úřad pro ochranu
osobních údajů
the office for personal
data protection

Information Bulletin 1/2013

Dear readers of our Bulletin,

this is the first issue of the Information Bulletin, a publication of the Office for the Protection of Competition, in 2013. This issue is aimed particularly at teachers and educators, but also parents, i.e., to everyone who works with and raises children and youth. At the same time, we would also like to address students and our broader readership.

Social networks, particularly Facebook, from the point of view of personal data protection and privacy, are the topic of this issue. The purpose is not to dissuade from the use of social networks, but to point out the possible risks related to them.

We would like call attention to the fact that protection of personal data and privacy is necessary in light of today's invasive technologies, and forgetting or underestimating this may have immense and sometimes even fatal consequences.

The Bulletin comprises articles written by various authors from various professions on "life on social networks". We have asked them to provide their views and opinions on social networks and give them a platform to discuss interesting positions and experiences somewhat more comprehensively, even though personal data protection, as the basic assumption for protection of privacy, is paramount for us. The many other points of view that this issue brings more or less indeed relate to the protection of privacy.

Each of us has the right to know who has access to our personal data and how the data are handled. Many things are in our own hands, however. Learning to move about in the on-line environment safely with certainty - the sooner the better -

is becoming a life imperative, i.e., if we do not wish to be manipulated by someone unseen or lose the power to freely make our own decisions.

Information and communication technology, the internet and media literacy are being included in school curricula and are being taught at schools in various forms. The Office for Personal Data Protection sees the role of teachers as indispensable in the process of such education as well. For this reason, this issue of the Information Bulletin is devoted especially to them. It mostly depends on them whether our civilization retains the values that it has attained over the centuries unscathed - such values include basic human rights, under which privacy falls.

mn

Social networks are a present day phenomenon

They are a good servant but a cruel master. And that is the approach that should be taken to them. It is important to know how to make them that servant. This particularly means making use of all of the possibilities available to keep personal data secure, at least to the extent that social networks allow. And if that is too little for you, i.e., privacy is more important to you and you would like to have it better protected, you should abandon the service and find other means to fulfil your life expectations. Do you really believe that the hundreds of contacts that you collect via social networks are all friends that you need for your life?

It is also important whether the users of those networks truly have the required knowledge to make use of the privacy protection “offered”. Sometimes I think that we are witnesses to absurd situations: Social networks are used entirely intuitively, especially by young people. It’s like getting behind the wheel of a car without having been taught to drive... I wonder whether parents and teachers know how much of the generation of their successors truly acquired that new literacy for working on a computer; it’s like knowing how to read, write and do maths: someone is better at it, someone worse, but no one is completely illiterate... But is it like that with working on a computer?

Although the Office for Personal Data Protection accepts thousands of complaints each year, I have to say that we have not encountered any complaints from anyone about their privacy being compromised by how they behaved on social networks. At the same time, however, we have information about the serious *consequences of using social networks.... We are also surprised to learn how carelessly people treat their privacy - we know that they are able to sign various documents, even contracts, without reading them properly... Very often they are then unpleasantly surprised.*

I would therefore wish that caution, common sense and certainty that we have the right to know what is being done with our private information, by whom and for what purpose, be as a matter of fact as breathing. That it be a matter of course that you have to read a document before signing it and that we learn that once privacy is lost - which is very easy through social networks - it can never be won back.

Igor Němec
President of the Office for
Personal Data Protection

Generation of a New Literacy

This Information Bulletin discusses the use of social networks from various points of view, especially from that of the generation of young people on the threshold of entering their professions.

There is no doubt that many from this generation have achieved their professional success at light speed thanks to their extraordinary knowledge and ability to work with communication technology and their understanding of the advantages of new communication technology and equipment, in this way surpassing most of their parents' generation and definitely their grandparents' generation. It would be farcical to suggest that they should be taken care of with regard to the use of social networks and privacy protection connected to this activity. It is quite certain that the biggest computer buffs need no help in this respect - even though many may have come to believe that privacy no longer exists and so can't be bothered with protecting their privacy. In such case, one can do nothing but hope that they don't get into a situation where they lose their privacy with no possibility of getting it back.

Most young people, however, are not the ones with above-average abilities; nevertheless, they won't be able to avoid using new means of communication once they enter any profession. And these individuals who have not "fallen" for computers or who are less interested in computers still wish to be a fully-fledged part of the new generation, and most recognise that social networks are required for this.

The Office for Personal Data Protection, in terms of its mission, cannot be anything but interested in the degree to which privacy protection is a familiar, obvious part of the life of that generation which is moving about so naturally within social networks, which seem to be tailored to the loss of privacy, despite being originally created for completely different ends. These statements are not intended to provoke, but to get us to start thinking about whether carelessness from a lack of knowledge will not one day prevail over our freedom to decide what should be publicly known about us. For this reason it is important to know how each of us is able to guard information about oneself, that is to monitor the movement of one's personal information in the virtual world.

As part of our annual "My Privacy! Don't Look, Don't Snoop!" contest, we tried to ask young people whether they know how to make use of privacy protection possibilities offered to them on the most personal data hungry network: Facebook. We have to admit that we didn't get many responses. Answering this question is definitely less entertaining than the assignments from the previous years of the contest. The majority of people chiefly want to have fun, and the young generation is no exception; in fact, the opposite is true. Nevertheless, the responses that we received are interesting - and we are adding them to the Information Bulletin. Perhaps as an inspiration about what to speak about with the young generation.

We have thus decided that this Bulletin will be devoted mainly to teachers - of course, parents are not precluded - and in it we will offer them the possibility to ask themselves questions, based on the published contributions, about the level of knowledge of their charges from the point of view their experience in the field of education. The contributions that we have included in the 2013/2014 Student Diary "Good Advice is More Valuable than Gold! How to Protect Your Privacy on Facebook" may help with this. This Bulletin will be distributed with the Student Diary. It should be mentioned that "Good Advice is More Valuable than Gold" is devoted to those who are not computer maniacs or "buffs".... If it proves that this *“handbook” for Facebook is not advice, that they think the information is trivial and a matter of course, then we will only be pleased. Please let us know that we have been wrong in thinking that they are unaware of this information. Our address: posta@uoou.cz. Please label your message with the word TISK. We look forward to working with you, dear teachers and parents.*

Hana Štěpánková
Spokeswoman of the Office for Personal Data Protection

PRIVACY
ON SOCIAL NETWORKS

Social Networks as Privacy Thieves

In the last five years, the use of the internet, social media and smart phones has skyrocketed. New devices have brought about a huge change in the way people communicate. They have improved access to information and the speed in which it is exchanged, the capacity of data transmitted by communication channels and increased the volume of video-information and information based on visual communication.

Benefits of New Media
and Social Media

New media and social media has improved the quality of our lives in many ways. Thanks to the popular social network Facebook, we can find long lost friends, find out how our former partners are doing, and quickly and flexibly invite friends to a birthday party or weekend trip. New media have thus brought a new level of quality to communication between people and, as the classic media theorist Dennis McQuail claims, they are an extension of human possibilities. We don’t have to bore visitors with two hours of looking at a photo album: you can now display your photographs on a social network and whoever feels like it can spend as much time as they like viewing them. What is more, at this time, the number of single households is growing, and new media and social networks are helping to relieve loneliness and allow us to operatively connect with friends who are on-line at the same time and with whom we can chat in a chat room.

The beginnings of the mass use of the internet were praised to high heavens by experts due to the democratic nature of new media. Its use was tied to the idea of the possibility for greater participation by individuals in public discussions on important topics. Communication via the internet is not centralised, as is communication via traditional media: press, radio, television. Communication channels are more open and allow anyone with access to the internet to help produce content and consume it. These two, once separate, roles - production and perception - have overlapped and people are moving between them faster. At one moment, people are passive consumers of a video placed on YouTube and next they are writing a comment on their blog. Theoreticians thus started using the term prosumer, a combination of the terms producer and consumer.

In connection with the internet, communication experts also anticipated a new form of political communication and the implementation of direct, not representative, democracy. People would be quickly and directly voting on public issues, problems and solutions to the problems, and representative democracy would be gra0dually replaced by direct democracy. Later it become clear that this optimistic change would not take place so quickly and the internet would be used by certain, rather political, movements. In terms of using the internet in elections, Estonia has been the most progressive of the European counties, having applied elements of internet voting in a number of elections already.

Over time it has become clear that the degree to which the internet would spread was too optimistic: even in the richest countries of the world there are substantial differences between people using new media and in the degree of access to new technology. Then the term “digital gap” appeared to describe the difference in use of new media from the point of view of socio-demographic characteristics of people. Use of the internet and smart phones is rather an issue that pertains to the younger population, the population with a higher education and higher income and urban rather than rural populations. At least that is what current statistics are showing us (see, e.g., the data published on www.spir.cz). Cases that the internet and new media may be used to spread racism and underage pornography have been discovered. The decentralised nature of new media then leads to the more difficult control of such media and more difficult regulation.

Dangers and Threats of Social Media

After the initial optimism tied to the use of the internet and social media, the first dark clouds and criticism began to appear. In the last few years, (especially) American psychologists (e.g., Rosen) have found that overuse of new media and smart phones also has a number of negative effects. There are a number of types of mental disorders tied to overuse of such media discussed most often: 1) **Obsessive behaviour** tied to the constant urge to check one's mobile phone during the day. Users have the tendency on the way to work to reach into their pockets and repeatedly check whether a new SMS are e-mail has arrived. Dinner in a restaurant with friends then begins with everyone putting their devices on the table and checking them regularly during the meal. In extreme cases, users have the feeling their telephone has rung or that they hear an incoming SMS, although that was not the case. 2) **Narcissism tied** to overuse of certain social networks, such as Facebook. This communication platform is directly based on the manifestation of interest in oneself. It entices us to write about ourselves, share our photographs and inform others how we feel at any given moment. Extreme users of Facebook are even choosing where to spend their free time according to whether they are sufficiently "telematic" and interesting for photographs to be later posted on Facebook. 3) **Attention disorders and hyperactivity**. Recently, use of new media has become more and more associated with multitasking - performing a number of communication tasks at once. Such phenomenon is increasing mainly among young internet users and consists in the user having a number of various "windows" open - from watching videos, through conversing in chat rooms, to writing reports - and moving quickly from one to the other. Moving quickly between different communication contexts - i.e., communication events with entire different functions - also means quick and short-circuited mental activity. Essentially, we don't allow or our mind to focus on one topic, but force it to move quickly between various communication tasks. Some psychological studies have discovered that intensive multitasking and overuse of new media leads to attention disorders and the inability to perform long-term activities focused on one task (Rosen). This could lead to learning disorders or other problems in the day-to-day lives of adolescents and students and the inability to deal with complex mental tasks requiring long-term concentration. 4) **Multiplication of mental identities.** Another serious problem that may ensue from the use of new media relates in particular to intensively playing computer games or using an environment that allows a user to create and experience a number of various identities. If a long time is spent “in the skin” of an imaginary character, it may become problematic for the user to differentiate between real life and computer reality and thus have problems moving between one and the other and differentiating between his real identity and his artificial identity (Rosen). This may also include a certain numbing to the real world, emotional suppression and lack of empathy, which could lead to certain fatal consequences for the individual’s social behaviour. 5) **Sharing personal data and protection of information.** More than any other kind of communication, internet communication contains more types of communication of the interaction type, labelled registration by theoreticians (Bordewijk and Khaan). This is based on the compilation of information about users in the form of various on-line forms and databases that we have to fill in to be allowed further access. We often fill in sensitive data about ourselves in such forms, and this data is often used for the marketing purposes of the company concerned. During repeated visits to these websites, we are welcomed immediately by personalised content that corresponds to our needs, interests and preferences. Social networks, including Facebook, work on a similar principle of aggregating person data. The only difference is that we place this personal information there ourselves.

Personal Data Protection and Facebook

Facebook and other social networks are an environment to which a host of users entrust a vast amount of privacy. Society is based on the fact that certain facts remain hidden as private or intimate and are made available only to our closest friends or to no one at all, whereas other information serves for our presentation outwards, publicly. Electronic media, especially in the second half of the twentieth century, has contributed substantially to blurring the line between the public and the private, and social media has put the finishing touches on this shift. Some information to which users are exposed on social networks are easily exploited either at the moment they are published or in the distant future. Users usually believe that their Facebook profile is sufficiently protected; however, they often do not know who is in their network of “friends” on Facebook and often also do not have sufficient knowledge of who all visits their Facebook profile. They then like to display private photographs revealing who they are in contact with and how intense their relationship is and what their personal social network is like. There are also cases where a user displays photographs that are acceptable at the time displayed - for example from a wild student party while still a student - but which may become a problem after a number of years when such person is in a different social role - for example when looking for work and communicating with a prospective employer. They may then lead to the person being perceived in a very negative light and rejected. Facebook users, especially younger ones, often do not think about what situation they will be in in the near or distant future and if their previous “posted privacy” can substantially hurt them.

Problems stemming from the reckless posting of information may, however, arise a lot faster. For example, seemingly harmless information about where we are at a given time. If we leave home for a longer period of time or go on holiday and provide this information on Facebook, we are letting the world know and this information could be an invitation to robbers (often when the information mentions how long we will be away - for example a photograph with a comment: “Finally in Croatia for two weeks!”). A photograph of the interior of your home will show your furnishing and your financial situation generally. The possibilities for your personal information being misused are numerous and each published piece of private information may put you in a disadvantageous position.

A complicated question that users as a rule don’t ask themselves is to whom the information, photographs, videos and other materials belong to once posted on Facebook. There is every indication that materials located on Facebook automatically become the property of the owners of this social network, and they can then work with the information without our control. There is thus the hypothetical question of whether a few years from now a photograph from that student party will pop up at an inappropriate time for us or whether our sensitive personal data will in fact be traded by someone.

Social media and Facebook may facilitate communication for us in many ways, making it more targeted, faster and more effective. We should not forget, however, that the communication is open and easily abused, and we should always think twice about what we are sharing on social networks or whether we know with whom and if security of the shared space is truly sufficient.

Tomáš Trampota

Tomáš Trampota is the director of the Institute of Communication Studies and Journalism of the Faculty of Social Sciences of Charles University, which covers the field of journalism, media studies and marketing communication and public relations. The author is interested in development trends of modern media, the current Czech media system and media theory systems. He is also the lecturer for the course Introduction to Media Criticism at the New York University in Prague. He is the author of the book Zpravodajství a Metody výzkumu médií (Reporting and Media Research Methods) and a numerous articles and professional contributions. In previous years he was the president of the network for Central and Eastern Europe (CEE Network) of the biggest European association for education and research in the field of communication (European Communication Research and Education Association) and vice-dean of the Faculty of Social Sciences of Charles University for public relations.

Internet, Privacy of Others
and Disturbing Oneself

Use of digital communication technology - be it a mobile phone, Facebook or the internet generally - is taking on truly massive proportions especially among teenagers. For a number of years now, these technologies are being used by practically all teenagers (about 95%) and the amount of time spent on them is ever increasing (in 2008, prior to the arrival of cheap and fast mobile connections, Czech teenagers spent 16 hours a week on average on the internet, and based on experience from the USA, we can assume that this time has increased substantially in the past five years). 1) Following the era of the twisted, unrealistic enthusiasm and fear mongering with respect to the wonderful benefits and threats posed by the internet, the time has come to find dispassionate answers to the question what today’s children are gaining and losing thanks to the fact that a significant part of their growing up is taking place through virtual, fragmentary and always accessible communication.

It is of course not possible to deny the positive and now relatively well documented benefits of on-line technology for coordinating and maintaining close relationships separated by distance, for being able to maintain contact with a far more extensive network of friends and for obtaining information or support, especially in connection with important decisions and in important life situations. But we should not forget that these facts have another, darker side.

According to the prevailing lifestyle, a fairly larger number of parents believe that their children are growing up somehow on their own, without really admitting the fact that the process of maturing is complicated and during which the child, through interaction with the environment, creates a set of ideas about what is "normal" and what is "common sense", even in such elementary cases such as the ability to create and maintain relationships, instantly communicate and respect the privacy of others. Based on this, a certain self-awareness and view of the world and its rules are created. What problematic aspects of using digital communication technology by children and teenagers should we keep in mind? Great attention is being paid to a lack of sense of privacy when sharing personal information and the risks arising from this, be it the risk of abuse of this information for the whole family (e.g., information about where the family is going on holiday) or so-called cybergrooming (gradually gaining the trust of children and then exploiting them). Here I would like to briefly call attention to two related problems related to the intensive use of social networks (such as Facebook) and that are far more subtle, less apparent and pertain to a substantially greater number of users.

A survey of American teenagers performed in 2007 showed that teenagers using social networks are more inclined to provide their personal data even in the off-line world. As the original primary function of Facebook is to publish photographs, this finding points to the shifting of the boundaries in the area of respect for the privacy of others. We don't even have to mention deterring examples of mothers who published nude photos of their young children or share photographs of a letter (always confidential) from summer camp. A typical user of Facebook is gradually socialised to a state where it seems normal to post the photographs of others without asking them whether they care or not. If the photo doesn't show a touchy situation, why should it be? The answer to this question is not a matter of course. If we were to talk with teenagers about the issues tied to social network use, we should not forget to discuss that not everyone views the issue of privacy in the same way. The line between what is understood as private, intimate or sensitive is not written in stone anywhere and the gradual overstepping of this line may lead to extremes that will appear normal to us. In adults, this issue is something to smile about, but its importance becomes all the greater to those who are learning respect for others.

Another problem that is partially tied to the issue of privacy is the intensive use of digital means of communication, especially laptops, during lessons. The Czech Republic is still waiting for a tide of measures like those that are being applied to the large number of American secondary and post-secondary schools: complete prohibition of mobile phones, tablets and laptops during lessons. There are two mains reasons for this: first, in the classic method of teaching with the teacher at the front of the classroom, it is difficult to control a student's activities, and not with regard to the student him/herself, but mainly with regard to those sitting behind him/her. If a number of students playing games or watching jokes and photographs on Facebook are sitting in front of a student interested in the lesson, it is very distracting even if the motivation to concentrate on the teacher is strong. Despite the protest of many students, I forbid laptops from being used in class and have seen no negative effects in the quality of the lessons by this move. Another reason speaking in favour of forbidding laptops and mobile phones in class is that these devices distract users and reduce the overall quality of lessons. 2) The objective of formal education is to teach not only a certain body of knowledge, but also self-discipline, respect for authority and the ability to focus on one activity for a longer period of time. Switching between learning and writing text messages and monitoring statuses on Facebook over the course of a few minutes lead to the development of thinking that is no longer able to focus on one activity for a long period of time. This conclusion is supported by a series of studies by American neurologists who compared the ability of children to concentrate and found that this ability was lower in children who devoted a lot of time to mobile telephone and internet use. 3)

A general recommendation is to try to explain to them that it makes more sense to use this technology at a certain specific time and that although it is possible to manage tomorrow's test while listing to music, playing on-line games and monitoring Facebook, the benefits of learning for a test consist in something else other than grades.

Petr Lupač

Petr Lupač works at the Department of Sociology of the Faculty of Arts of Charles University, where he is the lecturer for the courses General Sociology, Social Media, Theory of Diffusion of Innovations and Internet and Society. He took part in study and research internships at Kansas State University, New York University and the University of Liverpool. In the past, he worked at the Faculty of Humanities of Charles University and at the Institute of Moral and Political Philosophy of the Academy of Science of the Czech Republic. At this time, he is heading the project "World Internet Project - Czech Republic II: Analysis of the Social and Political Aspects of the Inequality of Internet Use." He is a member of the World Internet Project, the Masaryk Czech Sociological Association and the Association of Internet Researchers. He focuses on general sociology, social sciences and technology and the sociology of mass and new media.

Notes:

1) - The data used in this article come from the Czech Statistical Office, the World Internet Project - Czech Republic, and from measurement of the use of the internet as part of the American research centre Pew Internet & American Life Project.

2) - The negative effects of using laptops during lessons on student performance and amount of memorised information have been repeatedly confirmed by a set of experimental studies; an older article can be found in Psychology Today from 9 July 2010.

3) More details about this issue can be found in Time magazine, 27 March 2006, and the New York Times, 21 November 2010.

OPINIONS OF EDUCATION EXPERTS

On-line world and School

Information and Communication Technology (ICT) has entered into the various areas of our private, work and civic activities and there is no way it could have bypassed the field of education. In fact, technology is one of the primary factors affecting the development of human society, including education.

It is relatively clear how to protect students from the pitfalls and problems of the real world. There are programmes, procedures and methodological recommendations. The situation is much more complicated in the virtual world of on-line networks. Before we begin to address the issue, we should be aware of three basic things:

1.

The main difference between a student and teacher is not who is better at using ICT. The claim that students know more than teachers or that students will learn to use technology themselves, intuitively, and that it is thus not necessary to focus too much on ICT at school is expressly damaging. And what is more, untrue. In certain cases, some students may have better skills than teachers. But it is not a rule and, furthermore, it usually demonstrates a lack of skills on the part of the teacher and not on the quality of the knowledge or skills of the student.

The main difference between a student and teacher lies in the approach that they take to ICT. For today's children, technology is part of the world into which they were born. It is their nature to learn, and not even the complexity of a system or device is able to dissuade them, as they do not see how complicated something is because of their inexperience. They are ready to use a computer and everything that they gain access to through it in the same away as driving a car (better right away and by themselves). In this respect, the adult is at a disadvantage when faced with something new. He or she has tried many things and knows that in certain situations it is not easy to understand something sufficiently enough to enjoy it and get a satisfactory result. For this reason, adults (not only teachers) contemplate whether to invest energy in further attempts at something and learning something new.

2.

The assumption that the development of new technology will not stop is reasonable. **We will thus never have the opportunity to catch up in peace to what is escaping us in the field of ICT, even if we wanted to.** In fact, there will be ever more new knowledge and technology and opinions will often change. It is necessary to come to terms with this fact and the finds ways to prepare students for life in a world influenced by ever changing technology.

3.

By using new ICT, the nature and structure of our activities is changing; **as a rule, new work processes are set first and then, sooner or later, new social rules** that directly relate to the use of new technology take hold. For a period of time there is certain “anarchy”, a state without rules that would be observed by users. It takes time before social conventions take their place in the new environment. It is also necessary to prepare students for that.

What does internet bring to schools?

1.

Current digital multimedia devices are expanding in an unprecedented way the possibilities of teachers and student to access learning materials and give them the intended skills in practically all subjects.

Information in text, audio and visual form and teaching materials are available via the internet, as is possible contact with other students, schools, people and experts. Internet allows everyone access to a school’s teaching materials from anywhere and makes it easy for students and parents to communicate with teachers.

2.

A teacher who gradually and with determination develops the ability of students to determine how, when and why ICT should be used and leads them to the safe and responsible use of available ICT when doing school-related work, equips his or her students with skills that are necessary for life in our society.

It is clear that to keep students safe, it is not enough to set rules for using ICT in schools and only take the approach of prohibiting and restricting the use of ICT at school. It is becoming ever more common that students have their own devices (notebooks, tablets, mobiles...) that are able to connect to the internet. And the internet is becoming more and more available in various places, not only at home or school, but also in libraries, internet cafes, and even public transport. Rules and restrictions are necessary in schools, but it is also necessary to prepare pupils for situations that they will be facing in a world where they are unprotected.

For a better idea, here are a number of statistics from the publication Information Society in Numbers 2013 issued by the Czech Statistical Office (http://www.czso.cz/csu/2013edicniplan.nsf/p/9705-13):

Czech households with a computer in 2012:
- with children 91.1%.
- without children 58.5%

Czech households with an internet connection in 2012:
- with children 89.6%
- without children 56.5%

What should schools do to secure on-line safety for students?

1.

Incorporate the whole issue into lessons! So that students have the opportunity under the leadership and supervision of teachers to make use of the possibilities offered by the internet and social networks (essentially in a controlled environment with elements of social networks). In practice, they will learn good habits and will learn to avoid risks.

2.

Include the issue of on-line security and use of social networks into school educational programmes, as it is necessary for such lessons to take place in a coordinated and planned manner across all subjects and with regard to the abilities and ages of students.

3.

Support the development of professional knowledge and abilities of teachers and school management so that they are able to deal with this problem at school, incorporate it in lessons and respond appropriately to students’ problems and questions that could arise in class or at school.

4.

Incorporate procedures that ensure the safe use of the internet by pupils and safe behaviour on-line into school rules and the life of the school.

5.

Ensure effective security of school technology and infrastructure.

On-line Security and Social Networks in Frame Educational Programmes (GEP)

On-line security and the benefits and risks of using social networks should be particularly part of personality and social education, media education, health education and ICT, but guiding students to behave responsibly and safely on-line is the responsibility of all teachers who use on-line technology in class.

It is necessary to realise that technology does change and offers ever new possibilities for us (and thus even the potential for risk) faster than frame education programmes are reviewed and revised. For this reason, it is ever necessary to identify the risks and respond to them even though they are not expressly described in GEP. They implicitly appear in GEP there where protection of privacy, protection of health, prevention of socio-pathological phenomenon, personal safety etc. are dealt with.

Daniela Růžičková
National Institute for Education, School Consultancy Facilities
and Facilities for Further Education of Educational Workers

Daniela Růžičková works at the National Institute for Education (NIE) as an ICT trainer and expert for the Sector Council for IT and Electronic Communication under the National Qualification System project. She focuses on didactic innovation in the field of ICT and supports the incorporation of ICT into lessons and school life in general. She formerly worked as an activity manager for the Methodology II e-learning project and took part in developing the environment on the Methodological Portal (http://rvp.cz), where teachers would be able utilise e-learning courses as part of the further training of educational workers. Before joining the NEI, she worked as a teacher (mathematics, ICT) and vice principal at a basic school focused on foreign languages. At the school, she acted as ICT coordinator/methodologist and during the difficult period of the development of the school educational programme and first years of lessons based on it, also as SEP (School Educational Programme) coordinator.

Openness is What Connects Us to Children

Imagine the following situation: a young 13-year-old boy or girl is walking down Wenceslas Square in Prague or some other world renowned place and whomever they meet they give a card with their name, telephone and e-mail address on it. And then they take a picture with some of those passers-by as a souvenir. Wouldn't that seem strange to you? The openness with which young people move about on social networks is amazing - perhaps because you don't need to be shy when communicating in a virtual environment; information there spreads at the speed of light and the digital trace that you leave there is something like Hollywood's Walk of Fame. But our behaviour and regular communication (and social networks are part of our day-to-day life) have certain rules. This is confirmed to me also by being involved in one of the projects of the Children and Youth House in Vratimov, which was financed by the European Union.

When the Vratimov Children's Communication Centre was established in 2009, social networks - at least in the Czech Republic - were beginning their "boom". When creating programmes for children, which made use of very good technical equipment, we could of course not avoid the topic of safe internet, i.e., even behaviour on the networks.

It took our team a short time to agree that Facebook, for example, fully fulfils the desire of every youth to "fit in" somewhere, let the world know about them and use not only their language, but also see, for example, positive reactions to a posting, or just remain in the "shadows" of anonymity and without any apparent responsibility for what they post. And primarily before reminding ourselves that prohibitions have no use here and will be of no help. This of course was known since the time of our youth, but modern technologies have given everything a breath-taking speed. As if it were forgotten that from time to time each of us says, consciously or subconsciously, a half-truth or simply comments on something from our point of view - especially that what I can do, others can to.

Two projects provided great professional help in connection with testing the media for internet security: E-bezpeci (E-security), which is a project of the Faculty of Education of Charles University, and Saferinternet, which is a project of the National Centre for Safer Internet. On their websites we found, among other things, the rules for internet behaviour - netiquette, as well as other terms that we discussed with the children and elaborated through the “media”: cyberbullying, cybergrooming, cyberstalking, hoax, spam, phishing and so on. We tried to inform parents about our findings, but without much response. So we focused on children, adolescents and students.

What proved to be successful, and what we are applying today, was discussion about certain topics. During our media meetings, we worked in small creative teams, the objective of which was, for example, to create a presentation on the possibilities provided by social networks. The children’s interests were focused on Facebook in particular. There is nothing difficult about finding out about how to create a profile, how to secure it, what and what not to put on it. Everyone was able to list exactly how to behave on social networks. Then we, adults, began to ask questions and this is how a typical conversation looked like: “How old do you have to be to be on Facebook?!” “Thirteen.” “How old are you?” “Twelve.” “So how did you get on Facebook?” “Because I wrote that I was 36. Everyone does that.” “So let’s look at your profile, to see if you are following the advice that you gave. Let’s open it up on the interactive table.” “How come? You can’t do that!!” “We don’t understand. What can’t we do?” “Open my profile in front of everyone!” “But at this very moment 100 000 people could be looking at your profile and that doesn’t bother you?”

We believe that even though similar meetings had an open ending, i.e., without a specific conclusion, it gave everyone something to ponder. And that was and is very valuable. We noticed this in other media lessons, where there was discussion about computer games, especially those on-line, or about spammers, advertising, on-line shopping, as well also identity theft. The element that connected us and the children was openness. We understood that we don’t want to pontificate at all costs, but that we are imparting information that they should take into account. We tried to give an object lesson of how easy it is to mislead and be misled on social networks. Our colleague, a forty year old, created the profile Martina 15 and began to chat. We chose a number of students at random from schools that we worked with and our “Martina 15” began to communicate with the children. After some time, one girl wrote that she could not find a certain book about horses. Martin 15 responded that she had the book and if the girl gave her telephone, they would certainly make arrangement to lend the book. And the girl did. We did not publish the name of this girl or any details; it was enough at the time to show who in fact was Martina 15.

We proved to ourselves that obtaining personal data from some young people was very easy. And it is not enough for them to know how to protect themselves. The problem is much deeper than that and also pertains to parental control, or, more precisely, how great their interest is in their child, how their time together looks, and what their communication looks like. And the same is true in schools and other institutions. When it comes to modern media, the majority of youth have excellent knowledge of it, but many of them lack experience that the adult world should perhaps be obliged to pass on to them.

Eva Bělohlavá,
Children and Youth Centre Vratimov

Eva Bělohlavá acts as a leisure time educator specialising in media education for almost 20 years. She is a graduate of the Faculty of Journalism of Charles University. Media and children's media creation has been part of most of her life, and not only while a staff member of the Vratimov Children and Youth House, where, at the Children's Communication Centre, she teaches interested parties how to work with media. Eva Bělohlavá has also been teaching the subject "Communication Skills" at Jan Amos Komenský College in Ostrava in the Media Communications field.

How to Protect the Persona of an On-line Teacher

We hear about protection of personal data protection of internet users day after day. The media bombards us with cases of serious violation of the principles of ethical behaviour in the on-line environment, and breaking the law through such behaviour is not an exception, where such unlawful behaviour can no longer be seen as a simple misdemeanour, but as a crime. The school environment, where children naturally test the limits of what is possible, tends to be quite rich in such behaviour. In my work as a teacher of teachers, I often encounter the prevailing opinion that the internet and social media in particular are not bringing anything good, and so we should try our best to protect students from these revolutionary products of modern civilisation. I think it is necessary to think a little bit about this issue.

If we imagine protection to be in the form of forbidding children from using such technology, we will have to come to terms with the consequences of such measures. Technology has managed to wholly infiltrate life outside school and working with it is an important skill for each and every inhabitant of economically advanced countries. Trying to eliminate its effects only makes schools into museums where things have little to do with life outside school and with the work that graduates will eventually do. By continuing with such policies, schools are exposing themselves to a very dangerous situation where people will begin to ask what schools are actually good for. I would not like to see things get to a point where schools become nothing more than a babysitting service for working parents. It is extraordinarily difficult to convince most teachers that it is absolutely necessary to introduce technology into schools. The biggest obstacle is probably the fact that no one is asking them to do so directly. What is more, they are ill equipped and it's not an easy subject to teach. It requires relatively specific knowledge that is not taught through traditional teacher training programmes.

Obtaining full-fledged qualifications in the field of technology today means updating one's knowledge at the same speed that technology is developing at. Traditional studies may only initiate such efforts. Everyone then has to proceed on their own. It is not possible to manage without access to the latest knowledge. In reality, this means the need to master the functions of social networks, through which it is possible to connect to those teachers that Hippel calls lead users **(Hippel's technological innovation in education)** 1). They are today in the majority of cases willing to share their knowledge with others (e.g., the blog Pepoušův nápadník) 2) It is of course very beneficial when teachers do not restrict themselves to the domestic environment and try to be connected internationally.
Teachers have **(according to Prenský)** hitherto been considered immigrants to technology controlled space. And if even students view them in the same way, this state is unsustainable. Lessons are ever more moving to the on-line environment and are carried out through non-formal means. The teacher has to be able to link school activity with what students are doing on-line. It is no longer about posting an assignment on the web and receiving the completed work by e-mail. If we do not like what our children are doing on-line, we have to try to influence them positively. And so today, each teacher will in fact be dealing with an issue that David White,

professor of education technology at Oxford University, has fittingly described. Should a teacher rather become an on-line **visitor or resident?** 4)

Today, even a visitor is able to send an e-mail, download a file or find a train connection. They may use the internet, but they do not leave any traces of their presence behind. They are usually afraid that someone could use what they leave somewhere on the Internet against them. I often see similar fears even with our student teachers.

Pupils behave completely differently. Most of them desire to have a profile on social networks and be present even at a time when they can't be on-line. They are clearly on-line residents with all of the risks that ensue from this. I will remind the reader about the entirely silly effort to compete who has the most contacts, the reduced ability to perceive the significance of longer text, the possibility of becoming addicted to the need to constantly check for news **(Technology-Related Risks according to Rosen)** 5) and, what has been probably discussed the most widely, the lack of self-control when publishing personal data and photographs. The fundamental questions is, however, to what degree can teachers contribute to improving the current, often negatively perceived, situation. One thing I know for certain: prohibiting the use of mobile technology or publish own work, photos or videos in cases where it is not possible to directly ascertain personal data (surname, address, etc.) will not help the situation. This issue is described precisely by Julie Cunningham (see **Nameless, Faceless Children**) when she says: " I would say that they primarily need protection from themselves… that they need help moderating their web presence until they understand the full ramifications of things they say on-line. *I don't think that means they need to be anonymous. I do think that anonymity tends to foster less responsible behaviour, in both children and adults alike."*

The primary recommendation for what to do is in reality the same for students and for teachers. It is necessary to create one's persona in the role of resident, or to create one's "digital trace" systematically. As we always have to count on the fact that nothing is ever lost on the internet (**Let's Not Forget to Forget** 7), **Brewster Kahle and His Wayback Machine**); it is necessary to realise this from the beginning of one's virtual time there. There are too many cases where someone posts something that they later regretted **(Facebook Follies on HBO)** 9).

On the other hand, this does not mean that we should be afraid to reveal something about ourselves under any and all circumstances.

Teachers may have an educational influence in the on-line environment, but only if they are not afraid to share their opinions on-line. They have to determine the degree to which they will allow their lives to be public. White reminds us here that this line may depend on the persona we choose - one for contact with friends and one for students - but I would not recommend this too much. The risk of exploitation of “secret” information only shared with friends is significant. With full knowledge of the fact that I belong to one of the most communicative teachers around, I will try to show my own level of openness through specific citation from a **channel** 10) of the class **Educational Technologies of the 21st Century**, which I began teaching this year at the Faculty of Education of Charles University.

It is a commentary to the recommended American portal Personalize Learning 12) from 29 March 2013: “The very first video you come across (Water Music Video) reminded me of my own journey after knowledge. I wanted to become a sound engineer when in basic school and helped a number of my classmates’ bands. Sometime in 7th grade (at the time of the heavy “normalisation” of 1970), I got a fairly good idea and recorded a 15 min. strip about Lenin. We needed help from the school, where we had a studio. At the time, a new “board approved” principal arrived at the school. You wouldn’t believe how much this suited me. He sent me from classroom to classroom where I played it in Civic Education classes. Essentially, he created local star out of me with all of the consequences that later resulted from it (only the Czech teacher tried to give me a C, but to no avail). Later, in secondary school, where nobody knew my past work, I got a D for the first time in my life. The only thing I want to say is that one’s own creative work has an irreplaceable place already in school and that today’s possibilities are incomparably better than before. Technology is not the goal, however.”

The majority of top-notch teachers around the world today share some personal information intentionally in a controlled manner with the world around them. You will usually learn in what area they live, how big their family is, information about their pets or various interests and hobbies. Even information about certain public activities are good. The ability to assess what is appropriate to publish belongs to a set of skills that often fall under the term web literacy. And this should be cultivated in both pupils and teachers.

In conclusion, I would like to reiterate that all of the recommendations formulated here make sense only if none of you are indifferent to any violation of the rules. Every school has to have something like a code of ethics on how to behave on the internet **(Code of Ethics for Students and Teachers Working with Information)** 13) and its observance has to be enforced unconditionally. I am convinced that the best prevention is zero tolerance of offences. I recommend that school principals do not hesitate to call the police if there is the slightest suspicion of wrongdoing. And I would like to ask the police to also see their role as educators and accommodate the teachers' wishes. The best prevention of negative actions is the uncompromising punishment of perpetrators. But just the investigation itself and the presence of the police at school may be for many a lesson. Thank you.

Bořivoj Brdička

Bořivoj Brdička has focused on education technology for 30 years. He was there when our schools received the first 8 bit computers, and since then has focused on ascertaining how this technology should best be used in teaching. He tries to acquaint the public and especially teachers with this issue, mainly through Učitelský spomocník (Teacher's Helper) on the RVP portal (http://spomocnik.rvp.cz/). At this time, he works at the IT and Technical Education Department of the Faculty of Education of Charles University, where he teaches a number of subjects focused on ICT didactics in various types of occupational and non-occupational study programmes.

Notes: Links to websites in the text:

[1] *http://spomocnik.rvp.cz/clanek/16599/*

[2] *http://inapadnik.blogspot.cz/#*

[3] *http://spomocnik.rvp.cz/clanek/10639/*

[4] *http://spomocnik.rvp.cz/clanek/14339/JSTE-REZIDENT-NEBO-NAVSTEVNIK.html*

[5] *http://spomocnik.rvp.cz/clanek/17161/*

[6] *http://spomocnik.rvp.cz/clanek/11229/*

[7] *http://spomocnik.rvp.cz/clanek/15183/*

[8] *http://spomocnik.rvp.cz/clanek/17251/*

[9] *http://spomocnik.rvp.cz/clanek/17357/*

[10] *http://www.edmodo.com/public/ukvztech_ls13/group_id/2514570*

[11] *http://spomocnik.rvp.cz/clanek/17233/*

[12] *http://www.personalizelearning.com/*

[13] *http://spomocnik.rvp.cz/clanek/11865/*

CRIMINALITY AND ITS PREVENTION IN THE ON-LINE ENVIRONMENT

Selected Security Risks and the Virtual Environment

A lot has been written about social networks. From exclusively positive reactions to extremely sceptical ones that condemn this phenomenon as a decline in real social relations. Here, the social network Facebook comes up most often. Not by chance. Just like every country or region has certain specific characteristics and certain specific products or services that do well there, the most frequented social network in the Czech Republic is Facebook. It has managed to penetrate certain imaginary barriers in our society and, in the same way, overcome technological barriers, now being accessible via mobile phones, which fact has resulted in a sort of on-line symbiosis.

I do not intend to describe the various functions of this social network; rather, I will try to provide a healthy impartial look at it and, with regard to the area I am most familiar with, discuss the security risks and especially the crimes associated with this phenomenon, or rather the crimes associated with certain individuals abusing the service, to be accurate.

From the point of view of security, a service conceived in this way conceals a number of types of risks.

The first group of risks are the users themselves, who can be a relatively fundamental danger to themselves. Not in the absolute sense, but rather in the sense of ignorance of the terms and conditions of the service and how the service works. It all begins at the moment when a user begins to use the service. Very few users have reviewed in detail the terms and conditions of using the service. Our country is in no way different, and in our work we often come across individuals who are under the age of 13 and have a Facebook profile even though the terms and conditions clearly state that the service may not be used by persons under this age limit. It is also necessary to realise by posting content and information on the network, a user gives Facebook the non-exclusive, transferable, assignable, global and royalty-free right to use such content and information, although they still belong to the user. According to the privacy and application setting, the user makes this content and information available to the public, be it to a small group of defined friends or to anyone who will use the user's information as they wish. Due to mobile applications and expected sharing, it is possible for a user to state not only the information shared by him directly but also all other information created by him in, for example, a smart phone. Videos, photographs, automatic recording of GPS positions, etc. A user often does not even realise that he has set up the photograph sharing function and only learns of this fact after receiving comments from the people around him about photographs that he had no intention of ever making public. Such error may have serious consequences if the information is sensitive and has been shared without any restriction. Such information, when put together, is then a good lead for thieves to break into a well-furnished home, especially when they learn through the shared information where a user is located a given moment in time. Perpetrators who identify such break-in opportunities do not always do so impulsively; there have been cases where their actions have been planned over a longer period of time. In such cases, they took on a different identity and communicated with the victim or even became the victim's virtual friend. Children are the most open group in terms of divulging information; it is possible to acquire a lot of information from their profiles and they are very open in their communication with others.

Fake information and profiles fall into the second group of risks. Just like in other location on the internet, it applies to Facebook as well that although it appears legitimate on the outside, not all information and not every person is real. A good example of this is profiles that state, let's say, ten members of the given group will win a mobile phone every week. More and more users then become members of the page, and once a sufficient number of members are acquired, the status of the page changes. In the best case, the page changes into support for a politician; in the worst, the page changes into extremist propaganda promoting racial or ethnic hatred. There are also numerous fake profiles created with the objective of making fun of the person in whose name they have been created. This often arises as part of bullying, known as cyberbullying in the one-line environment. This, however, does not pertain only to children, as the term may suggest. The police have dealt with a lot of cases where adults were attacked in this way. Similarly, fake profiles are often created for fraudulent purposes, where the perpetrator uses the identity of someone else and such person’s ties to ask such person’s friends or acquaintances for money. These kinds of fake profiles, created for financial profit, are the most common. This is not only due to economic stagnation and inflation, but also because regular fraudsters are learning to move about in the virtual environment as well.

Exploitation and taking control of the accounts of strangers is the third group of risks. Passwords to accounts are obtained through hacking or social engineering. Not only will the perpetrator gain access to all sensitive information that the user need not have shared anywhere, but is also able to act credibly using the user’s identity. In such cases, the behaviour of the perpetrator may have a number of forms. From asking for money from the user to give back the account, through cases where the victim’s identity is used to carry out fraud, to exploitation of all of the victim’s sensitive information or its provision to a third party.

Whatever the possibilities for exploiting social networks, one should always remember that when making use of internet services, there is no such thing as absolute privacy, often through the victim’s own fault. Whatever is placed on the internet and especially social networks, although it is labelled private or intended for only a limited group of people, i.e. “friends” or “friends of friends”, is in fact public. For example, any “virtual friend” can take a screen shot or copy “private” content of a profile and send it onward, post it anonymously somewhere on a blog, and so on. And guaranteed privacy falls apart.

For this reason, it is necessary to continue to inform people and supplement education especially for youth, so that they realise the possible risks to their privacy or the privacy of their loved ones, if they enter the virtual world. We also must not forget that if we publish any content or information using the “Public” setting on Facebook, we are allowing everyone, including people off of Facebook, to access and use that information, and to associate it with ourselves (i.e., our name and profile picture).

On its website, Facebook itself says that it is important to keep in mind that any information shared, either in comments, notes or video chat, may be copied, posted or disseminated in a way that you may or may not have intended.

Karel Kuchařík

Karel Kuchařík heads the Information Criminality Department of the Criminal Police Service and Investigation Office of the Police Presidium of the Czech Republic. He *has been a police officer for the Police of the Czech Republic since 1995. His first work related to investigating economic crime. He then began investigating large-scale economic crime and organised crime. After the creation of the information criminality specialisation at the Police of the Czech Republic, he transferred to this division, where he has been active since 2001. He graduated from the Police Academy in Prague and the SROV Police Corps Academy. He completed many foreign training courses specialising in information technology exploited to commit crimes. He has actively taken part in specialised conferences and lectures and has publications concerning security in information technology, especially cybercrime.*

Author's note:

Last year, the Police of the Czech Republic handled about two thousand crimes committed exclusively using the internet and information technology. In addition to this, the Police of the Czech Republic uses the internet to investigate hundreds of cases. As far as social networks and especially Facebook go, the Police of the Czech Republic has registered 475 cases on the police hot-line over the last 152 days of the year, with the number of cases in the first 111 days of this year being 532 cases. Thus the number of cases in connection with Facebook is growing. This year we are dealing with 53% more Facebook-related cases than last year, which is almost five cases a day, seven days a week.

E-Synergie Project
- Scientific Research Centre for Electronic Communication Risks

The Crime Prevention Department of the Ministry of the Interior of the Czech Republic has for a number of years been working intensively with the Faculty of Education of Palacký University in Olomouc (FoE PU). In 2009 and 2010, experts from the Faculty of Education conducted E-Safety seminars focused on the issue of prevention of a dangerous communication phenomenon: cyberbullying. As part of this project, police officers from the preventive information group and specialists from the Criminal Police Service and Investigation working with youth, where such police officers and specialists come from regional directorates of the Police of the Czech Republic, underwent training. In 2009, the E-Safety project was shortlisted for the national round of the European Crime Prevention Award.

In 2010, the FoE PU submitted the E-Synergy project as part of the Operational Programme “Education for Competitiveness” based on a request by the

Ministry of Education, Youth and Sport of the Czech Republic and asked the Crime Prevention Department to become its partner. Other partners of the project included the Regional Directorate of the Police of the Olomouc Region and Vodafone Czech Republic a. s. The project is aimed at the risks tied to virtual communication in cyberspace and the prevention of criminality related to it.

The main tasks of the Ministry of the Interior as part of the project are of an educational nature. The plan is to train 150 students of FoE PU and 20 academic staff members during the course of the project. Internships, practicums, interactive workshops, and professional conferences are organised. This project is also being promoted via the European Crime Prevention Network.

The internships of FoE PU students at the Ministry of the Interior are being realised at the Czech Police Museum. Students attend lectures on various topics, such as: police efforts in the field of information criminality, police training, investigation of information criminality focused on children, legislation in the field of cyber environment, the National Coordination Mechanism for Searching for Missing Children, the issue of on-line payments, the risks on social networks, situation prevention - city camera systems and protection of personal data, the basics of safe behaviour on the internet based on the experience of the Police of the Czech Republic, etc.

As part of the project, students take part in similar events even at the other project partners. In this way they obtain new knowledge and experience that they would otherwise not obtain during regular classes at university.

Information and communication technology is a fascinating instrument that allows one to make virtual relationships and create virtual groups of people who would otherwise not meet in “real” life. Not every internet user is credible. Because of the anonymity of internet users, it is very difficult to guess who is located on the other end.

For protection in cybersphere, you should use a general nickname. You should not state your name, surname or address, post photos of your family, based on which someone can track you down. It is also important to realise that information about you can be “pieced together” from various sources.

Research over the last few years has shown that in the Czech Republic, 47% of minors have been victims of cyberbullying. The number of cases of stalking, cyberstalking and risky communication on the internet often ending in sexual abuse is rising. The increase in such dangerous phenomena is being registered the world over.

All components that are involved in a child's education, i.e., family, school and society as a whole, should take part in prevention. Just as children are being prepared for the real world, they have to learn to overcome problems that they can encounter in the virtual world.

Iva Fürbacherová
Crime Prevention Department of the Ministry of the Interior:

Note:
More information is available on the website of the E-Synergy project: www.esynergie.cz or, on the website of the E-Safety project: www.e-bezpeci.cz

Iva Fürbacherová joined the Ministry of the Interior in 1994 and since 2002 has been part of the Crime Prevention Department. At this time, in addition to cyberbullying, she is focusing on the issue of victims of crime, especially children who have become victims of serious crimes especially of a moral nature. She is in charge of a specific project for special interrogation room for child victims and witnesses of serious crimes, the main purpose of which is to reduce secondary victimisation of the victim. She graduated from Masaryk University in Brno majoring in social education.

As the Internet Develops, Its Potential Risks Are Also Growing

Children today are growing into an environment that does not distinguish between the real and virtual world. Parents often set up a profile on a social network for their child even before the child is born. Children are surrounded by an environment of which the internet forms a part and on-line communication is a matter of course. These internet natives, or Generation Z, as they are called, have been using the internet from the age of 3 - 4, as a number of studies show. Children spend time on-line twice as much as their parents think they do. Many encounter materials that depict self-mutilation, violent pornography, and cruelty to animals or sites promoting eating disorders. More than a quarter pretend they are older that they really are to gain access to certain websites.

Research carried out on a sample of 825 children aged 7 to 16 and 1127 parents, which was recently published on the Netmums website, show, for example, that children spend so much time on-line that one in three has problems with off-line activities that require concentration, such as reading a book.

The research showed that parents are rarely aware of what their children are doing on the internet. While three-quarters of parents believe that their children spend less than an hour on-line, according to children, the reality is two hours on average. Although two-thirds of children believe that they have encountered certain negative phenomena on the internet, only 22% of parents are aware of this.

Parents often believe that school will deal with these shortcomings and change their offspring's behaviour. Unfortunately, children are on the internet even in school, and consider on-line communication with their peers to be more important than lessons. Teachers often become victims of cyberbullying. Fake profiles are often created in their name, where they are ridiculed without even knowing about it, as most teachers don't have a profile on a social network.

The issue of deleting fake, offending profiles on social networks is no trivial matter. For example, Facebook - today globally and domestically the most used social network - allows fake profiles to be reported. However, if the number of reports and complaints regarding a fake profile does not reach statistical significance, the complaining parties rarely see the profile removed or get a response. In this sense, it is substantially more effective to turn to Horká linka - Hot-line (www.horkalinka.cz), which is operated as part of the Saferinternet project (www.saferinternet.cz). The Hot-line has direct contacts to the appropriate Facebook department in Ireland, and after verifying that the fake profile report is justified, the operators of the Hot-line work on having such profile deleted within 24 hours. It thus successfully deals with dozens of similar requests, as the statistics available on the Hot-line website show.

Fake profiles on social networks are often used to bully over the internet (cyberbullying). Parents often don't even notice that their children are being bullied, and if so, tend to deal with the problem in school. Schools have limited powers in this area, as cyberbullying does not take place in school and is not limited to school hours. It takes place in the on-line environment; what's more, the parents of cyberbullies may underestimate the problem and don't respond in a way that would prevent the aggression. In such case, the school is seemingly powerless. Teachers often do not realise that they can deal with such problems in cooperation with OSPOD, the office for the social and legal protection of children.

Interesting findings from the work of social workers and their experience with the internet are the results of the international SocialWeb-SocialWork project (www.socialweb-socialwork.eu), which is focused on educating social workers who work with children from disadvantaged families. These children may be, and often are, more likely to be exposed to internet risks, such as cyberbullying, but also exploited for child pornography, etc. Even a pupil from a well-situated family at an elite school may feel disadvantaged in an environment of pupils with an even better social standing; he or she may become bullied or be the bully and may be exposed to other risks and threats.

The best way to deal with damaging phenomenon on a social network that is very popular among children and youth, Facebook, which schools sometimes don't know what to do about, is knowledge of the basic and standard procedures and setting up systems for working safely with on-line technology and prevention of internet crime in school. The international eSafety Label project (www.esafetylabel.cz), which is intended for schools, can be of great help in this area. On the project website, which is undergoing its pilot phase, educational staff can find important information that will help them avoid and resolve problems related to the safe use of on-line technology at school. If a school is interested, it can take an assessment test that is based on European standards, and based on the result, verify the level of work in this area. Based on the results of the test, the school obtains a safe on-line environment certificate (eSafety Label) or a plan on how to set up the school on-line environment and how to work safely with on-line technology at school in order to receive the certificate. This individual action plan contains instructions how to create a safe, technically equipped environment for its employees and children.

The internet is ever developing and enriching its users with new ways to obtain information, new contacts and with new ways to entertain. Unfortunately, it also poses new threats. Other than Facebook, which is currently the most popular social site, there are new social networks appearing, such as Ask.fm, that are bringing new risks. Of course, it does not have nearly the same number of users as Facebook or Google+, but the popularity of Ask.fm is growing, especially among young internet users. Ask.fm is a specific network where people make use of the opportunity to ask any question and respond or look for a response to it entirely anonymously. Questions may be in text or video form and users can freely view the profiles of other people and ask them questions directly. The service is very simple - you can ask any individual or a group of users; you can also respond to all comments that follow. The primary selling point of the site is apparent full anonymity. The fact that anyone can ask anything entirely anonymously and without scruples is the biggest lure. This why sex, vulgarism, and harassment can appear in any topic and be so extreme as to lead to bullying.

The danger of the site lies in the fact that it is highly integrated into other social networks such as Facebook, Twitter, etc., where answers to questions can be "liked", appear on profiles, etc. There are also limits to "guaranteed" anonymity. Furthermore, the protection of privacy is not one of the network's priorities - everyone, including unregistered users, can see the questions and answers. It is not possible to set the level of privacy protection. Advice for beginners and young users about how to avoid certain problems is completely lacking. There is absolutely no point forbidding access to the site - if you want to prevent your children, wards, pupils from accessing certain sites, you expose yourself to the danger that they will hide their activities and not tell you when they find themselves in trouble.

The best solution is to show them that such network exists and what problems that seemingly harmless, at least from the point of view of an anonymous person, can cause. It is not possible to guarantee anonymity, especially when the "anonymous" services are linked to personal profiles on Facebook and other social networks. The most effective preventive measure is to set the rules that children should observe and to keep their trust. Only in this way will they not hide their problems, but can resolve them in time and avoid their often frightening consequences.

Despite the fact that the internet is a platform without which it is hard to imagine life today, it is necessary to be aware of the risks that its intensive use carries with it, especially for the target group of children and youth.

Jiří Palyza
National Centre for Safer Internet

Jiří Palyza is the executive director of the non-profit organisation National Centre for Safe Internet (NCSI). He studied Engineering Cybernetics at the Faculty of Electrical Engineering at the Czech Technical University and after many years in the field of publishing focusing on information and communicating technology, he has since 2013 been working for NCSI, where he is responsible for day-to-day operation and support the content of web presentations and related projects.

National Centre for Safer Internet is a non-profit, non-governmental association, whose objective is to increase awareness of possible on-line communication threats, promote positive content and responsible behaviour on the internet, help especially young internet users who get into difficulties and prevent the dissemination of materials with exploited children (child pornography) on the Internet. The NCSI is trying to point out harmful content and displays of inappropriate and risky behaviour in the on-line environment, and provide advice on how to avoid such cases.

Links to the various NCSI projects.

http://www.saferinternet.cz

http://www.saferinternet.cz/vzdelavani/swsw/index.php

http://www.saferinternet.cz/esafety-label/index.php

http://www.horkalinka.cz

http://horka-linka.saferinternet.cz/facebook

The Internet, Social Networks and Hot-line

Unpleasant experiences on the Internet began to appear as a discussion topic on the Hot-line in 2007. Even though the media is paying ever more attention to the risks of internet use, the number of calls about the internet have increased tenfold over the last six years. Last year, more than 300 clients contacted us about this topic. A sad experience from the Hot-line paradoxically copies the results of research conducted by AVG, which discovered that internet users are not very concerned about publishing intimate photographs on social networks and, conversely, are instead wary of relatively safe applications, such as internet banking.

Prevention is Important

Every adult should know how the internet can threaten their child/pupil and what to do in such cases. However, many adults think that they do not understand the internet well enough and that they cannot talk about the internet with children as a result. This should not be an obstacle, however. Ask your child to show you what they can do with a computer. Ask them what you want to know. You will learn something and you will find out what your child enjoys and how they entertain themselves. Don’t forget that even though your children and students surf the web and use terms that you do not know, you do have knowledge they don’t. Knowledge of social norms and, for example, the ability to assess the credibility of text or offers are acquired by age. It is this experience that may often help avoid serious problems. As a teacher, you have two possibilities. Catch up through self-study on important information or invite experts to the school to help you with lessons about the internet. Many institutions or organisations organise programmes for students of various ages that are focused specifically on prevention of internet criminality and on promotion of safe on-line behaviour. The offer of educational programmes, methodological materials and useful information can also be found on specialised websites. We recommend the following in particular:

- www.bezpecne-online.cz
- www.e-bezpeci.cz
- www.pomoc-online.cz

Parents, teachers, educators and anyone else interested in internet safety should read the publication issued by the Safety Line Association (Sdružení Linka bezpečí) entitled “Children and On-line Risks” (“Děti a online rizika”), which focuses on this issue. The publication is can be downloaded for free on the **Safety Line (Linka bezpečí)** website.

The Safety Line Association offers schools the Safety Line in Your Class project. In the block entitled The Virtual World and Me (Já a virtuální svět), pupils become acquainted in an interactive way with the most important internet safety rules. More information about the Safety Line in Your Classroom project can be found on the **Safety Line** website.

When They Get into Trouble or Where to Find Help

Both children and adults can get into a situation on the internet where they don’t know what to do, and need help or support. There is no need at such time to reproach oneself, be ashamed or think about one’s ineptitude. It is clear that it is up to experts to monitor in detail the development of the internet and modern technologies and know how exactly to respond in case of a problem. For everyone else, especially if they are responsible for children or adolescents, it is important to know where to look for help. Certain topics are very difficult to write or talk about or instil great fear. For this reason, organisations often provided help to entirely anonymous clients.

Call Us/Write Us

The Parents' Line is a helpline operated by the Safety Line Association. The number is 840 111 234 and is available Monday to Thursday from 1:00 p.m. to 7:00 p.m., and Friday from 9:00 a.m. to 3:00 p.m. Calls are charged at a preferential rate of CZK 1.60 per minute. Services are provided by the Parents' Line anonymously; it is therefore not necessary to provide any personal data. Parent's Line staff offer family, educational, social and legal advice to parents, grandparents and teachers and have contacts for other professional facilities and institutions.

You can contact the e-mail advisory centre of the Parents' Line at pomoc@rodicovskalinka.cz. It offers e-mail advice in the same areas as the telephone line does and guarantees a response within three days.

Turn to the Administrators

Websites, servers and social networks have both operators and administrators. It is in their interests to ensure that no inappropriate or harmful content appear on the website they operate. Contact information for the administrators should be part of every website. Don't be afraid to make use of them.

Contact the Hot-line

The Hot-line is a web service for reporting illegal or inappropriate web content. If you encounter a website promoting hatred and xenophobia, materials containing child pornography, explicit pictures, violence or any other unlawful materials, report it. You can also turn to the Hot-line if you are not sure whether the material is truly objectionable. Specially trained Hot-line staff will assess the information and, if necessary, pass it on to the appropriate authorities for action.

The vast majority of children and youth use Facebook intensively. The Hot-line website also offers many guidelines and links on how to deal with problems tied to this social network.

In the Czech Republic at this time there are two hot-lines where you can report objectionable or illegal content:

- Hot-line of the Police of the Czech Republic specialises in internet criminality, child pornography, etc.
- The Saferinternet Hot-line also offers direct cooperation with Facebook.

And Where Can Children and Students Turn?

If you do not dare to try lessons on internet safety and you do not have the possibility to invite experts to do so on your behalf, you still have one option open to you. Communicate information to your pupils about where they can turn in case they get into trouble on the Internet. The help that is most easily accessible to victims of internet crime is the Safety Line, which is intended for children up to 18 years of age and for full time students up to the age of 26. It is possible to contact the Safety Line:

- at the telephone number 116 111, which is free of charge and runs non-stop and anonymously.-
- at the e-mail address pomoc@linkabezpeci.cz, where we guarantee a response within three working days.
- via the chat room at the address chat.linkabezpeci.cz. -

Peter Porubský
Head of the Safety Line according to www.pomoc-online.cz.

Peter Porubský (33) studied psychology and biology for teachers at Nitra University in Slovakia (2003). He has devoted his professional career so far to social care, the non-profit sector and prevention of risky behaviour of children and adolescents. While studying, he worked for three years as a consultant for the Children's Rescue Line - the Slovak equivalent of the Safety Line. After completing his studies, he joined the non-profit Forum dárců (Donors Forum) as manager for education, research and company volunteer work programmes. He then was head of the SANANIM Contact Centre, which focuses on caring for people threatened by drug dependency. He completed SUR psycho-therapeutic training, telephone crisis intervention training, motivation conversation training and family advisory training.

He has lived in Prague since 2003. He has been head of the Safety Line since 2010.

ON (UN)SAFETY IN THE ON-LINE WORLD

Risk of Abuse of Webcams in the Facebook Environment

The social network Facebook, which is visited by more than 3.8 million Czech users, contains a host of instruments for communication in real time. These include classic text chat and videochat, which uses webcams. Unfortunately, there is an every growing number of cases where a videochat was faked and users viewed a spurious recording of a pre-created videoloop instead of a real time broadcast.

The phenomenon of faked video recordings probably arose in public videochats based on Chatroulette and is sometimes termed webcam trolling. The primary purpose of such fraud is to have fun at the expense of a pre-selected chatter who then fulfils orders or instructions from someone posing, for example, as a buxom blonde. Unfortunately, in this way it is very easy to extract a host of personal and sensitive information from the unwitting victim, beginning with a true photo of the face to a sexual video.

How Fraud Works

In order to carry out this form of fraud, you just simply buy on-line a programme for about $10 that allows you to create a virtual webcam, whose content can be changed as needed. Virtual webcams as a software instrument behave much like a real webcam. It can be linked to regular instant messenger as well as a videochat devise based on plugins for internet search engines. It is thus easy to infiltrate any web videochat - from Facebook videochat, through G+ Hangouts, to Skype, ICQ or any other programmes or environment supporting videochat.

Then you just record a videoloop that has a boy or girl sitting in from of a computer and chatting. Such video loops, showing both boys and girls, can be found on the internet in the dozens. What is important to note is that for the entire recording, the person does not talk. They pretend, for example, that their microphone is not working and so will be chatting to you via text and only their face will be seen on the screen.

Short Excursion into History

The first server that displayed such victims began about three years ago. At this time, one can find dozens on the internet; the most successful then have tens of thousands of views a day. The most widespread are servers with video sequences of children, especially boys of 13, for a “chat” leading to requests to show intimate areas of the body or masturbation. There are videos where the attackers’ requests focus on specific sexual practices, videos showing a number of victims at once have a great number of views. “Victims are manipulated in such a way that after a number of minutes of footage, they are fulfilling the attackers’ instructions and even heterosexual individuals are conceding to various sexual practices with friends of the same sex on video,” says Martin Kožíšel, internet security manager of Seznam.cz.

Abuse of Fraud for Cybergrooming

It is also relatively easy to use fake webcams to manipulate children to meet in person (cybergrooming or social engineering). Fake webcams look very real and children as a rule don’t know webcams can be fake. They may thus trust the person on the webcam enough to be willing to meet them in person. The degree of danger form falsified webcam recordings is thus higher than in, for example, situations where a child and aggressor exchange photographs.

How to Identify a Fake Webcam and How to Protect Yourself

The easiest way to identify webcam trolling is the lack of sound on the video. If the user on the other side of the webcam begins to make excuses that he or she does not have a microphone and can’t respond in real time, than the webcam is probably fake. Most available video loops do not contain sound; the displayed persons usually do not speak on the camera, communicating instead through text chat.

Another way to verify whether the broadcast is real or fake is to ask the person to verify their identity by some sort of text in real time that can be seen on the webcam, such as writing a name or date or agreed text on a piece of paper. It is easy to confirm the identity of the person in this way.

Cases in the Czech Republic

This year, the E-Bezpečí (E-Safety) project (www.e-bezpeci), registered a number of cases where manipulated video recordings from virtual webcams were used in communication. These were used especially to obtain sensitive material from victims and these materials were then used to blackmail the victims.

Examples of video loops used for falsifying records are available on www.youtube.cz.

Where to Find More Information

Further information on the risks of communication phenomenon tied to the internet can be found on the E-Bezpečí portal (www.e-bezpeci.cz) or on the website of the Sezname se bezpečně! (Meet safely!) project (www.seznamsebezpecne.cz). Both websites contain advisory sections where you can report cases of ICT misuse and ask for help.

Kamil Kopecký,
Palacký University in Olomouc, E-Bezpečí

Kamil Kopecký heads the Centre for Prevention of High-Risk Virtual Communication at the Education Faculty of Palacký University in Olomouc and has headed the national E-Bezpečí project since 2008. His pedagogical and scientific research efforts focus on media education, communication and information systems, modern trends in electronic communication and high-risk communication in the virtual environment. He specialises in risky behaviour in the virtual environment, crisis intervention, computer crime and safety research (cyberbullying, cybergrooming, sexting, stalking, cyberstalking, social networks, and personal data protection). He is the author of numerous scientific works focused on high risk behaviour of children in the virtual world, on crisis intervention and on crime prevention and safety research. He is an expert in safety research, development and innovation at the Ministry of the Interior of the Czech Republic - IS BVaVaI ČR (Information System for Safety Research, Development and Innovation) (since 2011), assessor/opponent for type A projects, FRVŠ (University Development Fund) (an agency of the Council of Higher Education Institutions), assessor/opponent for IS BVaVaI projects, SIPV lecturer (module P), member of the Czech Pedagogical Society (since 2009), TAČR (Technology Agency of the Czech Republic) opponent for the Alfa programme (since 2012), and member of the Czech Association of Educational Research. He is a stakeholder in more than 40 *grant projects, of which 80 percent are aimed at the area of high-risk behaviour on the internet. He works closely with the Police of the Czech Republic, Seznam.cz, Google CZ and Vodafone. He heads the on-line advisory on E-Bezpečí focused on dealing with high-risk cases of ICT abuse. The author's work is indexed in Web of Science and SCOPUS.*

Changes in Safety - Focus on Facebook

In the last three years we have seen a shift in the area of educating internet users and their greater discretion. But try asking someone directly. You will probably receive a general reply in the sense "I'm not doing anything wrong and I'm being careful." Intuitively we feel that being careful is simply not enough, even if we don't know exactly of what. In this short text, I would like to focus on a number of questions: What specific steps should we take to protect our privacy to the maximum extent possible? What risks are we exposing ourselves to? And have any changes taken place recently? Of course, many people have already discussed these questions. The problems facing us are of course more extensive and require experts to comment on them. As a sociologist, I however see one important thing when teaching students or in discussions with respondents: all these risks or too abstract for us. I would like to discuss them from the perspective of our daily lives.

I have decided that I will at least touch upon certain topics that seem substantial to me, such as the most widespread phenomenon of the last few years - the social network Facebook. Many of us know it well - or do we? When my students or I interviewed young people, it became clear that the majority of them are convinced that they are doing enough in terms of safety in cyberspace and definitely do not need any lectures on this topic. After all, it is they who grew up with the internet! When at the interview we ask them the specific steps that they have taken or what they are doing for their safety in cyberspace, we only get a shrug in response.

The Facebook phenomenon should call attention to one of the basic principles that the Internet continues to emphasise: we are always one step behind. Five years ago, the number of users in the Czech Republic was limited to a narrow community of university students; now, about three million people are using it. Not a week goes by that we do not read on websites on the development of technology and the internet about some changes related to this social network. New problems continue to arise that we will have to potentially resolve. It is not enough to learn "how and where to click", as was the case in the past with the vast majority or programmes, as such "magic button" may be somewhere completely different within a month. We have no alternative but to try to understand the issue.

Let's go back to our tour of Facebook. First we sign on. In the last few years, an important change has taken place: more and more often, we are connecting to it from our smart phone or tablet rather than from a classic computer. We entrust all our data to these devices. They no longer contain just a list of telephone numbers. Now they often contain our private data: diary, e-mails, text message archive going back two years, access to social networks, applications and, most recently, internet banking. Despite this fact, we do not block our phones and we0 leave them lying around. So sooner or later you find out, in the best case scenario, that the language of your mobile has been set to Hungarian, or worse, your friends will get a serious offer to go on a date with you. Both are essentially minor nuisances (unless the recipient of the message has long hoped to be asked out on a date with you). A great, but no less real problem occurs when a stranger get access to your accounts because you left your phone lying around.

You enter your password. Most of us, despite being able to name all the rules for passwords, have the same password for signing onto Facebook as when registered for the last e-shop where you bought something. And unless you have a bad experience with a stolen password, nothing will force you to change it. But then it's too late. Are we not right?

As a rule, once inside the social network, we move about freely. Of course, we sort of believe that only our friends see us, but usually that's not the case. Facebook, being a company, is of course interested in us sharing everything with everyone. Essentially, whenever you are not completely sure that the opposite is true, count on the fact that all your data are available to absolutely everyone. To make sure, browse through the privacy setting menu (it location and form often changes dynamically - but at the time of writing this article, it is on the blue bar at the top under the padlock symbol). Of course we are not doing anything illegal and thus have nothing to hide. It is, however, very useful to realise a number of things.

First, it's worth thinking about who you have listed among your "friends", your contacts in the social network (it is interesting how in the Czech context one website practically overnight changed and devalued the meaning of the word friend). You grandmothers? Your parents? Former, current and future partners? How much would the information you last posted surprise them? Especially if written at the spur of the moment (i.e., without thinking)? Other than family, we often have colleagues and teachers listed in our contacts. Who all is a member of a group that you contribute to? All that may seem trivial; nevertheless, each year, our students surprise us with their candour and openness regarding the quality of our lectures, alternative ways of elaborating papers and so on. And please don't think that we are spying on them; we only run across this information when it is offered to us by Facebook.

A more complicated situation typically arises when you post a photograph from the last weekend and tag your friends. Even they have their grandmothers, mothers, and bosses. Would they want their grandmothers, mothers and bosses seeing them on photos taken from the last successful birthday party? And would you? Let's go on. The vast majority of information on the network can always be tracked down. And can be tracked down even years from now. And if we add that it is now common practice that before a job interview, your possible employer gets an overview of information that you published on the Internet, it may be worth thinking ahead more than just six hours (after which Facebook assess your news as old and no longer offers it to you "friends").

The majority of users on Facebook rather watch what others are doing than actively contributing. One of the main functions of this social network is to express one's opinion by joining a group that promotes a certain long-term or short-term opinion, pertains to a particular interest or is of an entertainment nature. Especially in the past, renaming and changing the focus of a group was as a rather widespread phenomenon, so one day you could be a fan of a group called "For Better Carrots" and the next day the group would be supporting some sort of current politicised topic. At the time of writing this article, a similar, but much more current display of mindless trust, pertains to clicking on links that your "friends" have posted on their profiles. Especially when it comes to a simple link with an enticing photograph or general commentary in English ("Hey guys, you will like it!!" - especially if the link is posted on the profile of a person that does not have English as their first language or English is not their primary hobby), clicking on such a link could lead to various escapades. They usually end with your antivirus blocking potentially harmful software, but it is quite possible that invitations to the page that you just clicked on will be sent to everyone listed on your account.

Usually it is embarrassing and annoying. It is often hard to resist wanting to know something we do not know. Countless sociological experiments with a big red button labelled “Don’t press” end within a minute and say a lot about human nature. The last topic in this area is about applications, which are very widespread especially among Facebook users. Games, horoscopes, friend comparisons, “do you want to find out who has been viewing your profile?” (if this is your red button, I can promise you that still won’t find out if you enter this application), and others. Although most of them may be accessed from Facebook, they are operated by different companies that when you agree to the terms and conditions (have a read, it’s truly interesting reading) you, as a rule, are making all your access data available. In some cases, you are supplying all your contacts with an invitation to the application in question (you are then particularly disliked). As a rule, the data that you gave on Facebook is also given to the authors of various websites if, instead of registration you use the “sign in via Facebook” option.

I think it is generally not a problem learning how to identify possible risks (that I may have touched up in excessively layman’s terms), as most young people know how to do so already. The problem is that they are not up to date. Just as you can never help a smoker by listing possible future health complications. This especially concerns a set of common habits that we, who teach, write and speak about these issues, first have to learn to observe. Quite logically, not being part of a social network is for most young people not a solution. Immediate profit from the possibility to quickly and easily communicate always outweighs the possible risk of loss of data sometime in the future. Protection of our data should become a natural part of our stay on the internet. A good first step is to choose a suitable password to the most important services that we use.

Martin Buchtík.
Public Opinion Research Centre
Institute of Sociology of the Czech Academy of Sciences

PhDr. Martin Buchtík is the head of the Public Opinion Research Centre at the Institute of Sociology of the Czech Academy of Sciences. He completed his Master’s degree in Sociology at the Social Sciences Faculty (2009), where he is now a lecturer and working on his PhD. He focuses primarily on the methodology of socio-scientific research and on the issue of internet and cyberspace and social *cohesion. He is the co-author of LiveOnLine, a methodology concerned with internet education (www.liveonline.cz).*

Transfer of Personal Data from Personal Computers to the Internet

General Trend

We are generally monitoring the trend of transferring private data from personal computers to the internet - i.e., a great and greater expansion of so-called cloud solutions. This trend began about ten years ago with users shifting from-email programmes to webmail programmes (i.e., access to e-mail through websites), which has gradually expanded to a broad range of data-related tasks.

We can randomly mention on-line diaries, photograph archives, or even general storage sites providing an alternative to storing files on the hard drive. On the one hand, these services provide a much greater level of comfort, protection of data from loss and a broad range of possibilities for sharing and cooperation; on the other, in case of unauthorised use or access, there is the threat of an unprecedented compromising of a broad range of personal data.

If we consider the ever growing link between Facebook services (for example, you can access a lot of other services through one's Facebook account), it is more than fitting to adopt certain basic security measures.

Passwords

Use a combination of upper case and lower case letters, numbers and special symbols.

Use longer passwords (8 characters or more), but ones that you can remember.

Use a unique password for each service, i.e., make sure each password differs from other services.

Do not link important services together.

Use a two phase authentication (through a mobile phone, etc.), there where possible.

Protection of Children on Facebook

Facebook has become the most popular social network and even though the theoretical age limit to have a Facebook account is 13 (one has to confirm this when registering), children who are much younger are setting up accounts. Through these accounts, such children can be easily contacted by strangers, more easily and effectively than the previous popular chats and messengers such as ICQ.

We feel an increased need to speak with children about using Facebook and other social networks and if you do not have an overview of what social networks are, it will probably be necessary to connect to them.

Smart Phones

More and more children are using smart phones or tablets and it is important to be aware of the risks tied to it. If a telephone is stolen and it is not properly secured, an attacker can access an account linked through the telephone even without knowing the PIN code on the SIM card. Due to the prevalence of the Android system in the Czech Republic, this particularly concerns Google accounts. A Google account can contain e-mails (Gmail), diary or even search history. Breaking into it could mean a serious leak of personal data.

Jakub Chour, Filip Kábrt

Jakub Chour – studied sociology (Faculty of Social Sciences of Charles University). He focuses on performance marketing at the company H1.cz. He gives public lectures on e-mailing and display advertising, writes for Mediář.cz and works externally for the Rekonstrukce státu (Rebuilding the Country) initiative, for example.

Filip Kábrt - studied at the Faculty of Mathematics and Physics at Charles University. He works as a freelance IT consultant and programmer and is primarily interested in the internet and social networks. He acts as a lecturer of experiential education at the non-profit organisation Velký Vůz.

Cyberbullying and Cyberattacks on Social Networks:
Technical Possibilities of Prevention and Intervention

Cyberbullying is a modern phenomenon that is closely tied to the expansion of information and communication technology. Some serious cases of cyberbullying are today well known from the media; although cyberbullying is a phenomenon that should certainly not be underestimated, it is not as prevalent as the news in the media make it out to be. In this article, we first have to ask: What is cyberbullying and how does it differ from other cyberattacks? Then was can focus on the possibilities of prevention and intervention of cyberattacks on social networks.

Let’s first define the term cyberbullying. For something to be labelled cyberbullying, this phenomenon has to fulfil certain criteria:

1. It is aggressive and intentionally harmful behaviour via the internet or mobile phones - it is not a random attack or joke that was misunderstood, but intentional behaviour with the aim, of hurting the victim.

2. This aggressive behaviour is repeated - it is not a one-time event but a long-term problem.

3. The victim of such behaviour is unable to protect him/herself in a simple way - he/her is unable to stop this aggressive behaviour directed at him/her (in such case, this behaviour would not be repeated).

4. The victim sees it as harmful - the behaviour is unpleasant and hurts the victim.

Such described cyberbullying is a serious problem that leads to many negative consequences for the victim - lower self-esteem, anxiety and depression, deterioration of relationships with other people, psychosomatic problems, and sometimes even suicidal thoughts. Such cyberbullying is, fortunately, not common only 6% of Czech children aged 12-18 encountered this (see http://www.cyberpsychology.eu/team/storage/2012-Machackova-Online_obtezovani_a_kybersikana.pdf). Cyberbullying is often tied to bullying at school - essentially it is some sort of expansion of bullying at school to a different environment (i.e., on the Internet), where young people can be found. As this problem in most cases is based in the “real world” offline, it needs to be dealt with in the real world as well - it is necessary for both the school and the victim’s parents to become involved (see http://www.cyberpsychology.eu/team/storage/COST-2012-cyberbullying-Doporuceni_k_prevenci_kybersikany_ve_skolnim_prostredi_prehled_a_rady.pdf).

It is possible, however, to encounter aggressive behaviour that does not have all the attributes of cyberbullying. This is, for example, one-off unpleasant e-mails or messages, slander on social networks, theft of passwords and pretending to be someone else - with some of these attacks often being understood by the one doing them as jokes or teasing. However, even such cyberattacks hurt or are not pleasant (although their consequences are not as serious as cyberbullying). There are various technical forms of protection against such attacks to prevent the further continuation of such behaviour or minimise the chance of their occurrence.

Although this bulletin focuses primarily on Facebook, we shall focus on the following overview of recommendations, especially technical advice, in this environment. On Facebook, cyberattacks may take on the following form:

A. Private message seen only by the sender(s) and recipient.

B. News or other content (photos, videos) on the profile - other people see this content according to how the visibility is set or through labelling (or “tagging”) of the recipient in content published elsewhere on Facebook. Explanation: On Facebook, tagging allows you to, for example, add a link to the profile of the person depicted on the photograph - thus his or her name is indicated and by clicking on the name, you are transferred to his or her profile. Such photographs, although published on Facebook originally elsewhere, then appears in the profile of the tagged user.

C. Theft of a profile and user impersonation. This happens, for example at school, provided someone forgets to sign out of their profile. A classmate make take advantage of the situation and write an offensive profile status - for others, it looks as though the status was written by the owner of the profile although in reality it was written by someone else.

D. Creation of a false, offensive profile - someone creates a profile in someone else’s name and the profile is full of offensive content and other people believe this profile to be authentic.

What to do to prevent cyberattacks on social networks:

1.

The most important things is have the profile secured properly and set up so that no one, other than you, is able to log on, so that you can prevent things you don't like appearing on it.

2.

A properly secured profile is one that is protected sufficiently with a strong password that no one knows. The name of your pet or your date of birth, for example, is definitely not a safe password. A password should not make sense and should comprise a combination of upper and lower case letters, numbers and preferably other text symbols. So that you don't have to write down the password (that is also not safe), it's best to use an abbreviation of a phrase that you remember: For example "4&20BBBIaP" is in fact "Four and twenty blackbirds baked in a pie".

3.

Always sign out from your profile when leaving the computer. Never click the "remember login data" option offered by browsers on a public or someone else's computer.

4.

Set up a profile so that only approved users (i.e., people who we have in a list of friends) can see it. It is possible to set this up for everything that we post, but can be changed individually for certain content (e.g., certain photos can be set to be seen only by a number of friends and others for all Facebook users). It is also possible to divide friends up into a number of different groups and to give each group a specific setting - e.g., we can have a group of close friends that can see everything we add and then a group on which we place restrictions on what they can see, e.g., we allow them to see status updates but not photos.

5.

It is also possible to set up a group of people who can enter content on our profile and who can see the contents that we have tagged. In the same way, it is possible to set up content, so that we first have to give approval before someone can place content on our profile. This will help us avoid situations where someone tries to post vulgar photos on our profile.

6

An important warning goes hand in hand with setting up the visibility of profile - only add people we really want to and really know as our friends on Facebook. It is important to realise that on Facebook, in the vast majority of cases, we appear in our own name and in addition to our name, there is a vast amount of other identification data (if we fill it in) - place of birth, school attended. Some users even have their full address (which we certainly do not recommend). If we add a stranger as a friend and he/she has access to such data, we can be quite surprised to find this stranger on our doorstep one day.

What to do in case of cyberattacks on social networks:

1. Report it. Beside each content, Facebook offers the possibility to report to administrators whether the content is in some way objectionable (it is offensive, spam, or violates copyright). Such content is then assessed by administrator and, if the report is legitimate, erased.

2. It is possible to report theft of profiles or fake profiles to administrators.

3. Deleting a user from friends or blocking a user If someone sends an unpleasant message or posts unpleasant content, it is possible to set up the possibility to block this person. The blocked user then does not see your profile (and we cannot see his either), thereby preventing him from continuing such behaviour (in this case, sending unwanted messages or posting unwanted content on your profile).

4. Once we report the harmful content and block the users, it is worth paying special attention to the overall profile settings (see above), so that a similar situation does not occur again.

Similar advice applies elsewhere on the internet - when using e-mail, discussion forums, and so on. It is always important to have your account properly protected with a password, not be afraid of an annoying message and report such user. If we behave wisely and responsibly on the internet, we do not need to worry about cyberattacks. If cyberattacks start to repeat and morph into cyberbullying, it is important to deal with such situation “off-line” - if the bullies are classmates, the school needs to be contacted; if the bully is an adult, it is even possible to contact the Police.

Lenka Dědková

Note:
The author of the text was supported under the VITOVIN project (CZ.1.07/2.3.00/20.0184), which is co-financed by the European Social Fund and the budget of the Czech Republic.

What to Be Careful about When Working on Facebook

At this time, social networks are extremely popular. There are good reasons for this - these networks provide many benefits for their users. Their use also carries some disadvantages and risks, however. We will look at both aspects briefly. Let’s first summarise the typical features of on-line social networks: they are websites that allow users to create their own profile and set up a list of people with which they want to share this profile. In this way, a user’s “social network” is created - simply said, mutually interconnected profiles of people on this website are created. This network of friends is usually visible and can be easily monitored. This is the basic setup; various networks then add various applications and settings to differentiate themselves from each other. As the most popular social network in the Czech Republic at this time is Facebook (according to the latest statistics, there are just under 4 million profiles in the Czech Republic - see http://www.socialbakers.com/facebook-statistics/czech-republic), we will be talking specifically about it.

In addition to creating a list of friends, Facebook allows other activities that are used abundantly by users. It is possible to talks with others, post your status (a short message typically about what you are doing or thinking about at the moment), photos and videos, organise events or link to other websites. It is possible to communicate a message to everyone with just one click where, for example, a concert of a pop group is going to be held or, in the case of pupils and students, what was in that day's Czech test and where to find and print the best crib-sheets for chemistry class. Similarly, within minutes it is possible to not only show a new computer game commercial, but also a photo with a new haircut or an entire photo album from a weekend birthday party or from skipping school. All these activities can also be commented on and "liked", or content can be labelled with a thumbs-up icon. It is possible to "like" almost anything on Facebook - products, music, film, athletes. You can usually find anything you can think of on Facebook and respond to it with a "like" or a commentary.

Websites that you "like" are then displayed in your profile and other users can view them. Thanks to "likes", we can learn on Facebook what other people like and compare our interests or be inspired by them and then try out the "liked" (i.e., essentially recommended) thing. In this way we very easily maintain an overview of the lives of our friends and share interesting things. It is also possible to chat in private, and a large amount of communication that had previously been taking place on the internet via chat or ICQ has now moved here. Facebook supports various on-line applications, such as quizzes or simple games to entertain the user.

All in all, a lot of interesting things are taking place on Facebook that not only young people enjoy. Students simply like to share information and content that they like - thereby showing who they are a why they are interesting. And they like to boast about experiencing something interesting or being in an interesting place. In the same way, they like to follow the profiles of their friends and comment on experiences and information shared here.

That all of course took place even before Facebook - young people spoke to each other about their interests and lives, showed photos from holidays, gossiped about people, and copied crib-sheets. What changed with Facebook, other than the speed at which this is done today without being together physically, is the storage of records about their activities. Young people are really not aware of this feature of Facebook and, if they are, don't really care. But it is this feature that raises questions about the protection of privacy and personal data. It is important to realise that just like everywhere else on the internet, everything that we publish on Facebook can easily be copied and stored. When, for example, we publish a photo of ourselves that someone else likes, it can be downloaded immediately and stored as long as desired or posted elsewhere on the internet. If, over time, we decided to delete this specific photo from Facebook, no one can guarantee that half of our list of friends doesn't have it stored elsewhere.

The same is true for all other data - date of birth, statuses, "likes". Everything can be downloaded and stored, and even though we have deleted the original content, we have no control over the copies. At the same time, we never know in the internet environment where (and by whom) our data can be stored. Of course, a lot of things published by young people on Facebook are harmless - if they share a status or show a photo of the new bike they got for their birthday, this information will probably not be exploited. However, if they mention on their status how they cheated on a math test, they risk that this information will get to the teacher. This may happen even if they only have real friends in their list of friends. Over time they can fall out with a friend, and such shared information could be used against them as a form of revenge by the former friend.

But we can have control over what we publish about ourselves - it's enough to think about what information we really want to share, what not at all, and with whom we want (or don't want) to share it. This is applicable even in the off-line world. On Facebook there another question to ask: What are others sharing about us? The information that you cheated on a test can be posted by someone else. This information can begin to lead a life of its own and we have no control over it. For this reason, it is necessary to think not only about what we publish on Facebook about ourselves, but also what we post about others. Let's follow this rule: "What you don't want others to publish about you, don't publish about them."

Privacy issues on Facebook also have a different dimension. We should also think about the fact the Facebook itself stores data. Facebook also stores information (in addition to information published by the user) that other users (for now) can't access - e.g., the photos and profiles of users you are observing, what websites you are looking at and what links you are clicking on. In this way, it also obtains information about files you are sharing on Facebook (e.g., when they were created and who was the author). If you have GPS, Facebook records your position, in the same way that it does the IP address of your computer. Information about your movements is not obtained only by Facebook -- if you visit a page that is linked to Facebook (you can comment on it via your Facebook profile) and if you are signed into your profile on a tab beside it. Facebook will record your visit to the website in question and store it. In the case of data obtained by Facebook, deleting your profile won't help as Facebook stores it for a "as long as it is necessary to provide products and services to you and others (...)" (see http://www.facebook.com/about/privacy/your-info), which is so vague a formulation that it could mean "forever".

At the same time, Facebook obtains the non-exclusive, transferable, assignable and royalty-free global licence to this information as well as all content posted on Facebook. This means that it can essentially do what it wants with your information, including selling it to other parties. This fact is used by some employers who want to find out as much information about potential employees. Publishing statuses such as "Tomorrow I have an interview at an evil company that I hate" may likely backfire. Some interviewers even ask job candidates to open their profiles in the presence and then assess the profile to help them decide whether they want to employ the person.

Even though students are usually not concerned about future employment, it is wise to think about publishing content on Facebook and think about the long-term perspective. From this point of view, it is good to think about friends that we have on Facebook (and who now have access to our information). Even in cases where we trust them unconditionally now, imagine what relationship you may have with them in five or ten years. This also pertains to partners with whom we like to share everything possible, but in case of a breakup, it may be them who, because of a broken heart, misuse our information in the worst possible way.

Despite all other somewhat scary information about records and possible exploitation of information, Facebook has a lot of positives (also described above), thanks to which users will likely not stop using it just like that. Therefore, it doesn't make sense to force students to erase their profiles and scare them too much - we know how we ourselves respond to such pressure. What does make sense it to point out what Facebook does in fact store and what rights it has to this information and to call attention to the fact that other users may exploit the information posted. And then hope that they will always think before posting something on a social network.

Lenka Dědková and Hana Macháčková

Lenka Dědková is specialist at the Institute for Research on Child, Youth and Family at the Faculty of Social Studies at Masaryk University, where she is also studying for her PhD. under the Social Psychology programme. She focuses on internet psychology, especially on the risks tied to internet use, and on-line relationships.

Hana Macháčková is, at this time, a PhD student studying for her degree under the Social Psychology programme at the Faculty of Social Studies at Masaryk University. At the same time, she is employed as a specialist at the Institute for Research on Child, Youth and Family. She specialises in the social and psychological aspects tied to using the Internet and new media (e.g., using social networks and membership in on-line communities; the phenomenon of blogging; publishing information on the internet; risk of cyberbullying), especially in the case of adolescents.

Both authors are involved in the VITOVIN project (http://ivdmr.fss.muni.cz/projekt-vitovin) and contribute to analysing data from EU Kids Online II, the international project concerning on-line risks (http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/Home.aspx). In the Czech Republic, they worked with other colleagues in 2011 on researching cyberbullying in South Moravia and at this time are doing longitudinal research on on-line risks among Czech children across the Czech Republic. Both are also co-authors of the book Kyberšikana: Průvodce novým fenoménem (Cyberbullying: Handbook on a New Phenomenon) (Černá et al., in print).

Note:

The authors were supported under the VITOVIN project (CZ.1.07/2.3.00/20.0184), which is co-financed by the European Social Fund and budget of the Czech Republic.

SOCIAL NETWORKS AS SEEN BY PSYCHOLOGISTS

A Warning Is Not Enough

It's so easy today to share with others how your holiday in Spain was, that Anna is riding with no help on her tricycle, where a class reunion will take place, to post a photo of a new car. Who else but young people should have a good relationship with new technologies and new means of communication? The reasons are simple. Children do not know how to do many things and do not have any experience, so when they are learning to master the world around them, they, naturally, reach out enthusiastically for new things, for things that make life easier or what they promise to make easier... Children and youth are less resistant to advertising - they are attracted by everything "fantastic", cool and in, what they have to have, and what their idols have and use. Adults tend to be more reserved. Not because they wouldn't be able to learn to use the new devices, but rather because they don't see the added value compared to the way they are used to doing something and that they have mastered over the years. It is also true that adults see more of the risks.

They know that there are two sides to every coin. In this respect it is being proven that the lack of life experience of children and youth can lead to complications when using social networks. Children see no further than one step ahead, adolescents perhaps two, so often they act first and think later. What's more, they tend to be braver virtually than live. While they have developed certain restraints when dealing face-to-face and can see the results of their actions immediately in such situation, at home at the computer they can do practically anything. Something can be sent with one click, and then it ceases to exist and the consequences cannot be seen. Of course, this does not apply only to inexperienced children and adolescents. How many adults share their personal data only because someone, whom they don't even know, sends an e-mail requesting it!

I will not discuss the reasons for the popularity of social networks, but if we understand them better, we can possibly come up with ideas for prevention. There are many reasons; nevertheless, one cannot ignore the fact that years ago, children would come home from school, drop everything and go outside and play with friends. They played football, organised battles, played with dolls, built forts, sat on railings and talked and talked. Today they go from school to groups, to training, to flute lessons, prepare for entrance exams. They can't just go outside and be with their peers. On Facebook, it's as if they are with them in reality! And parents are happy that they're at home.

We believe that we should avoid problems with the inappropriate use of social networks. Every tool is appropriate. Neither teachers nor parents should ignore warnings until actual problems arise; they should collect and use cautionary examples. But giving warnings is not enough. For children it is difficult to accept abstract, unspecific warnings on the one hand and reject specific, pleasant, enticing and acceptable contact on the other. Certain private videos posted on a social network may seem fun rather than illicit feelings of fear of the possible consequences. It is therefore important to think through events and ask these kinds of questions: How does a person feel when his private feelings are made public? What can happen when someone accuses someone on a social network of some sort of wrongdoing?

There are even more general forms of prevention. We should teach children from an early age to protect their privacy and respect the privacy of others. In my opinion, parents of young children already err when, without their permission, they publish intimate stories about their children or look through their bags and drawers.

A part of the problem is, however, difficult to resolve. Children are fully dependent on adults for some time. In order for them to be able to use this help and want to use it, they have to trust adults completely - not only parents and grandparents, but also doctors and teachers. It is practically impossible for children to differentiate between people they can trust and people they have to be wary of. More understandable to them is the differentiation between people at home and strangers. But doctors are also strangers (and do in fact often do unpleasant things to them) as are teachers. We can teach children from a young age not to trust anyone. But that a very unfortunate position to take in life. For this reason, it is important to be part of a child's life to the maximum extent possible. To make it possible, we should reinforce the feeling that the child can trust us absolutely. A lot of adults unknowingly raise their children in a way that the children soon realise this it is not always a good idea to share everything with adults, and that it is better to lie than to tell the truth. As today children live a greater part of their lives outside the family, parents can't protect them from everything, but if their child trusts them, parents very quickly learn what happened and what the child is planning to do and so can very quickly intervene before greater damage happens.

Some authors and professional publications are of the opinion that children are incorrigible and have to experience problems first hand and only after they have a negative experience will they begin to behave more responsibly. I don't think that always has to be the case. But even if so, it is the parents' responsibility to not resign and offer children the possibility of guidance.

Václav Mertin

Václav Mertin, child psychologist with 38 years of experience, deputy director of the Department of Psychology of the Faculty of Arts of Charles University. Professional interests: educational, school and advisory psychology; specific learning disorders; shared care; home schooling. Extensive publication activities both for professionals and families. Most recently: for parents, Výchova bez trestů (Raising Children without Punishment) (Wolters Kluwer, 2013); for teachers, Problémy s chováním ve škole (Behavioural Problems at School) (Wolters Kluwer, 2013).

Addicted to Facebook?

Gambling (pathological gaming) is the only officially recognised non-substance-related addiction listed in currently valid diagnostic manuals. The situation is changing, however, and the number of studies admitting that humans are able to develop additions even without using psychoactive drugs is increasing. In addition to workaholism, compulsive exercising or addiction to shopping or sex (on-line or off-line), attention is turning to the internet as well. And this field is quite broad, still undiscovered and full of controversy. For example, among researchers, there is no agreement whether one can speak of addiction to the internet or addiction through the internet. The same holds true for social networks: Can someone be addicted to Facebook? Some claim that one can. Others argue that this concept has quickly become obsolete because this website today covers various different applications. Users can play games on Facebook, meet through it, bet, communicate with friends, watch videos and many other things, and it is important to differentiate between these activities.

Either way, from time to time people who have lost control over their use of social networks appear in the offices of addiction experts. Research shows that the majority of users use Facebook to keep contact with real friends and acquaintances. It is the need to keep in contact and have an overview that can lead to more and more excessive use. In 2010, for example, Greek physicians described an extreme case of a 24-year-old woman whose use of Facebook significantly interfered with her daily life. [1)] Controlling and updating her profile took five hours of her day, she lost interest in other activities and even lost her work. During a visit to her therapists, she used her smart phone to check her Facebook profile numerous times.

Such case is an exception; nevertheless, it illustrates the basic criteria of addiction. The state where some activity, such as Facebook, dominates over an individual’s thoughts and actions is termed salience. Another condition is a change in mood and tolerance, i.e., the need to increase the amount of an activity to achieve the same effect. Withdrawal syndrome indicates unpleasant feelings if the activity is denied to the persons and often leads to a relapse, a return to the previous pathological behaviour. A key criterion is the presence of conflict, i.e., the situation where the problematic activity negatively affects the life of the person concerned - be it a school or work commitments or interpersonal relationships. Research that was aimed at the above criteria in the context of social networks indicate that excessive use can, under specific circumstances, lead to a number of negative consequences, including restriction of off-line social contacts or a deterioration of school grades.

In order for problematic Facebook use to be identified, a team of Norwegian scientists have put together the six-point Bergen Facebook Addiction Scale. [2)] The scale comprises the following statements: (1) You spend a lot of time thinking about Facebook or planning how to use it. (2) You feel an urge to use Facebook more and more. (3) You use Facebook in order to forget about personal problems. (4)You have tried to cut down on the use of Facebook without success (5) You become restless or troubled if you are prohibited from using Facebook. (6)You use Facebook so much that it has had a negative impact on your job/studies. For each, it is necessary to decide whether the statement applies very rarely, rarely, sometimes, often, and very often. According to the authors, scoring "often" or "very often" on at least four of the six items may suggest you are addicted to Facebook.

However, no study that would examine what share of Facebook users face such a problem has been carried out to date.

The problematic use of Facebook is, according to the authors of the Bergen Scale, found most often in women and adolescents, which explains in particular the social nature of the network. The study results also show the relationship between addiction to Facebook and certain personality traits. Anxious people and people who are less certain in social situations have a tendency to use Facebook more intensively, as communication on-line appears easier to them than face-to-face communication. Conversely, ambitious people who know how to organise their time well incorporate Facebook easily into their day-to-day life as a useful helper.

Kateřina Škařupová

Kateřina Škařupová has devoted many years to users of illicit drugs, directly in the field and in research institutions. She is now a doctoral student and researcher at the Faculty of Social Sciences of Masaryk University, where she focuses on on-line addiction and computer games.

Notes:

[1] D. Karaiskos, E. Tzavellas, G. Balta, T. Paparrigopoulos, P02-232 – Social network addiction: a new clinical disorder?, European Psychiatry, Volume 25, Supplement 1, 2010, Page 855, ISSN 0924-9338, 10.1016/S0924-9338(10)70846-4.(http://www.sciencedirect.com/science/article/pii/S0924933810708464)

[2] Andreassen, C. S., Torsheim, T., Brunborg, G. S., & Pallesen, S. 2012 Development of a Facebook addiction Scale 1, 2. Psychological Reports, 110(2), 501-517. (http://www.amsciepub.com/doi/pdf/10.2466/02.09.18.PR0.110.2.501-517

RESPECT FOR PRIVACY

Education for Knowledge and Safety

The world of the internet is bringing us a number of effective and beneficial applications. Of the main ones, I shall mention at least two: the internet as an inexhaustible source of information and social networks as a communication environment.

Use of not only these, but all other possibilities that information and communication technology offers us, is tied to knowledge and literacy in this field.

Digital education, internet education, media education, new information and communication technology - current trends not only in teaching, but also in education and attitudes in society. Whether we like it or not, it is this new technology that to a certain degree organises and defines how we live. We are all aware that this trend needs to be grasped in time.

Children are usually much cleverer and more literate than parents and often even teachers in their knowledge and ability to work with digital media, information and communication technology. Nevertheless, they need guidance and where else than in school should children learn to work with this technology correctly and safely?

The authority of a teacher who knows how to give advice is indispensable. The task of teachers is truly difficult and venerable. Teaching guidelines may offer basic rules for teaching, but a lot depends on each teacher to what detail he or she should go and how to best introduce the digital world to their students. Teachers not only have the mentioned guidelines for their work, but can find a lot of useful and practical advice for their work on the internet, on specialised websites, as well also in various methodological handbooks, professional training courses and specialised literature. Even in this issue of the bulletin, experts who contributed with their opinions about the Internet and in particular social networks have provided a lot of links where to go for good advice.

Support for families and the continuation with a different form of teaching at home should be a matter of course. The objective is to help children understand this field and learn to work with these resources. The reward is the knowledge that the child will learn to use this type of technology to his or her benefit and learn to recognise the dangers and risks that are connected to its use.

To add variety to the spectrum of information herein, we provide a brief look at the Swiss school system and how they see this issue:

Swiss basic schools have focused on paying greater attention to media and digital education. “Knowledge of multimedia resources has become as important as reading, writing and arithmetic and should be practices already in the first grade,” recommends Irene Heimgartner from the Swiss Association of Children and Youth Organisations.

Although the guidelines do contain education in this field, its fulfilment has been placed at the discretion of teachers. According to the new guidelines known as 21, basic schools in the 21 cantons where teaching is done in German will have pupils working with the internet already from the first grade. During lessons, teachers will acquaint children with many useful features of various websites, but also the dangers they contain, how to protect yourself against cyberbullying and how to move safely about the internet.

Words of comfort for teachers who don't have much knowledge of digital media were provided by Döbeli Honegger from the University of Education in Zurich: “Of course, professional assistance is planned and schools will get money for it. Naturally, older teachers sometimes aren't as versed as their students. They can, however, provided something invaluable: life experience. [1)]

Note:

[1)] Source: Právo: 21. 3. 2013, Caffee supplement, page 2 – paraphrased.

Inside a Display Case - Something to Think about in Closing

We eat, drink, travel, learn, work, support our favourite club... We are social creatures and feel the need to share things while fresh. We have only one life and it is necessary to continue to enrich it. We like to share with others what we had for dinner, where all we were, what new things we learned or at least boast about our favourite football team winning, and we like to listen to the same. And that is why we join social networks.

My social networks used to be my classroom, the discotheque, the pub, the library entrance hall, the football field, etc. etc. Here I acquired important information and shared some, too. Some information found its way to other social networks that I or someone close to me was a member of. The social networks at the time were, to be honest, not very extensive, although we certainly wished the opposite were true. What is more, all messages disappeared irrecoverably from our minds or we struggle to make out their foggy contours.

In modern, or computer social networks, the situation is different. We can address the whole world without taking off our slippers (knowing a foreign language comes in handy, doesn't it?). And we may encounter the information we let out now even a hundred years from now. It's like something stored well in our closet. These prize possessions can, however, sometimes turn into skeletons.

Think thoroughly about what you put in your closet. That closet is not room reliably locked and located safe in your house, but a display case.

Jiří Maštalka
Legal Department
Office for Personal Data Protection

PUBLISHED BY THE OFFICE FOR PERSONAL DATA PROTECTION
EDITOR: HANA ŠTĚPÁNKOVÁ | SUB-EDITOR: MILUŠE NEJEDLÁ
EDITOR’S OFFICE ADDRESS: ÚOOÚ, PPLK. SOCHORA 27, PRAHA 7, 170 00 |
TELEPHONE: 234 665 286 - FAX 00 39 06 50957056 234 665 505
E–MAIL: POSTA@UOOU.CZ | INTERNET ADDRESS: WWW.UOOU.CZ
THE PERIODICAL IS REGISTERED IN THE PERIODICAL PRESS REGISTRY
UNDER NUMBER MK ČR E 10548.

PUBLISHED ON 16 JUNE 2013