The 8th International Scientific Conference
eLearning and software for Education
Bucharest, April 26-27, 2012
10.5682/2066-026X-12-088

LEARNING HOW TO BE A RESPONSIBLE CITIZEN IN THE VIRTUAL ENVIRONMENT

Gabriela SÂRBU,
Non-affiliated Independent Researcher, Bucharest, Romania
E-mail: gabriela.sarbu@gmail.com

Corina CADARIU
Constantin Brancoveanu Theoretical High School , Bucharest, Romania
E-mail: corina.cadariu@yahoo.com

***Abstract**: Virtual space and all its attached Internet services, mobile applications, computers and networks are extensions of our daily needs and life. But are most of us prepared to use them in a responsible manner? The global networking can be used not only with the good intentions. Some of the problems can be avoided with an Internet-usage literacy campaign. In this way users will be aware of their rights, their duties and the dangers that may arise if they treat electronic/Internet/mobile-issues as details not worthy for their attention. With small awareness and little knowledge of how the things work, regular users can be safer in the computer wastelands, mobile frenzy and Internet services nebulae. By buying a device, which can help you to enlist/write in a social network or on a blog, the user starts to share information that can be used against ones will. An unsecured computer or network, social engineering, fake websites can be avoided even by a regular user if there is enough knowledge upon these subjects. Banning Internet or avoiding technology in general is not the key for development, but learning how to operate and understanding the processes involved is the intelligent way. Knowing your computer, understanding how the network is actually working, securing your gateways to the Internet, comprehending and smartly using the tools of the available services from the Internet or for your mobile/smart phone will not make the user a programmer or an Internet geek, but a responsible citizen in the virtual environment. Internet-literacy is a must at any age, for all that are living in the 21th century electronic and real worlds.*

***Keywords:** e-Education, Security, Cybercrime, Vulnerability Management*

I. CHAPTER I – People and the Internet

Everything around us revolves around the Internet and even more than that. According to Cisco report [1]: *One of every three college students and young employees believes the Internet is as important as air, water, food, and shelter* but *regarding security-related issues in the workplace, seven of ten employees admitted to knowingly breaking IT policies on a regular basis, and three of five believe they are not responsible for protecting corporate information and devices*.

With the proliferation of Web architectures and applications, mostly developed with an eye for ready-to-market needs rather than security, the number of targets to attack is increasing dramatically [2]. Would this threat mean to pack back all our devices and never look on a webpage? Of course this question's answer will be a *NO* (written in capital letters, which in online environment is a loud statement, very loud). Like in personal preferences all is accepted unless it harms someone else. The thin line between secure and insecure is more evident in the cyberspace, but some little advices can be made from the start. If in childhood our parents advised us not to talk to strangers in the street, not to

give home key to anyone, not to invite people at home unless another member of the family was around and so on, some similar guidelines can be used also in the usage of devices/Internet. Doing a parallel with the first rules, we can easy identify some common sense tips for the Internet Era: patch your system, do not share your passwords with everyone around, do not open attachments unless you understand what it is and from whom, and more little tricks that can make a system safe or vulnerable. *Although we may never get to a state that we can definitively call "secure," we can take steps in the right direction* [3].

The society also tries to make us aware of the threats posed by an improper usage or lack of understanding of the virtual services:

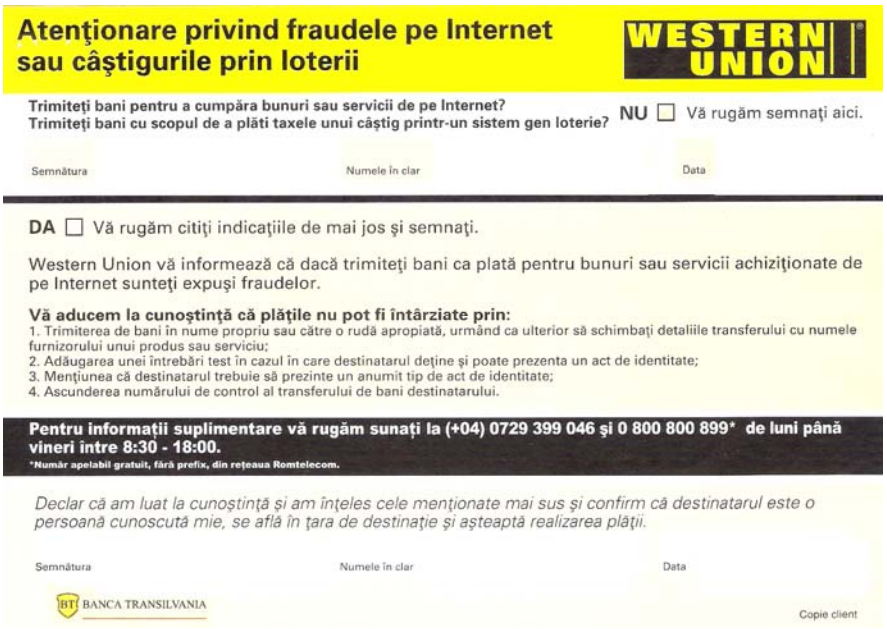

Figure 1. Awareness Flyer from a Romanian Western Union Partner

Returning to the Cisco report [1] and using our observations [see Appendix] the Internet threats are seen as part of someone's else problem and youngsters *believe their generation is at least moderately concerned about Internet security threats – although don't always use common sense to protect themselves or company assets* [1]. In fact the problem is more acute: most of the gadgets/Internet users lack in basic knowledge, just copying usage-behaviours from friends and colleagues, not understanding the meaning of their actions and ignoring all the warnings from the authorities or elder persons under the presumption *that they know nothing about what we are doing and they don't even bother to understand us*. The idea that Internet is free is their key motto, followed by the argument that *everybody does that* and that Internet is part of their generation, like a fashionable item (loved by the teenagers, hated by adults). Even if they encounter a flyer similar to Figure 1, they just sign it and ignore the content, assuming that they know better the issues related to Internet and everything is just a Next>Next> sequence, like in any application installing procedure. The apparent easiness to use devices, also the eagerness and rush to have and use the entire set of in-trend services/gadgets, completed with the fear not to fall behind the main wave make them more open to digital threats. As a high school freshman pointed out: *For example if you don't have a FB* (the abbreviation of Facebook account) *than you are a looser, if you are not printing your papers than you are obsolete*.

In our surveys we are using the The Parkerian Hexad, introduced by Donn Parker in his book *Fighting Computer Crime* and presented also by Andress [3], and watched how the key concepts of information security: the confidentiality, the availability, the integrity, the possession, the authenticity and the utility are matching with the field observations and also to have a terminology set up for a coherent workflow in collecting and presenting our data to and from our sampling target.

1.1. Security Issues terms within the Parkerian Hexad

The confidentiality as a component of privacy refers to our ability to protect our data from those who are not authorized to view it; the availability means the fact that we can access our data when we need it (sometimes we are not able to do that due, but when it is done by on outsider we will use the term DoS -denial of service- attack); the integrity of our data (not to be accessed by an unauthorized party or undesirably changed or deleted); the possession or control refers to the physical disposition of the media on which the data is stored; the authenticity refers to the author/creator attribute of those data while the utility will be treated also as the utility of that data for the owner/creator and for those who are trying to access them.

1.2. Cybercrime, H*Commerce

We are constantly bombarded with news about Internet events today. Cybercrime is up. Computer users need to watch out for the latest phishing attack trying to steal our identity, update our anti-virus to avoid infection, patch the operating system to avoid a hacker taking control, new zero day attack against smart phones, Facebook privacy compromised, someone took down Twitter, and now we are hearing about Cyber War [4].

*Cybercrime is a broad term that describes crimes committed via computers and the Internet by "hackers" who are driven to make money. Most cybercrime employs malware and social engineering to steal your personal information, which cybercriminals use to access credit and bank accounts. This practice has become so common and so lucrative it has developed into its own cottage industry, with participation by individuals around the world. We call this business of hacking Hacker Commerce, or H*Commerce* [5].

1.3. The ABC for Internet

Regarding at the threats and understanding that virtual does not mean hypothetical, when one is talking about the Internet, will be the first important step. *It will not happen' to me* is not a good start scenario, but prevention and cyber-immunization.

According to EU Kids Online Survey: *Opportunities and risks online go hand in hand. Efforts to increase opportunities may also increase risks, while efforts to reduce risks may restrict children's opportunities. A careful balancing act, which recognises children's online experiences "in the round", is vital* [6]. But, as a country, Romania is included in the *higher use, higher risk – new use, new risk* category.

Unfortunately our observations in one high schools of Bucharest also underline the conclusions for Romania, of the above mentioned survey:

Romania is one of the countries with the most time spent online, also one of the countries where children report the fewest internet skills. Intense use, coupled with low levels of skills, is likely to lead to more risky and harmful experiences online. […] Last, Romanian children aged 11-16 also experience above average data misuse.[…]

As one of the countries with a high use-high risk profile, Romania requires more intense adequate policy approaches: parental awareness of children's risks online needs to be enhanced, appropriate measures should be taken to increase children's self-protection and self-responsibility online, with an emphasis of children developing more digital skills and more effective coping strategies (preferably integrated into the national educational curriculum), that also stress the importance of social support (children being encouraged to talk more about their experiences online). Also, safety awareness centres should work towards disseminating information about the most prominent risks and about effective parental controls and mediation strategies, while also making them available in an easily accessible and user-friendly manner.[7]

The need of an ABC for Internet-usage in Romania especially for teens, but not neglecting the rest of the web-users either, is a problem that was a subject of our attention from 2009 [8]. The rise and fast pace of development of ICT (information and communication technology), the impressive array of new devices able to connect anyone from everywhere to the Internet, the risks that are not just teens' pranks or geek's revenges anymore, the illusion of knowledge that is encountered in most of the nowadays youngsters and the real security issues that can *disrupt a life or tear a family apart* [9] make

this problem more important not just to be debated, but also to be a project by itself and if possible included in the educational curricula. And again we want to underline that limitation of Internet access in schools or at home will not solve this problem, since the possibility of owing a device capable of surfing the web is valid for more and more individuals and the trend of overpassing the barriers is also an ability that learnt very fast.

II. CHAPTER II – Field Survey

Using the Parkerian Hexad method to identify information security issues and starting with the common belief that our Internet-savvy generation will be able to answer us about the questions relating to their online behaviour, we started a survey in one of the urban high-school.

The first survey made was a more quantitative one to be able to see if our teens are using computers and other devices, are using email/messenger/social interaction services to communicate among them and with online friends, how many hours are spending in front of the computer, what is the distribution of online time for school, study, entertainment. Secondary observations were made on how the girls and boys are using this online time and if there are differences in the distribution of activities. We are also trying to find out what are the expectations of children towards adults related to mediated communication and IT issues in general.

2.1. Constantin Brancoveanu high school's students – WebQuiz and its challenges

Creating a quiz for them was the easy part. In order to obtain more accurate responses we did not press them to tell their names, in fact, we let them present themselves as they would find appropriate to test their creativity and to impersonate a web-social environment. We also placed the quiz in an alternant view (using a landscape distribution of content with panels and various fonts, similar to a web page) to test their zig-zag attention and ability to cover the info-space and presented this as a WebQuiz 1.0.

An apparent interest in the subject was first observed, and in a few minutes participants were asking each other what they were filling. They were not able to respond individually and those who tried a little were stopped by the rest. The first big problem they encountered was the empty space regarding their brief self-presentation. Many decided, after few minutes, to skip that step and to start the quiz (many tests have no short bio, many participants forgetting to get back to fill it, rushing to finish the task). At the first sequence of questions, related to how many hours are they spending using a device to connect to the Internet many were intrigued because they never counted that time. Many said that if they could, they would be connected all day long to keep the pace with all the news from their friends' circle. Some said that their online time is cut down by their parents who insist that computer is not helping them to get the homework done, and online collaborative work is not aiding them for a real learning experience. Of course parents do not like how children are using parallel applications while they are sitting at the desk for projects and lessons. In the upper corner of the WebQuiz we put a small box, with small typo asking them if they like to read their horoscope online daily with a no/yes tick box answer. Many ignored that corner, and its content, leaving the question unanswered.

Another major rumour in the classes where WebQuiz 1.0 was tested was upon the *more in-depth* questions: how often they are updating their mobile/computer applications, how often are they scanning their PCs for problems, if their phone has a PIN code, if they let their friends accessing their home PC/devices in their absence, what is a PIN code (Personal Identity Number/ Personal Identification Number/pin as in the product to *keep* the phone secured/Post It Note), when they changed their email passwords, do they have alternate email addresses, do they have the same password for more services (Facebook account, email account, Skype account), are they usually sharing passwords with relatives or friends, did they lost an account from a service, how many email accounts or FB accounts do they have, what attachment are they scanning for malicious content: a ppt, a jpg, an exe, a pdf, or a zip file (multiple choice), are they first reading the content of the email or just click on the links provided if the sender is a friend, what if the sender is unknown, do they know how

to send a new email or just reply to the sender, to change information about a class/homework what is the primary instrument: email/messenger, do they set up preferences on the FB account (not only the template), do they know how to phone and hide their number, did they use an alternate FB account to make a bad joke, do they upload many photos on their accounts, do they usually press Like or put a comment, what is a 1337 language, when they last read about a software update and what is new about services they are using daily, what is a .rar file (a large picture, an archive, a program, something bad but I don't know how to explain), who did their first email account: a friend, the guy that set up my PC, my brother/sister, my parents/another adult relative, what is a browser (the PC program, an application to navigate, an antivirus), what PC platform are you using, when they have technical problem what they are doing (waiting for a friend/close relative to help out, calling the boy that made the PC, telling parents, trying to find the solution by themselves), what if they have a problem with a friend on FB (do they report him, ask for friend' help and online support, ask for an offline helping hand to solve it), do they have computer-skilled parents, do they want for their parents to understand what they are doing on PC.

Indeed our WebQuizzes are on paper. The sloppy way to deal with it is evident when observing our test papers, mostly because they took the papers to colleagues to compare and debate them. Most of the students from the same class have the same answers on multiple choices and tech questions. For 1.0 we did not set up a test atmosphere, we let them cooperate and change ideas. Most of them were reluctant to answer to questions related on how many accounts do they own under the pressure of the collaboration, but they had no problems answering on security questions or how they envision the parent-child relation: of course with no restrains. There was a tension when they were not able to answer some questions. Their first impulse was to take a phone and browse the Internet for an appropriate answer. We did not approve usage of devices, only personal collaboration. Even we stated that this should be an imaginary web-site page, with their short bio on top, most of the respondents were caught up in the tech quiz part and forgot about the bio (which was open to any info they wanted to share about themselves) and also they ignored the easy non-problematic inquiries. So we ended up with some serious questions answered, but found out more questions and more problems to look upon.

2.2. The Next Steps

To complete the survey we will want to carry out more samples from different areas of Bucharest, mainly high-schools, and we will try to cover also Informatics high-schools to test their students. So this pre-testing stage will be able to spot the problems that will be included in a project of On-line safety, using also a web platform as one of the main instruments. Into this initiative we want to develop a quick start brochure to help everyone in understanding *what is Internet, some security elements and what are the common threats* in just few clicks.

We are aware that this is just the beginning of our observations, but we hope to gather more colleagues in this little project and to be able to spot the real big problems and also to make teens aware of them and to develop safety-mechanism to cope with the challenges of the online environment.

Opportunity to use a new tool is always full of risks. *One reason that opportunities and risks are linked is because children must explore and encounter some risk to learn and gain resilience. Another is that exploring for information or fun leads to unexpected risks because the online environment is not designed with children's interests in mind. But more skills could reduce the harm that some children experience from online risk.*[10]

III. THE NEXT STEPS

In collaboration with a website owner, also interested in Internet security issues, who also observed the lack of sites dedicated to these problems, we will use the web to present our tips and tricks in a manner easy to understand and to apply for anyone, based mainly on the observations made via WebQuizzes and the other field problems that will arise. The section *On-line safety* from *http://i-security.ro/* will be part of our project to make people more aware of the threats that they are

encountering while web-surfing and how to maximize their efforts and efficiency in browsing for the wanted piece of information.

Another project will be the translation of the Romanian 1337 talk in a way that is similar to what can be found on the http://www.teenchatdecoder.com/ since teenagers already made a communication barrier using their SMS-like dictionary: something mixed up from English language, 1337 talk and Romanian, of course without any diacritical signs.

Becoming empowered and responsible digital citizens will be increasingly important as the internet becomes ever more embedded into daily life. […] *Supporting children and their parents in gaining digital literacy and safety skills* [… and] *promoting children's online opportunities, including their right to communicate and their need to take some risks is important to counter simplistic calls for restricting children's internet use. The ambition must be, instead, to maximise benefits (as defined by children as well as adults) while reducing harm (which is not necessarily the same as reducing risk). A critical lens should be sustained when examining public anxieties, media reporting, industry accountability or new technological developments to ensure that these do not undermine children's interests. Further, critical analysis of regulatory and technological developments should not assume that all users are adults, that parents can and will always meet the 'special needs' of children, or that children's interests are somehow antithetical to the public interest*. [10].

References

[1] Cisco, 2011. Connected World Technology Report. http://www.cisco.com/en/US/netsol/ns1120/index.html

[2] Tilborg, Henk C.A. van; Jajodia, Sushil (Eds.), 2011. Encyclopedia of Cryptography and Security. Springer, 2nd edition. Page 1374

[3] Andress, Jason, 2011. The basics of information security: understanding the fundamentals of InfoSec in theory and practice, Syngress Press. USA. Page 3-8

[4] Andress, Jason, 2011. Cyber warfare: techniques, tactics and tools for security practitioners, Syngress Press. USA. Page 1

[5] McAfee, 2009. Cybercrime, H*Commerce, and What You Can Do to Protect Yourself. http://stophcommerce.com/download/6259flyr_edu_cybercrime_0509_w_fnl.pdf

[6] Livingstone, Sonia; Haddon, Leslie, 2011. Final Report, EU Kids Online II. http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20II%20(2009-11)/EUKidsOnlineIIReports/Final%20report.pdf Page 2

[7] EU Kids Online 2010 - national recommendations. http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20II%20(2009-11)/National%20recommendations/Romania.pdf

[8] Sarbu, G, 2009. Internet, the Educational Instrument of the "Digital Savvy" Generation. In *Culture and Communication in European Union Conference*, Al. I. Cuza University Publishing House, Iaşi.

[9] About Hcommerce. About the Film. http://stophcommerce.com/

[10] Livingstone, Sonia; Haddon, Leslie, 2011. Final Report, EU Kids Online II. http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20II%20(2009-11)/EUKidsOnlineIIReports/Final%20report.pdf Page 43-45

Appendix

The WebQuiz 1.0 layout and more detailed results and analysis will be published also on *http://i-security.ro/*