University Students' Attitudes Towards e-Security Issues: A Survey Study in Tumaini University, Tanzania

Matti Tedre and Bukaza Chachage
Tumaini University, Iringa University College
P.O.Box 200, Iringa, Tanzania
{matti.tedre | bukaza.chachage}@tumaini.ac.tz

Abstract

Many functions of the information society, such as e-banking, e-government, and e-learning, are based on the idea of password-based protection of privacy, security, and electronic identity. In order to succeed, e-security requires technical, organizational, and institutional support, as well as user awareness. In this pilot study, we used thematic interviews and closed-ended questionnaires to examine students' attitudes towards issues of information security in a middle-sized Tanzanian university. The results suggest lax attitudes towards security issues, and give impetus to actions and further research on the topic.

1. Introduction

1.1. Background

Many electronic services in information society are based on strict information security and password-protected electronic identity. Our work in a medium-sized university in a developing country has given us plenty of anecdotal evidence, which tells that university students and staff members often disregard good practices of information security; for instance, sometimes they share their passwords with other students and staff members, and often lend their virtual identities to each other. As educators, we fear that inadequate understanding of information security issues is one of the potential hindrances to efficient utilization of e-learning tools in developing countries. However, there seems to be little serious research on e-security in developing countries.

In this exploratory research, in order to find out more about threats to e-security we interviewed three people who had succeeded each other as IT managers in a Tanzanian university between 1998 and 2008. Based on those interviews, we constructed a questionnaire for measuring students' perceptions about security and privacy issues concerning ICT systems. We administered the questionnaire to a number of students, and provide here descriptive statistics on the results.

1.2. Related Research

Information security and privacy are not only about technological solutions like firewalls and cryptography. Security also greatly depends on responsible behavior of users of computing systems [2]. No matter how secure a computer system otherwise is, negligence, social pressures, and inadequate education about computer security expose the system to security breaches [2]. The term *social engineering* refers to techniques that are aimed at gaining access to computing systems through the users of those systems. Social engineering techniques exploit human beings' natural want to trust others, their tendency to assist other people, and their will to gain favor in other people's eyes [2].

In Infosecurity Europe's annual survey 2008, the researchers found that out of a sample of 576 office employees in London, 21% were prepared to give away their password with the lure of a chocolate bar as an incentive for filling in a survey [1]. They also found out that 58% of the respondents reported that they would give their password over the phone if someone told them and said he or she was from the IT department. According to the study, one third of the people (31%) used only one password for all their accounts; followed by two (31%) passwords and three (16%) passwords [1]. Finally, it was found out that 43% of the informants change their password rarely or never.

Table 1 presents a list of top issues in information security, compiled by researchers at Auburn University

Table 1: Top Issues in Information Security

1. Top management support	6. Policy-related issues
2. User awareness training and education	7. Organizational culture
3. Malware	8. Access control and identity management
4. Patch management	9. Internal threats
5. Vulnerability and risk management	10. Business continuity / disaster preparation

[2]. Many of the top issues in information security—such as top management support, user awareness training and education, organizational culture, and policy-related issues—are strongly related to managerial issues. Of the items in Table 1, management support, vulnerability and risk management, policy-related issues, organizational culture, internal threats, and business continuity / disaster preparation are organizational issues. In the same table, malware and patch management are technical issues. Finally, user awareness and training is an educational issue. Building a culture of security and privacy is predominantly an organizational issue [6], but organizational changes usually require educational actions to make the changes effective.

Information society, especially electronic business and commerce, are based on trust and security [3]. For instance, password security is a sine qua non of e-banking, at least in the Western forms of e-banking: without a culture of secrecy regarding passwords, secure identification is impossible. Similar, e-government and e-voting will not be possible without a strictly protected e-identity. Hence, it is important to explore the issues concerning the issues of e-privacy, e-security, and e-identity, and to evaluate their impacts on electronic services. In this pilot study, we begin that research by exploring students' attitudes towards password and data security, and by analyzing the students' responses to issues that have consequences on how electronic services should be implemented and enforced.

2. Methodology

In this research study, we utilized two methods of inquiry: first, we interviewed three people who have worked at the college as ICT directors[1]. The first one's term was 1998–2004, the second one's 2005–2007, and the current ICT director's since 2007. From those interviews, and from existing literature, we extracted 22 questions and statements we asked students to rate. Those questions and statements were a part of a larger, 73-item questionnaire, which was aimed at charting students' needs and attitudes concerning Tumaini's computing facilities.

2.1. Interviews

Two of the three interviews were conducted as face-to-face thematic interviews, with an aim to uncover as many problematic aspects concerning information security in the college as possible. Whenever unexpected and unforeseen issues arose, the interviewer asked the interviewee to expand upon that issue. Interviews with the first and the current ICT directors of the college took about one hour each. The interviews covered the history of computer security at Tumaini University, along with a great number of observations and insightful commentary. The third interview, conducted with the second ICT director of Tumaini, was done via email because that person currently lives in Europe.

2.2. Questionnaires

The questionnaire used in this research was a part of a larger questionnaire, which surveyed the uses of Tumaini's computing facilities and the needs of students. That questionnaire had two aims: to map students' needs concerning computing facilities, and to survey students' opinions on the quality of Tumaini's IT facilities and IT support. A number of questions concerning information security were added to the questionnaire.

Information security questions were derived from the interviews described in the previous subsection, and from existing literature. We asked demographic questions about the respondents' age, faculty, gender, and year of studies. We also asked 19 background questions, which were aimed at surveying the technological background of the respondents and the respondents' habits of using computers. Those questions concerned issues such as which tools do they use (email, flash disks, floppy disks, network drive, network printers, WWW, word processors, spreadsheets), which devices or tools do they own (mobile phone, desktop computer, laptop computer, home Internet connection), and what are their habits concerning passwords (change frequency, knowledge of other students' passwords, using other students' printing quota, etc.)

After those background questions, we asked the respondents to rate their agreement, on a five-point Likert scale, with a number of statements concerning matters of e-security and e-privacy. Those statements were derived from literature and interviews, and they dealt with (*a*) privacy and safety of students' own files (3 statements); (*b*) password and username issues (10 statements); (*c*) malware issues (3 statements); and (*d*) issues of rules and regulations (6 statements).

2.3. Participants

There are 2526 students in Tumaini University, Iringa University College, and the male/female ratio is 52/48. Sixty-five questionnaires were divided between five teachers—one teacher per faculty—and those teachers were asked to randomly select a required number of students, and to administer and collect the question-

[1] Strictly speaking, the work title and work description have varied between those people, but basically they have worked with ICT infrastructure development, maintenance, and teaching.

naires. The response rate was 61/65=94%. In the received responses male/female ratio was 52/48 and average age was 26.3 years. There were 25 first-year students, 22 second-year students, and 14 third-year students.

We aimed at a stratified sample with a proportionate number of respondents from each of Tumaini's five faculties or directorates. We received 28 responses from the Faculty of Arts and Social Sciences (FASS), 14 from the Faculty of Law, 6 from the Faculty of Theology, 10 from the Faculty of Business and Economics, and 3 from the ICT directorate. Those faculties have 1115, 728, 242, 414, and 27 students, respectively. See Figure 1 for the distribution of respondents between faculties and the distribution of the student body between faculties.

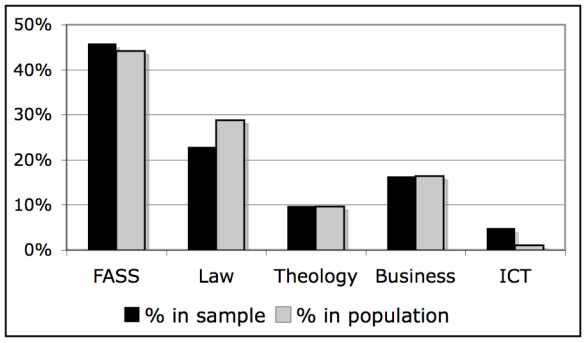


Figure 1: Distribution of Respondents By Faculty

2.4. Analysis

The three interviews were analyzed for issues concerning how people use Tumaini's computing systems. From initial coding arose five coarse, partly overlapping categories: regulatory issues, software issues, hardware issues, malware issues, and human issues. All of the respondents' concerns and observations fit those categories. Due to the small number and the focused nature of the interviews, no further categorizing was necessary in order to design a meaningful questionnaire.

As this was an exploratory pilot study, questionnaires were analyzed for descriptive statistics. The sample (n=61) was too small for inferential statistics or correlational analysis. The responses were analyzed for skipped questions in order to find out which questions need to be re-formulated or deleted. Also apparently conflicting responses were pinpointed (cf., e.g., Figure 2 and Figure 3) in order to refine the questionnaire for a larger-scale study. Finally, the last question, which was an open-ended question on refining the questionnaire, was reviewed for meaningful suggestions for the final version of the questionnaire.

3. Results

3.1. Interviews

According to Tumaini University / Iringa University College's (IUCo) first ICT director, passwords were first introduced to IUCo campus in the beginning of 2000, when IUCo got its first fully functional computer network. In the early years at Tumaini, IT support was concerned mainly with providing students and staff members with the ICT tools they need. Active Directory, which is Microsoft's authentication and authorization service for Windows-based computer networks, was introduced in 2003, and at that time the college began serious teaching about password security. One of the interviewees noted: "*In 2003 the password regulations were made very strict for students. It really cannot be done much more stricter* [from the technical point of view]." (Authors' translation)

Increase in malware—mostly viruses, spyware, and adware—and widespread adoption of Internet into use at Tumaini were strong incentives for updating computer security. Users often ignored warnings from virus programs, and clicked 'yes' without thinking about it at all. One of the interviewees remembered that at some point when the network did not have a bandwidth manager, malware often used a lot of bandwidth, and often one virus-infested computer took the whole network down. The interviewee noted that the question in the early days was about how to control the network, not about how to control the users. Floppy disks, and lately flash disks, have been a constant source of viruses, too. One of the interviewees expressed great concerns about the use of flash disks, and noted that students and staff use their flash disks at "virus cafés" and bring them to Tumaini.

From very early on in the computerization of Tumaini there were problems with students and staff members sharing their passwords with each other. One of the interviewees remembered that once a staff member had given a password to one of his/her students, who had given it to the next student, who had given it to the next student, and so forth. Then one of the students had changed the password, and the original owner of the account came to complain about not being able to log on.

One of the interviewees recalled: "*Regarding passwords, there has been a problem all the time*—[a problem] *which is connected to a different kind of thinking about privacy—that very many* [students] *share their usernames and passwords with others*. […] *At one point we noticed that 'who are these people sitting at our network lab?'*" (Authors' translation.) That is, not only did students share passwords with each other, but also with people outside the university. Some Tumaini

students had their friends in Iringa; and those students gave their usernames and passwords to friends who were not associated with the university. At some point the IT support found in the computer labs many people who were not related to Tumaini at all.

Two of the interviewees agreed that the biggest problem with password security is that users do not really understand the essence, the very idea of passwords. The interviewees differed, however, in their interpretation of whether that is a cultural phenomenon or not: One of the interviewees argued, "*They feel password can be just given to anybody. It's cultural.*" whereas another argued that in European countries password security has earlier been lax, too: "*The only thing when I think about cultural difference is that, that, regarding technology, this is perhaps, perhaps a younger culture.*" (Authors' translation) He argued that when he had worked some twenty years ago in a large technologically advanced company in Europe, password discipline was equally lax.

One of the interviewees noted that even when money is in the picture, password security is lacking. He remembered several times when he had queued for an ATM that people had come and given their ATM card and their PIN number to him and asked him to withdraw money for them. "*Like, when you go to bank, and you're in this ATM queue—very long queue—and somebody comes, sees you very close to the ATM machine, then he can come and give you the card and give the password.*" The interviewee argued that that is a sort of a cultural thing: people do not feel one could do something bad with another person's password: "*So the same with our students, especially on the password business. They do that a lot. They give passwords for each other. They give—they just exchange passwords.*"

According to the interviewees, there are a few things that force students to think about password security: their printing quota and their time quota. Each student is given four hours of computer time per week, and if they let other student use their time, they are not able to use the computers that week. Similar, each student is given a printing quota of 240 pages per year, and they are afraid that their friends use their entire printing quota.

Some of the more recent problems concern physical access to computing machinery and peripherals. One of the interviewees noted that one of the Tumaini's laptops was stolen, along with all its files. Another remembered a case where a faculty member had gotten examination questions from another faculty member's computer and handed those questions over to a student. One interviewee suggested that many data security issues are often neglected: computers are not configured to automatically enter password protected sleep mode; doors are often left unlocked; and when computers are withdrawn from use, data on hard drives is not overwritten carefully enough.

Finally, administrator passwords have been a problem from early on. One of the interviewees remembered that the head of finances had asked him for the super user password, and another one of the interviewees told that just before he was coming to the interview, a secretary had called him because she wanted to use a USB scanner with her computer, and to do that she needed the administrator password. One of the interviewees reported that he had once found out that a duly designated system administrator was using the super user password for all his tasks, including his regular work. The interviewees were very concerned about the administrator password security and about the consequences of that password leaking out.

3.2. Questionnaires

The respondents skipped a relatively small number of questions in the attitudes part of the questionnaire (5.8%), and interestingly, majority of the responses were at either end of the Likert scale: either strongly agree (30.9%) or strongly disagree (31.9%). Neutral answers were not very common (7.0%). Note that in this section superscript numbers[m.n] refer to questionnaire items.

Usage Statistics

The questionnaire study revealed that the respondents are constantly in touch with some ICT tools—which is somewhat surprising as the country in question is one of the poorest in the world. Every respondent (100%) owns a mobile phone[2.7], and 84% of respondents use Tumaini's computer systems weekly (54%) or daily (30%)[2.2]. Almost all of the respondents (92%) have an email address[2.3], and two thirds check their mail weekly (39%) or daily (28%)[2.4]. Some of the respondents (38%) have a computer at their household[2.8], and several (11%) own a laptop computer[2.9]. Home Internet connections are more rare, though, as only 8% of respondents reported that they have an Internet connection at home[2.10]. Those who have an Internet connection at home, spend an average of 11€ (20840 TZS)[2] per month on Internet, whereas those who do not have an Internet connection spend an average of 4€ (7220 TZS) per month on Internet[4.14]. Internet cafés are a relatively common thing: only 18% never visits Internet cafés, whereas 51% visits Internet cafés weekly or daily and 30% visit monthly.

Flash disks have superseded floppy disks, as 92% of respondents reported that they use flash disk for storing their files[2.13], whereas 18% of respondents reported that they use floppy disks for storing their files[2.14]. About

[2] 1 € ≈ 1934 TZS, 1 US$ ≈ 1227 TZS (April 24, 2008)

half (52%) of the respondents also reported that they use Tumaini's network drive for storing their files[2.12]. The most common application types that the respondents used were word processors (77%) and Internet browsers (75%)[2.15].

Attitudes Towards e-Security Issues

There was a strong consensus that passwords are necessary (84% strongly agree, 7% agree)[3.3.16], and that there are good reasons to regulate computer use with username and password (59% strongly agree, 15% agree) [3.3.11]. But although 87% of the users were strongly of the opinion that students should not be able to freely access other students' files on the network drive[3.3.19], there was much weaker consensus on other security-related issues.

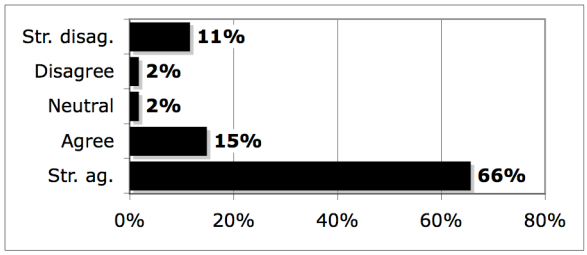


Figure 2: "It is okay to use my friend's username and password on university computers if he/she gives me permission to do that."

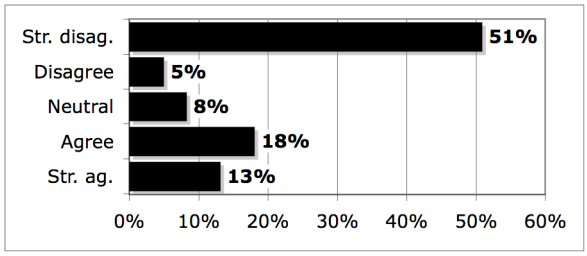


Figure 3: "It is okay for friends to share usernames and passwords"

Firstly, there was a strong opinion that using other student's account is allowable if that other student has given a permission to do that (66% strongly agree, 15% agree) (see Figure 2)[3.3.14]. However, a similar statement "It is okay for friends to share usernames and passwords" got much more mixed response, with majority (51%) strongly disagreeing (see Figure 3)[3.3.10]. Some 38% of the respondents knew the passwords of some other people, 39% sometimes used other students' accounts (Figure 4), and 59% sometimes used other students' printing quota.

Coming back to Infosecurity Europe's study [1], the results of the respondents' attitudes for giving their username to staff members were mixed. About half (48%) of the respondents considered that it is their responsibility to give their password if an IT support person asked for it, whereas 40% opposed that (see Figure 5)[3.3.12]. On the other hand, majority (66%) of the respondents disagreed or strongly disagreed that it is their responsibility to give their password if a professor asked for it (see Figure 6)[3.3.18]. This does not, of course, mean that the respondents would not give their password to their professors if a professor would actually ask for it—the strict hierarchy in Tanzanian university system might compel the respondents to act against their beliefs. The respondents had changed their passwords often: 16% once, 38% twice, and 36% more often (3.9 times on average). That is possibly due to the system, which requires users to change their passwords after every 100 days.

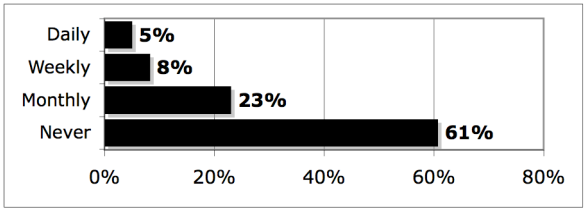


Figure 4: "How often do you use your friend's account?"

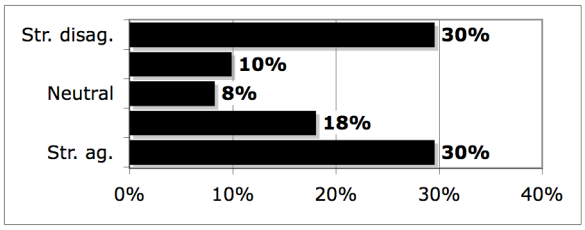


Figure 5: "If an IT support person asks for my username and password, it is my responsibility to give it to him/her."

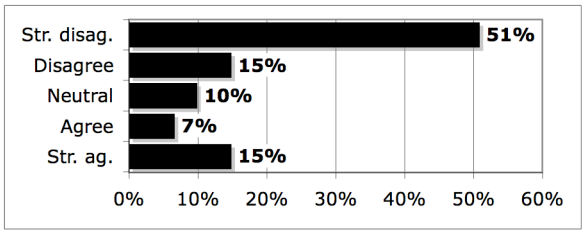


Figure 6: "If a professor asks for my username and password, it is my responsibility to give it to him/her."

There were great concerns about viruses: 76% of respondents agreed or strongly agreed that viruses are a serious threat to their schoolwork[3.3.8]. The attitudes about the amount of teaching about virus protection were mixed (nearly equally distributed on the scale)[3.2.2], and similar, there was no consensus about

whether virus protection programs are easy to use or not[3.1.9].

4. Discussion

The interviews of IT management supported the anecdotal evidence about lax attitude towards password security issues in Tanzanian universities. The main reasons for tightening security and privacy measures at Tumaini University are similar to those in the industrialized countries: increase in malware, misuses of computing and communication resources, and concerns about file security. The interviewees suggested that students at Tumaini University frequently give their usernames and passwords—not only to other Tumaini students but also to people outside Tumaini. This was confirmed by the questionnaire results. The interviewees argued that this is because the users do not understand the reasons for using passwords. If that is the case, then education can change the situation. The respondents, however, felt that password and username issues are emphasized enough in Tumaini students' computer training (43% strongly agree, 26% agree). Nevertheless, despite the training, students are indifferent to password security. This urges us to redesign our basic IT courses, and to conduct a longitudinal study on the effectiveness of education to the password security issue.

Viruses and other malware were one of the early incentives for updating Tumaini's computer security. The respondents strongly agreed that viruses are a serious threat to their schoolwork. The responses were mixes about whether virus protection issues are emphasized enough in Tumaini students' computer training. The effect of education to virus awareness and coping with viruses has to be established in a longitudinal study.

Although some researchers have suggested that there might be a difference between men and women about their attitudes toward password security [1], there seemed to be no significant correlation between gender and any of the other constructs. However, due to the small sample size in this study, that correlation needs to be further investigated in a larger study.

The interviewees held mixed opinions about whether lax password security is a cultural phenomenon or not. It might be a cultural phenomenon, or it might be a passing phase in the diffusion process of information and communication technology. Both interpretations are plausible, and hence the phenomenon requires further research.

This study has showed that there are many open questions concerning security issues in electronic services. Insofar as information society's electronic services—such as e-banking, e-governance, and e-commerce—depend on ideas of unique digital identity and strict password security, there definitely is some work to do before a change to an information society can effectively happen in Tanzania.

It has not been established that there is a difference between students in industrialized countries and the students in this study. Hence, the next stage in this research is to conduct a similar pilot study in Europe or the U.S., and from these pilot studies, construct a larger-scale study that measures the differences between attitudes towards e-security in an African university and a European or American university.

5. Acknowledgments

The authors wish to thank the three interviewees—Jyri Kemppainen, Raimo Haapakorpi, and Fredrick Ngumbuke—for their contribution. The authors also wish to thank Kokel Melubo, Julius Mtemahanji, Lucas Mwahombela, Alinanuswe Mwaikasu, Mpoki Mwakagali, Given Msigwa-Msomba, Oswald Ndelwa, Robert Mutasingwa Rwiza, and Merja Taavila for their help in data collection and data input.

References

[1] Infosecurity Europe, "Women 4 Times More Likely Than Men to Give Passwords for Chocolate", *Press Release*, Apr 16, 2008. Retrieved April 16th 2008 from http://www.infosec.co.uk/page.cfm/T=m/Action=Press/PressID=1071

[2] K.J. Knapp, T.E. Marshall, R.K. Rainer, Jr., F.N. Ford, "Managerial Dimensions in Information Security: A Theoretical Model of Organizational Effectiveness", *white paper, International Information Systems Security Certification Consortium (ISC)²*, 2005. Retrieved April 16th 2008 from http://www.isc2.org/download/auburn_study2005.pdf

[3] E.C. Lallana, *An Overview of ICT Policies and e-Strategies of Select Asian Economies*, Asia Pacific Development Information Programme / Reed Elsevier, India, 2004.

[4] G.L. Orgill, G.W. Romney, M.G. Bailey, P.M. Orgill, "The Urgency for Effective User Privacy-education to Counter Social Engineering Attacks on Secure Computer Systems", *Proceedings of SIGITE'04*, October 28-30, 2004, Salt Lake City, Utah, USA, pp. 177-181.

[5] S.L. Pfleeger, R.L. Trope, and C.C. Palmer, "Managing Organizational Security", *IEEE Security & Privacy, May/June* (2007), IEEE Computer Society, 2007, pp. 13-15.

[6] E.M. Power, "Developing a Culture of Privacy: A Case Study", *IEEE Security & Privacy, November / December* (2007), IEEE Computer Society, 2007, pp.58-60.