DE GRUYTER OPEN

STUDIES IN LOGIC, GRAMMAR AND RHETORIC 50 (63) 2017

DOI: 10.1515/slgr-2017-0027

Piotr Paweł Laskowski
University of Bialystok

INTERNET SECURITY – TECHNOLOGY AND SOCIAL AWARENESS OF THE DANGERS

Abstract. The article describes selected issues related to user safety on the Internet. This safety consists of a number of factors such as the technology that we use to communicate and to browse the Internet, and habits and behaviors that we have acquired and through which we can identify at least some typical hazards encountered on the Web. Knowledge of software and the ability to use it and to configure it properly as well as checking regularly for security updates reduces the risk of data loss or identity theft. Public awareness of threats continues to grow, but there are also new, previously unknown threats; that is why it is so important to inform of the dangers by all available channels of communication.

Keywords: security, privacy, threats, social networks, communication.

1. Introduction

The article is a report on the research focused on a group of Internet recipients who are students of the Institute of Sociology and Cognitive Science University of Bialystok. It's not a description of general security problems, but only makes an attempt to describe awareness of the risks the Internet poses to students. The reason for behavior analysis and knowledge of online safety were observations conducted during classes in the computer lab and usage of the Internet (students tended to leave web browsers with an active email account or not to log out the user profile on social networking sites). Exhaustive research was conducted on the student population due to its characteristics. In "Social Diagnosis 2015 – Objective and Subjective Quality of Life in Poland" one read that people aged 16–24 are the most common user group that uses a computer (97.2%), the Internet (97.5%), and the mobile Internet (35.9%). The undertaken research was to diagnose the level of awareness of the risks and perception of the

ISBN 978-83-7431-527-2 ISSN 0860-150X

dangers of the Internet network and to make them aware of the potential threat performed tasks pose. The research was conducted on 110 students in May and June 2016. 110 students responded to the computer assisted Web interview, including division yearbooks: 49,14, 22, 15,10 of all students in the numbers: 84, 18, 24, 32, which accounted for 55.55% total number of students.

2. Risk awareness

Security and privacy play a very important role in the daily activities related to the functioning of the Internet. We send and receive emails, we communicate via instant messaging and social networks. These are the most common tasks when using the Internet. 42% of Poles 16 years of age and above are using e-mail and 24% Internet communicators (Czapiński & Panek, 2015, p. 23). We buy online, we use Internet banking (this action was declared by 29% of Poles 16 years of age and above (Czapiński & Panek, 2015, p. 23). We read reviews and recommendations of Internet users. We leave traces of our presence everywhere and we show our preferences and tastes. Our presence on the Internet can be used by other network participants with malicious intent. Sensitive data are exposed to various risks associated with identity theft, loss of privacy, transmission of unwanted content, profiling, etc. Browsing the Symantec "Internet Security Threat Report" we read, that health services, hotels, and business services, but also educational websites are the most exposed to both dangers and risks associated with data loss (Symantec, p. 52). Our presence may also be exposed to insult or ridicule; we can be provoked by harsh and negative (offensive and aggressive) comments. Antisocial phenomena describing such behaviors are *trolling* (trolowanie) and *hate* (hejt) (Wawrzyniak, 2015, p. 35) – fairly common on the Internet and very hard to combat. These problems open up a discussion on the social norm online and the tightening up of the law (Klempka & Stimson, 2014).

Concerns about privacy, data protection, and secure user identification are the leading trends that are implemented in both new and developing applications intended for a broad spectrum of activities ranging from entertainment and communication, to shopping and online payments. In all cases the most important seems to be the human factor, which is user awareness about the dangers and safety rules. Inactivity and taking no notice of the threats can lead to serious consequences of the loss of sensitive data. It's essential to know activities described as good practice and

aquire the knowledge of what to do in case of violation of safety rules (Security Awareness Program Special Interest Group & PCI Security Standards Council, 2014). Programs can have enhanced protection capabilities, but incompetent use and incomprehensible options do not guarantee safety. Outdated operating systems and browsers with extra plug-ins are also a threat to people using them (Lockhart & Sagalara, 2007, p. 72). Having contact with the threat, and not being able to recognize it, is particularly dangerous for the Internet user. The ability to avoid danger is closely related to knowledge about the types of risks and familiarity with software which can be used for protection. Among a number of programs, both free and paid ones will find a whole range starting from the firewall and antivirus to protecting against malware and rootkits (15 Great, Free Security Programs, 2007).

3. Information and communication

We live in times of dynamic development of information technology and communication mediated by means of this technology. An Internet network user absorbs new technologies and uses them as if unconsciously, without effort. Information, created and published on the Internet, is widely available to all of us and can often overwhelm or cause excess information dizziness. We are unable to absorb it all with our mind so we use additional tools such as filters, which allow us to narrow down the broad stream of data to which we are exposed, to precise and clearly defined channels with specific issues of interest. We live with information available as the first and often the primary source flowing to us from the Internet. We can watch the news, favorite TV series, read editions of our preferred newspapers via the Internet. There we will discover what has happened in the world, we will find issues and articles of interest, we will see what our friends are doing at any given moment, or we will write and send information about our affairs. All this information creates a picture of us in the global network, which can be used by unauthorized persons. Our data can be used for illegal purposes. On websites where registration and logins are required we can lose access to our account, for example, through social engineering attacks aimed at password phishing, or because of software that was not properly secured. The use of dictionary passwords among the participants of the Internet network is a weak point, which we underestimate (Hadnagy, 2012, p. 30). We often use one standard password and when it is broken we lose access to all accounts where this password was used.

Table 1
When registering on websites how strong passwords do you set?

	Frequency	Percentage
letters and numbers	65	59.09
lower-case letters and capital letters, numbers and special characters	28	25.45
letters, numbers and special characters	15	13.64
only letters	2	1.82
Total	110	100.0

Source: own study[1]

The awareness of users continues to grow. Looking at the example of students we can conclude that the use of letters only in a password occurs sporadically. However, mixing numbers and letters, inserting additional uppercase and lower-case letters and special characters makes it much harder to guess passwords and causes brute force attacks to become very time consuming and cost-ineffective. Selected from the 10 most popular passwords observed during attacks is a "user name", "123456" and "password" (Owens, 2008, p. 3). It might seem unlikely, but they are often used as passwords for e-mail accounts or administration of the websites.

Through the Internet network we create and co-create information, we communicate, exchange ideas, we discuss. We have unlimited access to messages flowing through social media. This creates a huge amount of data ready for use. It should be noted that these data are used for example to prepare advertising aimed at us, specially crafted and targeting our current needs and tastes, but they can also be used for illegal purposes. These resources are referred to as the concept of *big data*.[2] Such a collection of high-volume, wide variety, and variability, is a very interesting source of information about our interests and preferences (Mayer-Schönberger & Cukier, 2014, p. 24). The potential of these data can be used by unauthorized persons. Lack of legal regulations, numerous software bugs, poorly protected data sets and their potential become a very attractive target for cybercriminals. The technology data protection available today is not sufficiently fast to use for large datasets (Toshniwal, Dastidar & Nath, 2015, p. 17).

The level of awareness of people creating a network of contacts and registering at websites, forums, and social networking sites is crucial for safety. On social networks users are prone and particularly exposed to dangers. There exist the problems of spam, the risks associated with social engineering, phishing, etc (Wüest, 2010). The risk is also related to the applications

themselves, which are not free from programming errors and often become the target of successful hacker attacks. Educating and informing about potential threats is extremely important. Recognition of possible attacks and development of positive habits to protect our private data and minimizing risky behavior is the key competence for safe movement and functioning on the Internet.

4. Social networks

Social networks are an excellent source of information about their users – appearance, habits, regularly performed activities, contacts, etc. The most popular service nowadays (Facebook), where we leave such data, was created in 2004. It is estimated that currently there are 1.65 billion registered active users during a month (Top 200 Facebook Statistics, 2016). Having an account on Facebook has become essential for functioning and full participation in a given social group. There, information exchange is flourishing, participants are engaged in virtual life, which of course also translates into real life (appointments, joint projects, etc.). This is confirmed by the results of a survey conducted among the students of the Institute of Sociology and Cognitive Science. It shows that **100%** are involved in Facebook social network. Other services are less popular. It should be noted that participation in one service does not exclude participation in other such services.

Table 2
Percentage of people participating in social networks – besides Facebook

Social network	Snapchat	Instagram	Google+	NK Nasza klasa	Twitter	GoldenLine
Participation (%)	54.55	46.36	40.00	20	4.55	4.55

Source: own study. Percentages do not add up to 100% – it was possible to choose more than one service.

Students willingly use communication possibilities offered by available social network sites. The increasing attractiveness of such services should also be associated with widespread access to the Internet from any location (universities, cafes, galleries) and with the growing amount of equipment which offers such access. Almost everyone now owns a smartphone with Wi-Fi and built in ready-to-use applications, which facilitate the exchange of

information and allow posting phone-taken photos or videos on social networking sites. One should take into consideration activities that can increase the security of participation in social networking sites such as:

- checking whether the device you use to log in for these services is appropriately protected by software,
- careful clicking on external links since they bring about the opening of the unknown and dangerous applications,
- using strong passwords,
- protection of confidential information and not sharing it with strangers,
- prudent adding of "friends",
- sharing only necessary information,
- thought out comments,
- setting such privacy that only trusted users have access to selected information (Shravani & Nagamani, 2012).

The market for mobile devices continues to grow, and with it grows the number of applications available for smartphones or tablets. These applications are easy to use, dragging your finger across the touch screen or in other words just 'tapping' it allows friends to watch our media and read the information we publish. The data we have and produce are becoming more dispersed; we store it on laptops, tablets, or smartphones. The popularity and capacity of external drives, where we can store our files in a so-called 'cloud', is also growing. There are many options, ranging from free services to paid ones, guaranteeing higher capacities or additional options unavailable in the free versions. This gives us convenient access to our data from anywhere in the world, which of course can only constitute our private resource. It should be noted, however, that the convenience of access to the Web, regardless of where we are, carries the risk of not so much as losing the data, but of unauthorized access to our confidential data.

Among students – according to the conducted survey – using the cloud to store files seems to be less popular (**51.8%** compared with a similar survey done in 2003 when it was only **2.8%**). This data presents a growing trend. In 2014, 21% of the EU population aged 16–74 reported using the cloud to store documents, photos, music, video, etc. The greatest use by country was Denmark – 42%, the United Kingdom – 38%, Luxembourg and Sweden 35%, and in comparing the ranking of Poland – it was less than one in 10 (Reinecke & Seybert, 2014). Popular sites offering such services give us a choice of course, as to the type of access to these files, whether they will be available to the public or will remain confidential. Whether we want to share data with others will depend on the configuration of services and assigning passwords to files and folders. The owner decides what can be

made public, and what will constitute confidential information inaccessible to third parties.

Profiles created on social networks have also resulted in changes to the webpages that we manage and to those we visit. Thus, each article appearing on a site gains some additional functionality. We can give it "likes" thanks to an additional plug-in, "tweet" it, or recommend it to Google+. All this results in an unprecedented abundance of information. With little effort we can be very visible in the Internet. We become conscious partners in the exchange of information and interaction between individuals. We interact with each other by analyzing artifacts left by users in the form of photos, videos, sound files, or just brief information, however much revealing. This results, for example, in the creation of an avatar similar to our own image. From this avatar outsiders can learn a lot about us, regardless of whether we like it or not. The phenomenon of self-creation appears to be widespread, where we have much higher virtues than in the real world. On the Internet we are more beautiful, wiser... We create our perfect reflection. We want to be perceived without flaws and defects, and that is how we try to portray ourselves.

On average, students spend 4.57 hours a day on the Internet with a median of 4. In "Social Diagnosis" one can read that the most active users of the new technology are young people (learning and studying). Smartphone owners in this group constitute almost 80%. Persons under the age of 24 years spend during the day 2 hours 22 minutes via the Internet (Czapiński & Panek, 2015, p. 390). The most common activities of students who participated in the survey are being on social networks – 70% of the respondents indicate it as the most important activity; equally important turned out to be: checking email 31.8%, and visiting information sites 30.9%. Awareness of the risks among respondents seems to be high – 61.8% declare that the Internet is not a safe place; 26.4% had no opinion. Students are also confident about their competence regarding threat related situations. When asked *"Do you think that you know how to safely use the Internet?"* 66.36% answered rather yes; 9.09% – definitely yes; 14.5% – neither yes nor no; 8.18% rather not and 1.8% definitely not.

5. Access to knowledge – identification of threats

Social, economic and technological development has resulted in access to information and knowledge about communities, but also to the preferences of each user who is a part of selected community sites. We have also gained connection to the Web at any time and from anywhere. We are no

longer constrained by time and space. We can reach for knowledge whenever we feel like it, we can also create it by sharing our experiences. Constantly, new e-learning platforms are being created, new courses are designed, instructional videos are uploaded and shared. Knowledge has become easily available. When we encounter problems we can conveniently find ready-to-use solutions on the Internet. We ourselves can also become a source of information as to how we managed to solve a dilemma. With the availability of information and communication capabilities we gain valuable and accessible sources. The exchange of information takes place on Internet forums, likewise thematic webpages are created, which describe particular issues. Information also appears on social networking sites. Fast access to materials about any risks is important. Alerts for phishing attempts or fake emails containing malicious attachments quickly appear on the Internet. Bank information websites warn and inform about potential hazards. Users exchange information about threats and ways to avoid them. Students also seem very alert to the Internet dangers. To the question *"Have you ever been the victim of fraud on the Internet?"* 17.27% answered yes; 82.73% answered no.

In detection of threats we are assisted by additional programs installed on devices with which we connect to the Internet – antivirus software, personal firewalls, etc. There are also patches to applications available, which improve safety and fix flaws in programs. Only careless users are exposed to a greater risk when they ignore this information, and they do not use additional security measures. The most common protection against threats from the Internet is an antivirus program – this is also confirmed by the survey – **91.8%** of students declare that they have antivirus software installed on their computers. Equally important is protection against unauthorized access from the Internet to the contents of computers. In this case the entrance is guarded by a firewall. The survey shows that firewalls are less popular than antivirus software (**49.1%** of respondents indicated use of a firewall), but for safe navigation on the Internet it is equally important. It filters outgoing and incoming Internet connections, and also monitors network traffic and stores events.

6. Types of threats

Digitized and indexed information can be found on the Web. There are books out there that were written long before the invention of the computer and the Internet. Analogue materials have gained a new life on the Internet, and have become widely available not only to a narrow circle. We can

find them, view them, and what seems to be very convenient, we can identify phrases or words appearing in these materials using the search function, which will return the result in a split second, without tedious page turning. This constitutes a collection which is referred to as new media (Manovich, 2012). There is also sensitive data on the Web which we leave when registering to websites, stores, forums or social networks. We leave traces of our presence when we download materials from the Internet, or when we visit pages that do not require user registration. Which data we willingly give and which we guard is an individual matter for each Internet user. Using first and last name along with publicly listed address information may endanger the user not only in the virtual world, which can result in identity theft or cyberbullying, but may also present real threats – we pass on tips for a burglar about our daily behavior. One reads about the procedures that protect our private data in many publications that we find on the network (CMOD Department of Finance, 2014). There will be issues of data encryption, transmission of information, remote access, etc.

Gaining access to data and passwords may be based on a method called "phishing". These are actions involving attempts to defraud the data by, for example, specially crafted messages pretending to be correspondence with a bank. In these e-mails the administrator asks for personal data and a password to verify an account. Pretext might be an update of the site, or a threat of closing an account for exceeding mailbox limit – the ingenuity of tricksters knows no boundaries. Compressed attachments that contain viruses or malicious scripts that can take control over a computer are often placed in e-mail messages; they can also erase data from the hard disk, and even encrypt the data so we will not be able to access it unless we pay the cybercriminals to unlock access. Quoting the report data Phishing Activity Trends of the first quarter of 2016 the number of phishing sites increased by 250% compared to the same period of the previous year and also detected 20 million new malware samples (Anti-Phishing Working Group, Inc., 2016, p. 4,8).

Sites that mimic their real counterparts (banks, postal services, etc.) may be more difficult for the Internet user to detect. The method which is applied by cybercriminals in this case is called "pharming". Adequate software is able to mask the true address of the site and we will be redirected to a fake website address. The vast majority of sites, which require submiting sensitive data when registering, are encrypted by HTTPS[3] protocol and authenticated with SSL or TLS certificates (Susłow, Słowik & Statkiewicz, 2014, p. 136). For the user this is visible in the address bar of a web browser. However, there may be occasions when HTTPS protocol and SSL/TLS

certificates are bought by the cybercriminal – the only difference then is in the URL address. The key, therefore, is alertness and above all user awareness about the threat.

There are various forms of online threats. Discussed above were the ones which I encounter quite often in my practice, and I have to cope with repeatedly. The damage caused by these risks can range from minimally damaging to those causing uncountable harm such as loss of data stored on your computer's hard disk or somewhere in the Internet. Dealing with security threats means constantly acquiring information about potential places and ways in which they can appear; it is also having the right software, careful use of programs and constant checking for updates, at least those described as critical. Carelessness and failure to supervise security measures is immediately used to our disadvantage, which leads to damage of software, unauthorized data acquisition, lost access to accounts etc. – there are countless types of possible detriments and it is impossible to name them all.

7. Technology and usability

In the world around us we are all users of the Internet, to a greater or lesser degree. Navigating through this vast network would not have been possible without assistive devices such as computers, laptops, smartphones, tablets. We have acquired technology with which, whether we like it or not, we need to be familiar to at least a basic extent. Without elementary knowledge about computers, operating systems, or computer programs, we can easily become digitally excluded. On the other hand, simplicity of use for the end user is the aspect that software manufacturers put a very strong emphasis on. Internet users are able to perfectly move around the world of various applications used for communication, fun, shopping, etc. This is a component of their social behavior. They co-create content without computer training thanks to a simple and user friendly interface. This simplicity is also a factor multiplying the amount of information available on the Web. Technology has become our tool and link with the virtual world, so it seems that its assimilation, at least at a basic level, should be a skill necessary for existence and survival in the world of the global Internet network. To survive there it is crucial to identify threats, and their early detection is possible through special programs mentioned in the above text. For web browsers we can find additional plug-ins blocking intrusive and annoying pop-up ads or unwanted additional pop-up windows. We can also find programs that block tracking of the websites that we visit. It is a common practice of popu-

lar social networks like Facebook, Google+ and Twitter to track sites visited by their users when they click "Like", "Follow", or "+1" buttons. If you are not sure about the security of your computer and the software that you use, if you want to take advantage of the Internet connection at a stranger's computer or in public use of an open Wi-Fi network, then you increase security by using the private mode (incognito) in the web browser. Browsing the Internet in this mode takes place without saving information about the visited webpages. Only about 9% of students use this option frequently or very often, and 32.73% have never used this mode at all.

Table 3

Do you ever use the web browser in the private mode (incognito)?

	Frequency	Percentage
very rarely	27	24.55
rarely	37	33.64
never	36	32.73
often	8	7.27
very often	2	1.82
Total	110	100

Source: own study

Seemingly insignificant, less known and popular information, and additional software, have a tremendous impact on perception and safe operation within the Internet space. These programs, even very complicated ones, have a simple and transparent interface for the casual user. More complex options that require extensive knowledge to configure are also available, but their simplified versions and default settings are often enough to feel safe and properly secure the devices on which we surf the Internet. Not without significance seems the awareness of users about the availability of free tools, which are based on open license. They constitute an alternative to paid software, and are not functionally different from their commercial counterparts, sometimes even surpassing them in practicality. The end user receives a fully valuable product without incurring any additional costs.

8. Summary

Awareness of the threats of the Internet seems to be a marginal aspect the end users, but only to the point when they become the victims. This can lead to loss of data or loss of identity in social networks. Adherence

to the basic principles of security becomes a necessity and mandatory function to be guarded by us only when we are confronted with the real threat. When it is not of concern to us, sometimes our awareness of the subject is negligible. The technology that gives us so much, can also deprive us of certain things. The types of threats depicted in this article are only a very small spectrum in comparison to what can actually be waiting for us in the vast global network of the Internet. In addition to viruses, Trojans, exploits, backdoors, etc., that is, scripts that can threaten the security of our data, the Internet itself can pose a hazard because we can become addicted to it. Staying too long in front of a computer, irritability, neglecting other activities, escaping from the problems in the real world to the virtual world are symptoms of Internet addiction. Intimidation and harassment via the Internet by third parties is also a common phenomenon, which is very hard to deal with. Harassment through the use of the Internet is referred to as cyberbullying, and it can take various forms such as publishing discrediting photos and videos, intimidation, humiliation and ridicule, or identity theft and impersonation of others. Therefore, it is of utmost importance to follow the rules of safe use of the Internet and to enjoy it reasonably within a limited timeframe.

Familiarity with technology is increasing, and our awareness of threats continues to grow. We become more informed users thanks to the experiences that we collect in the virtual world; we know more, we learn faster from our own mistakes, as well as mistakes made by others. So let us be aware of the dark side of the Internet and technologies associated with it. Let us follow basic safety rules, let us be prudent users of social networking sites. Let us make sure that our devices have up-to-date software, so that our experience with the Internet can be associated with pleasure rather than with torment.

Awareness of the dangers on the Internet among students is not sufficient and requires continuous information and teaching about good and safe habits. Setting weak passwords, publishing unauthorized private information, insufficient awareness of the configuration and operation of programs to protect against attacks from the network and often the lack of a relevant program installed on one's computer comprise the problem that seems to be perceptible in this group. We are spending more and more time on the Internet and with this gradual increase it is desirable that users' awareness of the most common threat should be raised. The software we use is also not free from errors. It may be so dangerous that any unware user will suffer from data loss or takeover. Contemporary times can be characterized by the saying that "everything can be hacked". Each device including

devices of everyday use, having a connection to the Internet will never be secure. Therefore it is important to anticipate potential risks and at the same time increase users' awareness and apply activities that will provide at least a partial sense of security.

NOTES

[1] CAWI (Computer-Assisted Web Interview) study conducted among a group of 110 students of the Institute of Sociology and Cognitive Science UwB in May–June 2016.

[2] Big data is a term that describes the large volume of data – both structured and unstructured – that inundates a business on a day-to-day basis. But it's not the amount of data that's important. It's what organizations do with the data that matters. Big data can be analyzed for insights that lead to better decisions and strategic business moves. Source: http://www.sas.com/en_us/insights/big-data/what-is-big-data.html [16.11.2016]

[3] HTTPS (Hypertext Transfer Protocol Secure) is an encrypted version of the HTTP protocol. To encrypt transmitted data cryptographic protocols are used commonly referred to as SSL or TLS protocols. SSL or TLS is used for example when connecting with online banking or Internet shops.

REFERENCES

Anti-Phishing Working Group, Inc. (2016, July 2). *Phishing Activity Trends Report 1st Quarter 2016*. Retrieved 11 11, 2016, from http://docs.apwg.org/reports/apwg_trends_report_q1_2016.pdf

Castells, M. (2010). *Społeczeństwo sieci*. Warszawa: Wydawnictwo Naukowe PWN.

CMOD Department of Finance. (2008, December). *Protecting the confidentiality of Personal Data*. Retrieved 11.11.2016, from https://www.dataprotection.ie/documents/guidance/GuidanceFinance.pdf

Czapiński J., Panek T. (2015). Diagnoza Społeczna 2015 – Warunki i jakość życia Polaków. Retrieved 11.11.2016, from http://www.diagnoza.com/

Hadnagy, C. (2012). *Socjotechnika: sztuka zdobywania władzy nad umysłami*. Gliwice: Wydawnictwo Helion.

Klempka, A., & Stimson, A. (2014). *Anonymous Communication on the Internet and Trolling*. Concordia University, Saint Paul, MN. Retrieved 11.15.2016, from https://comjournal.csp.edu/wp-content/uploads/sites/16/2013/12/TrollingPaper-

Kozinets, R. (2012). *Netnografia: badania etnograficzne online*. Warszawa: Wydawnictwo Naukowe PWN.

Lockhart, A. (2007). *125 sposobów na bezpieczeństwo sieci*. Gliwice: Helion.

Manovich, L. (2006). *Język nowych mediów*. Warszawa: Wydawnictwa Akademickie i Profesjonalne.

Mayer-Schönberger, V., Cukier, K. (2014). *Big data: rewolucja, która zmieni nasze myślenie, pracę i życie*. Warszawa: MT Biznes.

Owens J. (2008). *A study of passwords and methods used in brute-force SSH attacks*. Clarkson University. Retrieved 11.16.2016, from http://people.clarkson.edu/~owensjp/pubs/Owens_MS_thesis.pdf

PCWorld (2007, May 24) *15 Great, Free Security Programs*. Retrieved 11.11.2016, from http://www.pcworld.com/article/133631/article.html

Privacy Technical Assistance Center. (2011, December). *Data Security: Top Threats to Data Protection*. Retrieved 11.15.2016, from http://ptac.ed.gov/sites/default/files/issue-brief-threats-to-your-data.pdf

Reinecke P., Seybert S. (2014). *Internet and cloud services – statistics on the use by individuals – Statistics Explained*. Retrieved 11.15.2016, from http://ec.europa.eu/eurostat/statistics-explained/index.php/Internet_and_cloud_services_-_statistics_on_the_use_by_individuals

Security Awareness Program Special Interest Group, & PCI Security Standards Council. (2014). *Best Practices for Implementing a Security Awareness Program*. Retrieved 11.15.2016, from https://www.pcisecuritystandards.org/documents/PCI_DSS_V1.0_Best_Practices_for_Implementing_Security_Awareness_Program.pdf.

Shravani, R., & Nagamani, O. (2012). Analysis of Equivalence of Network positions and social roles. In *National Conference On Social Networking* (p. 33). Retrieved 11.15.2016, from http://repository.um.edu.my/26680/1/Jar-Kumar-Conference%20PROCEEDINGS-MAIL%20(1)%20(1).pdf#page=41

Susłow W., Słowik A., Statkiewicz M. (2014). *Chcę zostać informatykiem*. Gliwice: Wydawnictwo Helion.

Symantec Corporation. (2016). *Internet Security Threat Report Internet Report* (No. 21). Retrieved 11.15.2016, from https://www.symantec.com/security-center/threat-report

Symantec Corporation. (2015). *Keeping Your Private Data Secure*. Retrieved 11.15.2016, from https://www.symantec.com/content/dam/symantec/docs/white-papers/keeping-your-private-data-secure-en.pdf

Top 200 Facebook Statistics (2016, April). (b.d.). Retrieved 11.15.2016, from http://expandedramblings.com/index.php/by-the-numbers-17-amazing-facebook-stats/

Toshniwal R., Dastidar K. G., Nath, A. (2015). Big Data Security Issues and Challenges. *Complexity*, *2*(2). Retrieved 11.15.2016, from http://www.ijirae.com/volumes/Vol2/iss2/03.FBCS10080.pdf

Wawrzyniak M. (2015). *Hejtoholik czyli Jak zaszczepić się na hejt, nie wpaść w pułapkę obgadywania oraz nauczyć zarabiać na tych, którzy cię oczerniają*. Gliwice: Wydawnictwo Helion.

Wüest C. (2010). *The Risks of Social Networking*. Symantec Corporation. Retrieved 11.15.2016, from https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_risks_of_social_networking.pdf