sciendo

Management Systems in Production Engineering

2019, Volume 27, Issue 2, pp. 88-92

Date of submission of the article to the Editor: 12/2018
Date of acceptance of the article by the Editor: 02/2019

DOI 10.1515/mspe-2019-0015

SAFETY MANAGEMENT IN THE AGE OF INTERNET THREATS

Monika ŠTRBOVÁ
Constantine the Philosopher University in Nitra

Paulina KUZIOR
Silesian University of Technology

Abstract:
Contemporary world brings people more and more dangers. Creation of the Internet made it even easier to harm other users without consequences. However we still can do something about it. We can learn how to protect ourselves in the network. That is why it is so important to disseminate the main goals of safety management while using Internet. The paper presents main dangers awaiting for network users – both the youngest and the older ones, such as cyberbullying or phishing. The authors also point to the more frequent Internet addiction. The main goal of this paper is to indicate on how the on-line safety management should look like and how people can protect themselves from the dangers, of which they are sometimes even not aware. Children and adults shall be educated about the dangers in the Internet, and how to avoid them. Only then will they know, how to properly manage their on-line safety.

Key words: *cyberbullying, dangers, Internet, phishing, safety management*

INTRODUCTION

To define generations that are affected by information and communication technologies, there is no explicitly preferred term and its time limits. Literature indicates the following naming generations: Millennium Generation, Generation Y, Digital Generation, Online Generation. As a synonym homeland generation are using the term Generation Z, Post-Millennials, Net-Gen, digital natives [6]. The term that best describes today's generation of children is Generation Z, which we are referring to those children and adolescents who have a strong bond to information and communication technology. Mc'Crindle defines the generation Z with the help of the terms global, digital and visual [11]. It is a generation, which has access to smartphones, smart phone, through which They can connect with the whole world. Turner (2015) argues that the media of the current generation Z can help to escape from the emotional and psychological problems they face in offline mode. Generation Z uses the Internet to retrieve information and communication with others [15].

Mobile technologies, social media (internet, social networks, etc.) and the use of the Internet has become more important in the lives of teenagers in the last decade. Use of social media strengthens linkages with friends and helps develop new ones. Generation Z communicates with people who would not meet in the real world through the media. This communication and development virtual relationships and friendships are one of the characteristics generations Z and their standard. Cyberspace on one side provides new possibilities and forms of communication that beyond physical, geographical and cultural communication barriers, to the other is a threat to man for his impersonality, anonymity and declining interest in interpersonal personal communication [5].

Findahl [3] in the post *Preschoolers and the internet. Will children start to use internet when they start walking?* submit data, according to them even in countries, which are covered by Internet connection at a low level, children are active users of internet. For example China, where only 10% of the adult population are connected to the Internet, yet it is used by 39% of children. In most developed countries, most children over the age of 12 regularly enjoy the internet. It is clear, therefore, that the generation of contemporary children grows upright contact with the Internet.

Poor behavior habits in virtual space can turn into disregard for the basic principles of cyber security in adult life. If a child does not learn to protect their privacy and access private data, there is a good chance that they will not take care of the security of the data of the company in which they work as an adult. Such behavior will be particularly important in enterprises dealing with the broadly understood creative or production process, as well as their organization and management, e.g. production engineering.

Enterprises operating in this area are usually not small companies, but huge corporations, which also have considerable financial resources. Lack of appropriate security management in such an entity may result in the seizure of a significant part of resources by unauthorized persons, which will deprive the company of funds for further plans.

DANGERS ON THE INTERNET

Risks arising from the characteristics of the Internet and communication on it affecting our psyche. Concretely psychological well-being, healthy personality development, status, and contentment in life.

These are the negative phenomena associated with the Internet mainly:

- Internet addiction,
- Cyberbullying,
- dangerous „challenges“ for children

INTERNET ADDICTION

Ways to use the Internet are different and can not be considered as a whim of anyone who spends more time on the Internet. The problem arises when the excessive use of the Internet will bring to life the individual's complications in various areas – personal, psychological, family and social relationships, and in school or work environment. There is a gradual cut off from normal life, which is often affected by perceived only as an annoying necessity.

Young [17] developed a brief eight-item questionnaire which modified criteria for pathological gambling to provide a screening instrument for addictive Internet use:

1. Do you feel preoccupied with the Internet (think about previous on-line activity or anticipate next on-line session)?
2. Do you feel the need to use the Internet with increasing amounts of time in order to achieve satisfaction?
3. Have you repeatedly made unsuccessful efforts to control, cut back, or stop Internet use?
4. Do you feel restless, moody, depressed, or irritable when attempting to cut down or stop Internet use?
5. Do you stay on-line longer than originally intended?
6. Have you jeopardized or risked the loss of significant relationship, job, educational or career opportunity because of the Internet?
7. Have you lied to family members, therapist, or others to conceal the extent of involvement with the Internet?
8. Do you uses the Internet as a way of escaping from problems or of relieving a dysphoric mood (e.g., feelings of helplessness, guilt, anxiety, depression)?

Patients were considered "addicted" when answering "yes" to five (or more) of the questions and when their behavior could not be better accounted for by a Manic Episode.

CYBERBULLYING

Cyberbullying can be defined as “a form of bullying that uses electronic means such as email, mobile phone calls, text messages, instant messenger contact, photos, social networking sites, and personal web pages, with the intention of causing harm to another person through repeated hostile conduct” [13]. But, what is seen as cyberbullying can vary between different cultures, and even among different individuals. In addition, cyberbullying, as a term, is not recognized worldwide.

According to the European Commission (on the occasion of the 2009 Safer Internet Day) cyberbullying differs from face-to-face bullying in various aspects such as the anonymity that the internet provides, the capacity to reach a wider audience, the lack of sense of responsibility of perpetrators and the reluctance of victims to report incidents [14].

In the past, students could retreat to the safety of their homes to escape incidents of bullying. Once the bell rang, they could run home and were safe until the next day. The same cannot be said for cyberbullying. The impact of cyberbullying does not stop when students pass through the school door. Cyberbullying has invaded their homes, their bedrooms, and their personal laptops and phones. Even more insidious are the incidents of cyberbullying as they can be targeted directly to the individual, wherever they are, or on the Internet where anyone can see the victim’s torment [16]. Cyberbullying specifically may be it could have even more serious consequences than face-to-face bullying due to the variety of attributes that may accentuate the impact of the behavior. Depending on the particular circumstances, this may include a wider audience, anonymity of the bully, the more enduring nature of the written word and the ability to reach the target at any time and in any place, including the target’s home. Further, cyber bullies may feel emboldened because they cannot see their targets or their immediate responses, and believe that, because of their anonymity, they will not be detected. It has been suggested that this anonymity may increase the intensity of the attacks and encourage them to continue for longer than they would otherwise do face-to-face [1].

Willard [16] identified the following seven ways in which cyberbullying may occur: (a) flaming involves sending angry, rude, or vulgar mes-sages directed at a person or persons privately or to an online group; (b) harassment involves repeatedly sending a person offensive messages; (c) denigration is sending or posting harmful, untrue, or cruel statements about a person to other people; (d) cyberstalking is harassment that includes threats of harm or is highly intimidating; (e) masquerading is pretending to be someone else and sending or posting material that makes that person look bad or places that person in potential danger; (f) outing and trickery involve engaging in tricks to solicit embarrassing information about a person and then making that information public; and (g) exclusion describes actions that specifically and intentionally exclude a person from an online group, such as blocking a student from an IM buddies list.

EU Kids Online II has designed and conducted a major quantitative survey of 9-16 year olds experiences of online use, risk and safety in 25 European countries during 2010-12. Findings vary by child (e.g. age, gender),

country and risk type. EU Kids Online has classified the risks of harm to children from their online activities as follows. The classification distinguishes content risks (in which the child is positioned as recipient), contact risks (in which the child in some way participates, if unwillingly) and conduct risks (where the child is an actor) (see Table 1) [9].

Table 1
A classification of online risks to children

	Content Child as receiver (of mass productions)	Contact Child as participant (adult-initiated activity)	Conduct Child as actor (perpetrator / victim)
Aggressive	**Violent / gory content**	**Harassment, stalking**	**Bullying, hostile peer activity**
Sexual	**Pornographic content**	**'Grooming', sexual abuse on meeting strangers**	**Sexual harassment, 'sexting'**
Values	**Racist / hateful content**	**Ideological persuasion**	**Potentially harmful user-generated content**
Commercial	**Advertising, embedded marketing**	**Personal data exploitation and misuse**	**Gambling, copyright infringement**

Source: EU Kids Online [9].

Cyberbullying is closely linked to the growing penetration of ICTs at increasingly young ages. The press often echoes cyberbullying incidents, and this undoubtedly constitutes a reason for concern, not only at a social level but also from a scientific point of view, as attested by the objective data of the increased appearance of publications dedicated to this topic during the last ten years [10].

ON-LINE „CHALLENGES"

In recent years, there have occured also may dangerous, self-destructive, „challenges" for children and adolescents, which are available mainly through the Internet. Many of these actions are connected to both „contact" and „conduct" mentioned above. In the Internet, the children may often contact people, who have bad intentions and may therefeore demand a child to do something inappropriate.

One of the most dangerous action that children may be required to do is the „Fire fairy challenge". This game avails the image of the *Winx Club* fairies, a fairy tale known by thousands of young children all over the world. It contains an instruction on how to become a fire fairy. The children are told that if they want to become one, they need to wake up in the middle of the night, turn on the gas rings in the kitchen, then go back to their room, say a magic spell and go to sleep. They are informed, that when they wake up, they will become a real fire fairy [4].

Another dangerous way of cyberbullying children is the „Blue Whale Challenge". It consists in the fact that the child is obliged to perform certain tasks, and the whole game lasts 50 days. Tasks are imposed by a mentor, a player's guardian learned online. He gives the child a new goal to achieve each day, and the last task that the child shall perform is to make away with themselves by jumping off the roof of a high building [2].

Some kind of modification of the game mentioned is so called „Momo challenge". Momo is a virtual doll, who contacts her victim throuh WhatsApp. Momo wants the child do some certain task, mostly related to self-harm. If the user refuses to perform such action, Momo becomes angry, threatens and blackmails him. There is no other option but doing anything Momo requires to do, even if these actions may end up with losing one's life [18].

INTERNET DANGERS FOR ADULTS

However, the adult users of the Internet are also not quite save. They are often not aware of the dangers awaiting them on-line and therefore take up various actions, because they think (or have been told) it is neccesary do to so. It may result with various negative consequences, which may influence not only the user himself, but also his family or friends.

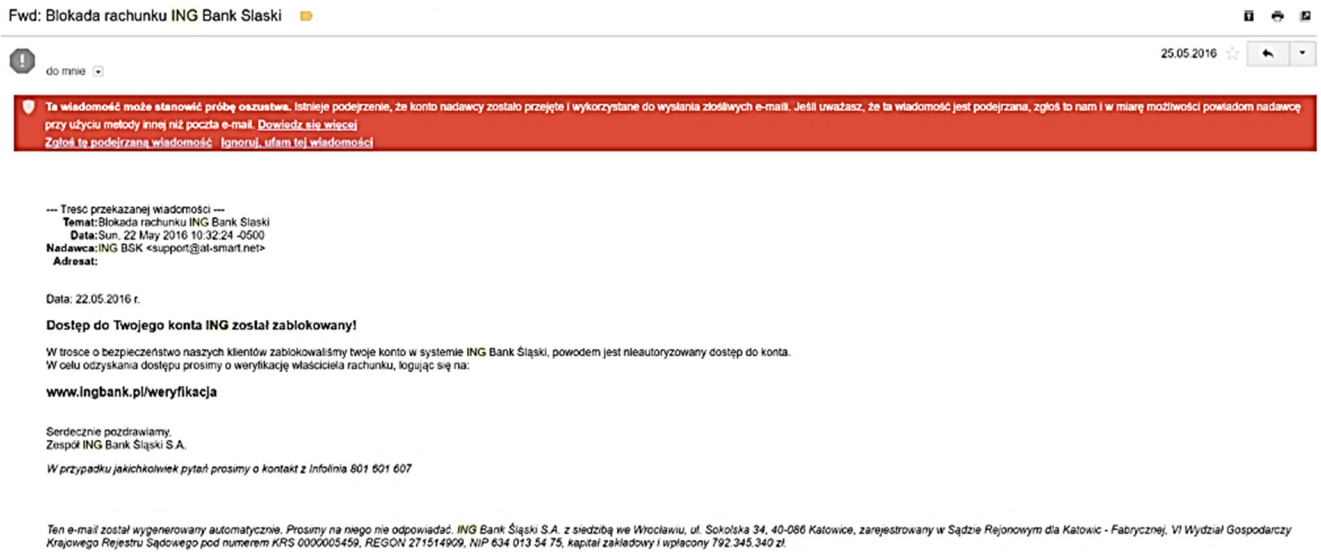
ON-LINE BANKING

Victims of cyber-crimes related to on-line banking are often not even aware, they have just become frauded. The most common form of such crimes is phishing. First of them is creating a fraudulent bank website and an e-mail message looking similar to the original messages being sent by banks. Phisher tries to persuade the on-line banking user to share with him some sensitive data, such as username, account password or credit card information. These information should be forwarder to the phisher by answering his e-mail and writing there all the data needed. This is the easiest way to get the required information, but it is not very effective.

Nowadays many people are aware that they shall not give any sensitive data through an e-mail. Therefore the phishers had to find another way to get such information from their victims. That is why they often create a fake bank website, that looks very similar to the original one, and then send an e-mail containing a link to this website. Then the victim, by clicking this link, is being redirected to a site, from which the phisher may get their login information. Thanks to such actions he may take over the victim's account and take all of the money from there [8].

Several Polish banks have instructed their clients not to answer e-mails which seem to be sent by the bank, but require answering with giving some sensitive data. One of those banks was ING Bank, whose clients got misleading e-mails, as illustrated on the graphic below (Fig. 1).

Neither the website domain, from which the message was sent, nor the sender's name were correct, and this should be the first sign that it may be phishing.


Fwd: Blokada rachunku ING Bank Slaski

25.05.2016

do mnie

Ta wiadomość może stanowić próbę oszustwa. Istnieje podejrzenie, że konto nadawcy zostało przejęte i wykorzystane do wysłania złośliwych e-maili. Jeśli uważasz, że ta wiadomość jest podejrzana, zgłoś to nam i w miarę możliwości powiadom nadawcę przy użyciu metody innej niż poczta e-mail. Dowiedz się więcej

Zgłoś tę podejrzaną wiadomość Ignoruj, ufam tej wiadomości

--- Treść przekazanej wiadomości ---
Temat: Blokada rachunku ING Bank Slaski
Data: Sun, 22 May 2016 10:32:24 -0500
Nadawca: ING BSK <support@at-smart.net>
Adresat:

Data: 22.05.2016 r.

Dostęp do Twojego konta ING został zablokowany!

W trosce o bezpieczeństwo naszych klientów zablokowaliśmy twoje konto w systemie ING Bank Śląski, powodem jest nieautoryzowany dostęp do konta.
W celu odzyskania dostępu prosimy o weryfikację właściciela rachunku, logując się na:

www.ingbank.pl/weryfikacja

Serdecznie pozdrawiamy.
Zespół ING Bank Śląski S.A.

W przypadku jakichkolwiek pytań prosimy o kontakt z Infolinia 801 601 607

Ten e-mail został wygenerowany automatycznie. Prosimy na niego nie odpowiadać. ING Bank Śląski S.A. z siedzibą we Wrocławiu, ul. Sokolska 34, 40-086 Katowice, zarejestrowany w Sądzie Rejonowym dla Katowic - Fabrycznej, VI Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS 0000005459, REGON 271514909, NIP 634 013 54 75, kapitał zakładowy i wpłacony 792.345.340 zł.

Fig. 1 Phishing e-mail message from ING Bank Śląski
Source: private archive.

NIGERIAN SCAM

Nigerian scam is a very sophisticated fraud. The aim of the scammer is to swindle of financial means and personal data sent him by the victims themselves, without any pressure, freely. They scammers may try to achieve their goals e.g. by sending the victims fraudulent e-mails, in which they offer a large amount of money to share. Sometimes the e-mails are written in (or more correct would be: are pretending to be written in) the receiver's mother's tongue, yet they are full of mistakes and errors (see Fig. 2). The point is, the receiver of such e-mail may get a huge amount of money from the sender, if he agrees to assist him. Such assistance is usually burdened with additional requirements, such as setting up a fictitious business or making a preliminary, small transfer to the sender's account. If the victim really does what they were asked to, the scammer already has all of their personal data needed to another fraud [12].

Pozdrowienia od Pierre Atkins Chamber & Associates.
Drogi przyjacielu,
Jestem adwokatem Pierre Atkins. Jak to wszystko z tobą, napisałem ci miesiąc temu, spodziewając się, że odpowiesz, jeśli chodzi o informację o pilności, którą ci przekazałem. W każdym razie, nie wiem, czy to dostałeś, czynie, to jest powód, dla którego wysyłam to przypomnienie. dotyczące przedsięwzięcia, które chciałbym z tobą załatwić. Mój zmarły klient, który zginął w wyniku śmiertelnego wypadku samochodowego z rodziną w drodze do pobliskiego kraju, pozostawiając ogromną ilość pieniędzy (9.211,000.00 USD) w banku tutaj, kontaktując się z tobą na podstawie tego, że masz takie samo nazwisko z moim nieżyjącym już klientem, aby pomóc mi bez problemu wnieść ten fundusz na twoje konto bankowe. Ale bądź pewien, że wszystko jest legalne i wolne od ryzyka. Odpowiedz mi, aby uzyskać więcej informacji.
Z poważaniem,
Prawnik Pierre Atkins

Fig. 2 Example of the "Nigerian scam" e-mail
Source: Private archive

SUMMARY

It should however be stated, that the Internet shall not be viewed as a tool constisting only from dangers and threats. It is the most powerful societal tool so far. It allows the users have unlimited access to the newest information, find news almost about everything they are looking for, but also it allows contacting other people, which may be even miles away one from each other. Yet, using the Internet without any consideration can lead to many negative consequences [7].

Children and adults shall be educated about the dangers in the Internet, and how to avoid them. Only then will they know, how to properly manage their on-line safety. The European Union supports preventive programs about online safety, software companies too.

For production engineering, whose role is among others organization and management of manufacturing processes, establishing security management principles should be a priority. Also, employees of enterprises should be trained in basic security rules, both personal and corporate. The company can not afford uncontrolled outflows of sensitive data, and employees are often unaware of how the extensive effects they can have on the unit they work for.

REFERENCES

[1] K. Conn, „Bullying and harassment: A legal guide for educators" Alexandria: ASCD, 2004.

[2] *Cyberbullying Taken To A Whole New Level: Enter The 'Blue Whale Challenge'* – Available: https://www.forbes.com/sites/andrewrossow/2018/02/28/cyberbullying-taken-to-a-whole-new-level-enter-the-blue-whale-challenge/#630eda0a2673 [Dec. 09, 2018].

[3] O. Findahl. "Preschoolers and The Internet: Will children start to use Internet when they start walking?" presented at the EU-kids online conference, London, Great Britain, 2009. Available:http://s3.amazonaws.com/zanran_storage/www.lse.ac.uk/ContentPages/14151569.pdf [Dec. 15, 2018].

[4] *Five-year-old girl suffers horrific burns after becoming the latest victim of 'fire fairy' game spreading online where children are told to secretly turn on gas rings.* Available https://www.dailymail.co.uk/news/article-4290590/Fire-fairy-game-tells-children-turn-gas-stoves.html [Dec. 09, 2018].

[5] K. Hollá. *Sexting a kyberšikana*. Bratislava: Iris, 2016.

[6] R. Juncor, J. Masrodicasa. *Connecting to the Net.Generation: What higher education professionals need to know about today's students.* Washington DC: NASPA, 2007.

[7] T. Keipi, M. Näsi, A. Oksanen, P. Räsänen. *Online Hate and Harmful Content: Cross-National Perspectives.* Abingdon-on-Thames 2016.
[8] P. Kumaraguru, Y. W. Rhee, A. Acquisti, L. Cranor, J. Hong, E. Nunge. *Protecting People from Phishing. The Design and Evaluation of an Embedded Training Email System.* Pittsburgh, 2006.
[9] S. Livingstone, L. Haddon, A. Görzig, K. Ólafsson. *Risks and safety on the internet: the perspective of European children: full findings and policy implications from the EU Kids Online survey of 9-16 year olds and their parents in 25 countries.* London: EU Kids Online Network. 2011.
[10] Mª Paz Prendes Espinosa, „Bullying and cyberbullying: two forms of violence in schools" *Journal of new approaches in educational research,* vol. 7, no. 1. pp. 1-2, 2018.
[11] M. McCrindle. *Generation Z Defined: Global, Visual and Digital.* Available: http://clairemadden.com/wp-content/uploads/2013/07/Generation-Z-Defined-Global-Visual-Digital_McCrindle-Research-2013.pdf [Dec. 15, 2018].
[12] *Nigeryjski przekręt – czym jest i jak nie dać się nabrać?* Available: https://www.infor.pl/prawo/prawo-karne/przestepstwa-komputerowe/2702803,Nigeryjski-przekret-czym-jest-i-jak-nie-dac-sie-nabrac.html.
[13] R. Ortega et. al. "The emotional impact of bullying and cyberbullying on victims: A European cross-national study" *Aggressive Behavior*, vol. 38, pp. 342-356. 2012.
[14] V. Pozza, A. Di Pietro, S. Morel, E. Psaila, *Cyberbullying among young people*. European Union, 2016. Available: http://www.europarl.europa.eu/RegData/etudes/STUD/2016/571367/IPOL_STU(2016)571367_EN.pdf [Dec. 15, 2018].
[15] A. Turner. „Generation Z: Technology And Social Interest", *Journal of individual psychology*, vol. 71, pp. 103-113, 2015.
[16] N. Willard, „Cyberbullying and cyberthreats" in *Tying it all together: Comprehensive strategies for safe and drug – Free Schools.* Washington, 2005.
[17] K. S. Young. "Internet addiction: The emergence of a new clinical disorder" *Cyber Psychology and Behavior*, vol. 1, pp. 237-244, 1996.
[18] *WTH Is Momo Suicide Challenge? 4 Tips for Students to Help Protect Their Siblings* –Available: https://typicalstudent.org/hot/news/momo-suicide-challenge-tips-for-students [Dec, 09. 2018].

PhDr. Monika Štrbová, PhD.
Constantine the Philosopher University in Nitra
Faculty of Arts, Department of Philosophy
Štefánikova 67, 949 74 Nitra, Slovak Republic
e-mail: mstrbova@ukf.sk

mgr Paulina Kuzior
Silesian University of Technology
Faculty of Organization and Management
Department of Applied Social Sciences
ul. Roosevelta 26, 41-800 Zabrze, Poland
e-mail: paulina.kuzior@polsl.pl