Augustyn Surdyk[1]

10 Towards electronic media awareness: The basics of security engineering in FL teacher education

1. Introduction

Foreign language teachers as well as students and graduates of philological studies, who engage more and more often in other professions (outside education), similar to all other people, are internet users. Likewise, unfortunately, they equally have to face the dangers arising from the use of these media, either for personal or for professional reasons. It needs to be mentioned that not all graduates of philological studies are prepared in the course of their studies to perform the job of a teacher, moreover, even those who are do not always choose to work in the field of teaching. The scale of the phenomenon is so large that it may be claimed, teachers in fact may soon transpire to be a minority among the graduates of philology studies[2]. Each year the number of specializations available to students of philology at Polish universities is rising. It enables the students to study and prepare for many other professions, outside the field of education. Among philology graduates there is a rise in the number of translators, whose work may eventually vary from single-person microfirms, through organised translation companies, to positions as translators employed by the European Parliament in Brussels as well as other specialists who become employed in various spheres of the economy and public life[3] in such professions as: intercultural communication trainer, intercultural conflicts mediator, cultural advisor and intermediary, advertising industry worker, journalist, columnist, written and spoken communication specialist, technical documentation editor, programmer and hypertext designer, linguistic design specialist of computer assisted educational systems

[1] Some fragments of this chapter constituted an article already published by the same author in the Polish language.

[2] Especially considering the ministerial decision to disband the Foreign Languages Teachers Colleges. *cf. Education in 2008/2009 school year*, 2009.

[3] On the basis of the list "Language professions" available on the website of the Institute of Applied Linguistics of Adam Mickiewicz University, Poznań; www.ILS.amu.edu.pl.

and other IT systems, human resources worker in business, public administration, union organisations, associations, religious or social organisations, clinical linguistics specialist, investigative linguist (working on phonoscopic forensic examinations and expert analysis for the police, in criminal investigations or in marketing), volunteer assistant or other worker in an MP's office, local authorities, governmental or diplomatic staff member. Finally, it should not be ignored that a philology graduate might become a Member of (European) Parliament, a member of the Cabinet or an otherwise important government representative, many of them being posts with a requirement of fluency in foreign languages, although, as has been observed throughout the last decades, this requirement is not always considered essential.

Within each of these professions philology graduates may need to use the internet for official as well as private purposes. If a private person's becoming a victim of cybercrime may be relatively harmless, while possibly distressing for the person involved (e.g. in the case of bank account theft, loss of data, loss or damage of software or hardware), then becoming a victim of internet mediated crime while using company computers, which often have access to a local intranet and databases (containing classified, confidential, restricted or top secret data) of a company (e.g. a bank, an insurance company and so on), or a public administration institution, could have grave consequences on a global scale (ultimately also for the security of the state), becoming a form of cyberterrorism. This is why educating an individual in the safe use of the internet, and raising awareness of the potential dangers related to them, may become a key element of a global policy conducted within the framework of security engineering design on various levels. Moreover, in times of rapid technological growth and development of new forms of internet communication, this education should be universal, mandatory, and start at the earliest levels of schooling[4]. The school curricula and programmes of studies allow such a knowledge to be conveyed within the framework of existing school and university subjects. However, unfortunately, there appears to be a lack of qualified specialists who could conduct such classes or training professionally and thoroughly[5].

The author of this chapter, being an academic teacher himself, decided to take steps to raise the awareness of applied linguistics students about the potential dangers which stem from the use of the internet. Due to his

[4] At lower levels of education e.g. during Computer Science classes, and at universities during related classes, including an extra programme of awareness raising for minors and their parents about other possible dangers of the internet (e.g. addictions, hazard, paedophilia, pornography, violence, abductions etc.) and about means of avoiding them.

[5] The unattractive level of salaries in education is the reason why Computer Scientists, who would be the most appropriate persons to conduct such classes, or even occasional specialised training (if no subject on the curriculum allowed such information to be included), choose more lucrative posts.

initiative an optional course "Multimedia in foreign language teaching" has been added to the study programme for extramural postgraduate studies of glottodidactics (teacher specialization) at the Institute of Applied Linguistics at the Faculty of Modern Languages and Literature of Adam Mickiewicz University, Poznań, in the academic year 2007/2008[6]. The course, besides acquainting the students with techniques of computer assisted learning of foreign languages, provides them with basic knowledge of the aforementioned dangers and of the means of their prevention. Moreover, a similar content, although with many more hours of classes, is offered in the training course for foreign language teachers entitled "New technologies for foreign language teaching", also brought into being at the aforementioned institute by the present author in the academic year 2009/2010. Another course, initiated the same year by the author, for foreign language teachers, entitled "Construcing educational games in foreign language teaching", despite a difference in the core of the course content, is still within the sphere of modern technologies, although limited to the scope defined by the course's title, and also includes information about the aforementioned dangers. The fact the author decided to take action in this field within the framework of training foreign language teachers determined the topic of this article in its current form. However, the title matter could well be broadened to the teaching of philology students in general. For the curricula of philology studies, contrary to many other humanist programmes, give more opportunities to convey such information along with practical vocational knowledge (in this case, within the scope of the use of new technologies, e-learning platforms and so on, in glottodidactics), although finding similar possibilities in the case of other faculties probably depends largely on the openness and good will of the directors of the particular departments and their lecturers. Paradoxically, though, in spite of the fact that the philology programme for teachers includes a course of "Information Technology" for the graduate students (B.A. studies)[7] most teachers are not properly educated in the field and do

[6] The course, lasting 20 hours, ending with an exam, available to 1st year extramural postgraduate students, was introduced due to the author's initiative while he performed the function of vice director of the Institute, in charge of extramural studies.

[7] According to government regulations concerning philological studies curricula should include a 30 hour IT course. The content of the course should include: the basics of IT, text editing, spreadsheets, databases, managerial and/or presentational graphics, online services, acquisition and processing of information –they should constitute a properly selected subset of information included in the modules required in order to achieve the ECDL– European Computer Driving Licence. Apart from the fact that successfully conveying all this knowledge and skills (e.g. the skill of spreadsheet and database management) within 30 hours would border on a miracle (especially in the cases of teaching total beginners), unfortunately there is nothing in the regulations related to security measures during use of the internet, which would undoubtedly be more useful and practical knowledge.

not appear to need new technologies in their didactic work, nor do they display the will to be better trained (Drews, 2008), justifying the fact by lack of motivation, low level of salaries, a lack of funds for training, and a surplus of work duties either at school or caused by the national Teachers Charter system of teacher promotion.

The problem of dangers stemming from the use of the Internet is undoubtedly important, because, despite the gradual growth of internet access, there are still some users who find it difficult to handle even the most basic functions of an email box (such as sending and receiving attachments), or manage ordinary text editing. It seems hard to believe (especially in the case of professions requiring continuous textual work), however this is still the reality. It does not only involve, as it might seem, older internet users, but is the case regardless of age. Therefore, it should come as no surprise that such persons will not be aware of dynamically developing cybercrime techniques.

The later part of this article contains a presentation and a short description of the most important dangers discussed during the aforementioned subjects and courses. It is followed by an enumeration of the means of avoiding the dangers. Unfortunately, due to the rate at which the phenomenon is developing there are no experts or fully up-to-date scientific publications, nor are there any in-depth studies of the topic that can keep pace with the constantly changing and surfacing new strategies, methods and techniques of say spamming. Thus, it is quite understandable that the phenomena closely related to internet activity, such as spamming, hacking and their varieties, whose existence began with the existence of the internet, were also first defined there (it is possible the authors of the definitions were themselves involved in spamming and hacking). Therefore, the following information will be largely based on sources found in the Polish and English sites of the free encyclopaedia Wikipedia.

2. Spamming

The term spam refers to unwanted and usually useless mail sent by means of email, newsgroups on the usenet (USEr NETwork)[8], as well as through internet communicators (instant messengers) such as Gadu-gadu, ICQ etc. It may also be propagated through search engines such as Google or Bing, blogs (blog spam, blam), Wikipedia, online advertisements (online classified ads spam), internet discussion forums, social portals, web programmes and peer-to-peer/P2P platforms used for file sharing (file sharing network spam), or online games. It also may be transmitted through fax, TV commercials,

[8] The worldwide system of newsgroups which may be used online.

or even information transferred by means of mobile phone texts (SpaSMS). The most characteristic feature of spam is the fact that it is a message sent *en masse* to undefined users, regardless of its content. In order for a message to be classified as spam it needs to fulfill three conditions:

- the content of the message has no relation to the identity of the recipient,
- the recipients have not expressed their agreement to receive the message,
- on the basis of the message's content it may be concluded that the sender may obtain benefits disproportionately larger than the recipient in consequence of sending of the message.

The origin of the word spam is interesting. It is a name of a very popular tinned luncheon meat, produced since the 1930's by an American company "Hormel Foods". The product used to be called Hormel Spiced Ham before the current name was adopted. The abbreviation was most likely coined on the basis of Spiced Ham or on the basis of the description of the tin's content source – Shoulder Pork and Ham. The product became especially popular during the 2nd World War. The circumstances of the name being first used for unwanted email are not known precisely, however, one of the hypotheses which is most often quoted is connected with a popular sketch by the famous comedy group "Monty Python's Flying Circus", from 1970. In one sketch a client inquiring about a restaurant menu learns that every dish included in the menu contains spam and there is no possibility of ordering anything without it, despite the outcries of the wife: "I don't like Spam!". The name of the product is repeated dozens of times in the sketch, with a culminating point when a group of Vikings sitting in the restaurant (as per the absurd style, characteristic of this now legendary comedian group) intones a song: "SPAM, SPAM, lovely SPAM, wonderful SPAM", drowning any further conversation and ending the scene[9].

There are two major types of spam sent via email:

- unsolicited commercial or advertising email (illegal in many countries, including Poland and the EU countries, on the basis of an EU directive);
- unsolicited non-commercial bulk email, e.g. social, charity, religious or political organisation appeals.

A third, and probably the largest, group of spam messages should also be distinguished. It only ostensibly belongs to the second of the above groups. Its content is not as important as the eventual desired reaction of the recipient (usually consisting of entering a website whose address is included in the content), which may bring benefit to the sender and the achievement

[9] Sketch available at YouTube: http://www.youtube.com/watch?v=anwy2MPT5RE.

of the goal. Mails which belong to this group are of various, more or less suspicious content, such as offers of fake versions of original products (e.g. brand watches), software, computer games, pharmaceuticals (most often medications increasing men's potency), diplomas from renowned universities (usually American), invitations to internet matrimonial agencies (in most cases Russian, or generally Eastern European), to erotic sites, or information about upcoming stock exchange events, which allegedly should bring great benefits to stock investors. Entering such a site is usually equivalent to downloading malicious software, discussed further in the later part of the chapter, which is automatically installed on the victim's computer and partially or fully takes over the computer without the user's knowledge of it. Computers which were thus acquired become botnets connected in a zombie network and start to work for the sender (spammer/hacker) in order to expand the sending of spam (without the owner/victim being aware of it) with the use of address books of their email programmes (email clients). The malicious software can also scan the content of hard disc drives in search of data regarding bank accounts, in order to enable the cybercriminal to rob the account or to obtain access to it later by means of phishing, discussed further below.

Chain email is another way for spammers to expand their databases of email addresses. The ones that pray on people's misery seem especially vile. Their chain emails which might be referred to as chains of sorrow or chains of bad luck are meant to evoke the recipients' pity. The mails include requests for funds in order to cover treatment for children (who are suffering from a serious, though not lethal, ailment) or a person undergoing rehabilitation (e.g. after receiving burns[10], following a serious operation etc.). The funds are supposed to be raised only as a result of forwarding of the mail (the money is allegedly going to be transferred to the people in need by the mail operator as per each sent email[11]). The content of mail from such a group is usually formed in order to imitate a letter from the despairing parents of a sick child. It is often filled with moving expressions and conveys the deep piety of the sender. If the email is forwarded, the spammer obtains all the mailbox addresses which were used by their unsuspecting victims.

[10] The author received spam of such a content, with a request for funds in order to pay for the rehabilitation of a scalded child, five times in six years. Every time the information was identical (including the child's age: always two years old), with an invariable photograph (possibly even an authentic one) attached.

[11] Spam of such type usually ends with a statement: "It is only a click for you, but the parents get 3 cents for each email sent this way. The email contains an html script which counts the number of times the email was sent and the payment is made by a company which measures the efficiency of mailing as a form of marketing." It is obviously quite preposterous.

Chain prophecies are a different kind of spam. They usually come attached with colourful presentations filled with wise thoughts and philosophical sentences and/or various (rather positive) advice (e.g. "how to be a good person", "how to live in accord with other people"). They end with a promise of dreams coming true (in wealth, professional, private or other matters) and good fortune being within arm's reach if only the email is sent to as many people as possible (the more addressees, the greater the chance, or indeed guarantee, of the dreams materializing). Sometimes examples of alleged strokes of luck are included, emphasising that the amount of luck depends on the amount of further people addressed. Chain horrors are similar in essence though with an opposite psychological mechanism involved. They contain a threat of misfortunes which may befall the addressee if the email is not forwarded further. They also come with examples of people who underestimated the danger and had to face the consequences. Some chain emails may include both types of techniques. They may present examples of rewards obtained for forwarding of the mail, as well as punishments befalling the persons who failed to do so. In order to recognize a chain email, the assistance of an increasing number of websites may be of help, e.g. atrapa.net, which gather and review chain emails, as well as give instructions on means of their identification.

Urban legends are in many ways similar to chain mails. They come in the form of a story, whose content may be characterized by the following features, following atrapa.net:

- the action has taken place recently,
- the main character is the narrator, a relative, a friend, or – more often – "a friend of a friend",
- the story is presented as true, with events which supposedly really did take place,
- it spreads spontaneously – the readers become the writers and pass the story on,
- it undergoes modifications, new details appear, others disappear, the modifications often are aimed to adapt the story to a local environment,
- the original source is usually unknown, often impossible to establish,
- it contains emotional elements (often humorous or macabre), warns of the fatal consequences of behaviour contradictory to the rules or customs of the local community, confirms the anxieties and the dread of evil lurking all around.

Despite the name, the setting of an urban legend needs not be a city, although the usual source of the legends is found in the modern culture of urban areas. It appears that the term urban legend has a precise meaning, though it is often broadened to any hearsay, false convictions, strange beliefs, anecdotes and so on. Those legends containing elements of a horror story

resemble the frightful Halloween tales of the American tradition. It is possible that a story passed by word of mouth is written down – nowadays typed in and posted online, with the sacramental "pass it on to all your friends".

A different set of "false positives" goals is represented by spam which contains warnings of new dangerous viruses, and the means of preventing their attacks on the operating system. The information about the viruses is of course false and if the victim follows the instructions included in the mail, the results are contrary, usually deleting or damaging important system files, which consequently leads to an operating system breakdown. It is thus a malicious sabotage of the software of the gullible victim who believed in the warning.

The subject of spam (within the content or the attachment) may occasionally be generally useful. It may be the correct, virtually textbook instruction of CPR, including self-CPR, in the case of cardiac arrest or a cerebral stroke. They occasionally are authenticated by mails allegedly attached by distinguished medical universities or academies. The usefulness of the information, especially considering the scale of the occurrence of such ailments in modern society, may certainly have a more efficient effect on the recipient than other spam luring methods (promises of awards, threats etc.), and may consequently encourage the mail to be forwarded in good faith. Nevertheless, the danger and the damage caused by its forwarding is not smaller.

There is also harmless spam such as chain emails with humorous content. The most famous of such kind of spam harks back to the above type, as it is an email which feigns a virus without being one in fact (a computer virus hoax). It is most often referred to as the "Albanian virus", in some countries also known as the "Irish virus", the "Amish virus", the "hand virus", or the "honorary virus". The name "Albanian virus" stems from a demeaning assumption that poor Albania is too technologically backwards to educate programmers skilful enough to construct a real computer virus. For example: "Dear Recipient! I am an Albanian computer virus, however due to the poor state of my country's information infrastructure I cannot do you any harm. Please, delete a file and forward me". The "Albanian virus", in actual fact, may be considered a deliberate parody of the truly harmful and more refined spam discussed above. However, it could also be used by spammers in order to expand their address database.

Another type of spam, which has been sent since approximately 2005, is sent *en masse* to recipients in particular countries in translations prepared by free automatic online translators. It makes a comical impression and has little chance of gaining credibility. It usually contains an inept translation of a text with the original in English below. It could constitute, incidentally, an interesting object for linguistic studies, e.g. translation analysis. Spammers occasionally make the error of sending their messages to recipients

who live in countries utterly alien to the ones which were meant to be the target of the spam, e.g. spam in Chinese sent to addressees in Europe/Poland. This may well be a result of faults in their target search technology. Such spam is bound to fail and simultaneously works to the detriment of the world community of spammers and hackers, if such a community may be defined, and weakens its potential impact. It does have, though, (or at least it should have, for more intelligent internet users) a positive effect in the form of raising awareness of the scale and range of spam.

The CISCO System company, an American company dealing with Internet security, published a report in 2009 with a ranking of countries which were the sources of the most spam that year (in trillions):

Brazil	7,7
USA	6,6
India	3,6
South Korea	3,1
Turkey	2,6
Vietnam	2,5
China	2,4
Poland	2,4
Russia	2,3
Argentina	1,5

The global results of spamming include:

- ❑ blocking of internet lines and using up space on the hard drives of individual recipients;
- ❑ slowing down of servers which have to process spam;
- ❑ loss of time of internet users forced to read and delete spam, delays and difficulties in receiving "normal" email (due to antispam blocks or an overflowing mailbox), to the extent of overlooking genuine mail in the flood of spam;
- ❑ cost of spam prevention for internet operators, the offload of such a promotion costs (in case the spam is an advertisement) onto the internet operators and the end-recipients of mail, which makes it a form of extortion;
- ❑ infringement of privacy and security of the recipients, threatening moral, religious or other beliefs, e.g. by sending unsolicited messages with a vulgar, pornographic, or otherwise unsuitable content;
- ❑ causing the danger of virus or malicious software attack;
- ❑ decreasing public trust in electronic media in general.

The means of protection against spam and its varieties are:

- ❑ it is essential to install good antivirus and anti-spyware software before going online the first time;

- spam must definitely not be answered, even if one only means to send an angry reply, or wish to flood the intruder's mailbox with spam in return;
- in case spam is systematically sent from the same address, it is best to inform the administrator and use an antispam filter, e.g. add the sender to the "unwanted list";
- spam must not be reacted to positively – by granting the enclosed requests, or most of all by visiting any proposed internet addresses, disclosing one's personal information, or forwarding;
- the email client should have JavaScript and HTML turned off, while attachments must not be opened or emails viewed automatically[12];
- it is useful to install updates of the email client and/or use non-standard email clients. The most popular ones, although offering a similar level of protection, are prone to be attacked more often by Trojan horses constructed in such a way as to make the email client cooperate with them;
- if possible, the email address should not be disclosed. If it is posted at sites open to anyone (such as regular websites, internet forums etc.), it should be presented in a covert form, e.g. by means of exchanging the symbol "@" with another symbol or a set of characters ("$", "#", "at", e.g. "address[at]domain.eu"), by replacing the dot in the address with the word "dot" (e.g. "address@domain(dot)eu"), or by means of using other antispam textual insertions (e.g. "_cut_it_" or "_NO_TO_SPAMMERS_"). Falsyfying the addresses hampers automatic programmes (harvesters) which scan the internet searching for "@" signs. The insertions are best added at the end of the address (e.g. "account@domain.eu_cut_it"), as placing it before the domain name, though protecting the addressee, may leave the email operator vulnerable to the unwelcome load of spam. If it is necessary to write an email address without modifications, it is advisable to use a different email account, or an email alias for the purpose. A number of the mentioned insertions may nowadays transpire to be insufficient against constantly improving harvesters. As for now, publishing the email address in the form of a picture, instead of as text, is the most efficient technique for protection against harvesters. Webmasters may, on the other hand, take a better care of the users' safety and instead of publishing a list of email addresses they could introduce less convenient, but more secure contact forms.

[12] Automatic viewing of pictures in emails may have an identical result as clicking on links. The spammer's database is updated with the information that the mail address is active and the emails are read. In consequence, more spam may be sent to the address.

The methods of spamming which have been perfected over decades have evolved into a series of increasingly more refined and efficient varieties. The most important of them, especially the ones referred to by the name of scamming, are discussed in subsequent parts of the chapter.

3. Scamming

Scamming, also referred to as confidence trick, confidence game, or: bunko, con, flim flam, gaffle, grift, hustle, scheme, swindle, bamboozle, is a variety of spamming found mostly in the same media as spam, based on gaining the trust of a victim ("the mark") by a fraudster ("a confidence man", "con man", "confidence trickster", "con artist") or his associates ("shills"), and deceiving the message's recipient by means of information that the person has or may become a beneficiary of a particular wealth, e.g. a lottery prize (usually a multimillion amount in American dollars, British pounds or euros) which was gained because, say, the email address of the recipient was drawn in a lottery, or an inheritance was discovered. It may also suggest a large escrow or coax the recipient to engage in shady transactions. In the case of the "lottery prize", the victim is eventually required to disclose detailed personal data, bank account passwords, in order to "verify the data and make the money transfer". In effect the person may fall victim of a bank account robbery, e.g. through later phishing attack and/or by means of malicious software.

A case involving an escrow or inheritance is known as the "Nigerian scam", "Nigerian swindle", or "scam 419"[13]. Such a message is deliberately constructed in a way which suggests the addressee was chosen at random (the sender is not concealing it), or because of a similarity of the person's name to the name of the alleged bequeather. In one of the "Nigerian scam" varieties a swindler posing as a lawyer, a representative of a deceased person (usually in tragic circumstances, e.g. an airplane crash in Africa), openly proposes the inheritance be shared (usually split in half). It is usually a multimillion amount, in American dollars, kept at a closed bank account which belonged to the late person. Afterwards the hoaxer extracts money from the gullible victim under the pretence of alleged banking fees, bribes etc., which have to be paid in order to recover all the money from the departed person's account. The first mail is automatically generated. If there is a reply, then the following correspondence is conducted by a man, i.e., the scammer. The mails are made to look credible because they are addressed

[13] This is the number of the Nigerian criminal code which concerns the crime. The Nigerian Central Bank warned against this kind of fraud as early as in 1998. Examples may be found in the appendix.

to a specific recipient, i.e., an addressee whose name is often identical with the name of the accident victim in the mail's title and content, often with a correct form of address etc. The frauds even refer to authentic names of airplane crashes from the last decades (and on their basis the seuolers perform an internet search for potential relatives). They state precise information about the crash (a date, flight number, site of the crash, addresses of popular websites with information about the event). They also include real addresses of lawyers' offices (probably accomplices in the scam) with phone and fax numbers, business cards, emblems/logotypes, photographs, links to existing sites (authentic or more often fabricated), which all add credibility to the message. Such emails' content is usually written in correct English, in the language of formal correspondence. They occasionally are also filled with religious expressions (possibly depending on the target country). The mechanism of the psychological influence of such a type of scam is based on people's gullibility, the temptation of quick and easy enrichment, even if the money is of a shady origin (or downright criminal). Such a thought may be too strong a temptation even for people who believe themselves to be honest and righteous. It may be claimed that this is one of the most intricate scams, which makes it one of the most dangerous ones.

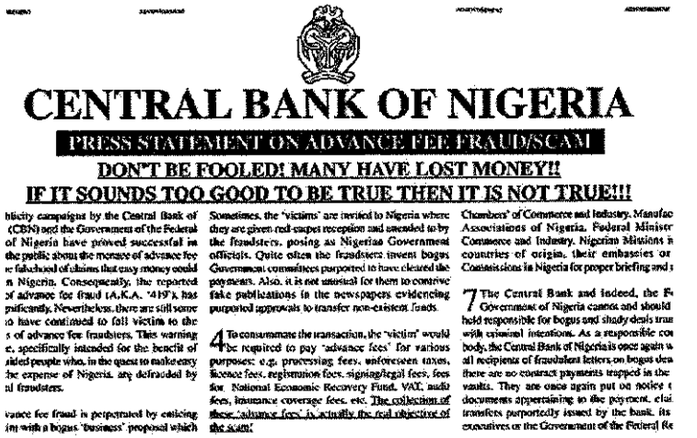
The second most popular kind of such scam emails are sent by an alleged widow, daughter or another relative (usually female) of a deceased or imprisoned important official from an African country, who managed to amass a multimillion fortune in hard currency or gold (currently frozen at a bank account) doing shady business (e.g. weapon deals with the USSR). Spam of this type first appeared in its current form already back in the 1980s. Since 2010 such emails have increasingly referred to a country not from Africa but from the Middle East, e.g. Kuwait, and the escrow sums may be slightly smaller presented in Euros and earned honestly, which makes them appear more real. Occasionally there are other scams, using the same mechanism, written allegedly by "terminally ill" millionaires themselves, who wish to share their fortune as they have no heir. Recently there have also been spams allegedly written by American soldiers serving in Iraq who purportedly found a fortune belonging to high officials in Saddam Hussein's regime, or even the fortune of the dictator himself, and who wish to share it with the addressee on a similar basis.

The same basic mechanism is used by scam messages which offer matrimonial agency services (usually Russian), aimed mainly at men, as a result of which the victims' money is swindled in order to cover alleged travel expenses, lodgings and so on, related to the arrangements of a meeting with a candidate for a wife. In less refined varieties of such a scam a "starving", poor woman from Russia, or another post-USSR country, writes an email, complaining e.g. of "the lack of a stove which could keep her house warm" (since this should give the reader pause as to how such a person is able to

go online, therefore the email pre-emptively explains, for example, that the person can use the internet only at work). The woman continues to explain that she is begging for financial help (e.g. in order to buy a portable heater, which will enable her to endure the severe winter) from random addressees.

This method of fraud was known in the period between 1904 and 1911 (back then it was about help in collecting a ransom for an alleged Russian prisoner in a Spanish prison). According to snopes.com, around 1997, about 100 million dollars were extracted from American citizens within fifteen months with the use of this method. In extreme cases, as a result of such fraud there have even been cases of abductions and deaths of the scam victims if the gullible addressee decided to go on a long trip, e.g. to Nigeria or other indicated places, or resolved to search for justice on his own having discovered that he had been deceived.

Fig 1. The warning of the Central Bank of Nigeria against "scam 419" (Pręgowski, 2011).



CENTRAL BANK OF NIGERIA

PRESS STATEMENT ON ADVANCE FEE FRAUD/SCAM

DON'T BE FOOLED! MANY HAVE LOST MONEY!!

IF IT SOUNDS TOO GOOD TO BE TRUE THEN IT IS NOT TRUE!!!

hlicity campaign by the Central Bank of (CBN) and the Government of the Federal of Nigeria have proved successful in the public about the menace of advance fee e fabricated claims that easy money could n Nigeria. Consequently, the reported of advance fee fraud (A.K.A. "419"), has pitifully. Nevertheless, there are still some to have continued to fall victim to the s of advance fee fraudsters. This warning e, specifically intended for the benefit of sided people who, in the quest to make easy the expense of Nigeria, are defrauded by al fraudsters.

vance fee fraud is perpetrated by enticing im with a bogus "business" proposal which

Sometimes, the "victims" are invited to Nigeria where they are given red-carpet reception and attended to by the fraudsters, posing as Nigerian Government officials. Quite often the fraudsters invent bogus Government committees purported to have cleared the payments. Also, it is not unusual for them to contrive fake publications in the newspapers evidencing purported approvals to transfer non-existent funds.

4 To consummate the transaction, the "victim" would be required to pay "advance fees" for various purposes: e.g. processing fees, unforeseen taxes, license fees, registration fees, signing/legal fees, fees for National Economic Recovery Fund, VAT, audit fees, insurance coverage fees, etc. The collection of these "advance fees" is actually the real objective of the scam.

Chambers" of Commerce and Industry, Manufac Associations of Nigeria, Federal Ministr Commerce and Industry, Nigerian Missions i countries of origin, their embassies or Consulates in Nigeria for proper briefing and

7 The Central Bank and indeed, the F Government of Nigeria cannot and should hold responsible for bogus and shady deals tran with criminal intentions. As a responsible co body, the Central Bank of Nigeria is once again w all recipients of fraudulent letters on bogus dea there are no contract payments trapped in the vaults. They are once again put on notice documents appertaining to the payment, clai transfers purportedly issued by the bank, its executives or the Government of the Federal Re

4. Examples of social engineering: phishing and pharming

The mechanism of social engineering, with phishing as one of its basic methods (another name for phishing is spoofing), is one of the most refined fraud varieties. It is based on impersonating a person or an institution of trust (e.g. a computer scientist, a network or bank administrator, etc.) in order to perform a swindle and gain a material benefit. Online social engineering (SE) may be accompanied by telephone methods. There is also a text message form of phishing, called SMiShing.

The basic assumption of social engineering is the fact that a human is most often the weakest link of any security system. Instead of using

advanced technologies in order to break into a particular system, it is sometimes easier to gain access to it directly from its employee by means of deception. Kevin Mitnick is the man considered to be the creator of this kind of attack. He is also believed to be the "godfather of hacking". As he once wrote about himself in one of his publications (2004: 4), "it is much easier to trick someone into giving a password for a system than to spend the effort to crack into the system".

According to Mitnick (2003), an attack by means of SE comprises of four cycles:

1) searching for information – gathering information related to the attack,
2) gaining trust – considers persons who are to be the source of information,
3) using trust – e.g. in order to gain an unauthorised access to the system,
4) obtaining information – acquiring confidential information or an access to resources to which the intruder is not entitled.

The aim of phishing is gaining a financial benefit by means of extracting of data, authentications, passwords from a victim, with the aim of overtaking an email account, and consequently using it for further sending of spam, and/or gaining access to a bank account, credit card etc., in order to rob the financial assets. Phishing in such a form has an individual dimension, it concerns an individual victim. The mechanism employed on a larger scale may be used for breaking into bigger, corporate computer systems, invigilation and confidential, secret or other data theft, which would force the company to bear the costs of repairing the damage done by such saboteur activity, or put the company in danger of losing credibility and stock value, to the extreme point of bankruptcy. At the level of public administration, the method of phishing may threaten state security and be considered espionage.

Banks and internet auctions are popular targets of attacks by means of phishing. Such an attack is usually based on sending spam to a large group of potential victims directing them to a website which looks indistinguishably similar to a bank website, while in reality it serves the purpose of intercepting of data submitted by the victim. Another typical way of extracting data is information about an alleged danger of an account's expiration and the need of its reactivation (which involves providing confidential data of various kinds, including the account password), or about the overflow of the mailbox on the operator's server. In both cases a phisher provides an active link to a website whose address looks correct at first glance. However, it contains small differences which are easy to overlook, e.g. www.paypai.com instead of www.paypal.com.

The term phishing is most often deciphered as **password harvesting fishing.** It was reportedly coined in the middle of the 1990s by crack-

ers who attempted to steal accounts at the popular AOL site (America OnLine). A different theory claims that the term originated from the surname of Brian Phish, who allegedly was the first credit card thief in the 1980s who used psychological techniques. According to yet another theory, Brian Phish was a fictional character used by spammers to identify each other. The term phishing could have also been inspired by another term –phreaking (phone + freak)– a different, older method of telephone network security breakings, usually in order to obtain a free or a cheaper telephone connection.

Example 1.[14]

> Attn: Edu User
> This is to inform you that we are would be performing mentainance on our web database and this might cause some damages to your mail usage, to avoid your mail account from been affected, you are advised to reply to this mail with your valid password attached as this is to prove that your edu account is still in use and also we need to upgrade your Edu account. Please coporate with us and provide your password here: {.....}. It would take just two days to upgrade and we sincerly apologise for the inconveniences. Thank you for using Edu.

Example 2.[15]

> Dear AMU mail User,
> Due to congestion in all UAM!web mail users accounts, Uniwersytet im. Adama Mickiewicza w Poznaniu be shutting down some unused web mail account. In order to avoid the deactivation of your web mail account, you will have to confirm that is a present use account by clicking the secure Link Below. The personal information requested is for the safety of your account. Please leave all information requested.
> click here : secure login
> https//accoun.amu.edu.pl
> Web Upgrade Team
> © Uniwersytet im. Adama Mickiewicza w Poznaniu, ul. Wieniawskiego 1, 61-712 Poznań

The content of the emails representing this kind of phishing is sometimes less sophisticated and detailed, less meticulously constructed, and aimed probably at more gullible recipients, as the following example illustrates.

[14] The original spelling was retained.

[15] The dangerous links from the addresses included in the following content were removed. Judging from the lax text edition and a different font used to write the university name, the content was constructed universally, in order to enable using a name of any university. In the alleged administration panel website address there is a deliberate error ("accoun" instead of "account"), which the recipient may overlook at first glance.

Example 3.[16]

> You have exceeded the storage limit on your mailbox. You will not be able to receive new mail until you upgrade your email quota.
> Click on the below link to fill the account upgrade form.
> http://beam.to/webmaster-Account.upgrade.Form
> System Administrator 192.168.0.1

Pharming is a more dangerous, and also more difficult to detect, form of phishing. It is an attack method within the framework of SE, based on redirecting an internet user who has correctly typed an address to a false website which imitates the official one, usually a bank website, in order to extract data (passwords etc.), in order to rob the bank account, credit card etc. The name is a result of combining the words phishing and farming.

In order for a correct URL (Uniform Resource Locator) to lead to a false website, another attack has to be performed first. Usually one of the two methods of such an attack is executed:

- an attack based on contaminating a global DNS (Domain Name System) server, in order to associate a real URL with a server containing a false website stealing confidential data.
- an attack with the use of trojans, which modify the user's system local files which are responsible for the initial URL name translation into a false IP (Internet Protocol) address, omitting the global DNS server.

In the vast majority of cases it is enough to use standard antivirus programmes with updated virus databases in order to successfully protect a computer from a pharming attack. There is also a growing number of programmes specializing in protection against pharming (the so called anti-pharming software), however, both the software as well as the term itself are controversial in IT circles. Its opponents believe the term pharming to be a marketing neologism which is used only to persuade banks there is a necessity to buy the new security packages.

The basic means of protection against phishing and pharming attacks is most importantly making sure whether the viewed website which requires confidential information is original, reliable and safe. In order to ensure the safety of the website, its SSL certificate (Secure Sockets Layer) should be checked. The certificate should be issued by the legal owner of the site. It may be checked by clicking on the padlock icon in the browser. It should be visible next to the address line while visiting such sites (bank sites etc.). Moreover, the address itself should begin with "https://" (Hypertext Transfer Protocol Secure).

A rather spectacular example of recent activity by means of the social engineering methods on a larger scale was the breaking into the intranet of

[16] The dangerous link was removed from the address.

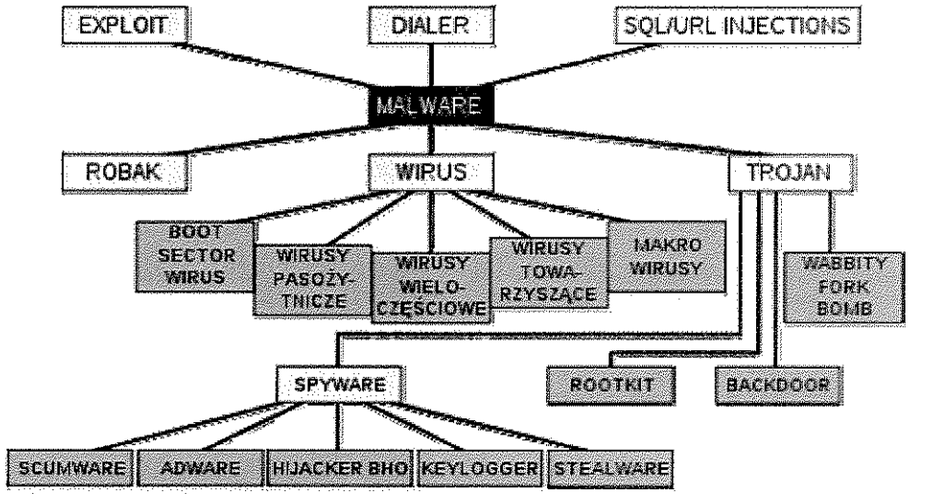
the Google company branch in China in 2010. During the attack, virus infected emails, with a specially constructed content, were sent to the employees – potential victims, whereas the senders were falsified. Unfortunately, there is little unclassified information on the matter; most probably any leaks were prevented by USA counterintelligence. For there are reports the attack could not have been successful without the aid of the Chinese intelligence cells.

5. Malicious software

The aforementioned spamming attacks may be accompanied by (or be the consequence of) the use of malicious software (malware) attached to a message either as a separate attachment or encoded within it, or even encoded within the message itself (the use of the HTML code conduces it). As a result, just receiving the message and opening it and/or its attachment may fulfill the spammer's goal, even without forwarding it further. The most popular kinds of malware, presented in the following chart, are briefly defined below.

Fig 2. Kinds of malicious software

(Malicious software, Wikipedia, 2011)



Kinds of malicious software are:

1. Virus – a programme or a fragment of a hostile code which attaches itself, overwrites or exchanges another programme in order to be reproduced without the user's consent. Due to various kinds of infections, the viruses may be divided into the following: boot sector viruses, parasitic viruses, multi-partite viruses, companion viruses, macro viruses.

2. Worms – malicious software similar to viruses, reproducing only online. Unlike viruses they do not need a "host" programme. They often replicate through email.
3. Wabbit – a resident programme which does not reproduce online. In effect of its activity one particular operation is performed, e.g. reproduction of the same file until the computer's memory resources are exhausted.
4. Trojan – it does not reproduce like a virus, however, its activity is equally harmful. It hides under a name, or within a file part, which seems useful. Besides the proper activity of such a file, the trojan performs background operations, harmful to the user, e.g. it opens a computer port which can be used as an entrance for a hacker attack.
5. Backdoor – takes over the control of an infected computer allowing certain administrative operations to be performed, including deleting and saving files. Similarly to a Trojan, a backdoor imitates other files and programmes which are often used. It enables the intruders to control the operating system through the internet. It performs its activities without its victim's knowledge or consent.
6. Spyware – software collecting information about a person or an organisation without consent. The information may include data on visited websites, passwords, etc. It often appears as an additional or hidden component of a bigger programme, immune to deletion or interference by the user. The spyware may perform operations without the user's knowledge – change the operating system register and the user's settings. Spyware may also download and run files from the internet.
   - ❑ scumware – a jargon, collective name for software which performs unsolicited operations in the computer,
   - ❑ stealware/parasiteware – software used for internet account robbery,
   - ❑ adware – software displaying advertisements,
   - ❑ Hijacker Browser Helper Object – browser plugins which perform operations without the user's consent.
7. Exploit – a code making it possible to directly break into the victim's computer. In order to introduce changes or take over the control of the computer, it exploits a loophole in the software installed on the attacked computer. The exploits may be used for attacking websites whose engines are based on script languages (a change of content or taking over of administrative control). They may also attack operating systems (servers and clients) or applications (office software, browsers or other software).
8. Rootkit – one of the most dangerous hacker tools. It is based on masking the presence of certain running programmes or system processes (usually related to the administration of the attacked system by the hacker). The rootkit is compiled into (in the of infected installation) or injected into essential system procedures. It is normally difficult to detect as it does not appear to be a separate application. The installation of a rootkit is usually the last step after breaking into a system which is to be infiltrated or from which data is to be stolen.
9. Keylogger – scans and saves all the keys pushed by the user. Due to its activity, addresses, codes, passwords, and other precious information typed by the user may be captured. The first software keyloggers were visible in the operating environment of the user. Nowadays they are increasingly often invisible to the administrator. There are also keyloggers which are hardware instead of software.
10. Dialer – a programme connecting the computer with the internet through a different access number than the one chosen by the user. Usually it is an expensive commercial service or a foreign number. Dialers may only cause damage to the owners of analogue and ISDN digital telephone modems. They appear mainly on erotic websites.

Less malicious software includes:

- ❑ false alarms concerning purported, new and dangerous viruses (false positives); a false alarm is also an alleged discovery of an infected file, which may occur due to the activity of antivirus software with the highest level of heuristic analysis,
- ❑ computer pranks, usually played on beginner, unaware computer users.

Below there is an example list of the most popular software used for the detection of spyware, adware, trojans, keyloggers, programmes scanning network ports, or programmes used to perform DoS type attacks, which may be active in the operating system without the users knowledge of the fact:

- ❑ Ad-Aware
- ❑ Anti Keylogger
- ❑ a-squared Free
- ❑ AVG Anti-Spyware
- ❑ CounterSpy
- ❑ Emsisoft Anti-Malware
- ❑ PestPatrol
- ❑ Spy Sweeper
- ❑ Spyware Doctor
- ❑ Spybot Search & Destroy
- ❑ XSpy Shield Gold

6. Hacking/cracking

Spammers and people using other, aforementioned forms of harassment via email or other forms of internet mediated communication, often belong to one of the following hacker groups (in most cases to the first one). The

following kinds of hacking are generally distinguished (with the names analogous to the classical western film stereotypes of recognizing the positive or the negative character by the colour of his hat[17]):

- *black hat* (acting on the borders of the law or clearly outside it),
- *white hat* (acting fully legitimately),
- *grey hat* – crackers (acting partly both ways).

One of the most spectacular recent examples of hacker activity on a massive scale were the attacks of the "Anonymous" organisation[18] –one of the biggest anarchy hackers organisations in the world– referred to as operation "Payback", conducted on 9-10.12.2010, aimed, among others, at the Visa and Master Card websites. It was meant to be the hackers' revenge for hindering the activity of Wikileaks, where, since December 2010, thousands of secret documents were revealed, including diplomatic papers, notes and correspondence of the USA administration and diplomacy employees (over 200,000 documents, including 972 dispatches concerning Poland). The documents contained information compromising, or at least inconvenient, to the USA diplomacy, e.g. opinions on heads of countries (their personal features, habits, weaknesses, matters which should rather be mentioned in private conversations, as well as those more sensitive, which should be avoided at all etc.), relations with the particular countries, and other vital data.

7. Means of protection

Besides the aforementioned means of protection against spamming and its derivatives, the basic principles of safe internet use may be put as follows. The following operations are among the most important means of internet danger prevention:

- installing antivirus and antimalware programmes,
- constantly updating their databases,
- regular antivirus and antimalware scanning of all hard drives,
- employing network firewalls,
- "hygiene" while using the internet and email (discussed in detail in part 2 of this chapter),
- checking the data transfer encoding while making online payments (HTTPS).

In conjunction with the line of reasoning put forward in this chapter, a few more remarks may be added to the above list: education of citizens,

[17] There is no agreement to this classification among the IT community.

[18] The group announced its intention of attack on the popular social portal "Twitter" one hour before.

especially educators, concerning awareness of dangers and the means of avoiding them, ideally starting from the level of primary education, which would hence involve teacher studies.

In case there is a suspicion of a spammer/hacker attack, a service administrator (email administrator, post office, bank, internet auctions etc.) should be immediately informed. The passwords to one's accounts should also be changed without delay. The passwords themselves, increasingly more numerous, at email services, social portals, instant messengers, internet forums, online libraries, should also be handled according to a few basic rules. The PCWorld.pl website, published along a paper computer magazine, enumerates five most typical errors made during password creation (after Daszkiewicz *et al.,* 2010), and presents the means of avoiding them.

Error 1 – the password is too short, it may be quickly broken

Internet users usually choose passwords which are too short, as they are easier to remember. Unfortunately, the easier it is to remember, the less safe it is. The following estimation demonstrates how long it takes for a password to be broken by force. The force breaking is an operation of a programme which attempts to guess the password by way of gradually testing all possible combinations. Let us assume the password is six characters long, with the characters being only lower case letters. It means there are 26 characters to choose from. Considering the length of the password, it equals 308 915 776 combinations (26 to the power of 6). This seems a large number. However, a modern computer with a fast processor is able to break such a password within just 10 seconds.

A safe password should be at least eight characters long. Moreover, it should contain both small and capital letters. To break such a password by means of force would take approximately two months. Every single character more, or employing symbols of different types (digits, punctuation marks, and other special characters), dramatically extends the time necessary to guess it.

In the case of using the password abroad it is better to forgo the special characters (at least temporarily) or at least make sure which keyboard-shortcuts are used for the characters in the particular country.

Error 2 – the password is too simple, it may be quickly broken

The password is too easy to break because it is a word which can be found in a dictionary (of any language). The length of the password in such cases is a secondary matter. The easiest way of breaking such passwords is a "dictionary attack". The method of such an attack is similar to force breaking, however, the elements tested are not characters but words contained

in a dictionary file. Even a personal computer of an average computing power would not need long to test an entire dictionary of an average size.

The dictionary file may contain regular words with a list of numbers. Therefore, it is not advisable to use, for example, a date of birth as a password. Passwords created according to a certain model are equally easy to break. Thus, it is prudent to avoid chains of characters such as 12345, qwerty (characters next to each other on the keyboard), or abcdef. Ideally a good password should not be found in any dictionary, which means it should be void of any sense.

Error 3 – the password is written down on paper or digitally

Even the best password may become useless if it has been written down in an form which is not enciphered, anywhere on the hard drive. It may be spotted by a hacker or by malware. Some users even send their passwords to their mailbox, so as to be able to use them wherever they may be. Others write them down on a piece of paper, where they may be read by an unauthorised person.

It is best to remember all the passwords. This may be difficult if the passwords are remarkably difficult. If one wants to keep them on the computer, a special password manager should be used, working as a special safe. Passwords gathered in it are enciphered, and thus safe from theft. The safe itself is protected with a main password. This should be especially secure, as it is the only defence protecting other passwords. Moreover, the main password must not be written down anywhere. It also, naturally, must not be forgotten, otherwise all the other passwords would become inaccessible, as the main one would be nearly impossible to break. In order to store the passwords safely, certain free software may be used, such as KeePass Password Safe Professional 2.10, or KeePass Password Safe 1.17. It works with the Windows XP, Windows Vista and Windows 7 operating systems.

Error 4 – using the same password for years

Many users have employed the same password for many years. This is very risky as it may be detected by an aggressor at some point, without the user's being aware of it. In such a case the hacker would have an unlimited access to all the password protected data and may, for example, read the victim's correspondence for many months. According to the PCWorld questionnaire (2008), over 39 percent of internet users never change their passwords, whereas another 34 percent do it very rarely.

Passwords should be changed regularly. It requires a degree of creativity. It may be then advisable to use a password generator. Such a tool may be found in the aforementioned KeePass Password Safe programme. The

programme will automatically generate a new safe password for it. In order to see the password in an unmasked form, an icon next to the password window should be clicked. A few more clicks lead to the generating of new possible passwords. The conditions which a new password must meet may be configured in a special menu. Using of special characters is a possible option too.

Error 5 – using the same password to all accounts

With the growing number of services which require passwords in order to log in, such as mailboxes, the operating system, ZIP and RAR archives, social portals, internet forums, instant messengers and so on, a very large number of passwords to remember may amass. It is a relatively common error to use the same password for all of such services. It is convenient, as there is only one password to remember. However, if anyone manages to detect it, spot it, steal it, or break it, a large loss may be endured. An aggressor would simultaneously obtain access to all the services of the user, including the ones which may contain confidential, enciphered data. Hackers are used to testing the passwords they have already obtained at other services of the user, where logging in is required.

As a resut, one password should not be used for many services. Each login should be accompanied with a different password. In order to be able to remember them, the passwords should be kept in a special password manager, such as e.g. the mentioned KeePass Password Safe.

To sum up, an unbreakable password is long, i.e., eight characters is an absolute minimum. It should contain both lower and upper case letters, as well as digits and special characters. Passwords from dictionaries should be avoided. It is best to use a password generated by a special password generator (e.g. the KeePass Password Safe programme). Under no circumstances should the passwords or any other access codes be written down in an overt form on a hard drive. They must also not be written down on a piece of paper, as they may be espied by unauthorised persons. Moreover, our passwords should be changed every few weeks.

The ESET company (a producer of antivirus software) presented another nine rules of creating passwords which are easy to remember (Sobiech, Makosz, 2011: 66):

- Join and intertwine letters of two words, using lower and upper cases, e.g. "purple pottery" = PpUoRtPtLerEy.
- Intertwine letters of any word with digits, e.g. "flash 9708" = f9L7a0s8H
- Join two words, using any symbol as a connector, e.g. PurPl-EpTtery.
- Use special characters in the password (!@#$%).
- Create the password with a deliberate mistake, e.g. bread = BraEd.

- ❑ Use upper case letters in unconventional places, e.g. mAnchEstEr.
- ❑ Create a password as a blend of initial letters of words forming a longer sentence, e.g. IMioT (Iron Maiden is on tour).
- ❑ Exchange letters with digits – E=3, A=4, T=7 etc., e.g. K4$74 (kasta).
- ❑ Do not use the same password for numerous services or computers.

8. Concluding remarks

Foreign language teachers, attacked by a hacker, may undergo certain private losses, nevertheless, there is little chance their workplace would be in danger of Social Engineering attacks (schools usually are not targets which would be attractive enough for hackers[19]). However, philology studies graduates, including would-be teachers, who find employment at large corporations (e.g. banks, as translators or office workers), may inadvertently cause a lot of trouble to their employers should they be unaware of the dangers of SE.

The weakest link in security systems, the one most vulnerable to Social Engineering attacks, is still the human. Thus, an elementary education in the field of safe internet use for an individual could turn out to be the way to ensure global security. The educational system, on all levels (including the philology studies), provides the means to achieve it. This should not be underestimated. Consequently, well qualified instructors, teachers, and lecturers, who pass the necessary knowledge on in a professional and reliable way, should be made available.

Works Cited

- Drews, Marcin. (2008). „Gry komputerowe a analfabetyzm funkcjonalny i informacyjny". In: Augustyn Surdyk, Jerzy Zygmunt Szeja (eds.). (2008). *Kulturotwórcza funkcja gier. Gra w kontekście edukacyjnym, społecznym i medialnym. Homo Communicativus* 2(4).
- Kasprzycki, Dariusz. (2005). *Spam, czyli niezamawiana komercyjna poczta elektroniczna: zagadnienia cywilnoprawne*. Kraków: Uniwersytet Jagielloński.
- Kennedy, Amgus J. (1999). *Internet*. Trans. Joanna Białko, Piotr Fraś, Piotr Goraj. Bielsko-Biała: Pascal.
- Miller, Samantha. (2003). *E-mailowy savoir-vivre*. Trans. Jolanta Kasprzak-Śliwińska. Poznań: Dom Wydawniczy Rebis.
- Mitnick, Kevin, Kasperavičius, Alexis. (2004). *CSEPS course workbook*. Henderson, NV: Mitnick Security Publishing.
- Mitnick, Kevin, Simon, William L. (2003). *The art of deception: Controlling the human element of security*. Indianapolis: Wiley Books.

[19] It may be an easy "training" target for the so called script kiddies, i.e., juvenile hackers-amatours.

- Mitnick, Kevin, Simon, William L. (2005). *The art of intrusion: The real stories behind the exploits of hackers, intruders & deceivers*. Indianapolis: Wiley Books.
- Zdziarski, Jonathan N. (2006). *Spamowi Stop! Bayesowskie filtrowanie zawartości i sztuka statystycznej klasyfikacji języka*. Trans. Leksem. Warszawa: PWN.

Internet sources[20]

- IS 1: Advance-fee fraud, http://en.wikipedia.org/wiki/Advance-fee_fraud
- IS 2: Chain letter,http://en.wikipedia.org/wiki/Chain_letter
- IS 3: Companies Fail DefCon Social Engineering Security Test, eSecurityPlanet.com, http://www.esecurityplanet.com/features/article.php/3896386/Companies-Fail-DefCon-Social-Engineering-Security-Test.htm
- IS 4: Computer hacking, http://en.wikipedia.org/wiki/Computer_hacking
- IS 5: Cyberterrorism,http://en.wikipedia.org/wiki/Cyberterrorism
- IS 6: Cyberterroryzm, http://pl.wikipedia.org/wiki/Cyberterroryzm
- IS 7: Education in 2008/2009 School Year, (2009). Statistical Information and Elaborations, Warszawa: Central Statistical Office, http://www.stat.gov.pl/cps/rde/xbcr/gus/PUBL_e_oswiata_i_wychowanie_2008-2009.pdf
- IS 8: Education in 2009/2010 School Year, (2010). Statistical Information and Elaborations, Warszawa: Central Statistical Office, http://www.stat.gov.pl/cps/rde/xbcr/gus/PUBL_e_oswiata_i_wychowanie_2009-2010.pdf
- IS 9: Exploit (computer security), http://en.wikipedia.org/wiki/Exploit_(computer_security)
- IS 10: Exploit, http://pl.wikipedia.org/wiki/Exploit
- IS 11: Granger, S., (2001). Social Engineering Fundamentals, Part I: Hacker Tactics, http://www.securityfocus.com/print/infocus/1527, http://www.knowyourenemy.eu/attachments/File/NsP-docs/CompleteSocialEngineeringDoc.pdf
- IS 12: Hacker (computer cecurity), http://en.wikipedia.org/wiki/Hacker_(computer_security)
- IS 13: Haker, bezpieczeństwo komputerowe, http://pl.wikipedia.org/wiki/Haker_(bezpiecze%C5%84stwo_komputerowe)
- IS 14: Haker, slang komputerowy, http://pl.wikipedia.org/wiki/Haker_(slang_komputerowy)
- IS 15: Idą święta – uważaj na oszustów w sieci, (2010). http://tech.wp.pl/kat,1009779,title,Ida-swieta-uwazaj-na-oszustow-wsieci,wid,12918700,wiadomosc.html?ticaid=1b5fb
- IS 16: Inżynieria społeczna (informatyka), http://pl.wikipedia.org/wiki/In%C5%BCynieria_spo%C5%82eczna_(informatyka)
- IS 17: Kevin Mitnick,http://en.wikipedia.org/wiki/Kevin_Mitnick
- IS 18: Kevin Mitnick, http://pl.wikipedia.org/wiki/Kevin_Mitnick
- IS 19: Krakowiak, I., (2010). Czy można rozpoznać sztuczki inżynierii społecznej, http://www.idg.pl/news/360704/Czy.mozna.rozpoznac.sztuczki.inzynierii.spolecznej.html
- IS 20: Łańcuszek internetowy, http://pl.wikipedia.org/wiki/%C5%81a%C5%84cuszek_internetowy
- IS 21: Malware, http://en.wikipedia.org/wiki/Malware

[20] All sites accessed on 15th March 2011.

- IS 22: Nigeryjski szwindel, http://pl.wikipedia.org/wiki/Nigeryjski_szwindel
- IS 23: Pharming, http://en.wikipedia.org/wiki/Pharming
- IS 24: Pharming, http://pl.wikipedia.org/wiki/Pharming
- IS 25: Phishing, http://en.wikipedia.org/wiki/Phishing
- IS 26: Phishing, http://pl.wikipedia.org/wiki/Phishing
- IS 27: http://www.pcworld.pl/news/356910_1/Piec.najczestszych.bledow. przy. tworzeniu.hasel.html
- IS 28: Pręgowski, M., P., (2007). „Nigeryjski przekręt" z Putinem w tle, http:// technoblog.gazeta.pl/blog/1,84947,4648026.html
- IS 29: Rusiecki, P. (2007). „Internetowy aspekt inżynierii społecznej czyli nieautoryzowany dostęp do zasobów informatycznych przedsiębiorstwa". In: *Teoretyczne podstawy tworzenia SWO i strategie budowy e-biznesu.* 231-238. http:// swo.ae.katowice.pl/_pdf/133.pdf
- IS 30: Sawyer, J., H. (2010). Real-world attacks with social engineering toolkit, DarkReading.com, http://www.darkreading.com/blog/227700548/real-world-attacks-with-social-engineering-tookit.html
- IS 31: Seltzer, R. (2011). The Serge Solovieff mystery – a WWI variant of the Spanish Prisoner scam, http://www.samizdat.com/solovieff.html,
- IS 32: Scam, http://pl.wikipedia.org/wiki/Scam
- IS 33: Scamming, http://en.wikipedia.org/wiki/Scamming
- IS 34: Social engineering (security), http://en.wikipedia.org/wiki/Social_engineering_(security)
- IS 35: Spam, http://pl.wikipedia.org/wiki/Spam
- IS 36: Spamming, http://en.wikipedia.org/wiki/Spamming
- IS 37: Sysło, M.M. (2011). „Technologia informacyjna w edukacji", http://www. snti.pl/snti/files/ti_w_edukacji.pdf
- IS 38: System argentyński: Nie daj się oszukać naciągaczom finansowym, Bankier. pl, (2011). http://www.bankier.pl/fo/kredyty/multiarticle.html/910448,1,poradnik.html
- IS 39: Web bug, http://en.wikipedia.org/wiki/Web_bug
- IS 40: Wirus albański, http://pl.wikipedia.org/wiki/Wirus_alba%C5%84ski
- IS 41: „Wypowiedzieli wojnę <<zdrajcom Wikileaks>>", (2010). http://www. tvn24.pl/12691,1685462,0,1,atak-hakerow-nazdrajcow-wikileaks,wiadomosc. html
- IS 42: Złośliwe oprogramowanie, http://pl.wikipedia.org/wiki/Z%C5%82o-%C5%9Bliwe_oprogramowanie

Appendices[21]

1. An example of the "Nigerian scam" no. 1

Hi,

My name is Elena, I am 32 year and I live in Russian province. I work in library and after my work I allowed to use computer when it possible. I finded your email in internet and I decide to ask you for help.

[21] Authentic spam emails' content in its original form. For the sake of your own safety, please, make sure you do not follow the instructions included in the quoted emails, do not reply to them, and do not enter the websites whose links are included.

I have 7 year daughter, her father abandoned us and we live with my mother. Due to crisis my mother lost job and our situation became very difficult. Price for heating our home is very high and we cannot afford it anymore. The winter is coming and weather becoming colder each day. We don't know what to do and we very afraid. We need portable stove which give heat from burning wood. We have many wood in our region, but we cannot buy this stove in local market because it cost equivalent of 193 Euro and very expensive for us.

If you have any old portable wood burning stove, I pray that you can donate it to us and organize transport of its to our address or help us to buy it in our local market. This oven are different, they are from cast iron and weight 100-150kg.

I pray for your help and I hope that our situation will improve soon.

From all my heart I wish you a Merry Christmas and a Happy New Year.

Elena.

2. An example of the "Nigerian scam" no. 2

Avu 7 Rue 14 zone 3
Abidjan Cote D'ivoire
Africa.

Dearest one,

Grace and peace be multiplied unto you. I know my mail might be a surprise to you but never mind 'cause I'm contacting you in good faith. However, accept my sincere apologies if it doesn't meet your personal ethics, although there certain times in one's life that whether or not one indicates interest for certain assignment, people would still look up to him or her.

I am Mother Melanie Lizwelicha from Namibia. The survivor of Archdeacon Johnson Lizwelicha who untill his death on september 2006 after a brief illness served as an Archdeacon in the St.Micheal's Archdeaconry in Ivory Coast for nine years. We were married for eleven years though we hadn't issue. Since his death I decided not to re-marry at least for sometime.

When my husband was alive he deposited the sum of three million, seven hundred thousand Dollars ($3.7M) in a renown Bank here in Abidjan, Cote d'Ivoire (i'll give you the Bank details when I hear from you and more trust develops.) However, I've been staying in the hospital (Cancer center) for sometime now due to complicated cancer problem, and at present, my Doctor confirmed to me that I have little chance to life due to the nature and complications associated with the sickness, so I eventually decided to donate the fund to the Church where my husband served.

However, the Bishop of Korhogo (a town in the North-Central region) had recently received information that my late husband "Johnson" lived an immoral and lewd life, hence my donation was considered to be tainted since I inherited it from my husband. The Bishop now rejects it.

On this note, I've decided to donate this fund to a religious organisation, help foundation or a trust worthy individual who will utilize this money the way I am going to instruct herein.

I want the fund to be used on orphanages, disaster victims, helping the widows and the forgotten ones in the society. "Blessed is the hand that giveth" is a timeless message that has always been in my heart.

I took this decision because I don't have any child that will inherit this money and my health has taken a turn for the worse, and my husbands' brother who lives abroad is an atheist and doesn't care nor show any interest in the affairs of my family.

I am not afraid of death because I know where I am going. I want you to always pray for me also. My happiness is that I lived a worthy life.
Whosoever that wants to serve the Lord must serve him in spirit and truth. Please always be prayerful all through your life.
Looking forward to hearing from you.
Peace be unto you
Melanie.

3. An example of the "Nigerian scam" no. 3

-----Original Message-----
From: Habib Nurudine [mailto:habib.nurudine@luckymail.com]
Sent: Thursday, March 17, 2011 5:03 AM
To: undisclosed recipients:
Subject: AWAITING YOUR URGENT RESPOND PLEASE.

FROM THE DESK OF MR.HABIB NURUDINE.
DIRECTOR FOR FOREIGN REMITTANCE DEPT
AFRICA DEVELOPMENT BANK (ADB)
OUAGADOUGOU, BURKINA FASO.
CONFIDENTIAL PLEASE.

My name is Mr.Habib Nurudine,Director of foreign remittance Dept of africa development Bank(ADB) Ouagadougou Burkina faso. I have decided to seek a confidential co-operation with you in the execution of the deal described here-under for our both mutual benefit and hope you will keep it a top secret because of the nature of the transaction, During the course of our auditing, I discovered an unclaimed/abandoned fund, sum total of US$16,000,000.00 (Sixteen Million United States Dollars Only) in an account that belongs to one of our foreign customers Late Mr. Graham Gardner who died on 31 of May,2009 in the ill-fated Air France Flight 447 which crashed on its way to Paris from Rio de Janeiro Airport in Brazil;& lt; BR>& ;nbs p;& lt; A href="htt p://www.dailymail.co.uk/news/w%20orldnews/article-1190 034" target=_blank rel=nofollow> http://www.dailymail.co.uk/news/worldnews/article-1 190 034 /Air-France-flight-44 7

Now our bank has been waiting for any of the relatives to come-up for the claim but nobody has done that. I personally has been unsuccessful in locating any of the relatives, now I sincerely seek your consent to present you as the next of kin to the deceased so that the proceeds of this account valued at {US$16,000,000.00} can be paid to you for the benefit of both of us instead for this money to be return into my bank treasury as unclaim dividend.

All that I require from you is your sincere co-operation, trust and utmost confidentiality to enable us conduct this transaction successfully. I assured you that this transaction will be executed under a legitimate arrangement that will protect you from any breach of the law both in your country and here in Burkina Faso once the fund is transferred to your bank account. Upon your consideration and acceptance of this offer, please proceed immediately and send to me the following information.

-Your Full Name,
-Your Contact Address
-Your direct telephone Number
_Your occupation
_Your country.

This information will enable me to upload your data into our bank database to reflect in the bank network system that you are the named next of kin of this fund and I will guide you on how to open communication with the bank and make the claims for onward transfer of the fund to you, please note that we have few days to carry out this deal, Your kind rapid response is highly appreciated.

Thanking you in anticipation for your response.

My Dearest Regard,

Mr.Habib Nurudine.

3. An example of spam no. 1

Do you feel yourself defective while having no high education, but you are eager to change your job for something better? We know how to help you. There's no need to graduate from the University to get a prestigious job anymore. You can easily get a diploma you need just calling us by these phone numbers: 1-718-989-5740 (if you live in US) or +1-718-989-5740 (if you are calling from outside US). Best Universities, Masters' and Bachelors' degrees are available! Prove others that you worth something big and prestigious. Leave your contact data at the voice mail calling phone numbers pointed above and we will get in touch with you in a while to help you change your life for better!

4. An example of spam no. 2

Google Incorporation's.
Stamford New Road,
Altrincham Cheshire,
WA14 1EP
London,
United Kingdom.

Winning No: GUK/877/798/2010
Ticket No: GUK/699/33/2010
Google Verification Code: 947831
Notification Date: 05/11/2010.

GOOGLE 11TH ANNIVERSARY WINNING NOTIFICATION.

We wish to congratulate you once again on this note, for being part of our winners selected this year. This promotion was set-up to encourage the active users of the Google search engine and the Google ancillary services. Hence we do believe with your winning prize, you will continue to be active and patronage to the Google search engine. Google is now the biggest search engine worldwide and in an effort to make sure that it remains the most widely used search engine, we ran an online e-mail beta test which your email address won 550,000.00GBP {Five Hundred And Fifty Thousand Great British Pounds Sterling}.

We wish to formally announce to you that you have successfully passed the requirements, statutory obligations, verifications, validations and satisfactory report Test conducted for all online winners. A winning cheque will be issued in your name by Google Promotion Award Team, You have therefore won the entire sum of 550,000.00 {Five Hundred And Fifty Thousand Great British Pounds Sterling} and also a certificate of prize claims will be sent along side your winning cheque.

Sir. McClintock Gilbert
Foreign Transfer Manager
Google Security Department.
Email: customercaregoogle@winning.com

You are advised to contact your Foreign Transfer Manager with the following details to avoid unnecessary delay and complications:

VERIFICATION AND FUNDS RELEASE FORM.
(1) Your contact address.
(2) Your Tel/Fax numbers.
(3) Your Nationality/Country.
(4) Your Full Name/Sex.
(5) Occupation/Age.
(6) Alternate email if any.

The Google Promotion Award Team has discovered a huge number of double claims due to winners informing Close friends relatives and third parties about their winning and also sharing their pin numbers. As a result of this, these friends try to claim the lottery on behalf of the real winners. The Google Promotion Award Team has reached a decision from headquarters that any double claim discovered by the Lottery Board will result to the canceling of that particular winning, making a loss for both the double claimer and the real winner, as it is taken that the real winner was the informer to the double claimer about the lottery. So you are hereby strongly advised once more to keep your winnings strictly confidential until you claim your prize.

Congratulations from the Staffs & Members of the Google interactive Lotteries Board Commission.
Sincerely,

Dr. Donald Lloyd.
Google Promotion Award Team.

5. An example of scam no. 1
-----Original Message-----
From: Outlook [mailto:Service@live.com]
Sent: Tuesday, March 15, 2011 10:59 PM
To: undisclosed-recipients:
Subject: http://hilfrlof.com/owa.eu.dodea.edu/CookieAuth.dll/

COPY the link and Visit Our Web for more Updates If you could please take 2-3 minutes To get your account in perfect Secure line

6. An example of a chain message at a social portal no. 1
Facebook is recently becoming very overpopulated,there have been many members complaining that Facebook is becoming very slow. Records show that the reason is that there are too many non-active Facebook members and, on the other side, too many new Facebook members.

We will be sending this message around to see if members are active or not. If you are active please send to at least 15 other users using Copy+ Paste to show that you are still active. Those who do not send this message within 2 weeks will be deleted without hesitation to create more space.

Send this message to all your friends and to show me that your still active and you will not be deleted.

Founder of Facebook,
Mark Zuckerberg