IADIS International Journal on WWW/Internet
Vol. 13, No. 1, pp. 57-71
ISSN: 1645-7641

A CROSS-CULTURAL AND GENDER-BASED PERSPECTIVE FOR ONLINE SECURITY: EXPLORING KNOWLEDGE, SKILLS AND ATTITUDES OF HIGHER EDUCATION STUDENTS

Sunil Chaudhary. *University of Tampere, Finland.*

Yan Zhao. *University of Tampere, Finland.*

Eleni Berki. *University of Tampere, Finland and University of Jyväskylä, Finland.*

Juri Valtanen. *University of Tampere, Finland.*

Linfeng Li. *Beijing Institute of Petrochemical Technology, China.*

Marko Helenius. *Tampere University of Technology, Finland.*

Stylianos Mystakidis. *University of Patras, Greece and University of Jyväskylä, Finland.*

ABSTRACT

Preparing students adequately against online-attacks is a constant teaching and learning challenge, no matter how many advanced security-related courses have been developed for higher education curricula worldwide. Recently emphasis has also been put on online identity theft and social awareness in general. The authors research the knowledge, skills and attitudes of future IT professionals, from a cross-cultural and gender perspective. The available data were collected from international students in Software Engineering and other IT related disciplines via a questionnaire. The processed data revealed that (i) students are not free of security misconceptions, which security education is called upon to address and (ii) courses about online security can be part of a strategy for increasing social awareness on privacy protection. This pilot survey also revealed that the following issues are crucial: (a) the cultural and gender dimensions, (b) personality traits and (c) teaching methodology and learning environment used for security education. The researchers specify strategic guidelines in higher education for timely privacy protection and citizens' security. The information provided in this study will be practical and useful for curricula design and formal/informal learning practices. Hence, courses on security can be thought-provoking, interesting throughout the learning process and effective regarding the learning outcomes.

KEYWORDS

Online security/privacy, Phishing, Adult/higher education, National culture, Gender, Pilot survey.

1. INTRODUCTION

The sentence "*Only amateurs attack machine; professionals target people*", quoted by (Schneier, 2000) denotes the weightiness of online security (semantic attacks in particular). The frequency of online identity theft (from phishing) could be attributed to the psychological manipulation of people's vulnerabilities, which is technologically less sophisticated, inexpensive to conduct, and effective, meaning more rewarding in many ways for the online identity thieves (like phishers). Phishers and fraudsters in general use:

(i) advanced technological knowledge
(ii) current societal and situational information, and
(iii) various intelligent combinations of (i) and (ii) above

In so doing phishers try to exploit evoked feelings from turbulent and unstable societal circumstances such as war situations, financial crises, sudden earthquakes, tsunamis, ethical conflicts and many other in their attempts to gain people's trust for successful phishing (Chaudhary et al., 2015a; Chaudhary et al., 2015b). Alarmingly, undertaken surveys and research studies revealed that people lack proper knowledge about phishing (Friedman et al., 2002; Dhamija et al., 2006; Karakasiliotis et al., 2007; Jagatic et al., 2007; Odaro and Sanders, 2011) and other online-attacks. In fact, people are inherently vulnerable to human nature in general and their emotions (e.g., gullibility, greed, love, and fear) which increase their inability to distinguish phishing and other online-attacks. These conditions make human-on-the-Net the weakest link in online security (Chaudhary et al., 2015b).

Simply realising many types and levels of technical security measures cannot alone solve the socio-technical problem of phishing as long as people fall for phishing and other social engineering tricks. The reasons for this can be traced to the psychology of deceit (see e.g. Ford, 1996). The latter necessitates the efforts for educating people and raising their awareness on phishing attempts and cyber security through learning. It has been found that informative teaching can potentially be an effective anti-phishing strategy (Kumaraguru et al., 2009). There is a challenging duty to motivate people to care about their security, because of the following reasons:

(i) security is rarely the primary concern of people,
(ii) people are not motivated to read about security,
(iii) it is difficult to teach people to make right decisions without misjudging non-threats as threats (Kumaraguru et al., 2007) and
(iv) people can, from beforehand, possess various misconceptions related to security (Kirlappos and Sasse, 2012).

In general, formal, non-formal and informal adult education (see Valtanen et al., 2014) have an ethical obligation and social responsibility to design courses that guarantee the safety of people's everyday online transactions and interaction in cyberspace. Advancing people's awareness, knowledge and competencies through appropriate knowledge/information providers can result in better and timely protection of people's vulnerabilities and privacy. After all, early (or as early as possible) relevant security education can prove to be the most cost-effective option in information society as a proactive approach (Chaudhary et al., 2015a;

Chaudhary et al., 2015b). The next research questions provide a focus towards the needs that must be addressed in such curricula design.

Research Questions:

RQ1. Are there any cross-cultural differences and misconceptions in the attitudes, knowledge and competences regarding online security/privacy in university students?

RQ2. Do both male and female university students possess the same attitudes, knowledge and competencies regarding online security/privacy?

RQ3.Would it be beneficial for society if formal, non-formal and informal adult education to design security courses that guarantee citizens' safety in cyberspace?

While designing a course or curriculum for online security, a key factor is how to design a 'novel' and inspiring one which can be effective and improve learners' motivation. Learning can be motivating, at least when the curriculum will match the learners' expectations (Brophy, 2004). This could happen if the instructors consider the students' attitudes, skills and competencies, and knowledge on security. This is a way to involve people and consider their experiences while designing future courses that will enrich the end-users' holistic knowledge, change attitude and improve digital competencies and other skills. Towards discovering the latter in order to collect and understand the end-users' experiences and needs, the authors used a pilot survey questionnaire to gather data (explained in detail in section 3). All the data presented and analysed in this paper were collected during the pilot survey phase that also served as questionnaire testing.

2. SOCIETY AND LEARNING ABOUT CYBERSECURITY

As Bernstein (1971) argues: "*how a society selects, classifies, distributes, transmits and evaluates the educational knowledge it considers to be public, reflects both the distribution of power and the principles of social control*". It has been argued that the most satisfactory account for the curriculum is given by a modernist, positive reading of the development of education and society (Cohen et al., 2007). This has its curricular expression in Tyler's (1949) influential rationale for the curriculum in terms of four questions:

1. What educational purposes should the school seek to attain?
2. What educational experiences can be provided that are likely to attain these purposes?
3. How can these educational experiences be effectively organised?
4. How can we determine whether these purposes are being attained?

Past curricula on security and respective learning methods did not particularly focus on online security, since online threats were less in number and not so technologically advanced. Online identity theft was not as common 10 years ago as it is nowadays. Hence, there is a need to enrich and advance traditional security teaching with theoretical and practical knowledge and cater for digital competencies that a citizen and IT professional in particular should possess in order to handle everyday online safety problems, e.g. recognising phishing attacks. Some online situations are rather complex requiring specialised information that needs to reach every Internet user. For the society this information sharing can lead to increased public awareness and trust to the social structures (see e.g. Markova and Gillespie, 2008). Meaningful learning approaches, based on Internet users' experiences, could

(i) increase useful knowledge,
(ii) change attitudes and
(iii) develop digital competencies to fight phishing attacks.

The educational purposes, practices and learning outcomes should comprise (not compromise!) the essential user experiences that otherwise count for informal or experiential learning.

Academic curricula of IT and Software Engineering have recently tried to accommodate and widen software quality engineering with useful theoretical and practical epistemological and empirical knowledge, which adequately responds to the needs of the phishing victims. This approach emphasises corrective and reactive maintenance. Inevitably, these software maintenance methods and techniques exhibit social responsibility and can, in the long run, lead to increased human awareness in the information society. On the other hand, advancing further learners' awareness and digital competencies could equip humans with protection mechanisms for their vulnerability and privacy. This learning strategy will, in turn, improve information systems/artefacts software quality as a proactive and preventive maintenance approach (Chaudhary et al., 2015b).

Further than people's awareness about phishing attacks (Li, 2013; Li et al., 2014) and readiness for the phishing situation, social awareness and social consciousness are needed for adopting a proactive, and where possible predictive, software quality engineering approach; thus, not simply following a reactive problem-solving method (Chaudhary et al., 2015a).

Security and online security in particular (see e.g. Helenius, 2002) in cyber society is a dynamic concept which raises other human-related issues such as law and order, politics and other socio-cultural issues (see e.g. Berki, 1986). Thus, designing courses and curricula for cyber security requires the following considerations:

a) gauging the attitudes, competencies and skills, and knowledge of the learners (i.e., end-users) on security and
b) the learners' interests in educating themselves.

Accordingly, a) and b) above will help to determine two significant factors that are detrimental for the success of learning, namely:

(i) the misconceptions and weaknesses of the future IT professionals, so that they can be the focus of teaching about online security and
(ii) the learning platforms/media through which they prefer to acquire the new knowledge.

The authors further emphasise that utilising *formative assessment* in courses for online security (where questionnaire like ours can be helpful) to amend instructional strategies, activities, and content based on students understanding and performance, would certainly improve the teaching and accelerate the learning processes.

3. QUESTIONNAIRE DESIGN, PILOT SURVEY PARTICIPANTS, AND DATA COLLECTION PROCEDURE

We used a questionnaire (in hardcopy) which consisted of fifteen closed and semi-closed questions and one open question to collect data during a pilot survey. The closed questions were either on the *Likert item* or *multiple choice* formats.

The questionnaire was particularly designed to investigate the following issues:

- Attitudes, competencies and skills, and knowledge on online security and privacy in adult education learners, from a cross-cultural and gender perspective. While constructing the questions we considered the next:
    - When participants assess themselves regarding online security and privacy, are there any differences in the level of competence from their own actual competencies?
    - Will/can the learners who had attended any formal education courses related to security (not necessarily online security) in the past outperform those who had not?
    - How does the national culture define or affect the sense of online security and privacy?
    - Is there any effect of gender in the attitudes, skills and competences, and knowledge regarding online security/privacy?
- Experienced and preferred learning methodology/environment. We considered the following question in variations:
    - Which pedagogic methods/environments would the learners like to use while learning about online security and privacy?

In order to attain the first objective, we included a question asking how the participants self-assess their competencies and knowledge of online security/privacy. The succeeding questions were designed to comprehensively assess their competencies and knowledge in reality. In this case, there is a possibility that the participants can answer one thing, but in practice do not demonstrate that. To handle that, our questionnaire included questions which cross-checked the consistency of (e.g., verified the final answers) one another, the so called "guard questions". For example, when we asked the participants what they look for in a website to trust it, their answer was supposed to be something; but in another question when we asked them to select trustworthy Uniform Resource Locators (URLs) from a list containing a mixture of legitimate and phishing URLs (see Chaudhary, 2012), the selections did not always coincide with their previous answer. By this survey technique, we captured and analysed the respondents' misconceptions and weaknesses about online security and privacy, to an apparently large extent.

To accomplish the second objective, we further questioned the participants about:

(i) their interest in learning about online security/privacy,
(ii) the materials they have so far used to learn about these and
(iii) how would they prefer to learn in the future.

Past research studies show that learning-preferences and learning-styles can be critical factors for effective learning (Berki and Valtanen, 2007; Siakas and Economides, 2012). This is the reason why in this pilot research study the researchers consider the need for designing the learning spaces which should be customised to learning preferences and styles.

We distributed the questionnaire in English language to the international course participants who had attended only the first two weeks (three introductory lecture sessions on general security testing) of an advanced MSc/Ph.D. level course on "Testing, Security, and Trust". The course was delivered and taught during the first semester of the academic year 2014-2015. There were thirty participants, of whom twenty-four were male and remaining six female. All the participants were MSc level students majoring in Software Engineering, Computer Science, or Databases and Information Retrieval. According to their nationality, we classified them in three groups: (i) fifteen from China; (ii) nine from Finland, (iii) six from 'other countries' that are Pakistan, Nepal, Iran, England, and Vietnam.

At the beginning of the session we thanked the participants for their willingness to participate in this pilot survey, disseminated the questionnaire, and informed them that answering all the questions will take around twenty to twenty-five minutes but they can stop answering at any time they wanted. That is, answering is not forced. They all answered all the questions while a few finished earlier (in fifteen minutes) and a few others finished later (in around twenty-seven minutes). There were mostly Chinese participants in the latter group, who finished later and Finnish participants in the former group who finished earlier. The Chinese participants received the version of some (not all) of their questions in Chinese, since the Questionnaire was already translated in that language. During the questionnaire testing we confirmed that in China the questionnaire must be disseminated in Chinese. In India and Nepal though, that are target countries to collect data, the questionnaire will be in English. We also do not plan to translate from English when the questionnaire will be used for African countries. There are ongoing translations of the final questionnaire to be in Finnish and Greek languages for future data collection.

In order to ensure that the participants expose their own views and not the outcome opinion by discussing terms and concepts with their friends or copying from friends, some of our multilingual and multicultural research team members who came from China, Finland, Greece, India, and Nepal were present invigilating the whole data gathering process and gave explanations if requested in the participant's native language. We did not collect any personal data, e.g., age, id, name, email and/or other details. We guaranteed the confidentiality of all the participants.

4. DATA ANALYSIS AND RESULTS DISCUSSION

Since the number of our sample participants was only thirty we performed the data analysis using Microsoft Excel sheets. To assess the participants' competencies and knowledge we evaluated every answer from them and graded them on the *Likert scale* 1-5. The questions were designed to evaluate the following:

(i) familiarity with phishing and anti-phishing terminology
(ii) awareness of the media used to conduct phishing attacks and
(iii) knowledge about the characteristics in email/websites that are significant for differentiating between a legitimate and phishing email/website

The final grade was an outcome of the mean value of all the relevant questions' grades.

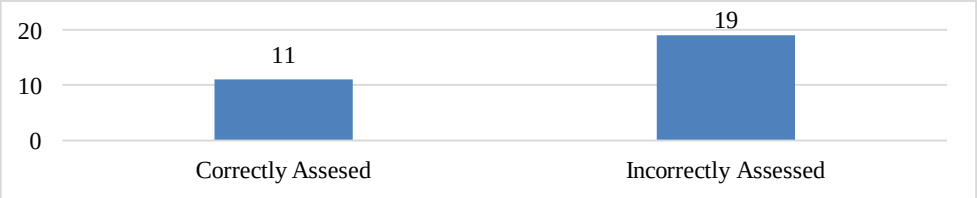

Figure 1. Correct versus incorrect self-assessment

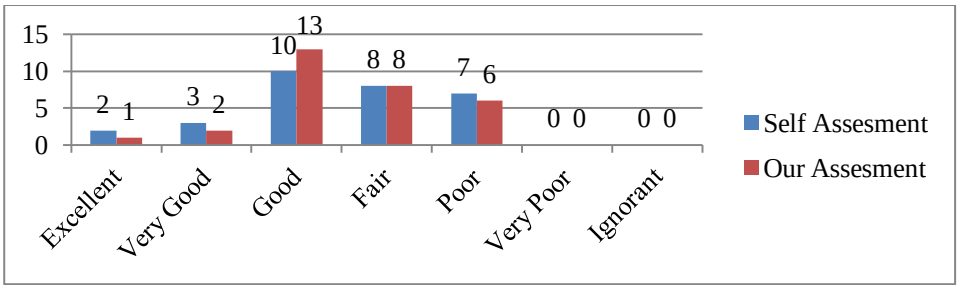

Figure 2. Competencies level of online security and privacy (self-assessment vs. our assessment)

Only 37% of the pilot survey participants had been self-assessed correctly (see Figure 1). This coincides with the result of Halevi et al. (2013), according to whom people are poor at estimating their vulnerability to phishing and other online attacks. Only 50% of the questionnaire respondents had assessed themselves the same as what we found out through our own assessment (see Figure 2). Our main assessment criteria considered the consistency and correctness of their answers in the guarding questions for the precise relevant subject knowledge. In the remaining, they had either slightly over- or under-estimated themselves in their self-assessment, except one respondent who had been self-assessed as 'Excellent' but was found to be only 'Fair' in our assessment. More importantly, 47% of the participants were either average (i.e., Fair) or below average (i.e., Poor). This reveals lack of necessary and essential knowledge; thus these IT students (and future IT professionals) are very much susceptible to phishing attacks and other online threats. This is more frightening when we realise that the participants are master level students majoring in Computer Science and related disciplines. Further, as graduates they will shortly be responsible for guarding online security through teaching others, protecting companies and organisations as employees and the list can go on.

Reflecting on *national culture* (Hofstede, 1980; Siakas et al., 2005), it was revealed that 33% of the Finnish participants over-estimated their knowledge, whereas 50% of the participants from 'other countries' under-estimated their knowledge in their own assessment. In the case of Chinese participants, 33% over-estimated and 27% under-estimated their knowledge in their own assessment.

Similarly, 33% of the survey participants lacked serious knowledge about the different social media and other online media through which potential phishers and fraudsters could target them. Even the rest of the participants exposed some deficiency level in general awareness, i.e., they were unfamiliar with several media that are often used to conduct phishing attacks. Further, they overlooked significant properties of online security/privacy like 'correctness of URL', 'warning issued by the web browser and anti-phishing tools', 'information requested by the website or email', 'SSL/TLS certificate used by the website', 'correctness of email address'. Unfortunately, they rather prefer their online security level to be dependent on less reliable properties such as e.g. related to the look-and-feel of the website or email when in need to differentiate between a phishing and a legitimate website/email.

Outcome 1: Students with basic knowledge on security are not free of cyber security misconceptions and they do not alone realise their weaknesses through which they can become exploited by online fraudsters.

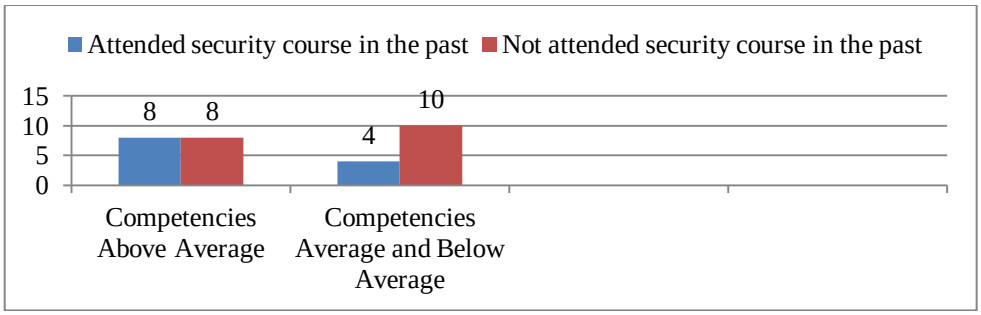

Figure 3. Competencies level of online security/privacy (Taken any security course in the past? Yes vs. No)

We found out that attending some general security course in formal education improves the competency level of online security and privacy (see Figure 3). 67% of the participants who had attended security courses through formal education in the past **were found to be above average, whereas 44% who had not attended any security courses were above average**. There might be some limitations in this result because we had requested not to consider: (i) the current course of "Testing, Security, and Trust" they were attending; this in fact was a course with the cyber-security concepts be exposed later on, after this pilot survey, and (ii) other courses like computer networks, information systems, and other that discuss online security to a limited extent. Some participants might have attended some of these but did not count any of them as a distinct security course.

Outcome 2: Security courses in adult education are necessary and effective for educating about online security and privacy. However, many courses may not be up-to-date or well designed. 33% of the students who had attended security courses in the past did not perform well in very important questions.

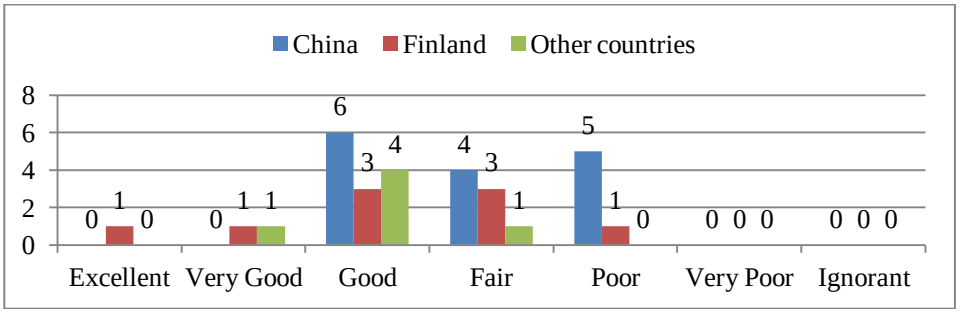

Figure 4. Competencies level of online security and privacy with respect to nationality

Next, we found out that the Chinese participants could be more susceptible to phishing attacks, whereas participants from 'other countries' were more competent regarding their knowledge on online security and privacy (see Figure 4). Only 40% of the Chinese participants had a competency level of online security and privacy above average, whereas

83% of 'other countries' participants were above average. Likewise, 53% of the Finnish participants had an above average competency level of online security and privacy.

A reason behind the poor performance of the Finnish participants may be related to the fact that they trust their country's authorities and agencies as responsible to curb phishing attacks in Finland, a rather high digital culture and technology country. Perhaps this is the reason that the Finnish participants did not seem to feel the same urge of educating themselves as the participants from 'other countries'. Another reason may be because only 44% of the Finnish participants had encountered phishing attempts in the past, whereas the percentage for participants of 'other countries' was 83%. The latter mostly belonged to a number of remarkably lower than Finland digital culture and technology countries. Possibly more frequent online incidents and prior exposure to phishing attacks have improved the 'other countries' participants' socio-cognitive and digital skills to recognise phishing attempts.

The poor performance of the Chinese participants was in contrast to everything stated in the aforementioned paragraph. Even their past encounters with phishing attacks did not seem to guarantee raising awareness and readiness. 80% of them said that they have encountered some kinds of phishing attacks or online identity theft in the past. This may be because the questionnaire was in English, and several Chinese participants had problems understanding the question in English, initially. We anticipated that so we attempted to handle the problem by translating and making the questions available in Chinese Mandarin, whenever they faced some difficulty in English-written questions understanding.

Surprisingly, the understanding of what is confidential/private data and what is not varied a lot according to nationality and/or national culture. For instance, most of the Finnish participants considered certificate (e.g., certificate of marriage or birth) and medical information as confidential. But for most of the participants from China and other countries, this information was not private or confidential. Apparently Finland has better e-health systems than all the other countries considered in this pilot survey, and the Finnish people are socially more aware of the risks occurring from the revelation of health-related confidential data and information to a wrong person. For instance, medical identity theft online could have severe consequences for the patient, resulting in fake claims of health insurance compensation. This fact alone may have encouraged the Finnish participants to classify medical information as confidential. Likewise, an impact of the tag word 'certificate' in 'marriage/ birth certificate' may have caused the Finnish participants to consider these certificates to be private and confidential. Many of the Finnish participants who said 'marriage/ birth certificate' to be confidential did not categorise 'date of birth' and 'marital status' as confidential. Astonishingly, in the list of twenty data items we showed to the international course and survey participants there was not a single item upon which all the participants agreed for it to be private and/or confidential! In fact, they did not even agree to the confidentiality of sensitive information like social security number and passport number!

Outcome 3: The cultural dimension is a necessity to be considered (Nisbett, 2011) in the curriculum design and training courses for online security/privacy. This will lead to revealing possible weaknesses and misconceptions of what is private or not according to different (national) cultures. It will also provide exposure about the security facts through comparing and contrasting similarities/differentness of different cultures to the learners. Thus, curricula will present international knowledge and the learners will eventually be more knowledgeable by knowing other culture(s) and practices of security.

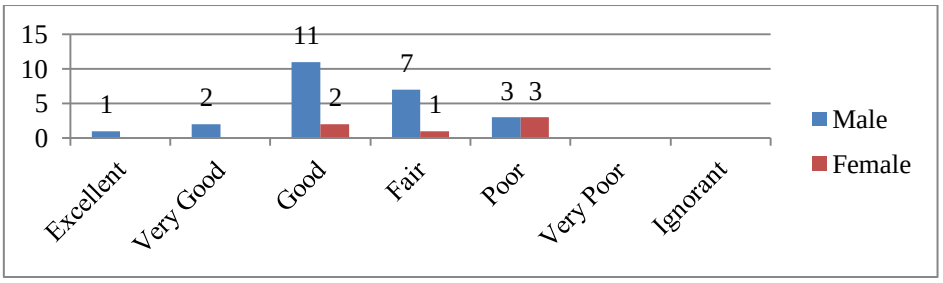

Figure 5. Competencies level of online security and privacy with respect to gender

In the context of gender (Fox-Keller, 1985; Adam et al., 2004), the male participants were found to relatively be more competent with online security knowledge than the female participants. 58% of the male participants were of good level and above it whereas the percentage is only 33% in the case of female participants (see Figure 5). This result reconciles with the findings from the past studies like Jagatic et al. (2007), Shen et al. (2010) and Halevi et al. (2013). The latter suggest that females are more susceptible to phishing attacks than males. A possible limitation, however, can be that the female participants were significantly lower in number compared to the male participants; that fact alone may skew the final result.

Although this result matches with the findings from some past studies, it was also surprising. For instance, Shen et al. (2010) consider the main reason for this knowledge gap between the two genders and further explained that a female could possess less technical knowledge and training. However, in this pilot survey both the male and female participants had almost the same level of education; more importantly all of the them had majored in Computer Science, Software Engineering or related disciplines. Conversely, even Halevi et al. (2013) found that computer expertise has no any correlation to the ability of detecting online attacks. Therefore, a more satisfactory explanation can be the personality traits of the two genders; there exists a correlation between personality traits and susceptibility to phishing attacks (Halevi et al., 2013).

Outcome 4: Personality traits and gender differences are equally important to consider for designing curricula and courses about online safety/security. For example, Halevi et al. (2013) suggested that phishing defence (or online security) should be tailored to people with certain personality traits. Earlier, Gefen and Detmar (1997) also considered gender differences in the perception and use of e-mail.

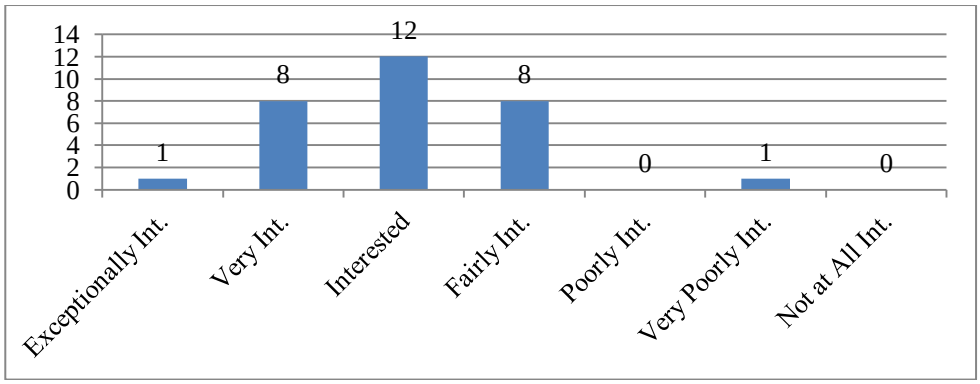

Figure 6. Interest in online security and privacy

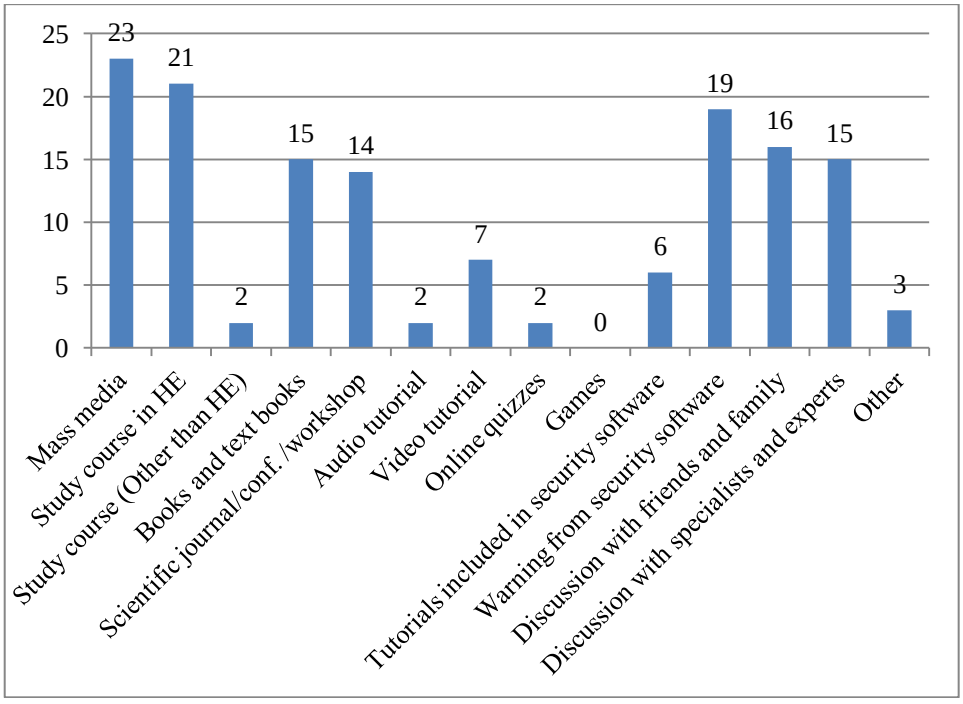

Figure 7. Materials used to learn about online security

All but one respondent were personally interested in online security and privacy (see Figure 6). Most of the participants use 'mass media', followed by 'security course in higher education' and 'warning from security software' to describe their formal and informal learning resources and methods about online security and privacy (see Figure 7). Further, while they were asked, in another question, about preferred ways of learning, they replied that they prefer more formal ('security course in higher education') followed by informal ('mass media') ways of learning in order to learn more in the future. Around 39% and 14% of the participants selected 'security course in higher education' and 'mass media', respectively. Other responses

were 'discussion with specialists/experts', 'warnings from security software' and so on. The least preferred ways were: 'playing games', 'watching video', and 'analysing case studies'.

Outcome 5: Using a teaching method and/or learning environment that has predominantly been accepted and is popular among the potential learners can help to make the learning process more interesting and more efficient, for learners and instructors.

On the overall research outcomes: Internet users in social media, online services, virtual communities and elsewhere face security risks and privacy violations every day. Not surprisingly online security comprises 'hot' topics and interests for the learners, instructors, and general Internet users. For instance, people do not always know which of the (material and immaterial) assets they possess is worth of stealing, particularly if some piece of information has no value to them at the time they are online. At the same time, however, this information can be priceless to phishers or/and other fraudsters. Hence, so far the authors' motivation has been to identify a ground of common interests for all stakeholders of the informational societies (Karvonen, 2001) to participate in higher/adult education initiatives for proactive online protection and public awareness.

To our knowledge so far, there is no related research study focusing on the points we presented and analysed here. Based on the responses, the authors also suggest to promote the concept and principles of *'usable security'* (Kumaraguru et al., 2009; Chaudhary and Berki, 2013). Thus, the need to consider diverse learnability and usability along with security as interconnected and significant software quality properties for effective online protection. This consideration can also raise the levels of interest, performance and effectiveness in the learning process.

5. CONCLUSIONS, LIMITATIONS AND FUTURE RESEARCH AGENDA

The authors collected data through a questionnaire in a pilot survey for investigating and analysing the students and future IT professionals' learning needs for adult/higher education courses about online security/privacy.

The gathered data pointed to a rather alarming general result: even higher education students majoring in Computing, Software Engineering, and IT-related disciplines hold dangerous misconceptions of online security/privacy. Several of them lack even basic knowledge of protection mechanisms and do not have essential digital competencies. Having curricula about online security and privacy in adult formal (e.g., state), non-formal (e.g., work training) and informal (e.g., mass media, accidental learning) education (Valtanen et al, 2014) can be practical and helpful to educate people about e.g. phishing and other frequent online threats. However, the curricula should be properly designed and updated accordingly.

The courses' content and context have to be more up-to-date and pragmatic, considering cyber-people's various identities, interaction and realistic cyber-threats (Jäkälä and Berki, 2013; Singer and Friedman, 2014; Payton and Claypoole, 2015). New knowledge is built upon learners' previous knowledge, which also determines the course, conditions and quality of learning (Gagne, 1977; Biggs, 1996). Thus, the curricula should not only target imparting new knowledge but also eliminate the misconceptions about online security/privacy in education and society. Furthermore, the teaching methodology and learning environment should carefully be selected. Our research study captured that security knowledge/information delivery using the wrong method/media can disinterest the learners and could significantly decrease their interest.

When universities and organisations become a dynamic hub of diversity, and people from different nationalities come under the same roof, it is necessary to consider national culture (Siakas et al., 2005; Nisbett, 2011) in the design of an international and multicultural curriculum. When various races and ethnicities must co-learn and co-work (Hofstede, 1980), the foremost necessity is the learning about others' culture and viewpoints through their social realities and worldviews. In some cultures certain activities may be considered non-harmful for security due to ignorance, different practices, and different social surroundings. Our findings revealed that the majority of people in China and other countries do not consider their medical information to be private and confidential.

People's social awareness can act as a protection mechanism in the social context of cyber-society. Anti-phishing guidelines, adult education programmes, and simple trust management strategies can make people re-think online interaction. Ideally, people should acquire useful social skills and digital competencies, while the Law and Justice could be able to utilize predictive practical information. Increasing instructors/learners awareness by adopting socio-cognitive and social computing approaches could raise the people's critical knowledge and prediction capacity on phishing attempts. (see Chaudhary et al., 2015a).

This research study, being socio-cognitive and socio-cultural in nature, was based on a pilot survey for questionnaire testing; this, together with the small multicultural learners' sample size, were two main research limitations. The final and significantly improved after the pilot survey questionnaire will initially be used to collect data from three European (Finland, Greece, UK), three Asiatic (China, Nepal, India) and three African countries. Larger sample sizes are obviously needed in order to find out more about national culture and its influence in learning about security and in order to outline needs and strategic steps to be taken in adult education for timely protection in cyberspace.

The researchers were faced with the necessity to enrich the questionnaire with more questions (e.g., about cloud services security) and also made considerable changes in the format and structure of it. In fact, there might be a need for a second questionnaire testing before it is disseminated to the people of the aforementioned and other countries.

The gender perspective in IT (Fox-Keller, 1985; Adam et al., 2004) is a certain area of the researchers' interest (Berki and Cobb-Payton, 2005) since until now some of our initial findings contradict and some confirm other research studies' results. It is, for instance, a not surprising finding (not illustrated herein by gender percentages) that in our pilot survey, women IT students/professionals under-estimated their knowledge about security in comparison to men IT students/professionals who over-estimated theirs.

Studying the attitudes, personality traits, knowledge and digital competencies of both male and female learners in different (national) cultures worldwide could bring about educational reforms following a cross-cultural understanding and collaboration among humans.

Drawing from the principles of total quality management, problem-focused education and virtual learning, the authors propose: 1) strategic teaching and research directions for improving academic curricula, and 2) a customised for security teaching and socio-centric learning process. Multicultural and multidisciplinary online curricula design with extra-curricular activities in virtual learning environments should be in the future agenda. It also seems that in courses about security a balance between the yet unrecognised formal education and easily accessible informal learning should be organized.

Overall, it is the researchers' firm belief that through improved knowledge on diverse learnability, usability, and privacy/security, the following future scenarios in e-society can be avoided:

(i) people will become ultra-cynical toward any human contact and will stop trusting and
(ii) people will totally abandon any technology-based communication, become online or offline nomads and stop using the Internet

The cross-cultural and gender differences in learners' socio-cognition and perception, resulted and demonstrated in ground-breaking design principles for curricula and courses about security, can be surprisingly thought-provoking and open-minded for initiating a new era of security education.

REFERENCES

Adam, A. et al. 2004. A decade of neglect: reflecting on gender and IS. *New Technology, Work and Employment* 19(3), pp. 222-240.

Berki, R.N. *Security and Society. Reflections on Law, Order and Politics.* 1986. J. M. Dent & Sons Ltd. London and Melbourne.

Berki, E. & Cobb-Payton, F. 2005. *Work-Life Balance and Identity in a Virtual World: Facts, Tensions and Intentions for Women in IT*. Isomäki, H. & Pohjola, A. (Eds) Lost and Found in Virtual Reality: Women and Information Technology. pp. 275-296, University of Lapland Press: Rovaniemi.

Berki, E. and Valtanen, J. 2007. Critical and Creative Mathematical Thinking with Practical Problem Solving Skills – A New Old Challenge. *Proceedings of 3rd South-East European Workshop on Formal Methods. Service-Oriented Computing*; *Teaching Formal Methods*. Thessaloniki, Greece, pp.154-170.

Bernstein, B., 1971. *Class, Codes and Controls, Vol. 3: Towards a Theory of Educational Transmissions, pp. 47*. Routledge, London, UK.

Brophy, J., 2004. *Motivating Students to Learn*. Lawrence Erlbaum Associates Publishers, London, UK.

Biggs, J. 1996. *Enhancing Teaching through Constructive Alignment*. Higher Education 32: 347-364, Kluwer Academic Publishers, the Netherlands.

Chaudhary, S. 2012. *Recognition of Phishing Attacks Utilizing Anomalies in Phishing Websites.* MSc Thesis. SIS, University of Tampere.

Chaudhary, S and Berki, E. 2013. Challenges in Designing Usable Anti-Phishing Solutions. *Proceedings of SQM XXI Quality Comes of Age.* London, UK, pp. 189-200.

Chaudhary, S. et al., 2015a. *Time up for phishing with effective anti-phishing research strategies*. International Journal of Human Capital and IT Professionals (IJHCITP), 6(2), pp.49-64.

Chaudhary, S. et al., 2015b. Exploring Attitudes, Knowledge and Competencies for Security Technology: A Cross-Cultural Survey in Higher Education. *Proceedings of International Conference on ICT, Society and Human Beings.* Las Palmas de Gran Canaria, Spain, pp. 11-18.

Cohen, L. et al., 2007. *Research Methods in Education, pp.35-36.* Routledge, London, UK.

Dhamija, R. et al., 2006. Why Phishing Works. *Proceedings of SIGCHI Conference on Human Factors in Computing Systems*. Montréal, Canada, pp. 581-590.

Ford, C.H. 1996. *"Lies! Lies! Lies! The Psychology of Deceit"*. American Psychiatric Press, Inc. Washington: DC.

Fox-Keller, E. 1985. *Reflections on Gender and Science*. Yale University Press: Yale.

Friedman et al., B. 2002. Users' Conceptions of Web Security: A Comparative Study. *Proceedings of Extended Abstracts on Human Factors in Computing Systems*. Minneapolis, MN, USA, pp. 746-747.

Gagne, R.E. 1977. *The Conditions of Learning*. Holt-Saunders International Editions: USA. Third Edition.

Gefen, D. and Detmar, S. W. 1997. Gender differences in the perception and use of e-mail: An extension to the Technology Acceptance Model. *MIS Quarterly 21(4)*, pp. 389-400.

Halevi, T. et al., 2013. A Pilot Study of Cyber Security and Privacy Related Behavior and Personality Traits. *Proceedings of WWW 2013 Companion*, Rio de Janeiro, Brazil, pp. 737-744.

Helenius, M. 2002. *A System to Support the Analysis of Antivirus Products' Virus Detection Capabilities*. Ph.D. Thesis, Department of Computer and Information Sciences, University of Tampere.

Hofstede, G. 1980. *Culture's Consequences: International Differences in Work-Related Values*. Beverly Hills: Sage.

Jagatic, T. et al., 2007. Social Phishing. *Communications of the ACM*, Vol. 50, Issue 10, pp. 94-100.

Jäkälä, M. and Berki, E. 2013. Communities, Communication and Online Identities. In Warburton, S. & Hatzipanagos, S. (Eds.) *Digital Identity and Social Media*. Information Science Reference, IGI. pp. 1-13.

Karakasiliotis, A. et al. 2007. *An Assessment of End-user Vulnerability of Phishing Attacks*. Journal of Information Warfare, 6(1), pp. 17-28.

Karvonen, E. (Ed.). 2001. *Informational Societies: Understanding the Third Industrial Revolution*. Tampere University Press: Tampere.

Kirlappos, I. and Sasse, M.A., 2012. Security Education Against Phishing: A Modest Proposal for a Major Re-think. *IEEE Security and Privacy*, Vol. 10, Issue. 2, pp. 24-32.

Kumaraguru, P. et al., 2007. Teaching Johnny Not to Fall for Phish. *ACM Transactions on Internet Technology*, Vol. 10 Issue 2, Article No. 7.

Kumaraguru, P. et al., 2009. School of Phish: A Real-World Evaluation of Anti-Phishing Training. *Proceedings of Symposium on Usable Privacy and Security*. Mountain View, CA USA, article no. 3.

Li, L. 2013. *A Contingency Framework to Assure the User-Centred Quality and to Support the Design of Anti-Phishing Software.* Ph.D. Thesis, School of Information Sciences (SIS), University of Tampere.

Li, L. et al., 2014. Towards a Contingency Approach with Whitelist- and Blacklist-based Anti-phishing Applications: What do Usability Tests Indicate? *Behaviour and Information Technology*, Vol. 33, Issue 11, pp. 1136-1147.

Markova, I. and Gillespie, A. (Eds). 2008. *Trust & Distrust*. Sociocultural Perspectives. Information Age Publishing, Inc. Charlotte: NC.

Nisbett, R. E. 2011. *The Geography of Thought: How Asians and Westerners Think Differently and Why*. Nicholas Brealey Publishing: UK.

Odaro, U.S. and Sanders, B.G. 2011. Social Engineering: Phishing for a Solution. *Proceedings of the IT Security for the Next Generation-European Cup 2011*, Erfurt, Germany.

Payton, T. and Claypole, T. 2015. *Privacy in the Age of Big Data. Recognizing Threats, Defending your Rights, and Protecting your Family*. Rowman & Littlefield: London.

Schneier, B., 2000. Semantic Attacks: The Third Wave of Network Attacks. https://www.schneier.com/crypto-gram/archives/2000/1015.html#1

Sheng, S. et al., 2010. Who Fall for Phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions. *Proceedings of ACM Conference on Human Factors in Computing Systems*, Atlanta, Georgia, USA, pp. 373-382.

Siakas, K. et al. 2005. Global Software Development; the Dimension of Culture. *Proceedings of IADIS Virtual MCCSIS 2005 - Software Engineering & Applications*., pp. 386-391.

Siakas, E. and Economides, A. 2012. Adaptive Learning: Mapping Personality Types to Learning Styles. *Proceedings of INSPIRE XVII: Education matters*. Tampere, Finland, pp.29-41.

Singer P.W. and Friedman A. 2014. *Cybersecurity and Cyberwar, What Everyone Needs to Know*. Oxford University Press: NY.

Tyler, R., 1949. *Basic Principles of Curriculum and Instruction*. Chicago IL, University of Chicago Press.

Valtanen J. et al., 2014. Reflections on the Quality of Formal and Informal Learning. *Proceedings of INSPIRE XIX: Global Issues in IT Education*, Southampton, UK, pp. 107-122.