DE GRUYTER OPEN

ICTE Journal

2015, **4**(2): 50–65
DOI: 10.1515/ijicte-2015-0009

ICT TEACHERS AND TECHNICAL E-SAFETY: KNOWLEDGE AND ROUTINES

Václav Šimandl,
Department of Informatics, Faculty of Education,
University of South Bohemia, Jeronýmova 10, České Budějovice, Czech Republic
simandl@pf.jcu.cz

Abstract

The article looks at how competent ICT teachers in primary, lower secondary and high schools are as regards the issues of Internet safety, the use of secure passwords, protection against malware and data back-up. Specific knowledge and routines are described whilst discussing the ways teachers are influenced in these areas.

In-depth semi-structured interviews have been carried out with chosen ICT teachers. Teachers were presented with several situations from the issue in question and the way they reacted in given situations was observed. Data gained from the interviews and the triangulation that had been carried out was processed through open and axial coding.

The results of our investigation show that teachers do usually try to behave in a relatively safe way but their reasons for such behaviour differ greatly. The main external determiners include reactions to a certain negative experience, active self-study of the issue and organised instruction (not only at high schools and universities but voluntary attendance of courses). Factors preventing teachers from behaving as safely as possible have been identified. It may be due to working or teaching limitations. Teachers might lack professional knowledge or there could be a problem with security, perhaps being time-consuming or difficult to remember passwords.

Keywords

ICT teachers, e-safety, routines, secure passwords, antimalware protection, data back-up, open coding, axial coding

Introduction

The issue of e-safety is of primary importance to both researchers and the general public. According to Barrow and Heywood-Everett (2006), e-safety is concerned with the protection of the user and his ICT against the negative elements that may arise while using ICT. Livingstone and Haddon (2008) summarised and categorised risks, ranking all of the following

negative features as elements of e-safety: exposure to illegal content, exposure to potentially harmful content, encountering sexual/violent/racist/hate material, misinformation, (problematic) user-generated content, challenging content (e.g. suicide, anorexia, drugs, etc.), contact with strangers, cyber-bullying, advertising/commercial exploitation, illegal downloading, gambling, giving out personal information, invasion of privacy and hacking. As the area of e-safety is relatively broad, this article will deal with a narrower area of so-called technical e-safety. This area includes the issues of malware, sharing personal data, identity theft, the drawbacks of email communication (spam, hoax, phishing) and computer crashes (Šimandl, 2013).

The following text will briefly deal with studies concerning the knowledge and routines of ICT users as regards e-safety, with an emphasis on technical e-safety. It is based on our previous research which is described in (Šimandl, Zelenka and Sadil, 2013).

Knowledge and routines of ICT users

A lot of studies have taken an interest in children and young people's knowledge and routines as regards e-safety. Cranmer, Potter and Selwyn (2008) say that primary school pupils are vulnerable at their age, aware of very few strategies to protect themselves from prevailing danger. In addition, many pupils struggle to understand the issue and are unable to assess danger in a rational way. Lower secondary level pupils lack the ability to comprehend and critically evaluate online content and manage their online behaviour (Symantec Corporation, 2010). Beránek (2009) claims that pupils are aware of real e-safety threats but they lack basic safety regulations and refuse to accept "adult rules". This seems to coincide with the opinion that users are most likely to feel that they will never be affected by problems of technical e-safety nature (Lang et al., 2009). McCormick and van Otterloo (2011) mention children aged as young as 10 to 13, claiming their online activity closely mirrors that of an adult, with them forced into complex social situations that require adult reasoning – well before they are ready.

Most adults are aware of the risks of using ICT but many of them do not know how to cope with the dangers or what good e-safety practice is. Many end users do not use technologies to reduce the risk of data loss or leak of confidential information, such as data backup, coding of content in confidential outgoing emails or checking incoming emails with an antivirus program (Lang et al., 2009; Steganos GmbH, 2008; Garrison and Posey, 2006; Symantec Corporation, 2009). Choosing and handling computer passwords seems to be a problem (Lang et al., 2009; Garrison and Posey, 2006; Teer, Kruck and Kruck, 2007), with only a few mobile devices adequately protected by passwords (Get Safe Online, 2010). While personal computers are likely to be protected by firewall, antivirus, antispyware and automatic operating system updates (Teer, Kruck and Kruck, 2007; Get Safe Online, 2010), only a small number of smartphone owners considered installing an antivirus program (Ponemon Institute, 2011). The need to focus on this issue is emphasised by the fact that most ICT users admitted to having experienced a cybernetic attack like a malware attack, phishing attack or identity theft (Get Safe Online, 2009).

The role of the school and teachers in avoiding e-safety risks

Due to the lack of knowledge, understanding and skills among various groups of adult ICT users (Byron, 2008; Becta, 2006), parents cannot be relied on to educate their own children in e-safety matters (Becta, 2006). According to Becta (2006), one of the basic conditions for eliminating e-safety risks is education and training. Livingstone and Haddon (2009) claim that schools are best placed to teach children the digital and critical literacy skills required to maximize opportunities and minimize risks. Schools should focus on education aimed at the safe and responsible use of ICT (Byron, 2008) and should carry major responsibility in teaching them the appropriate behaviour and critical thinking skills to enable them to remain both safe and legal when using the Internet and related technologies (Becta, 2005; Becta, 2007).

The role of the teacher seems to be crucial to ensuring children's e-safety. Teachers are required not only to provide children with knowledge of technical e-safety issues but also to bring them up to be responsible ICT users. Teachers are expected to set good examples for students with respect to such ICT issues as privacy, copyright, data backup, and virus protection (Buettner et al., 2002).

Despite the emphasis placed on schools and teachers, there has been no significant investigation into teachers' technical e-safety knowledge and routines, an exception being research concerning teachers' use of social network sites and their virtual friendships with pupils (Šimandl, Zelenka and Sadil, 2013). According to Livingstone and Haddon (2008), there is a need for research focused on the teacher's e-safety literacy and his ability to teach these topics (Spielhofer, 2010). It is also important to clearly define how teachers can be supported to teach this topic (Spielhofer, 2010). Teachers themselves claim their ICT colleagues should be responsible for e-safety education (Papavasiliou, 2009) so it would be suitable to focus on them. Furthermore, the urgent need for research of this kind within the Czech school system is supported by the fact that not even a quarter of all ICT teachers are actually qualified to teach the subject (Rambousek et al., 2007).

Study of the knowledge and routines of ICT teachers as regards technical e-safety

Due to the lack of evidence on the knowledge and routines of teachers in the matter of technical e-safety, we have carried out research in this area. Its aims are as follows:

- To map the current professional knowledge and routines of ICT teachers in the area of technical e-safety
- To analyse significant factors determining how such knowledge and routines are acquired by ICT teachers

Methods

The research was designed and carried out as qualitative. According to Ferjenčík (2010), quantitive research is usually confirmatory and has a deductive character while qualitative research is more explorative and heuristic with an inductive focus. However, we have not found any theory on the acquisition of e-safety knowledge and routines (the lack of scientific evidence

in this area has been discussed above). Therefore, we consider the qualitative approach more suitable.

Research participants

Participants chosen for the research were primary, lower secondary and high school teachers of Informatics, Information and Communication Technologies, ICT and other similar subjects. The research involved questioning 13 participants. These were chosen according to several factors – qualified to teach ICT, type of school (lower secondary or high school), length of service, size of towns teachers work in, age and gender.

Three research participants were chosen as qualified high school ICT teachers with relatively little experience in schools (approx. five years). Two participants were chosen as teachers teaching ICT for their first or third year but not qualified to do so, each with a very different approach to ICT self-study. Another two participants were chosen from trainees having completed lifelong education studies for ICT coordinators. Although neither of them is a qualified ICT teacher, they have long-term experience of teaching ICT at high school, interest in the field and further education in it.

In order to include participants with experience at lower secondary schools in the research, two lower secondary school teachers were approached. They had already cooperated through short-term training programmes before. Both teachers taught in schools in smaller towns. Another participant was chosen due to his position as headmaster. Three teachers not qualified to teach ICT were added to the list of participants. For these three, there was no evidence of them having attended courses or training concerning ICT. These participants were chosen particularly on grounds of age, which ranged from around 35 to 65.

Data collection

Data collection involved individual meetings with each research participant. A semi-structured in-depth interview formed the basis of each meeting. Each interview lasted about 50–70 minutes. Research participants were informed of the aims of the study and assured anonymity. They were subsequently requested to take part in the research and to agree to have their interview recorded on a voice recorder.

The triangulation concept was incorporated into data collection (Švaříček, 2007b). Research participants were asked to fill in a short didactic test, based on case study questions. The aim of this test was to find out participants' knowledge of technical e-safety and how they would react in specific situations. The teachers were given a printed e-mail with a hoax message and asked for a practical example or written description of how they would react to this message. Following the principles of triangulation, so-called follow-up and confrontational questions were included in the interview (Švaříček, 2007a), adding depth and explaining any possible difference in how teachers behaved and how they replied during the interview.

Data analysis

Analysis of acquired data was based on the open coding method. The analysed text was divided into units and these units were allocated a certain code that represents a certain type of reply and differentiates it from the others (Šeďová, 2007). Codes from the generated list were subsequently grouped into categories according to internal similarity (Strauss and Corbin, 1999). Open coding was followed by axial coding, which aimed to create associations between categories and subcategories via the paradigmatic model (Strauss and Corbin, 1999). The principle of constant comparison was included in the process of overall analysis (Šeďová, 2007). The aim of this comparison was to find differences within data sources relating to one research participant and within data concerning various participants.

Ensuring quality control of the research

Besides using triangulation for data acquisition (as described above), researcher's logs were kept, capturing ongoing metainformation as research was carried out. Efforts were made to preserve the consistency of questions posed to research participants by making a written list of them and the coding of several of the first interviews was checked to preserve the consistency of data coding.

Results

Analysis of the interviews identified several categories related to teachers' knowledge and routines in the area of technical e-safety and how they are shaped. The basic categories are External influences on routine, Internal influences on routine, Personal relation to ICT, Barriers to protection, Specific protection routines, Drawbacks of protection and Subjective assessment of knowledge & routine. These categories are linked via mutual relationships, as shown in Fig. 1.

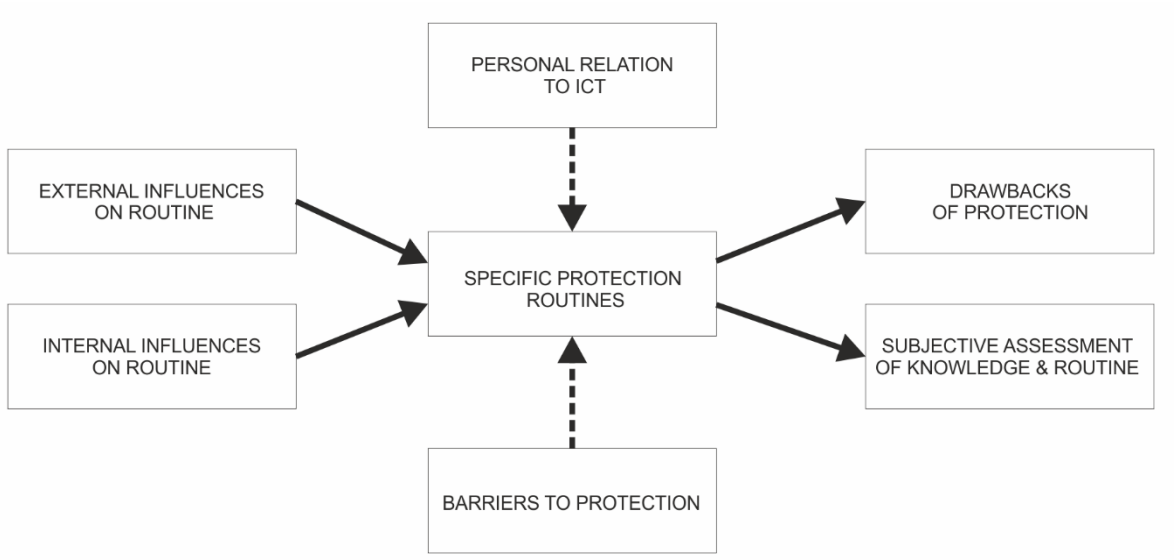

Fig. 1: Relationships between categories in the model of forming knowledge and behaviour of ICT teachers

The central category in the model is *Specific protection routines*. This category deals with ways teachers protect themselves against negative elements while using ICT. Methods of protection are mainly affected by the causal categories *External influences on routine* and *Internal influences on routine*. Whereas external influences relate to the outer world (for example attended instruction or experience), internal influences concern the teachers' personality and their view of the world, for example (lack of) trust, the role of the teacher, etc.

The category Specific protection routines is to a certain degree influenced by the categories *Personal relation to ICT*, which deals with the teachers' relationship to the teaching of ICT subjects and to ICT itself and *Barriers to protection*, which include influences preventing teachers from protecting themselves as much as possible in specific situations.

Teachers' subjective opinions of their own knowledge and routines in the area of technical e-safety have been captured in the category *Subjective assessment of knowledge & routine*. The category *Drawbacks of protection* concerns the negative consequences that teachers encounter from the methods of protection they use. The following text goes on to describe individual categories.

External influences on routine

ICT teachers' behaviour is directly influenced by the external world. External influences can be divided into areas of experience, self-study, organised instruction and administrators' warnings.

Experience. A significant factor influencing teachers in the area of technical e-safety is previous experience, particularly something negative experienced as a result of disregarding rules. One of the teachers accounted: "*I was really gutted to lose a unique piece of work which I never managed to piece back again since then, so I started to protect myself in such a way. If it hadn't happened, I wouldn't be so thorough.*" Teachers can be influenced by situations encountered while doing their job (e.g. as school network administrator) or by problems that close friends or acquaintances have run into. However, behaviour will not be influenced by a negative experience alone. Teachers also need to be aware of the mistake they have made and the amount of damage they have caused.

> ***Case study 1.*** *During the research, we recorded the case of a teacher whose school computer became infected. As the computer could not be used for everyday work, the IT department had to be informed. They discovered the problem had been caused by a virus, which they removed. The teacher remarked that he was not aware of a specific mistake that might have sparked the incident and blamed it on an unspecified lapse of attention while working on the Internet, which, he added, can happen. In his words, a teacher's behaviour would not be influenced by this incident.*

Experience does not only lead to safer behaviour but may also incite teachers to disregard recommended procedures if they are restricted by such procedures and not aware of any clear benefits from them. The following citation concerns the need to regularly change passwords: "*I did it but then I got them mixed up. New password – old one – new one – old one (…), so I just kept using the same one*."

Self-study. ICT teachers educate themselves in the area of technical e-safety. Important sources for them are ICT textbooks, specialised ICT literature and the Internet, going on specialised websites in the aim of understanding a certain area or solving a specific problem. If they do not have enough time for this study or are unable to understand the problem, they ask more experienced colleagues or renowned ICT experts to explain the matter to them: "*I find a lot on the Internet and have people around me who understand it as well, so I try to understand the stuff myself and if I get to the point where I don't know, I might refer to them*".

Instruction. Organised instruction influences teachers in the area of technical e-safety. Teachers not qualified to teach ICT acknowledge the benefits of in-service training and courses. Teachers qualified to teach ICT do not speak much of the influence of university classes. Their remarks are not convincing and any instruction of the topic seems to have been confused with other sources of information.

> ***Case study 2.*** *During the interviews, we were surprised by the speed and accuracy at which one of the newly-qualified teachers recalled the rules for creating computer passwords. We asked her whether she had gained this knowledge at high school or university and she replied: "No, I first read about that in a textbook that I bought myself when I started to teach ICT".*

Case study 2 might hint that, at certain universities, lessons of technical e-safety for pre-service teachers are underestimated or overlooked. In that case, these qualified ICT teachers would be forced to study the issue of technical e-safety subsequently, just like their non-qualified colleagues.

Warnings from administrators. Teachers regard calls to carry out certain actions as prompts for safe behaviour. These prompts come from the computer network administrator, operating system administrator or online service administrators. For example, one of the teachers stated: "*Sometimes I get a message (telling me to change my password) from the school (…), so I do it everywhere. If I'm on doing it anyway*." While some of the teachers accept the content of these calls and try to behave accordingly (see citation above), others do what is required of them but are not fully convinced it is the right thing. Take the example of creating a computer password that is long and sophisticated enough to meet the service provider's demands.

Unintended opportunities. Some teachers get into unplanned situations and use them to gain knowledge and inspiration on how to stay as safe as possible. That might be from news in the media or it could be from a research interview, as shown in case study 3.

> ***Case study 3.*** *Whilst researching, we met a teacher who was curious during the interview, replying to our question on whether he had thought up a defence strategy against spam: "(…) I have no defence strategy because it doesn't worry me. And if it doesn't worry me, I don't do anything about it. But if something like that exists, tell me about it".*

Internal influences on routine

ICT teachers' behaviour is affected by influences originating from their personality and view of the world. The teachers' personality influences the decisions they make: trust or distrust, caution and fear, pragmatism or scrupulosity, thought and awareness of the role of the teacher.

Trust vs. distrust. Teachers distrust strangers on the Internet, worried about possible danger, whereas they usually trust companies who they have had a positive experience with. Distrust of strangers can be in the form of an unwillingness to trust information provided on an unknown website or to have oneself registered in return for providing certain data. They are willing to overcome this distrust provided the given service has been critically acclaimed by somebody they know well. Teachers partly distrust renowned services, worried about security issues and possible misuse of confided data: "*I wouldn't save my personal data there (in a cloud). I have tried to remove nearly all my photos and I just have a few there and I would never put any data on Google or Microsoft.*" On the other hand, they trust these services as regards their confided data being protected against loss or damage. As for trusting the technical security of their computer against threats (antivirus, antispyware and others), teachers differ in opinion. Some believe their security will stop a perspective threat: "*I trust the antivirus program would let me know if there was a virus in it.*" Others are more careful and do not want to limitlessly rely on technical solutions.

Teacher's approach. Teachers adapt their behaviour to ensure professionalism. In fear of losing authority or in an effort to keep work and private life separate, teachers try to keep a certain distance from pupils. Some teachers try to be cautious with their pupils in fear of coming under threat from them: "*I'm afraid (...) and especially at school because our current students are hackers. They can get into a lot of things and I believe they could even get into my email if they wanted.*" For many teachers, teaching ICT provides the motivation to improve their technical e-safety knowledge and take an interest in new trends: "*Of course, it is motivation for me to search for it because I am an ICT teacher*."

Pragmatism vs. scrupulosity. While some teachers admit to behaving pragmatically, others claim they behave scrupulously. Take the example of registering for unknown online services, where some of them are, in their own words, willing to enter false personal details, whereas others reject such behaviour: "*(...) I tend to consider whether I need to make the registration at all or not. And if it is absolutely essential, I usually give true information (...)*".

Thought. Teachers do not make decisions on their actions formally on the grounds of generally valid precepts but make efforts to think about a specific problem and try to find a way to meet their own needs or demands from their social circle whilst remaining safe: "*Like a colleague puts his travel albums there (publically on Google+). I don't see anything wrong with that but it has to be differentiated, there has to be a limit.*" As some security procedures are restrictive (see chapter Barriers to protection for details), they are not used in all situations by teachers, who try to think about the value or confidentiality of data to be protected or, being exposed to a potential risk, elect an appropriate strategy according to that. The following statement illustrates the intensity of data backup: "*Photos are (...) probably the most important thing I make backup copies of. Maybe I make more backup copies of them than of documents, which should probably be vice versa.*"

Fear of consequences. A motive for safe behaviour is fear of the consequences of a possible incident if rules are disregarded. Teachers are worried about their privacy and possible abuse of their personal data, identity abuse, fraud, the loss of data stored in the computer and the effects of a virus.

Personal relation to ICT

The category Personal relation to ICT expresses the teachers' approach to the teaching of ICT subjects and to ICT itself. This area covers a discussion of how given teachers became ICT teachers, how they perceive their role and in what ways they use ICT outside the classroom.

Relationship to ICT teaching. Teachers either qualified or not qualified to teach ICT were questioned as part of our research. Teachers not qualified to teach ICT usually stated that they had started to teach ICT because there was no other more suitable candidate in their school: "*Because it also had to be taught at school and other teachers were not keen on it, I kind of studied it and got into it.*" Teachers not qualified to teach ICT have different opinions on whether university study leads to a good understanding of technical e-safety and the ability to teach this topic. Some of them do not consider the absence of a university ICT education a handicap for them and they feel it might be compensated by long-term experience in the field. Others do not agree with this opinion and feel they are disadvantaged: "*Well, they (newly qualified ICT teachers) are definitely more in the know about that. Because they have been doing it from scratch, from the foundations and they have the latest possible information. Whereas we get to know stuff like in reverse (...)*".

Relation to administration and using ICT. The teachers who were approached for the study differ in their relation to ICT administration. While some administer their computer by themselves, others state that they are not computer administrators but users. Differences can also be found in their relation to school ICT administration. While some, in their own words, are responsible for ICT administration at school, other teachers stated that they are not involved in this activity and ICT at school is administered by other people.

There are disparities in the extent teachers use ICT outside the classrooms. Some of the teachers, in their own words, use the Internet quite rarely and communication via ICT is not one of their strengths while others use a whole range of Internet services and actively use social network sites.

Barriers to protection

In the matter of e-safety, teachers' behaviour is affected by influences which prevent them from protecting themselves as well as they can (for example pressure on publishing personal information, lax approach or lack of time). These influences originate in their external environment, their personality and lack of expertise and abilities.

Lack of expertise prevents teachers from making funded decisions in a specific situation, where their interpretation of a problem can be inexact and they can be put at risk. Take the following citation concerning a teacher's computer getting infected by a virus: "*(...) because there was a (window), I wanted to display the content so I clicked on something and it went off. So it must have been (a virus) because instead of displaying some content, it started to do something in my computer*". Lack of expertise and ability is demonstrated both by the inexact use of terminology (for example "*the cross for clicking is sometimes fake*") and by the teachers' explicit remarks: "*I don't involve myself in this because I know I am incapable*".

External obstacles. Teachers perceive obstacles which originate from their external environment and which their e-safety principles are confronted with. These obstacles include pressure from around them to publish personal information. Take the need to state one's e-mail address on the school website or when registering for various services. Another obstacle is the need for rapid communication with pupils, due to whom some teachers decided to abandon their principle not to enter into friendships with their pupils on social network sites: "*...mainly (I entered into a friendship) because of a competition, because we needed to be in touch with them and I didn't want them to call me. So I chose Facebook, that we would work it out on Facebook (...)".*

Some teachers do not feel good about the imperfection of technical solutions and the possibility that the means of prevention they use could fail. One of the teachers summed this up by stating that "*Any machine is merely a machine and has many faults.*"

Internal obstacles. Teachers are prevented from the safest possible use of ICT by obstacles that originate from the type of person they are, the way they feel and the amount of time they have. Teachers can find themselves in risky situations because they are in a hurry or tired or when they, in their own words, lose concentration: "*When I'm tired, I don't really think much and I start to do things automatically, so mistakes are more likely to happen*". Teachers abandon ideal methods of protection because they become lax and lack time: "*... my other passwords are like that because they're easy to write, so I don't have to tap in the alphabet plus twelve numbers (...)*". A similar obstacle to security is the amount of remembering that is needed, which leads to rules concerning computer passwords being disregarded.

Teachers are aware of disregarding rules and defend their decision by explaining that higher security is not needed due to the type of data they have: "*If I had the feeling that I have something private there, then I probably would... It's the type of stuff that if someone read it, it wouldn't be the end of the world...*"

Some teachers stop being cautious when the potential threat comes from someone close. Take the words of a teacher regarding opening suspicious e-mail attachments from people he knows: "*I trust acquaintances and friends in this respect when they send me something by mail.*"

Drawbacks of security. If teachers decide to behave in the safest possible way, some security obstacles become security drawbacks. Take the time demands of security, being deprived of certain information (for example on social network sites), forgetting a strong password that has been regularly changed or important messages being marked as spam by an antispam filter.

Specific protection routines

The central category of our model concerns specific ways ICT teachers protect themselves against the negative effects of using ICT. It is made up of both procedures for prevention and procedures for dealing with consequences. The following text covers general methods of protection and goes on to look at individual areas of technical e-safety (i.e. data loss, malware, computer passwords, unwanted mail and privacy administration).

Teachers' reactions to a specific problem can be very different. Some try to resolve a situation on their own, searching for initial help on the Internet, whereas others turn to local ICT

specialists with requests for advice. In the same situation, other teachers would ask an ICT specialist they know for direct intervention without any prior efforts to solve the problem by themselves: "*Because I'm not such an IT geek who can get by on his own. And especially when these people are around you (...), so you don't do it by yourself*." If they are not familiar with suitable local ICT specialists and are unable to solve a problem on their own, they turn to specialised companies.

Making backup copies. Teachers use a wide range of media to make backup copies of data – external hard disk, USB flash disk, cloud service (an e-mail inbox or a type of data storage like DropBox), CD or DVD. Many of them make backup copies of their data in various ways, most often choosing an external hard disk as primary backup medium. Some teachers see printing or including in an online photo gallery as a specific backup method for photos: "*Because I have already sent them (certain photographs) to rajče.net, so at least they wouldn't get lost there. (...) True, they wouldn't be in five megabyte format, but I would simply have the photos*".

While some claim that they make backup copies of their data at regular intervals, others make backup copies of data they have just been working on or have edited: "*I make backup copies whenever I work on something. If I am working on something and it's finished, I make a backup copy. If I haven't been working on anything, what should I make a backup copy of?*"

Protection against malware. Our study has discovered two basic approaches to antivirus protection. While some teachers actively carry out antivirus checks, others rely on the fact that the antivirus itself will inform them of any threat. Both groups base their antivirus protection on antivirus software with a regularly updated virus database. Where teachers are warned of a threat (from a file or website), they accept this advice and delete the file or go off the suspicious website.

There are disparities in how teachers behave when surfing the net. Some try to avoid high-risk websites but others go on them aware of the possible threat: "*I know there could be a possible threat, but even so I have a look when I need to or when I'm interested in it. Yeah, it often warns me that the website contains some dangerous material so I usually close it.*" Among them, there is a group of teachers who do not avoid websites with high-risk content but go on tried and tested sites where they have not experienced malware as yet. We have not spoken to any teachers who have been on high-risk sites using a virtual computer environment or similar approach.

Account security. As a rule, teachers use several various passwords to secure their accounts. For access to services dealing with highly confidential information (particularly Internet banking), they use a unique password which they do not use for any other service. Some teachers use one common password for access to mutually related services, whereas others claim they choose a different password for each service. As a rule, for those services that are not considered important by individual teachers, they use one common password for the security of all these services. On the other hand, we have met examples of teachers who, in their own words, use one single password or a few very similar passwords for all services.

Teachers usually use a relatively long password for important services. While some, in their own words, make up passwords that meet recommended parameters, others create passwords

by connecting several words and not including all advised symbols. However, we have also met an example of a teacher whose passwords contained some of his personal details.

As far as regularly changing passwords is concerned, teachers' opinions differ. While some do not change their passwords at all, others claim that, for important services, they regularly change them several times a year. To prevent themselves from forgetting passwords, some teachers create lists of them and some teachers share their passwords with members of their family.

Protection against unwanted mail. Most teachers prevent the delivery of spam to their e-mail inboxes but some teachers see spam as an unavoidable feature and do not seek protection against it. Those who block spam try not to publish their e-mail address on websites or modify the address to stop spam robots using it. Some teachers set up a second e-mail account to use when registering for online services but not for everyday communication. On receiving an unwanted e-mail, teachers usually delete this message or mark it as spam. Where an unwanted business offer is received, some teachers try to unsubscribe from further receipt of a given company's offers.

Where a hoax is received, teachers make a decision based on the seriousness of the message. If the content of the message concerns them directly, they, in their own words, usually try to verify the message with independent sources. If the message warns of a general threat (for example, the alleged health risks of everyday food items), many teachers refuse to verify such a message: "*I don't even study whether or not it can be true because like in that situation I always lose. Whether it's true or not, don't bother about it. Because you can't verify it."* For most teachers, principle sources for verifying messages are civil service information portals and sources searched for via an Internet browser; only a few teachers mentioned services monitoring hoaxes (e.g. Hoax.cz). Teachers generally refuse to pass on hoax messages but some admit to passing on an important message after having thoroughly verified it.

Protection of privacy and use of social network sites. Most teachers try not to publish personal information or photographs on the Internet and if they do, they claim that they publish materials which they consider fitting. The typical approach is to publish selected personal photographs or information about their private life only for a narrow circle of people, both on social network sites and off it. Take a teacher who remarked: "*I use Picasa to store my photos so, when I'm on another computer, I can show them to others*."

ICT teachers use social network sites to different degrees. While some use social network sites often, others are either occasional users or completely reject it. Some teachers are passive users of social network sites, looking through content placed by their friends but not creating content themselves. However, not all teachers behave in this way. Some publish personal information, as shown in Case study 4.

> ***Case study 4.*** *During the triangulation process, we were searching for information on research participants in the part of Facebook accessible to the public and we found photographs in a business card layout in the profile of one of the teachers. The photograph portrayed the given teacher with his dog and his car was standing in the background with a clearly visible registration number. Apart from the teacher's full name, his address and*

mobile phone number had been inserted into the photograph. Other photographs also contained information about the teacher's private life (his interest in cycling, ownership of a certain breed of dog, and car registration number). Although the stated information cannot be considered confidential, the teacher's approach greatly differs from those teachers who try not to publish any information about their person on social network sites, not even in their circle of friends.

Some teachers try to cancel social network site and community server accounts which they no longer use, due to efforts to control personal information that has been online and to remove traces of any previous activity. One of the teachers accounted: "*I know there can still be something from the past even though I have tried to cancel sites like Spolužáci.cz and other similar ones. (...) And I don't want anyone to access this information about me.*"

Subjective assessment of knowledge & routine

Part of our research has investigated how teachers subjectively evaluate their technical e-safety knowledge and routines. As a rule, teachers called themselves laymen, learning gradually and saying that they knew "enough" about the issue for their own needs and the tasks they are required to do. One of the teachers stated: "*I am as able as I need to be at a particular moment. If I needed to expand on anything, I would have to devote more time to it and look into it more (...)*". There were also opinions expressing fear of a lack of knowledge, personal experience and ability to cope with perspective safety issues: "*I have never had a bugged computer and I am really lucky it has never happened to me. Because there were loads of obstructions and difficulties and who knows if I would be able to manage that (...)*". On the other hand, we also met teachers who called themselves specialists rather than laymen, feeling they had become experts in the matter.

Although teachers usually know the principles of safe behaviour, some admit to disregarding them: "*I teach students about changing passwords and using long ones but I get the feeling that I don't keep to that myself. Despite knowing it in theory.*"

Conclusion

There has been a great deal of discussion regarding the key role of schools in meeting the need for an e-safety education program aimed at children and teenagers. However, there has yet been no investigation of the professional knowledge and routines of teachers, not even of ICT teachers. Teachers in the area of technical e-safety should not be seen as mere theorists but also as personalities who can greatly influence pupils through their own example.

Our research has identified the routines and knowledge of teachers in the area in question. Teachers usually try to behave safely but there are very differing reasons for such behaviour. In terms of safer behaviour, teachers are influenced both by external factors (e.g. a negative experience they might have had or a course they might have attended) and by their personality and view of the world (e.g. their awareness of the role of the teacher). However, teachers are also affected by influences that prevent them from behaving in the safest possible way. This might be due to workload or teaching, not having time for security measures or the lack of

expertise in e-safety. Our research has largely dealt with each type of influence separately but they clearly coincide with each other – either having a synergic or opposing effect or mutual influence.

Future research will need to reveal what kind of mutual relations exist among the above mentioned influences and what the most significant determiners of knowledge and routines of ICT teachers are. If we succeed in understanding how technical e-safety knowledge and routines are formed, we will be able to improve the quality of pre-service teacher education and in-service teacher training.

Acknowledgement

The research was supported by the project GAJU 017/2013/S.

References

BARROW, Ch. and G. HEYWOOD-EVERETT. *E-safety: the experience in English educational establishments* [online]. Becta, 2006 [cit. 20120715]. Available from http://dera.ioe.ac.uk/1619/1/becta_2005_esafetyaudit_report.pdf

BECTA. *E-safety: Developing whole-school policies to support effective practice* [online]. Coventry: British Educational Communications and Technology Agency, 2005 [cit. 20130202]. Available from http://www.wisekids.org.uk/BECTA%20Publications/esafety.pdf

BECTA. *Safeguarding children in a digital world: Developing a strategic approach to e-safety* [online]. Coventry: British Educational Communications and Technology Agency, 2006 [cit. 20120914]. Available from http://webarchive.nationalarchives.gov.uk/20101102103654/http://publications.becta.org.uk/download.cfm?resID=25933

BECTA. *Signposts to safety: Teaching e-safety at Key Stages 3 and 4* [online]. Coventry: British Educational Communications and Technology Agency, 2007 [cit. 20111130]. Available from http://www.education.gov.uk/publications/eOrderingDownload/signposts_safety_ks3and4.pdf

BERÁNEK, L. Information systems security education for future teacher at secondary and primary schools. In *Journal of Technology and Information Education* [online]. 2009, **1**(2), p. 89–93 [cit. 20120815]. ISSN 1803-537X. Available from http://www.jtie.upol.cz/clanky_2_2009/beranek.pdf

BUETTNER, Y. et al. *Information and Communication Technology in Education: A Curriculum for Schools and Programme of Teacher Development* [online]. Paris: UNESCO, 2002 [cit. 20120415]. Available from http://unesdoc.unesco.org/images/0012/001295/129538e.pdf

BYRON, T. *Safer Children in a Digital World: The Report of the Byron Review* [online]. Nottingham, United Kingdom: Department for Children, Schools and Families [of UK], 2008 [cit. 20120322]. ISBN 978-1-84775-134-8. Available from http://dera.ioe.ac.uk/7332/1/Final%20Report%20Bookmarked.pdf

CRANMER, S., J. POTTER, and N. SELWYN. *Learners and technology: 7–11* [online]. British Educational Communications and Technology Agency, 2008 [cit. 20120416]. Available from http://dera.ioe.ac.uk/1630/1/becta_2008_learners7to11_report.pdf

FERJENČÍK, J. *Úvod do metodologie psychologického výzkumu: Jak zkoumat lidskou duši*. Praha: Portál, 2010. 255 p. ISBN 978-807-3678-159.

GARRISON, C. P. and O. G. POSEY. Computer Security Awareness of Accounting Students. In *2006 Southwest Decision Sciences Institute Proceedings* [online]. Oklahoma City, USA: Southwest Decision Sciences Institute, 2006 [cit. 20120202]. Available from http://www.swdsi.org/swdsi06/Proceedings06/Papers/A04.pdf

GET SAFE ONLINE. *UK Internet Security: State of the Nation: The Get Safe Online Report* [online]. 2009 [cit. 20120604]. Available from https://www.getsafeonline.org/media/Reports/Get_Safe_Online_Report_2009.pdf

GET SAFE ONLINE. *UK Internet Security: State of the Nation: The Get Safe Online Report* [online]. 2010 [cit. 20120604]. Available from http://www.southtyneside.info/CHttpHandler.ashx?id=12345&p=0

LANG, M. et al. Social Networking and Personal Data Security: A Study of Attitudes and Public Awareness in Ireland. In *Proceedings of International Conference on Management of e-Commerce and e-Government (ICMeCG)*. Nanchang, China: IEEE Computer Society, 2009, p. 486–489.

LIVINGSTONE, S. and L. HADDON. Risky experiences for children online: Charting European research on children and the Internet. In *Children & society* [online]. 2008, **22**(4), p. 314–323 [cit. 20120413]. ISSN 0951-0605. Available from http://eprints.lse.ac.uk/27076/

LIVINGSTONE, S. and L. HADDON. *EU Kids Online: Final report* [online]. LSE, London: EU Kids Online, 2009 [cit. 20111024]. Available from http://www.lse.ac.uk/media@lse/research/eukidsonline/eu%20kids%20i%20%282006-9%29/eu%20kids%20online%20i%20reports/eukidsonlinefinalreport.pdf

McCORMICK, A. and L. van Otterloo. Average UK 11-year-old has “adult skills” in technology, AVG research reveals. In *AVG* [online]. Amsterdam: AVG Technologies, 2011 [cit. 20120918]. Available from http://now.avg.com/average-uk-11-year-old-has-adult-skills-in-technology-avg-research-reveals/

PAPAVASILIOU, S. *Survey: Promotion of internet safety into the school curriculum* [online]. SaferInternet.gr, 2009 [cit. 20120530]. Available from http://insafecommunity.saferinternet.org/c/document_library/get_file?uuid=553e7cbd-8841-4d27-a7b6-adf936f8cd94&groupId=10221

PONEMON INSTITUTE. *Smartphone Security: Survey of U.S. consumers* [online]. 2011 [cit. 20130202]. Available from http://aa-download.avg.com/filedir/other/Smartphone.pdf

RAMBOUSEK, V. et al. *Výzkum informační výchovy na základních školách*. Plzeň: Koniáš, 2007. 359 p. ISBN 978-80-86948-10-2.

SPIELHOFER, T. *Children's online risks and safety: A review of the available evidence* [online]. Slough, United Kingdom: National Foundation for Educational Research, 2010 [cit. 20121004]. Available from http://www.nfer.ac.uk/nfer/publications/COJ01/COJ01.pdf

STEGANOS GmbH. *The state of computer privacy: Steganos 2008 survey into PC security* [online]. 2008 [cit. 20120202]. Available from http://www.steganos.com/uploads/media/Steganos_Press_Release_2008-10-24_SurveyPCusersGraphicsWhitePaper.pdf

STRAUSS, A. and J. CORBIN. *Základy kvalitativního výzkumu: Postupy a techniky metody zakotvené teorie* (S. Ježek, Trans.). Boskovice: Albert, 1999. 228 p. ISBN 80-85834-60-X.

SYMANTEC CORPORATION. *Norton Online Living Report 09* [online]. 2009 [cit. 20121004]. Available from http://us.norton.com/content/en/us/home_homeoffice/media/pdf/nofr/NOLR_Report_09.pdf

SYMANTEC CORPORATION. *Norton Online Family Report: Global insights into family life online* [online]. 2010 [cit. 20121004]. Available from http://us.norton.com/content/en/us/home_homeoffice/media/pdf/nofr/Norton_Family-Report-USA_June9.pdf

ŠEĎOVÁ, K. Analýza kvalitativních dat. In R. Švaříček and K. Šeďová, et al., Kvalitativní výzkum v pedagogických vědách (p. 207–247). Praha: Portál, 2007. ISBN 978-80-7367-313-0.

ŠIMANDL, V. Kompetence učitelů ICT v oblasti technické e-bezpečnosti. In *Information and Communication Technology in Education - Ph.D. students' section* [CD-ROM]. Ostrava: Ostravská univerzita, Pedagogická fakulta, 2013, p. 114-131. ISBN 978-80-7464-325-5.

ŠIMANDL, V., J. ZELENKA and J. SADIL. Výuka digitální bezpečnosti v českých školách. In *DidInfo 2013*. Banská Bystrica, Slovakia: Univerzita Mateja Bela, Fakulta prírodných vied v Banskej Bystrici, 2013, p. 229–236. ISBN 978-80-557-0527-9.

ŠVAŘÍČEK, R. Hloubkový rozhovor. In R. Švaříček and K. Šeďová, et al., Kvalitativní výzkum v pedagogických vědách (p. 159–184). Praha: Portál, 2007a. ISBN 978-80-7367-313-0.

ŠVAŘÍČEK, R. Triangulace. In R. Švaříček and K. Šeďová, et al., Kvalitativní výzkum v pedagogických vědách (p. 202–206). Praha: Portál, 2007b. ISBN 978-80-7367-313-0.

TEER, F. P., S. E. KRUCK and G. P. KRUCK. Empirical study of students' computer security practices and perceptions. In *Journal of Computer Information Systems*. 2007, **47**(3), p. 105–110.