za/reporting; http://www.cyberaware.org.za/;
https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/cyber-security-policy-of-south-africa

official websites. Yang *et al.* (2014) point out that information seeking is costly, especially when people have to choose which source of information to trust. An assumption that people will go to official websites does not acknowledge this cost. Moreover, this does not acknowledge the reality that people are social animals, and rely on each other. When they are faced with uncertainty it is likely that they will consult trusted individuals first. There is evidence that attests to the role society and communities play in meeting an individual's information needs (Varela, 1992; Bruner, 1990; Kuhlthau, 1991). The reality is that many rely primarily on peers for advice, support and information needs (Bruner, 1990). In this paper the validity of the two assumptions, in terms of whether they apply to a student body, will be explored.

2. Why people do not take smartphone precautions

There is a great deal of evidence that computer users behave insecurely and that their actions potentially compromise the systems they use. For example, they do not control access to their mobile phones by using passwords or PINs (Weisbaum, 2014; Kaspersky, 2015). They choose weak passwords (Moore, 2015) and do not change their passwords regularly (Ring, 2014). They also do not use anti-virus software (ejinsight, 2015) and fall for Phishing attacks (Zetter, 2015). Why? Two primary reasons emerge from the literature. The first is related to the history and provenance of security software, and the second is related to human tendencies and propensities.

Security software provenance

Early security research focused on providing *technical* security mechanisms. These were often developed without consulting the 'human in the loop' despite user interaction being essential to their efficacy. In essence, these security mechanisms were designed *by* experts, *for* experts. As more non-experts started using technology the flawed nature of this paradigm became obvious (Adams & Sasse, 1999).

Whitten and Tygar (1999) point out that users do not apply security mechanisms, despite their knowing they ought to, because the mechanisms are not usable enough. They define *usable* secure software as software that: (1) ensures that people are reliably made aware of the security tasks they need to perform, (2) ensures that people are able to figure out how to successfully perform those tasks, (3) does not allow people to make dangerous errors, and (4) makes its users sufficiently comfortable with the interface to continue using it.

Much researcher effort has gone into improving the usability of security tools in the intervening years. A number of new usable security solutions have been made available, often as Add-ons or Apps, but, in reality, these have not yet been widely accepted or adopted. It has become clear that improving usability is not sufficient, in and of itself, to improve the situation. Clarke *et al.* (Clarke, Furnell, Stewart, & Lacey, 2012) argue strongly against a technocratic approach to information security, recommending that the needs of the user be focused on. It is wise also to reconsider what other factors are impeding adoption, by focusing on the human user.

Deterring Factors

By reviewing the literature, the researchers have attempted to explore the impact of human nature on the uptake of mobile security. Renaud *et al.* (Renaud, Volkamer, & Renkema-Padmos, 2014) suggest that there is a kind of progression towards secure behaviour. It starts with awareness of the problem, which confirms the first assumption above, and then proceeds through

a number of other stages, during each of which a smartphone owner can be deterred or distracted from acting securely.

The general lack of information is also confirmed by (Harbach, Fahl, Rieger, & Smith, 2013). However, even with awareness, other aspects can deter secure behaviours: *lack of concern, lack of understanding, lack of compulsion, lack of knowledge of available countermeasures and lack of determination* to carry things through. The lack of awareness, lack of concern, understanding and determination is confirmed by (Shirazi & Volkamer, 2014; Weirich & Sasse, 2001) with Weirich and Sasse also emphasizing the lack of *response efficacy*: the perceived ability to take the measures the smartphone owner is well aware of.

Harbach *et al.* (Harbach, Fahl, & Smith, 2014) investigated knowledge of security risks. They reported that people were indeed aware, but that they did not really apply that awareness to what they were doing at that moment. They make a fair point that people in the modern world have to deal with multiple demands for their attention. Given that this is so, security sometimes does not feature high enough to be given consideration, this could therefore also be referred to as *lack of attention***.** Lack of attention is a fact of 21st century life, suggesting that security simply gets pushed down when other more prominent attention grabbers are present (Anderson & De Palma, 2012).

Gaw *et al.* (Gaw, Felten & Fernandez-Kelly, 2006) mention the need for interfaces to be tailored toward individual people's needs, so a *lack of personalisation* can lead to rejection. They also mention the need for security to be more visible, so that decisions made by the system do not conflict with what the user wants the system to do. This points to *lack of visibility* being an issue, and confirms the *lack of control* factor identified by (Harbach *et al*., 2013).

Summary

Based on this literature review, awareness and knowledge constitute necessary, but not sufficient, pre-conditions for people to act securely. The deterring factors identified in the preceding section may cause someone not to behave securely despite awareness and adequate knowledge of how they ought to act. These factors have to be acknowledged as part of the bigger picture, but this is not the focus of this paper. The focus is on security awareness. Figure 1 depicts the progression from new ownership to secure smartphone behaviour, without suggesting progression down the path is inevitable or predictable, merely that this path is required for knowledge to be gained.

3. Methodology

To explore the validity of the two assumptions an investigation was carried out with two groups of university students as participants and investigated:

1. How aware are people of smartphone security issues, and does a Computing education make a difference?
2. Where do people go for advice about security?

It was decided to deploy students in a third year Computer Science course to act as researchers and gather data about smartphone security. This exercise was also used to make the students

themselves more aware of the security issues, and trained them in carrying out user-centred research ethically.

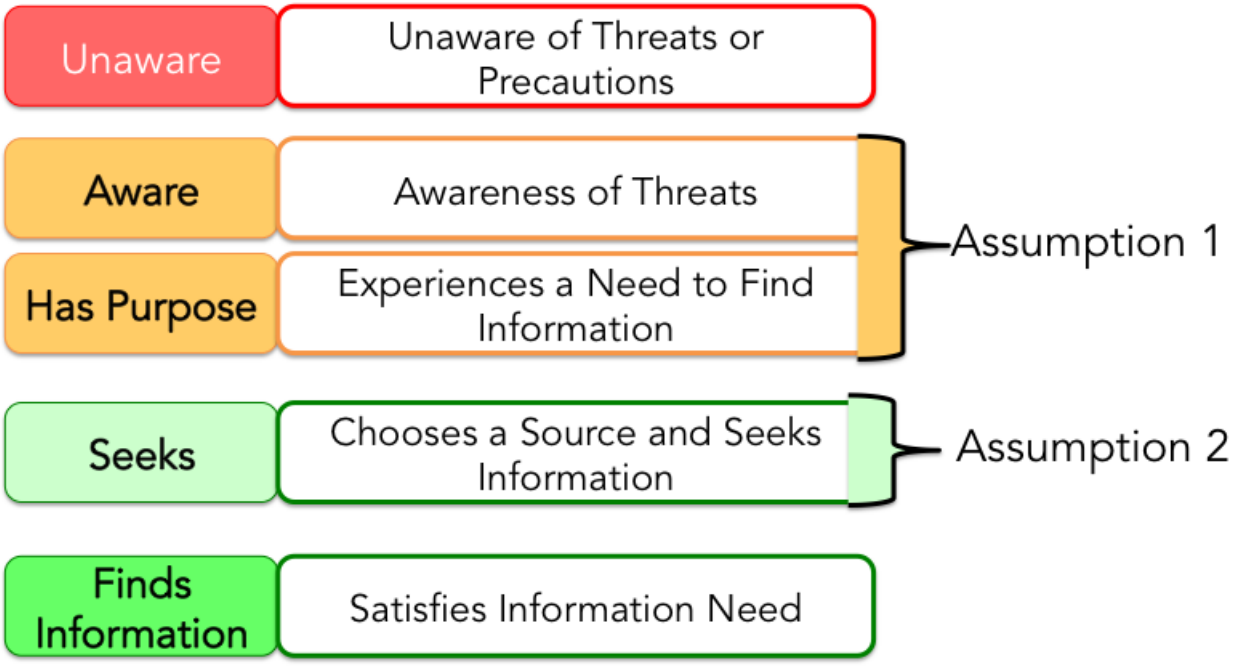

Figure 1: Path towards knowledge of security threats and precautions

Student teams were instructed to assume that they were employed by a large smartphone company who wanted to determine how aware smartphone users are of security and privacy. Student researchers were instructed to interview two randomly selected fellow students; one who had never taken a Computer Science course, and the other who was currently a Computer Science student (but not in the same class i.e. not doing the same project). This allowed the researchers to determine whether a Computing education (1) had an impact on awareness, and (2) whether other people consulted these students for advice.

Students were provided with a semi-structured interview to guide their interviews and to ensure that findings could aggregated.

Each team was required to write a report about the individual team member findings and to compare their findings with the literature addressing security and privacy issues. For the rest of this report the two groupings will be referred to as: Non-Computer Science (NCS) and Computer Science (CS) students.

4. Results

In 2015, 84 students were interviewed (42 CS and 42 NCS). About a third of the selected participants were female, however 21% of the CS participants whereas 50% of NCS participants were female. The majority (90%) of the participants were born in South Africa. Most (64%) of the participants grew up in cities, 25% in small towns and 11% in rural areas. On average the

participants have been using smartphones for 4 years (minimum 1 and maximum 10 years). Most (77%) always have their mobile phones within reach.

4.1 Security behaviour (indicating awareness & knowledge)

It was found that significantly more (88%) CS participants regularly installed system updates and upgrades on their mobile phones, as compared to the NCS group (67%) (χ^2=4.5; p=0.0334)[2]. When installing new applications slightly more of the NCS participants (40%) divulged their location whereas only 26% of the CS group did so (χ^2=1.9; p=0.1649).

Data encryption on sensitive information was used more often by the CS participants (55%) compared to 24% of the NCS group (χ^2=8.4; p=0.0037). Advice about security was sourced from the Internet and from other smartphone users, but no difference was noted between the two groups (χ^2=6.1; p=0.1089).

Thirty-five percent of participants said that they would never share password/PIN with others, 33% said they would share their password/PIN with family or friends, 20% indicated that they would share in cases of emergency, 7% would sometimes do it and 5% did not protect their phone with a password/PIN. No difference was found between the groups (χ^2=1.4; p=0.8516).

When participants were asked if a PIN/password is shielded when entered (when unlocking their phones in the presence of friends) 27% said no and 29% said yes and some (44%) indicated the situation would dictate their behaviour. The two groups did not differ in their behaviour (χ^2=4.9; p=0.1815). Participants in general, when they shared their passwords, did not regret it (CS=77%; NCS=61%)(χ^2=1.9; p=0.1614).

Significantly more (59%) of the CS participants know what encryption was, as compared the NCS group (34%)(χ^2=8.6; p=0.0136) and significantly more of the CS participants use encryption (43%) as compared to 15% of the NCS group (χ^2=7.4; p=0.0243).

In Figure 2 it can be seen that the two groups felt very similarly with respect to social media and its impact on security issues. Figure 3 demonstrates that participants avoided using particular mobile functions due to their perceptions of its security or privacy implications.

4.2 Sources of advice

Both groups felt public media failed to provide helpful information about smartphone privacy/security issues (CS=62%; NCS=69%)(χ^2=0.5; p=0.4752). However, they indicated that social media did satisfy their needs (CS=58%; NCS=61%)(χ^2=0.1; p=0.7503). Significantly more CS participants (29%) offered security advice to other smartphone users, as compared to the NCS group (7%)(χ^2=7.8; p=0.0205).

[2] Quantitative data were analysed statistically using a statistical package SAS®.

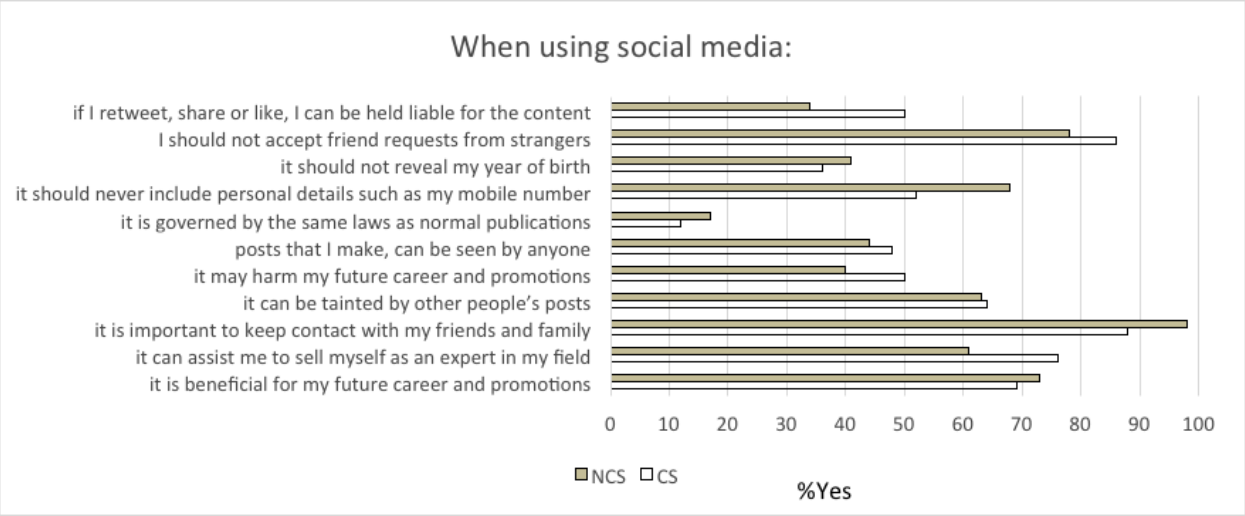

Figure 2: Social media perceptions

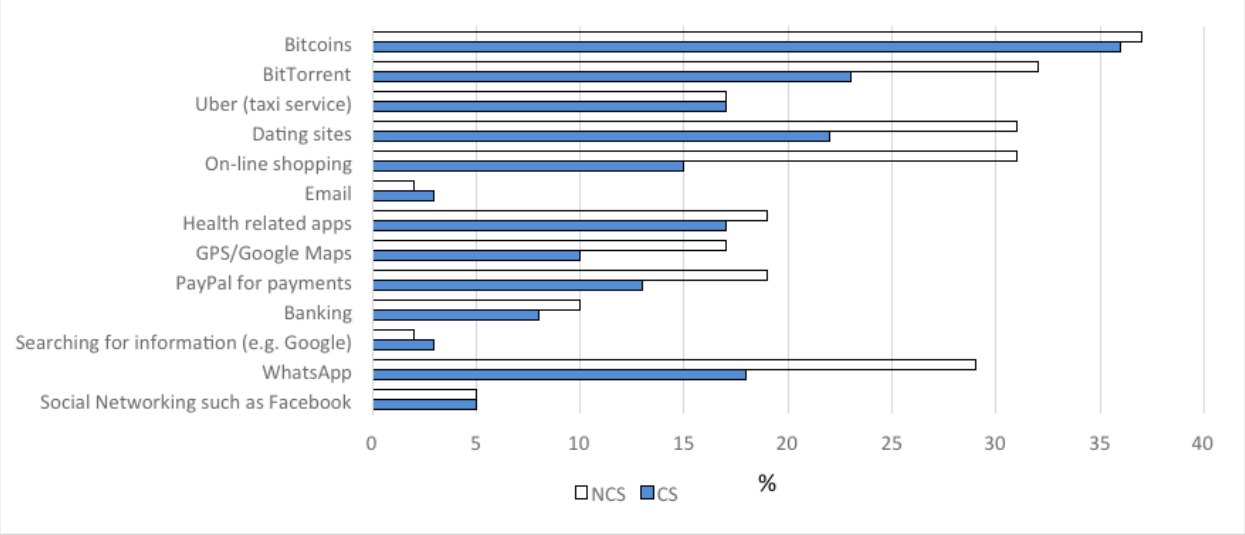

Figure 3: Non-use because of security or privacy implications

5. Discussion

This section returns to consider the two assumptions. Those who are doing their best to give smartphone owners the requisite knowledge so that they can secure their devices and resist attacks generally believe that making information available online is the way to reach as many people as possible at a reasonable cost. This research examined the two assumptions that would need to be true for such a broadcasting approach to be effective.

5.1 Awareness Assumption

Awareness of advised secure behaviours was surprisingly low, even amongst this well-educated sample. For example, very few (less than 15%) of both groups knew about social media being governed by the same laws as normal publications and that a person can be held liable for the

content that is retweeted, shared or liked (about 50%). Yet most (approximately 70%) realized that irresponsible posts on social media could harm future career opportunities.

Security behaviours are a decent indicator of awareness, since no one will perform the behaviour without the requisite awareness. Awareness is a necessary pre-requisite, but not a determinant. Comparisons between those educated in Computer Science and those who were studying other subjects show that a CS education has a definite impact on mobile security awareness. We noted significant differences in terms of applying system updates, encrypting information and being able to offer advice to other people about security issues. CS participants, by clearly being more aware than the other students, coinfirmed the benefits of a computing-related education.

Even amongst CS participants awareness was not guaranteed. For example, only 55% of CS participants encrypt sensitive information. Moreover, students across both groups shared passwords equally, something that one could expect education to deter. This confirms that awareness does not necessarily lead to further information seeking, nor does knowledge infallably lead to secure behaviours (Renaud & Goucher, 2014; Greig *et al.*, 2015).

5.2 Sources of advice and information preferences

Participants said they consulted the Internet and friends to get advice but they said that public media was less useful than Facebook, where they consulted friends. The problem with consulting the Web is that they have no way of verifying the accuracy of the proffered advice (Flechais *et al.*, 2013), which could leave them vulnerable but with a false sense of security. The students seemed to have come to the same conclusion, finding Facebook more helpful in terms of getting good advice.

Consulting peers might also be risky, but at least they are in a position to judge the trustworthiness and expertise of the people they request advice from. The fact that CS participants gave advice to others significantly more often than NCS participants suggests that people *are* indeed seeking out knowledgeable peers to consult. The use of social media, across both groups, confirms this tendency to consult friends. The fact that public media was considered not to offer helpful advice is telling – one would have expected the media to play a role in educating the public but they seem to be failing at this. Source preferences should inform future strategies to assist the man and woman in the street. It should be possible to foster and encourage this kind of peer-wise assistance more than is currently the case by ensuring that key people within the community have the requisite knowledge to provide advice and assistance to others.

6. Conclusion and future work

Hackers target anyone who is vulnerable and many smartphone owners are extremely vulnerable since they do not take precautions or use tools to protect their privacy and ensure resilience to attack. This is the case despite the efforts of governments and other bodies to publish reliable and helpful security related advice. The two assumptions need to be valid for this advice to make a difference. To conclude, awareness is variable, with a computing education paying dividends in this respect, but not guaranteeing secure behaviours and precaution implementation. It was also confirmed that students consulted their peers when they needed advice about security issues. This means that security support to smartphone users needs to be altered. Posting information on the Web with the intention of informing those who need it is probably misguided, as it will not significantly impact on general security awareness and lead to secure behaviours.

In future, the project will include societies from other countries and the questionnaire will be expanded to include more community-orientated questions.

7. References

Adams, A., & Sasse, M. A. (1999, December). Users are not the enemy. Commun. ACM, 42(12), 40–46.

Alghamdi, D., Flechais, I., & Jirotka, M. (2015, July). Security Practices for Households Bank Customers in the Kingdom of Saudi Arabia. In Eleventh Symposium On Usable Privacy and Security (SOUPS 2015). USENIX Association.

Alnajim, A., & Munro, M. (2009). An Anti-Phishing Approach that Uses Training Intervention for Phishing Websites Detection. In 6th international conference on information technology: New generations (pp. 405–410). IEEE.

Anderson, S. P., & De Palma, A. (2012). Competition for attention in the information (overload) age. The RAND Journal of Economics, 43(1), 1–25.

BBC. (2015). 'Phishing' scam cost London woman nearly £50,000. http://www.bbc.co.uk/news/uk-33257129. Accessed 29 November 2015.

Bruner, J. (1990). Culture and human development: A new look. Human development, 33(6), 344-355.

Case, D. O. (2012). Looking for information: A survey of research on information seeking, needs and behavior. Emerald Group Publishing.

Clarke, N., Furnell, S., Stewart, G., & Lacey, D. (2012). Death by a thousand facts: criticising the technocratic approach to information security awareness. Information Management & Computer Security, 20(1), 29–38.

Derr, R. L. (1983). A conceptual analysis of information need. Information Processing & Management, 19(5), 273-278.

ejinsight. (2015). Beware of 'see group photo' text message on your phone. (http://www.ejinsight.com/20150505-beware-see-group-photo-text-message-your-phone/ Accessed 10 May 2015)

Flechais, I., Jirotka, M., & Alghamdi, D. (2013, April). In the balance in Saudi Arabia: security, privacy and trust. In CHI'13 Extended Abstracts on Human Factors in Computing Systems (pp. 823-828). ACM.

Ford, D. (2015) Online banking fraud increases 48% year-on-year. IT Governance Blog. 30 March. http://www.itgovernance.co.uk/blog/online-banking-fraud-increases-48-year-on-year/. Accessed 29 November 2015.

Gaw, S., Felten, E. W., & Fernandez-Kelly, P. (2006). Secrecy, flagging, and paranoia: Adoption criteria in encrypted email. In Proc. of the sigchi conference on human factors in computing systems (pp. 591–600). Montreal, Canada.

Greig, A., Renaud, K., & Flowerday, S. (2015) An Ethnographic Study to Assess the Enactment of Information Security Culture in a Retail Store. World Congress on Internet Security. Dublin. October. IEEE

Harbach, M., Fahl, S., Rieger, M., & Smith, M. (2013). On the acceptance of privacy-preserving authentication technology: The curious case of national identity cards. In Privacy enhancing technologies (pp. 245–264). Springer.

Harbach, M., Fahl, S., & Smith, M. (2014, July). Who's Afraid of Which Bad Wolf? A Survey of IT Security Risk Awareness. In Proc. of computer security foundations symposium. Vienna, Austria.

Jansson, K., & Von Solms, R. (2011). Simulating malicious emails to educate end users on-demand. In 3rd symposium on web society (p. 74-80). IEEE.

Kaspersky. (2015). Consumer Security Risks Survey. From Scared to Aware: Digital Lives in 2015. Accessed 2 December 2015. https://kasperskycontenthub.com/usa/files/2015/08/Kaspersky_Lab_Consumer_Security_Risks_Survey_2015_v2.pdf

Kirlappos, I., & Sasse, M. A. (2012). Security education against phishing: A modest proposal for a major rethink. IEEE Security and Privacy Magazine, 10(2), 24–32.

Kritzinger, E., & von Solms, S. (2010, Nov.). Cyber security or home users: a new way of protection through awareness enforcement. Computers & Security, 29(8), 840-847.

Kuhlthau, C. C. (1991). Inside the search process: Information seeking from the user's perspective. JASIS, 42(5), 361-371.

Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007). Protecting People from Phishing: The Design and Evaluation of an Embedded Training Email System. In Sigchi conference on human factors in computing systems (pp. 905–914). ACM.

Li, Y., & Siponen, M. T. (2011, July). A Call For Research On Home Users' Information Security Behaviour. In PACIS (p. 112).

Maurer, M.-E., De Luca, A., & Kempe, S. (2011). Using data type based security alert dialogs to raise online security awareness. In Proceedings of the seventh symposium on usable privacy and security (p. 2).

Moore, D. (2015). Stupid users pick lame passwords. (http://www.normantranscript.com/news/business/stupid-users-pick-lame-passwords/article_a44f6405-df64-52b8-bf80-da6188c51256.html Accessed 10 May 2015)

O'Dell, J. (2014). 65% of all email gets opened first on a mobile device — and that's great news for marketers. http://venturebeat.com/2014/01/22/65-of-all-email-gets-opened-first-on-a-mobile-device-and-thats-great-news-for-marketers/. Accessed 2 December 2015.

Renaud, K., & Goucher, W. (2014). The Curious Incidence of Security Breaches by Knowledgeable Employees and the Pivotal Role a of Security Culture. In Human Aspects of Information Security, Privacy, and Trust (pp. 361-372). Springer International Publishing.

Renaud, K., Volkamer, M., & Renkema-Padmos, A. (2014). Why doesn't Jane protect her privacy? In Springer (Ed.), Privacy enhancing technologies - 14th international symposium, pets (p. 244-262).

Ring, T. (2014). Change passwords? People can't be bothered, survey shows. (http://www.scmagazineuk.com/change-passwords-people-cant-be-bothered-survey-shows/article/385634/ Accessed 10 May 2015)

Shirazi, F., & Volkamer, M. (2014, Nov). What Deters Jane from Preventing Identification and Tracking on the Web? In The 13th workshop on privacy in the electronic society (wpes 2014) (p. 107-116). Scottsdale, AZ, USA.

The European Network and Information Security Agency (ENISA). (2010, Nov.). The new users' guide: How to raise information security awareness. Retrieved from http://www.enisa.europa.eu/ publications/archive/copy_of_new-users-guide

Varela, F. (1992). Autopoiesis and a biology of intentionality. In Proceedings of a workshop on Autopoiesis and Perception (pp. 4-14).

Weirich, D., & Sasse, M. A. (2001). Pretty good persuasion: a first step towards effective password security in the real world. In Proc. of 2001 workshop on new security paradigms (pp. 137–143). Cloudcroft, NM.

Weisbaum, H. (2014). Most Americans don't secure their smartphones. (http://www.cnbc.com/id/ 101611330 Accessed 10 May 2015)

Wilson, T. D. (1999). Models in information behaviour research. Journal of documentation, 55(3), 249-270.

Whitten, A., & Tygar, J. D. (1999, Aug.). Why Johnny can't encrypt: a usability evaluation of pgp 5.0. In Proc. of the 8th usenix security symposium -volume 8 (pp. 14–14). Washington DC, USA.

Yang, Z. J., Aloe, A. M., & Feeley, T. H. (2014). Risk information seeking and processing model: A meta-analysis. Journal of Communication, 64(1), 20-41.

Zetter, K. (2015). Email phishing attacks take just minutes to hook recipients. (http://www.wired.com/2015/04/email-phishing-attacks-take-just-minutes-hook-recipients/ Accessed 10 May 2015)