Should Cyber Security be Taught in Schools?

Instructor: Dr. Craig Derksen
PHIL-110-01
Aug 2014

Abstract

In light of today's technological advancements, a huge responsibility of maintaining secure computer systems lies at the feet of the user (1). However, there is still a lot who fail to apply existing network security knowledge, to minimize the scope of breaches, which creates serious problems that require a clear action for four main reasons (2). First, the increased use of Internet-enabled devices has led to the rise of cyber-crime (3). Second, the shortage of cyber security professionals poses a threat to the Canadian national security (4). Third, the limited knowledge of how much important taking security measures is, can affect the person and everyone else in the network (5). Fourth, children are less savvy and less aware of the dangers of mishaps and misbehaviors on the Internet ground. This is a major concern because it makes children an attractive hub for cyber bullying and cyber-attack (6). Therefore, two approaches are suggested in order to reduce our vulnerability. One is training employees and the second is including computer security in the school curriculum (7). Some argue against the latter as an expensive process (8). Others argue that it is only an IT issue (9) while some others believe that computers can be fully secured. Therefore, there is nothing to be worried about (10). In conclusion, we expect that those reasons act as a wakeup call for officials, hence will extend understanding and awareness of the importance of teaching computer security at the K-12 level (11).

(1) As the digital world increasingly grows we are becoming more and more dependent on technology. Unfortunately, computers and data are not completely secure and perfect. Data is often roaming around us and there is always an available gap for breach and attack. Thus, anyone can be easily targeted. Although chances of getting hacked might not be inevitable, they can, however, be reduced to some degree. Today, many people make mistakes that cost them loss of their privacy and security (Pfleeger). This is mostly due to lack of knowledge and negligence. Therefore, there exists the need for users to become knowledgeable about computing and possible network security risks, which compromise data integrity.

(2) An analysis of computer security breaches reveals that a vital component of network security is outside of fortified technological firewalls; individual user behaviors do determine network vulnerabilities. Therefore, individual users who are more concerned with convenience and think of data authentication and identification as a burdensome component put themselves and others at risk of theft and fraudulent practices (Pfleeger). This highlights the missing gaps in our current understanding of data security and technology, which presents a very serious matter that requires attention for four main reasons.

(3) First of all, as technology doubles every year, "Political use or misuse of the Internet has also increased dramatically" (Pfleeger). The rise of unethical hacking poses a threat to industries' secrets and intellectual properties. For example, in early 2011, hackers targeted Saskatchewan federal government computers in order to gain information about the Potash Corporation, one of the world's largest fertilizer companies. This attempt was unsuccessful but it is alarming as it shows why this issue requires national attention (Jeremy, 2011). Another

example is the series of international cyber-attacks at the Canadian Nortel Corporation (the Northern Electric and Manufacturing Company) over a span of almost10 years. It was found out later that hackers had free access to the company's data for many years without being detected, which indicated vulnerable gaps and holes in the network. The extensive damage these attacks had caused, led to the bankruptcy of the company in 2009 (CBC, 2012).

(4) Secondly, the limited awareness of Internet security has created a skills shortage in this field in Canada. Public safety officials warned in a report to The Star Newspaper in January 2012 that the old lab facilities, lack of emergency policies, and trouble recruiting cyber specialists is threating the government's ability to counter online criminals and Internet attacks. Although, in 2010, the federal government had allocated a five year, 90 million dollar plan to secure government, business, and personal computers, Rafal Rohozinski and Adrien De Beaupré, experts and IT security consultants, both agreed that the plan is not enough and it only constitutes a fraction of what other countries had invested towards their online safety (Gillis, 2012). "Canada will have to make cyber security a priority by investing more resources and devising a clear action plan" said Rafal.

(5) Third of all, the lack of knowledge on an individual level affects data security and privacy of the person, or even others in the network. In other words, not taking necessary security measures for home computers and personal devices such as IPads or smartphones is a real danger. Instances of such important measures are: running an antivirus software, antispyware, software firewall, backing up data regularly, updating the operating system, hardware firewall, wireless encryption, using strong passwords or passphrases for all accounts,

connecting only to known WIFI providers, understanding phishing/scamming and not falling for it, visiting trusted websites, and making online purchases only from reputable websites. (US Department of Homeland Security)

Failing to follow these crucial guidelines could put someone in a position of becoming a victim of identity theft or even worse, losing all of their money. A person who thinks that their information on their devices is not important, could also allow their computer to act as a zombie in which hackers perform attacks on other peoples' computers through a network of zombies by not maintaining basic security measures.

(6) The fourth reason why cyber security is significant and requires action is because of the higher degree in which children's' behavior can badly affect their lives. Today kids switch from one digital device to another with ease and without issues. Preschoolers and kids aged 5-12 are one of the fastest growing groups of computer users (Gutnick, 2011). With the availability of touch screen devices such as IPads and IPhones, kids play video games and socialize with each other too. Also, almost every teenager in North America is registered to a social networking website such as Facebook or twitter. In fact, recent studies show that teenagers write about half the blogs nowadays. However, the real problem here is that they reveal too much personal information. Two out of three teenagers provide their age, three out of five reveal their location and contact information, and one in five gives their full name (Walker, 2011). Not to mention the rate at which they post photos and shop online with insecure passwords.

This is an issue because it makes children an easy and attractive target for phishing, scams, cyber bullying, and internet predators. "According to the Federal Trade Commission, 31 percent of reported victims of identity theft are young people". These kids not only bring harm to themselves, their data, and their reputation, but they could also get their parents in trouble too. For example, in 2011, an 8-year old child managed to spend about 1400$ on Smurf's Village on her mother's IPhone (Kang, 2011). This and many other examples like this, only go to show how things could get out of control without awareness.

(7) Because of those four reasons, we need to trace back to the root of the problem in order to contain it and solve it. In this case it is either the individual user, whether it is a kid or an adult, or the employee who slips up. Therefore, we have two different approaches here. The first one is to provide training to employees or adult users at home. This will ensure a relative reduction of cyber-crime. However, in order to build an effective secure system nationwide, we should start with schools. Teaching computer classes with attention to Internet security should be embedded in the school curriculum. There is no question that kids are fast learners and this will ensure that they will absorb this knowledge and put it to good use. On the personal level, this will reduce the risks of potential attacks and spread awareness. On the corporate level, this will at least prepare a security mindset and could guarantee the increase of a security-savvy workforce in the future.

(8) Some people argue that taking this approach is going to be very expensive because schools are not prepared for this. The national public schools will require enormous resources in order to provide teachers with adequate training. Therefore, they think that it is the parents'

primary responsibility to educate their children about cyber security. In an American survey "State of K-12 Cyber ethics, Cyber safety, and Cyber security Curriculum," only one third of the teachers thought that teaching cyber security is a requirement, 71 percent of administrators believed that it is a requirement, and 79 percent of teachers thought that parents should primarily contribute (Walker, 2011).

It is true that including cyber security in the school curriculum might be costly initially as some people say, but ultimately it will pay dividends for the next generations. There is also no doubt that parents have to step up too with spreading awareness, however, it has to be a shared responsibility between both home and school.

(9) From a different perspective, some people in the business world argue that cyber security is an Information Technology (IT) issue; therefore, only IT technologists should be concerned about it (Touhill, 2014). This is not true anymore because cyber security is the responsibility of everyone. All departments in a business should acquire at least a basic knowledge of what cyber security is about. In his book "Cyber security for Executives," Gregory Touhill, a cyber-security and IT consultants for many big and small companies, explains that in organizations cyber-security is not just technical but rather a business imperative. It is more about risk management and protecting the business and its assets. Therefore, all managers at all levels should involve everyone in producing effective, efficient, and secure systems. Taking this into consideration, it is going to benefit employers immensely if the employees hired were to know a bit about security, and this is where teaching cyber ethics and security becomes important.

(10) In the same business environment, some argue that companies can be 100% secure, therefore, they do not have to worry about it so much. Jack Phillips, who works as a manager at the Institute for Applied Network Security explains that this is just an illusion. Risk cannot be eliminated entirely but we can lessen our vulnerability. Technology is changing always, and hackers are always finding new ways to penetrate secure systems (Evens, 2006). Again, it is all about assessing risks and active monitoring. Otherwise, if we were able to create completely secure systems, we would not have seen an increase in cyber-crime and we would not have needed more specialists nor needed to think about teaching kids cyber ethics at schools.

(11) Eventually, cyber-security is relatively a new discipline (Touhill, 2014) and it is growing because technology is becoming more and more central to our everyday lives and to the way businesses and governments operate. That is why the Canadian school system should be redesigned to include computer classes with special attention to security as a mandatory requirement rather than an elective course.

References

Aviva Lucas Gutnick, Michael Robb, Lori Takeuchi, Jennifer Kotler. *Always Connected: The new digital media habits of young children.* New York: The Joan Ganz Cooney Center at Sesame Workshop, 2011.

Cecilia Kang, Washington Post. *In-app purchases in iPad, iPhone, iPod kids' games touch off parental firestorm.* Feb 8, 2011. http://www.washingtonpost.com/wp-dyn/content/article/2011/02/07/AR2011020706073.html?sid=ST2011020706437.

Evens, Kate. *Total security is just an illusion.* June 20, 2006. http://searchsecurity.techtarget.com/news/1195022/Total-security-is-just-an-illusion.

Gregory J. Touhill, C. Joseph Touhill. *Cybersecurity for Executives: A Practical Guide.* Wily, June, 2014.

NEWS, CBC. *Nortel collapse linked to Chinese hackers.* Feb 16, 2012. http://www.cbc.ca/news/business/nortel-collapse-linked-to-chinese-hackers-1.1260591.

Pfleeger, Dr. Charles, Pfleeger Consulting Group, Washington D.C. "Computer security." n.d.

Safety and Security Center, Microsoft. *Teach kids online security basics.* n.d. http://www.microsoft.com/en-gb/security/family-safety/childsafety-internet.aspx.

Security, US Department of Homeland. *Home Network Security.* Dec 5, 2001. https://www.us-cert.gov/Home-Network-Security.

Tim Walk, Nation Education Association. *Who's Responsible for Teaching Online Safety?* May 31, 2011. http://neatoday.org/2011/05/31/whos-responsible-for-teaching-online-safety/ .

Warren, Jeremy. *Post Media News.* December 2, 2011. http://www2.canada.com/story.html?id=5803576.

Wendy Gillis, TheStar News. *Canada has poor security against cyber attacks, documents warn.* June 7, 2012. http://www.thestar.com/news/canada/2012/06/07/canada_has_poor_security_against_cyber_attacks_documents_warn.html.