TRANSCOMP – XIV INTERNATIONAL CONFERENCE
COMPUTER SYSTEMS AIDED SCIENCE, INDUSTRY AND TRANSPORT

information security,
survey

Zygmunt MAZUR[1]
Hanna MAZUR[1]

SELECTED ASPECTS OF INFORMATION SECURITY

Providing information security is not an easy task. A difficulty in providing computer security is the fact that it must be a continuous process and not a one-time activity. It is tremendously important that the basic rules should be followed and good practices should be used. In order to assess the knowledge of these rules and their observance, a survey was conducted by the authors among students of three various faculties of different universities. This paper presents the results of the survey conducted and discusses its results.

WYBRANE ASPEKTY BEZPIECZEŃSTWA INFORMACYJNEGO

Zapewnienia bezpieczeństwa informacyjnego nie jest zadaniem łatwym. Trudnością w zapewnieniu bezpieczeństwa komputerowego jest fakt, że musi to być proces ciągły a nie jednorazowa czynność. Niezmiernie ważne jest przestrzeganie podstawowych zasad i stosowanie dobrych praktyk. W celu oceny znajomości tych zasad i ich przestrzegania, zostało przeprowadzone przez autorów badanie ankietowe wśród studentów trzech różnych kierunków studiów z różnych uczelni. W pracy przedstawiono wyniki przeprowadzonej ankiety i omówiono jej wyniki.

1. INTRODUCTION

Providing information security is not an easy task. The published results of research conducted among management staff of companies and enterprises demonstrate that managers are aware of the importance of teleinformation security but it is not reflected in reality – the occurring incidents contradict it. Naturally, the most secure are those computers and their resources that are isolated from computer networks and with no possibility to copy data to external storages. Yet, the necessity of effective work and co-sharing of resources imposes connecting personal computers to computer networks. An additional difficulty in providing computer security is the fact that it must be a continuous process and not a one-time activity. It is tremendously important that the basic rules should be followed and good practices should be used. In order to assess the knowledge of these rules and their observance, a survey was conducted by the authors among students of three various faculties of different universities: Informatics of Wrocław University of

[1] Wrocław University of Technology, Institute of Informatics, POLAND; Wrocław 50-370; Wyb. Wyspiańskiego 27. Phone: +48 71 320-42-23; Fax: + 48 320-42-23
E-mail: {zygmunt.mazur, hanna.mazur}@pwr.wroc.pl

Technology, Administration of Wrocław University and Biology and Environment Protection of Agricultural University. The chapter presents the results of the survey conducted and discusses its results.

2. BASIC RULES OF PERSONAL COMPUTER RESOURCES SECURITY

The measures taken to protect the computer resources and provide security of work in the network should not significantly limit and slow down work at the computer. Besides, the cost of these security measures should be adequate to the value of the resources protected. Therefore, it is very important to adjust the security solutions to the needs and financial possibilities of the user and the importance of the resources protected. The basic security methods, possible to be applied even by beginners, and without considerable financial outlays, are the following:

- installation and updating of security software and virus base;
- scanning of the computer due to the occurrence of spyware programs and deleting them from the computer;
- not using personal accounts at generally accessible computers, e.g. university, hotel or internet café computers (or frequent change of passwords);
- limiting the use of accounts on social portals or proper configuration of them, familiarizing oneself with the security and privacy policy of these portals;
- proper using, modifying and keeping of access passwords;
- deleting the history of websites and temporary folders browsed;
- keeping control of information made available at websites and social portals;
- not keeping account logins and access passwords to at places easily accessible to other people or in computer folders;
- using the program keyboard to enter passwords in order to protect against intercepting information in case of keys pressed on the keyboard;
- keeping control of computer security system, updating and adjusting it to current needs and changes;
- avoiding visiting websites that are potentially dangerous;
- observing computer work and responding to untypical behaviour (e.g. slowing down of computer work, erasing files, change in the file sizes, etc.);
- automatic updating of the operation system;
- physical protection of the computer;
- making back-up copies of important data and files;
- keeping important files as hidden ones or in hidden folders;
- hiding the computer IP address, e.g. through using a proxy;
- using encoded connections;
- using separate accounts to make financial transactions (with limitations to the value of sums taken out, number of transactions in a given period, etc.) and keeping control of the transactions made;
- deleting cookies files or putting them automatically in the Trash folder;
- permanent deleting of files, deleting unnecessary files from the Trash folder.

In the further part of the chapter we will present and illustrate with charts how these recommendations are followed by the group of students polled.

3. PROTECTION OF PERSONAL COMPUTER RESOURCES BY THE RESPONDENTS

The basis of work in a computer network is limited trust in other people, continuous control of the security systems used and their updating [1,2]. Following the recommendations mentioned in item 2 of this paper is in many cases sufficient to perform one's work safely in the Internet network (but of course not always). A survey was conducted by the authors to check whether these recommendations, which seem to be obvious in theory and not difficult to follow in practice, are observed in reality. Students of three universities were chosen as a research group.

3.1. Research methodology

Participation in the survey (elaborated by the authors of the chapter) was voluntary and anonymous. The answers from the survey forms were only used to make overall, statistical lists and general analyses.

The survey was performed among students of different faculties of three Wrocław universities: Wrocław University of Technology (WUT), Wrocław University (WU) and Agricultural University (AU). The following number of students participated in the survey: 103 3rd-year students of Informatics of the Faculty of Computer Science and Management of Wrocław University of Technology, 53 4th-year students of Administration at the Faculty of Law, Administration and Economics of Wrocław University, and 61 students of Agricultural University (3rd-year students of Biology at the Faculty of Biology and Animal Breeding, and 2nd-year students of Environment Protection at the Faculty of Nature and Technology).

The survey form included 17 questions connected with information security, out of which 13 questions were of a test type (not necessarily with a choice of one answer only), while 4 questions were open ones. Providing answers in writing to particular questions was optional – the respondents did not have to answer all the questions and some of the students used this possibility. The survey was conducted in 2008/2009 in order to learn and assess the security methods used by the students to protect their data collected on the computer and when making use of network services as well as for the purpose of verifying the recommendations concerning computer security [3]. It was intentional to choose students of Informatics who due to the field of study selected and their interests are likely to have broad knowledge on the threats of loosing data and methods of protection against them, and to give a comparison – students of other fields (Administration, and Biology and Environment Protection). The students of Informatics polled, however, did not have in their curriculum an obligatory dedicated course in information security or teleinformation security. Many of the issues regarding security were discussed within different courses (obligatory and optional ones), e.g. issues of operational systems security, and data and information science administrator's role and tasks.

4. SELECTED SURVEY RESULTS

Due to the extensiveness of the survey we will present only some of the results to the questions asked.

Students, like other internet users, frequently make use of web browsers. The highest number of the students polled (59%) who familiarized themselves with the security policy of the browsers they used were from Wrocław University of Technology (Fig.1).

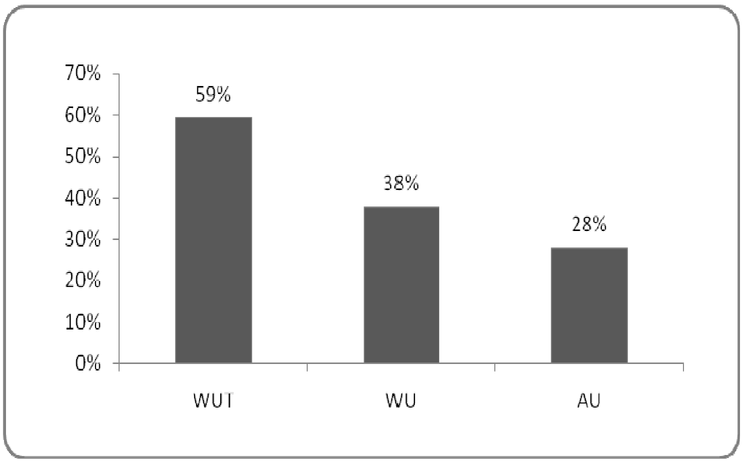

Fig.1. Percentage comparison of answers regarding familiarizing oneself with the security policy of the web browsers used

The high percentage of respondents ignoring the warning that a website is not safe proves that little importance is attached to the Internet security. As many as 74% of students of WUT, 64% of WU and 38% of AU do not resign from browsing websites indicated as dangerous ones (Fig.2). This situation is worrying because a user who can see this warning many times, and he knows that a given website is safe, gets used to such situations, ignores a warning of this type, which in turn considerably decreases his vigilance and as a result his own computer may get infected.

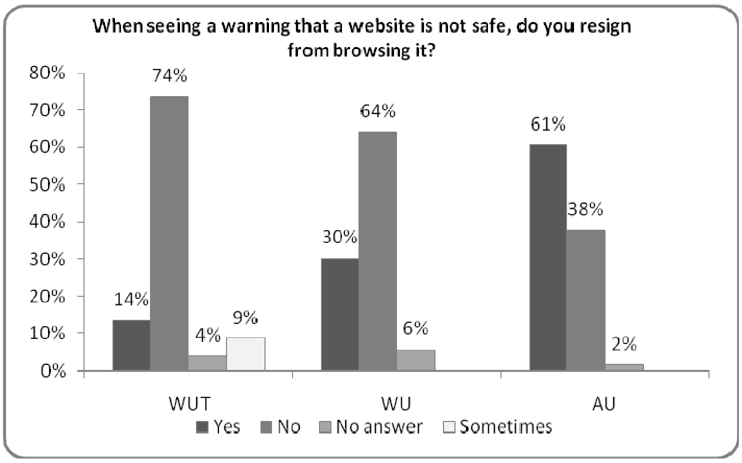

Fig.2. Illustration of the respondents' reaction to websites perceived as dangerous ones

It is commonly known that security software should be installed – antivirus, antispam, antispyware and firewall one. The percentage presentation of the amount of software installed on the respondents' computers is shown in Fig.3. What may be surprising is the lower percentage of the respondents installing security software representing Informatics (WUT) than from other fields of study (Administration of WU, and Biology and Environment Protection of AU). The reason may be a frequent exchange of hardware and lack of time for the installations (which of course is absolutely no excuse).

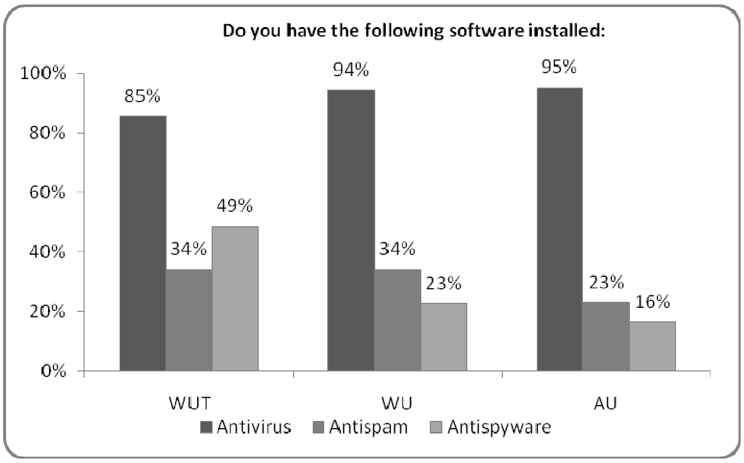

Fig.3. Percentage presentation of the number of respondents installing security software

It might seem that students of Informatics follow the required rules of providing computer security to a higher extent, thus it may be surprising that they take first place as for data loss as a result of harmful software activity (Fig.4) and as a result of computer or software failure (Fig.5).

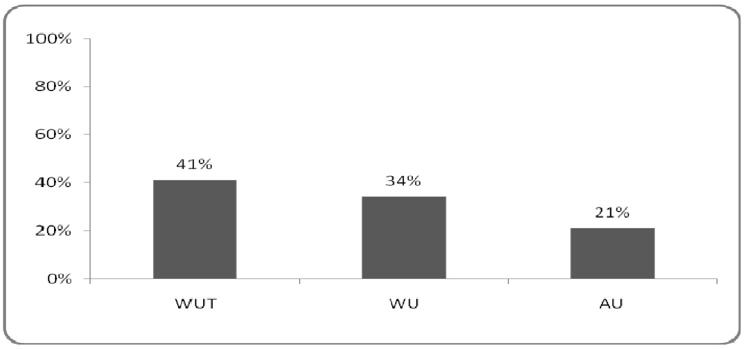

Fig.4. Percentage presentation of respondents who lost data as a result of harmful software activity

An explanation of this state, however, may be a fact that students of Informatics far more frequently use the computer to do work/student projects and install far more different types of software than the remaining respondents. For this reason, however, they should protect their computers better.

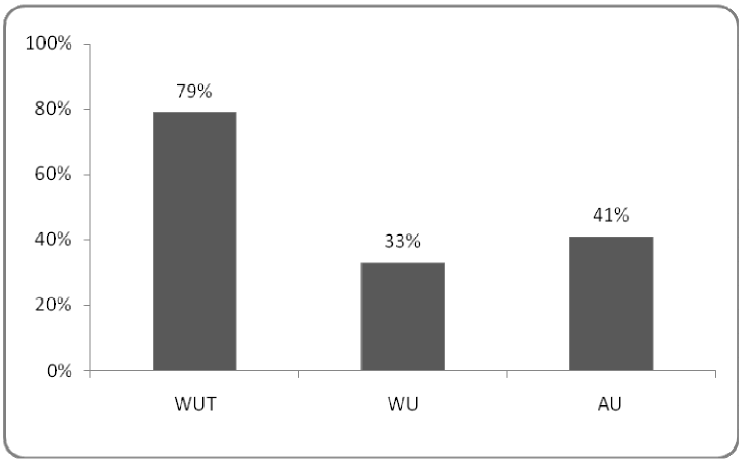

Fig.5. Percentage presentation of respondents who lost data as a result of computer or software failure

The survey conducted demonstrated that 60% of WU students polled do not change their internet account passwords (Fig.6), while as many as 64% of them conduct financial transactions by the Internet (Fig.7).

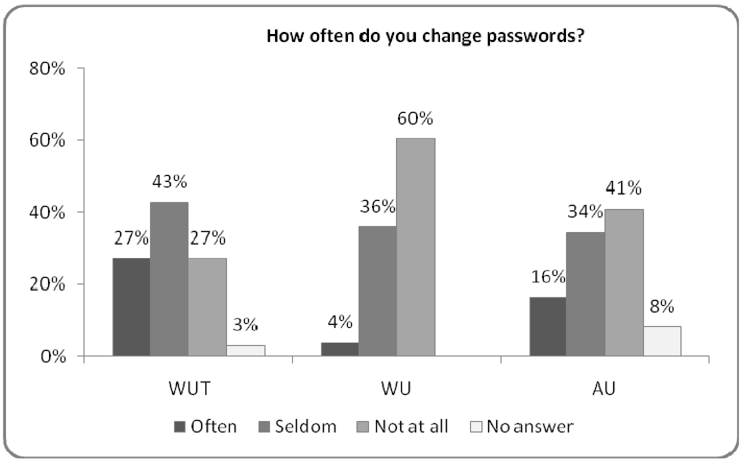

Fig.6. Frequency of the change of passwords by the respondents

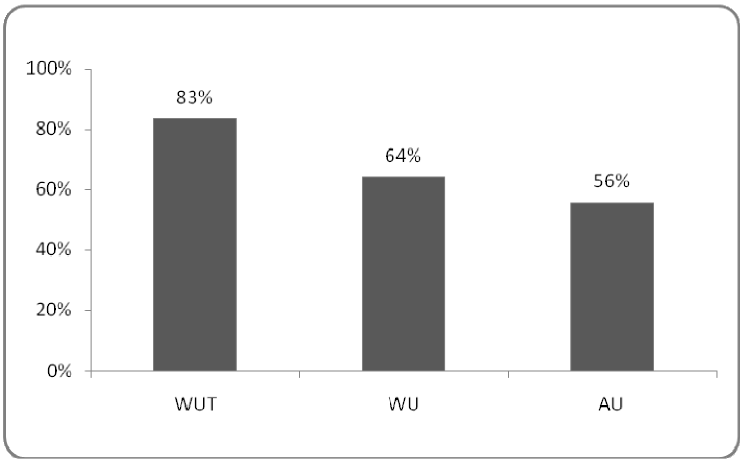

Fig.7. Percentage presentation of conducting financial transactions by the Internet

As results from the survey, the financial transactions are conducted for quite considerable sums, taking into account the fact that they are performed by students (Fig.8). The most numerous group in percentage, which has a bank account separated for this purpose, is the group of the students of Administration of WU (Fig.9).

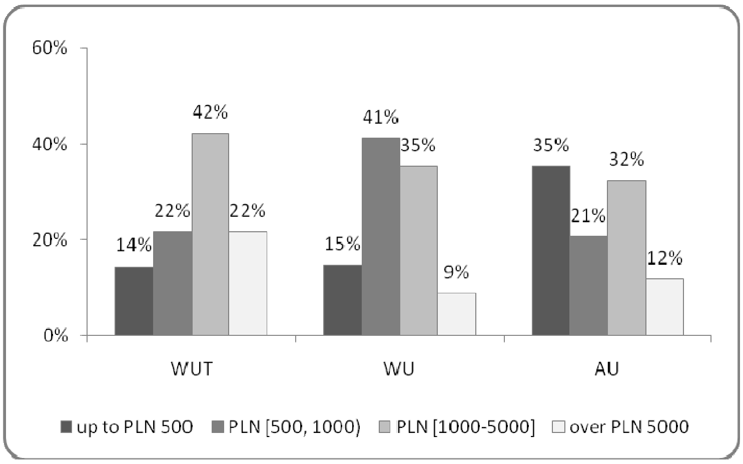

Fig.8. Percentage presentation of the number of respondents conducting financial transactions in given ranges of sums within a year

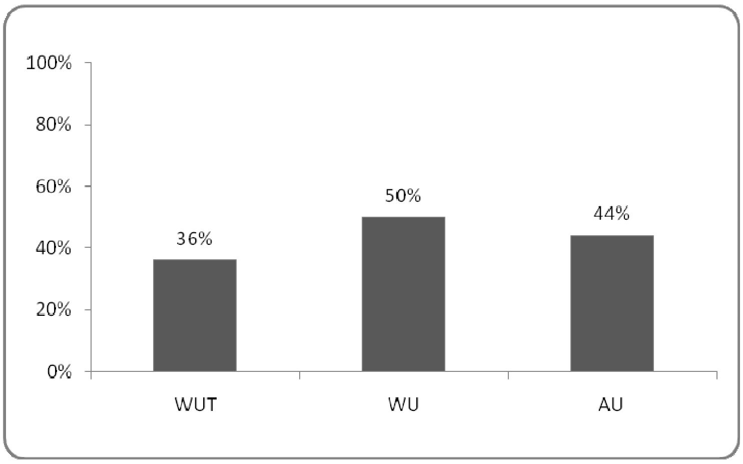

Fig.9. Percentage presentation of the respondents having a separated account to conduct financial transactions by the Internet

It results from many generally accessible research papers that employees, due to convenience, very often write down internet account passwords on slips of paper which they place at a visible or easily accessible place (in a notepad, in a drawer, on the monitor screen, under the keyboard). The students polled came out far better in this respect. As many as 82% of WUT and WU students polled do not write down the passwords anywhere (Fig.10).

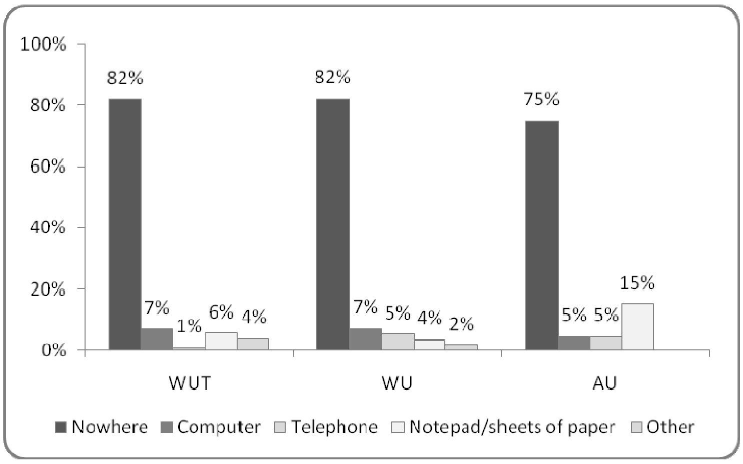

Fig.10. Place of keeping passwords by the respondents

3. CONCLUSIONS

It is often difficult for people to believe that even a seemingly unimportant piece of information is a valuable datum for a refined attacking person. For this reason, they ignore the basic security measures, do not take proper care of their personal data and correct protection of their personal computers.

The survey conducted demonstrated that not everybody uses the recommended requirements regarding providing security of the data collected on personal computers and of safe work in the Internet network. However, the highest number of the respondents using good practices represents Informatics of WUT. Due to the field of study selected these are people who are more aware of the threats, and make use of the computer hardware and security software more freely. The conclusion is that more emphasis should be put on constant indication to computer users of possible threats and methods of preventing them.

The people using internet services must be aware of existing dangers. The contemporary information technologies developing quickly offer more and more opportunities not only to users in the scope of security but also to fraudsters in the scope of attacks. The use of basic simple rules, however, is not simple for everybody. Therefore, free-of-charge training programs in information security should be conducted, and easily accessible information and education materials in this scope should be made available.

4. REFERENCES

[1] Mazur Z., Mazur H., Mendyk-Krajewska T.: *Security of Internet transactions*, In: Internet - technical development and applications, Tkacz E. and Kapczyński A. (eds), pp. 243-251, Berlin; Heidelberg: Springer, 2009.

[2] Mendyk-Krajewska T., Mazur Z..: *Software flaws as the problem of network security*, In: Internet - technical development and applications, Tkacz E. and Kapczyński A. (eds), pp. 233-241, Berlin; Heidelberg: Springer, 2009.

[3] Mazur Z., Mazur H.: *Security of Internet transactions – results of a survey*, In: Internet - technical development and applications, Tkacz E. and Kapczyński A. (eds), pp. 253-260, Berlin; Heidelberg: Springer, 2009.