Early Security Adopters

Marcelo Carvalho, CISSP, CISA, CRISC

Sao Paulo State Faculty of Technology - FATEC
Bell Aliance st., 225 - Sao Caetano do Sul - SP – zip: 09581-420

ABSTRACT

This article discusses how security issues affects kids and teenagers in their daily use of Internet communication tools and their risk profile. Understanding their behaviour and security threats exposure is part of an ongoing state-wide project here described that delivers security awareness training and performs surveys at school classes.

General Terms

Information Security, Information Security Awareness.

Keywords

Security Awareness, Social Internet, Child Safe and Security.

1. INTRODUCTION

Information Security is a broad term that refers to protection of assets (computational or not) to reduce risk exposure by applying them appropriate controls. This is done addressing one or more CIA security pillars and is usually restrictive by nature opposing to functionality features of systems and environments. These very functionalities are appealing to us and as well to kids and teens as they facilitate communication and virtual interaction. The main goal for this type of tool has been broad information sharing regardless the risk that may pose to an inadvertent user. Social media as well as other Internet based communication tools users seems to believe that convenience comes first.

Securing those features by applying this controls doesn´t have to be exclusively technical, negatively impacting their easiness of use explicitly. In fact some effective controls are performed in directive/administrative level such as trainings known as Security Awareness programs. A balance to functionality and security features is an ideal situation based on risk evaluation. The more we're aware of risk exposure more willing to protect ourselves we tend to be.

We are all subject to some security risk degree according to information use, systems interaction and behaviour profile among other characteristics. Moreover, the security or lack of it is not a static object that can be permanently determined. As technology evolves, the environment we´re attached to or even our task changes so the threats implied do too. The determination of security control level is hence an important and sometimes not easy decision to make assessing this characteristics, preferably including information owner participation.

The determination of an acceptable security risk level is normally responsibility of some designated individual or group. Accepting our profession is directly related to corporate security decisions, then CSOs, CIOs and CTOs are usually those persons. But what happens outside this world? Who determines security exposure to regular people (specially to youths) in their regular tasks involving system access and information use on the Internet and other communication medias?

Considering that digital divide is shortening and more and more people are connecting themself using communication tools worldwide, there might be a huge number of people not aware of potential danger or proper security orientation to deal with.

This article discusses the lack of security orientation/education and assistance from part of the above described population: children and teenagers. A state-wide project is described that aims to fill this gap by providing in-class (school) security awareness training. Also, the surveys made showing their security understanding (profile), security exploitation cases (suffered) are described and commented.

2. SECURITY FOR YOUNGERS

When we open our favourite books or browse for information security articles, we´re mostly interest in latest attacks, super physical security locks and data-center safes, new or updated protocols, system audits or highly qualified security frameworks, automated protection systems or guidelines, right?

Believe me, that´s not what´s interest kids and young Internet users. Our survey showed that the majority of them (see Table 1) doesn´t even heard of basic security concepts like password protection before receiving the training. The same figure shows also that many of the access comes from mobile phones (smart-phone browsing capable device) so leaving the security control to parents isn´t a feasible at all. Instead, education programs aiming to kid's specific needs needed to be developed.

To teach security for youngers we hence found that we needed to start very low and take advantage of every opportunity to try survey this population using Likert and Guttman scales [1] to figure their security knowledge profile. We used quantitative/qualitative approaches [2] to formulate a short and yet assertive questionnaire for security behaviour profile investigation. We actually spent a considerable amount of time constructing a couple of survey options until we´re sure retrieving desired information [3]. A mistakenly training scope decision could easily lead to lack of interest from audience or even project objective failure. As seen on (Figure 1), not only the initial questionnaires but the subsequent ones performed after lecture presentations allowed us to keep optimal content alignment and constant understanding of target audience knowledge and demands.

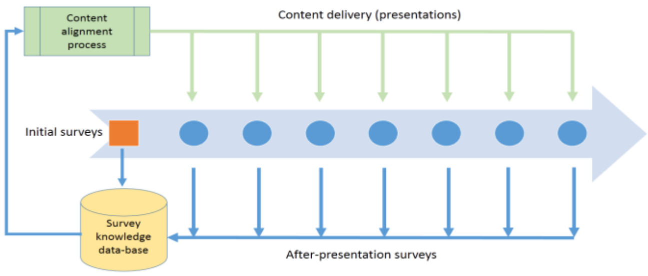
Content alignment process
Content delivery (presentations)
Initial surveys
Survey knowledge data-base
After-presentation surveys

Figure 1 - Project content formulation framework

Our education system (despite local and regional specifics) tries to fill our students with all necessary knowledge to build a solid formation including several different disciplines. Despite that, very useful and tightly related to any individual's needs in regular life activities are somehow neglected like financial education and others. The same gap applies to information security and how to protect them from common threats.

According to our first impressions, the education challenges not only resides on lack of information security familiarity but also in the way (media) they use to connect themselves to the Internet.

Table 1 - Initial student's population partial description

Question	Average reply
How many hours are spent online daily?	4,2
Do you mostly access Internet social media and communication tools via home computer?	Yes – 58% No – 31% (from mobile) No – 2% (don´t use Internet) No – 9% (from other people's computer)
Have you ever heard about or previously received information security related training?	Yes – 3,5% No – 96,5%
Have you been victim of information security attack at least once?	Yes – 8% No – 40% Don´t know – 52%

Some of this numbers though are not consistent to broader (country-wide) census research recently published. The amount of people accessing Internet from home considering whole Brazilian population representation for example is consistently higher: 69% [4]. Inferring that for our specific target audience the connections performed outside their home are done unassisted from parent or teacher supervision/control, our advisory approach must then focus on their behaviour rather than technical controls as they´re mostly on their own.

Hence and considering the timeframe exposure shown and the fact that a great deal of this students often uses other people's device (OPD) for Internet connection, we took a wider approach consideration. Any training based only on security software remedies or advocating adult supervision doesn´t seemed to fit their needs. We then decided to focus our efforts in two main fronts: parent's education (through printed hints and advisor material) and student's education (through 1 hour basic lectures).

The contents for the second approach included the following highlights:

1. Privacy issues
2. Safe browsing and e-mailing
3. Digital-tatoo
4. Threat examples

Although separated in different topics, we produced the content material emphasizing privacy issues in various aspects.

Private information (PI) threats including Personal Identifiable Information (PII) is perhaps one of the most commented topic in information security journals articles including IJCA's. Although many tools and frameworks suggests and proposes different mitigations for communication and social tools scenarios [5] such as alerts and automatic risk detection based on "revealing" words or expressions, we stress this must be preferably a user-centric behaviour approach.

The ubiquitous virtual presence and social networking information sharing are addressed in those four topics.

1-2. The PI issues and safe-browsing and e-mail topics explores mostly the need for safely identify and trust communication peers. In social networks that also includes the concept of attempting to connect to friends of a friend in their relationship chain (multi-hop trust) and share private information. As far as concerns trusting peers, the farther from user direct social relationship the harder is to establish enough certainty that is safe sharing information down the hops. The privacy problem arises when we allow the social app to get informed about our location pattern, likes and dislikes, and of course when we get so involved and trustworthy in our online relationships that we start sharing daily routines, trips, goods acquired, our photos in front of our cars (license tag shown) and so on.

Differently from chat or e-mail tools where users more explicitly send information to destination, social tools can masquerade those sharing easing PI leak.

3. Digital-tatoo adverts for the spreading capabilities of the WEB and the lack of PI control after content publishing due replication issues. Like in real world, once printed, the tattoo (information) can't be completely erased. At this topic we also discuss about cyber-bullying and its reflection on personal and virtual offendant's life. Something published with bullying intentions for instance, can hardly be erased from the Internet even if a court determines content link deletion as users comments, replies and forwarding often outscope communication tool initially used.

4. While describing information security threats examples, we take advantage of news´s and hot topics on the WEB to demonstrate and describe common attacks. Surprisingly, at this moments we usually receive feedbacks and testimonies of students identifying themselves as previous victims. Those case' information are also used to retro-feed presentation content production process described earlier (see Figure 1).

3. STUDENTS AS TEACHERS

We all know what study strategy best fits us. Some of us best performs by writing and reading content material, some needs a more visual or tactual experience or even an applied situation. I luckily found that passing my understanding to others was an efficient way to learn more and ever since I encourage others to do the same. This project uses our university's student participation to disseminate security content to youngers, stimulating this learning approach.

We witnesses a very positive result from choosing young students to act as teachers (student-teacher) for this project.

The bond created during lecture to children was a great surprise as audience seemed to feel at ease by knowing they´re also students like them. Student participants often outperformed in scholar's activities after project engagement and a sense of reward by making a difference in audience routine was clearly noticed.

3.1. Our Security Awareness Project

The developed project began at June 2012 and comprises three universities participation leaded by author as an IT/IS professor in Brazil [6][7][8]. It delivers security awareness training by using customized audio/video presentations specially designed to "talk" to children and teenager needs using their language. The initially targeted audience were universities' curb located schools, gradually expanded for more distant ones. This population called our attention due their security understanding absence and their natural exposure to the threats we all see described in the various issues of this journal (including the very basics concepts), perhaps because of their very age and lack of life experience.

The project rapidly gathered information security university course students (29 enlisted by now) from latest semesters who´d like to share their accumulated knowledge to the younger society around them acting as teachers. We formed different groups each equipped with presentation material to reach separated target audience (8-11 and 11-14 years old) and started to contact nearby schools for training scheduling thru project partnership.

Although not intended to, we felt that our initial presentations caused some sense of panic as more and more critical unsecure situations and attack descriptions was presented during classes. So carefully discussed amends were made softening the content to match audience understanding level.

A drop in the ocean

We managed to cast at least three project appearance per month since its starting date, thus reaching approximately a total of 690 children/teens at the first six months. The forecast for this semester is even better and the preview by the end of July is that we´ll add 1300 more to the count. Although consistently increasing numbers, this might sound very few if you take an entire population. In fact it is, considering the amount of children in school age just for the state of Sao Paulo-Brazil [9], we'll need to manage reaching 8.728.170 more students. Even reasoning a 3.3 growth ratio in student-teaching team per month in this project, (Figure 2) it shows a very hard to solve scenario.

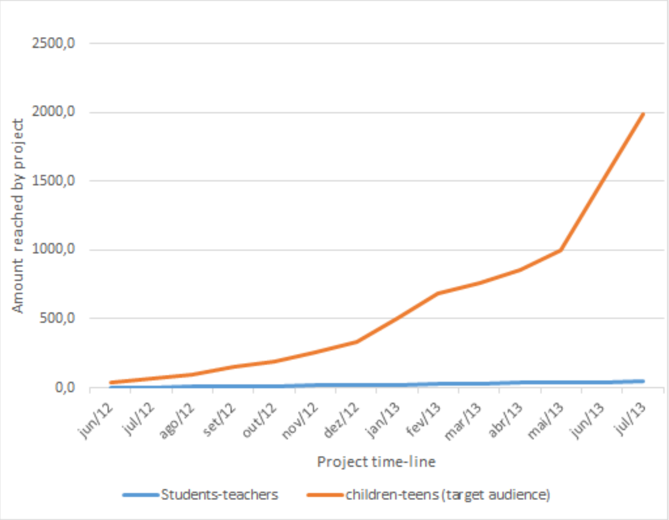

Figure 2 - Project reaching projection for Sao Paulo's student population

3.2. Collected Survey Results

A more in depth look at our targeted audience showed that the Internet usage profile also changes if you take sex and age into consideration. Comparing to a recent (2011) external survey including whole Brazilian population analysis [4], all the evaluated aspects showed differences from our target audience, including some uses simply absent (not mentioned in survey's replies) for a certain age and sex.

Table 2 - Internet content access population comparison (National survey vs. Project survey)

Internet Use	**Appearance in survey questionnaire**		
	Kids	**Teens**	**External survey**
Watching movies or videos (streaming)	M:23% F:8%	M:38% F:4,4%	M:62% F:53%
Music Download/Listening	M:49% F:35%	M:56% F:53%	M:55% F:47%
On-line gaming	M:18% F:Not mentioned	M:22% F:2%	M:48% F:35%
Blogging	M:34% F:49%	M:27% F:61%	Not mentioned
Social networking	M:25% F:28%	M:37% F:69%	Not mentioned
E-mailing	M:Not mentioned F:Not mentioned	M:8% F:3%	Not mentioned

1) *Main internet usage:* Exploring the Internet usage detailed results, we found that music listening, blogging and social networking were the main interests for this population. Considering the associated risks from available apps and platforms to do so, we concentrate our recommendations on restrictive configurations. As sharing privileges and security restrictive options are not set by default on this tools, the risks are simply invisible to most users. The first step for safe use should be opt for it into settings.

2) *Unsecure behaviour:* Being polite was one of the answers substantially found while asking users "Why will you accept an invitation from strangers to connect/join?". Presumably, this behaviour (like in real social life) refers to

our inability to say “NO!” and to be considered rude by others doing so. Being rude in this case might mean being secure.

Another noticed behaviour in social networking tools use is related to the artificial intelligence embedded on apps. This tools main goal is better interconnect users. Hence, relationships considering common contacts, preferred discussion topics, geolocation and other characteristics are used to automatically suggest new connections by e-mailing them or directly within app interface. As more and more user-to-user connections are made inadvertently (no proper vetting), more difficult is to keep trust relationship tightly under control.

Photos and videos posting are also a very common insecure posting behaviour from studied population that drove project’ attention. Willing to receive more “likes”, positive feedbacks and other user’s comments, they leave privacy restrictions aside opening up for a larger group of people. The new “tag photo” face recognition functionalities shows user identity (name) in all casted images to any friend or follower within contacts chain. The same goes to “add location” feature that can position user movements on the map, including time-line tracking. Moreover, the photos and video contents sometimes reveals PII directly, exposing users to social engineering and other attacks. The most common scenario to that was home address exposure at picture back plane.

A more serious mistaken behaviour was found on social networking users (teenage users) with regard of contact interaction. A significant percentage (12,2%) declared that often migrate virtual relationships to personal interaction (personal meetings). That behaviour is particularly concerning in the cases that the virtual friendship was established without prior offline knowing of other end. We know that in several scenarios, one saying be someone at your age and sharing the same likes and dislikes in virtual world is not necessarily that way in real life. Real world interactions with potential criminal intent persons are out of scope of our training but certainly and educator/parent preoccupation.

3) *Security incident history:* Frightening results came from respondents who claimed being victims of threats here discussed. Bullying attack (a.) and kidnaping attempt attack (b.) are two selected incident history found among project audience for discussion. All studied population are subject to these threats, although the collected testimonies were found only at our teen portion results.

a. Bullying attacks were harassment type messages/posts received by our kids and teens. Hateful, threatening and xenophobic messages as well as war callings (soccer fans) were the most cited in this category. 4% and 7,1% of kids and teens respectively declared that at least once were subject to anonymous or contact-list related messages of this type. The anonymous type posting seems to encourage this aggression scaling to wider proportions [10]. Extreme cases of this type of embarrassment usually results on school absence or even course cancel from kids’ parents. Physical aggression were commonly reported on those cases [11].

One of the kids that openly declared himself attacked during a presentation was personally interviewed. The main interest at the time was to understand at what point his parents were involved. He declared: “I could no longer drop the bus at the school’s station, so I told them”. This children was clearly traumatized and was later diagnosed depressed. That proves parents and educators need pay close attention on student’s Internet activity as much as possible to early detect this type of problem.

Bullying is not a new thing but the presence of the Internet element is spanning group frontiers exposing even more the victims. Bullies impacts their prey’s life even after school hours. Education has an important role in this aspect as it’s a 100% behaviour related issue. The question perhaps is: “Are we ready to assist them?”. European Network and Information Security Agency (ENISA) has launched a new report in 2011, listing educator risks on this duty in face of cyberbullying:

- The risks that teenagers will develop activities and behaviour patterns that escape the sphere of influence of guardians, such as second life, cyber activities, uncontrolled virtual meetings etc;

- The risk that adults will not have the knowledge and tools to control online activities;

- The risk of failing to provide and maintain a secure digital environment for teenagers to use;

- Inability to fulfil the care duties within school;

- Risk of failing to defend oneself due to lack of knowledge, evidence and legal framework.

b. Although statistically irrelevant (1 reported case only), the kidnaping attempt was selected for discussion due its danger degree. The dangerous characteristic of this case as previously briefed at project description is its real world interaction. Just imagining a teen wondering to date a good-looking guy met on the Internet and being taken or forced to go elsewhere by an adult chilled my spine.

Luckily, this survey report content mentioned an attempt only. The answer described that once found that the dating mate was an elder person, the teen girl quickly go away. Whilst analysing this and other creepy detail answer I was thinking the potential bad ending and hence researched for similar cases. Was that really a deviation from responses padron or were we simply not aware this was commonly reported?

A quick google search demonstrates that this is quite common. Some facts numbers of similar cases sometimes are described as online grooming (preparing sexual abuse). Child Exploitation and Online Protection Center (CEOP) in UK claims that 25% of children and young people have met offline someone they only previously contacted online [12]. According to FBI’s website [13],” a child goes missing every 40 seconds in America. That comes to 765,000 children a year”. A face to face encounter of online mates are certainly among those numbers.

3.3. Related projects

Many national and international projects are engaged with security awareness presentations worldwide. Some of them are designed to kids only and others to parents/carers, either related to government’s initiatives, professional class entity or independent projects. As seen on (**Figure 3**), the main deliverable types are offline (in-class) and online material.

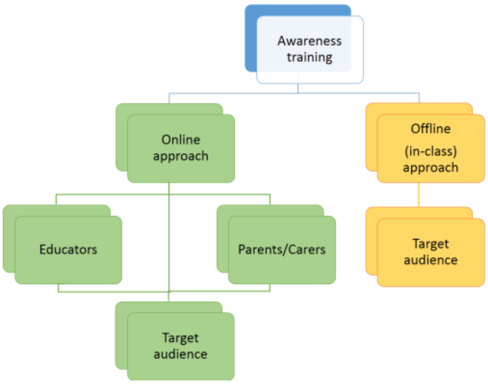

Figure 3 - Main awareness projects deliverable types

ISC2 Safe and Secure project available in Switzerland, Canada, Hong Kong, the United Kingdom, and the United States is an international example. It has a similar target audience and it's designed to ISC2 members participation only as teachers (https://www.isc2cares.org/safe-and-secure/).

A more independent but nationwide scope limited project is called C-SAVE from National Cyber Security Alliance. Also meant to deliver volunteer presentation on schools, this project was born after a survey made on 2008 stating that only 22% of regular kids' teachers were comfortable enough to teach about cyber-bullying, identity theft and other types of cyber-crime by their own.

Another example based on web presentations is available from SANS at http://www.securingthehuman.org/resources/presentations. The project is called "Securing The Kids" and was designed to help parents understand the risks their kids are facing.

India also delivers brochures guidelines describing safe behaviour on common tools (Social Network, Chat, E-mail, etc) directly to kids thru Department of Electronics and Information Technology project http://infosecawareness.in/children. A similar proposal was developed here in Brazil using brochures but not specifically designed to children (http://cartilha.cert.br/).

3.4. Information Security within a Regular School Program

In England, U.S. and other countries, students now have information security lectures as part of their regular curriculum.

Aligning IS topics with regular content can help increasing the skills of an entire future workforce of security early adopters. Integrating security topics into the curriculum can also help address issues of online safety within school' computational environment [14].

PII issues and other security concerns in school environment are being addressed by guidelines and government regulations. The Children's Internet Protection Act (CIPA) concerns about student access to offensive content over the Internet on school and library computers [15]. By the same token, Children's Online Privacy Protection Act (COPPA) and The Family Educational Rights and Privacy Act (FERPA), regulates the collection of personal information about children and student records on the Internet [16][17].

As we all know though, the human interaction tends to be the weakest link mostly so no guideline or regulation can succeed with no proper attention to children education.

4. CONCLUSIONS

As we have seen from different examples including our project, information security awareness programs dedicated to children and teens can promote positive results rapidly. The replication effect seen in schools where the theme was previously discussed in early visits indicates that once the topic is explained it has a natural interest among students audience. The advices and lessons learned during presentation are shared and quickly spread. Although focus on the functionalities benefits from Internet communication tools, this audience got interested on security themes.

Privacy issues, virtual relationship abuse and computer infections are prevalent worries according to our project experience and survey results. We should pay attention on what content is being accessed and which social interaction is being performed by the children and teenagers so proper protection can be delivered. Early security adopters can protect themselves from known threats by behaving securely.

The project reach is still very shy but there are other similar educational programs aiming same public and disseminating information security topics worldwide. Also, we can all do our share by leveraging discussions to the ones next to us.

IJCA readers, come and join educational initiatives and make you too the difference on IS learning at schools near to you!

5. REFERENCES

[1] Bohrnstedt, G. Reliability and validity assessment in attitude measurement. In Gene F. Summers, Attitude measurement. 1998.

[2] Light, J.; Yasuhara, K. Analyzing large free-response qualitative data sets — a novel quantitative-qualitative hybrid approach. Frontiers in Education Conference, 2008.

[3] George, C.P. A Machine Learning Based Topic Exploration and Categorization on Surveys, 2012.

[4] ICT Households and enterprises 2011. Survey on the use of information and communication technologies in Brazil, 2012.

[5] Hirose, M. A Private Information Detector for Controlling Circulation of Private Information through Social Networks, 2012.

[6] Senac University - http://www.sp.senac.br (last viewed 03-03-2013)

[7] Fatec Faculty - http://www.fatecsaocaetano.edu.br/ (last viewed 03-03-2013)

[8] Brazillian Institute of Advanced Technology – IBTA - www.ibta.com.br/ (last viewed 03-03-2013)

[9] IBGE – Students in school age population. http://www.todospelaeducacao.org.br/educacao-no-brasil/numeros-do-brasil/dados-por-estado/sao-paulo/ (last viewed 03-03-2013)

[10] Cyber bully attacks Minneapolis Washburn students. http://www.kare11.com/science_technology/article/991771/484/Cyber-bully-attacks-Washburn-students (last viewed 03-02-2013)

[11] Cyberbullying leads to school attack. http://www.iol.co.za/the-star/cyberbullying-leads-to-school-attack-1.1230431#.UUInkBfvsgk (last viewed 03-02-2013)

[12] CEOP Strategic Overview 2009-2010 - http://www.ceop.police.uk/publications/ (last viewed 03-15-2013)

[13] FBI and the National Center for Missing & Exploited Children. http://www.fbi.gov/news/podcasts/inside/inside_071211.mp3/view (last viewed 03-15-2013)

[14] Schools learn hard lesson in information security protection. Infosecurity Magazine, 2011. - http://www.infosecurity-magazine.com/view/16816/schools-learn-hard-lesson-in-information-security-protection/ (last viewed 03-13-2013)

[15] The Children's Internet Protection Act, 2001. - http://www.fcc.gov/cgb/consumerfacts/cipa.html (last viewed 03-13-2013)

[16] The Childrens Online Privacy Protection Act, 2000. - http://www.ftc.gov/bcp/conline/pubs/buspubs/coppa.htm (last viewed 03-13-2013)

[17] The Family Educational Rights and Privacy Act, 1974. - http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html (last viewed 03-13-2013)