INFORMATION SECURITY EDUCATION: WATCHING YOUR STEPS IN CYBERSPACE

Tharindu SENANAYAKE
University of Moratuwa, Faculty of Information Technology, Moratuwa- SRI LANKA
125060P@uom.lk

Suchinthi FERNANDO
Rutgers University, School of Communication & Information, New Jersey- USA
suchinthi.fernando@rutgers.edu

Abstract: This paper discusses the importance of providing at least a basic education in information security to all users of any information and communication system, regardless of whether they are information technology professionals, students of computer or information sciences, or not. It explores how any person sharing and communicating their information assets with others could be subject to information security threats, and studies certain known cyber-criminals and black-hat hackers, and their cyber-actions and cyber-crimes in order to depict the importance of acquiring an understanding and awareness of information security, so that users of information and communication systems may prepare and strengthen themselves against imminent information security threats.

Keywords: Information Security Education, Awareness, Risk Perception, Cybercrimes, Cybercriminals, Information Security Behavior

Introduction

Information technology (IT) education has become an integral part of education regardless of the subject being taught. Even for professionals and students not working or majoring in computer science or information science related fields, the use of IT may come in multiple forms; sometimes as a tool for delivering the subject matter and assessments such as in learning management systems, presentation slides, etc., and at other times as a tool for creating systems to make practice of that subject convenient and more efficient, i.e. health management systems, online banking applications, and numerous other such subject-specific computer and information technology systems. Thus, basic skills such as basic programming, database development, web interface development, etc. are also studied by most non-computer professionals in order to help them put their knowledge of their specialized subject into practice. A most important concept regarding computer and information science which is often overlooked, however, is information security. Yet, information security is an integral part in any computer system which stores information and allows its users to access and share that information, since a good system should be more about proper and secure sharing and communication of information instead of simply allowing access to available information regardless of whether each user should be allowed access to that information or not. According to Harris and Maymi (2016), the IT industry is growing much faster than people can be educated to properly maintain it, thus leaving less time for IT specialists and security professionals to discover new security practices and procedures and giving more time for hackers to learn how to circumvent these security mechanisms (Harris & Maymi, 2016). Additionally, any user of an information and communication system, whether it be an online banking application containing digitized financial information, a health information system containing both digitized and non-digitized information regarding medical history and so on, or a seemingly simple social networking site which allows the user to share their personal information with other users, should have sufficient knowledge about information security in order to properly utilize the information and communication system they use, while ensuring that their privacy is protected and that the information is only shared and communicated with the proper people through proper channels. Therefore, this paper discusses the importance of information security education not only for students majoring in computer and/or information science, but also for designers, developers and users of any information and communication system.

Importance of Information Security Education and Awareness

A thorough education in information security would have to cover certain basic, yet mandatory, subject areas. These information security subject areas comprise of Access Control Systems and Methodology, where specific users or user roles are identified and access to information is controlled based on user privileges by user authentication and authorization to access, Telecommunications and Network Security, where communication systems, network structures, devices, protocols, remote access, etc. are considered, Security Management Practices, which entail classification of data, policies, procedures, standards, guidelines, risk assessment and management, personnel security training and awareness, security budget versus needed protection, etc., Application and Systems Development Security, where the way information security is integrated in the software development life cycle is considered, along with change control, application security, development practices and risks, malicious code, etc., Cryptography, which is the art and science of disguising data using symmetric or asymmetric algorithms, hashing, etc., Security Architecture and Models, where operating states of the operating system, kernel functions, memory mapping, security models and architectures are studies, Operations Security, which takes personnel and job functions, training, auditing, resource protection, preventive, detective, corrective and recovery controls, and standards compliance and due care, etc. into consideration, Business Continuity Planning and Disaster Recovery Planning, where resource identification and value assignment is conducted and business impact analysis is performed to enable crisis management, plan development, implementation and maintenance, Security Laws, Investigations and Ethics, where laws, regulations, crimes, software licensing and privacy, evidence types and admissibility into court, incident handling, etc. are considered and how to perform digital forensics while maintaining the chain of custody etc. are studied, and Physical Security, where perimeter security, restricted areas, authorization methods and controls such as biometrics, swipe cards and tokens, pass codes and personal identification numbers, etc., motion detectors, sensors, alarms, intrusion detection and intrusion prevention, fire detection, prevention and suppression, heating, ventilation and air conditioning, fencing, security guards, etc. are considered. Certified Information Systems Security Professional (CISSP) exam defines eight CISSP domains as Security and Risk Management, Asset Security, Security Engineering, Communication and Network Security, Identity and Access Management, Security Assessment and Testing, Security Operations, Software Development Security (Harris & Maymi, 2016), which comprise of the above subject areas.

Even though the concept of information security began with its focus being mainly on technological aspects (Bishop, 2003), the importance of the role played by the human aspect pertaining to information security was recognized during the past two decades (Fernando, 2014), with international standards such as ISO/IEC 270001 (2005), etc. emphasizing why human resource security needs to be taken into consideration when managing information security. In fact, the users of a system are considered as the weakest link in security, and according to Lacey (2009), information security has of late shifted its focus where its role has changed from being technology-oriented to one that is more management-oriented (Lacey, 2009). Companies and organizations dealing with vast amounts of data and information are not the only subjects at risk of information security breaches. Anyone with a computer or any other communication device connected to a network could be subjected to information security threats and attacks. Most present day attacks such as social engineering, spear phishing, or collusion from an insider, etc. require a human component to succeed (Williams, 2011), where people are mostly tricked into revealing confidential information to others. Thus, it is important not only for information security professionals and computer or information science students to be aware of information security, but simply any person using any communication device for any purpose, whether it be professional or personal, needs to be aware of information security threats, vulnerabilities, and basic countermeasures against these threats and vulnerabilities.

The information security subject areas and domains listed above are important for information security professionals to perform risk analysis, identify countermeasures, and implement solid security practices to help protect facility, network, system, and information by efficiently and predictably balancing risk with service (Harris & Maymi, 2016). For most users of information and communication systems, however, a basic information security education on how to protect oneself in cyberspace would suffice. In the present day where everyone is more or less digitally interconnected with each other, being ignorant of information security vulnerabilities and possible threats is not an option. Yet, for most users of information and communication systems, ignorance is bliss. In fact, Schneier (2008) discusses how the human brain perceives security and explains how when one's perception of security diverges from the reality, and the perceived risk is thereby less than or greater than the real risk, the countermeasures implemented in order to avert that security risk also diverge from what is actually necessary (Schneier, 2008). Further, Gonzalez and Sawicka (2002) state that proper perception of risk can help keep risk below the 'accident zone' by maintaining security measures above a certain threshold (Gonzalez & Sawicka, 2002). Thus, it is of utmost importance to properly understand the very real security risk taken by all users when sharing and communicating information in today's world. An interesting approach to this is to study about the adversaries from whom one should protect their information assets. These adversaries, the dark knights of cyberspace, are cyber criminals who perform illegal actions and are called black-hat hackers or crackers, to distinguish them from white-hat or ethical hackers. The approach adopted in this paper to provide an understanding of the very real information security threats to users of information and communication systems, is to study certain practices which were followed by some known black-hat hackers, in order to understand the importance of information security education, where information security vulnerabilities lay, and how to strengthen oneself against information security attacks by taking required countermeasures against such vulnerabilities. The remaining sections of this paper explores practices of certain known hackers in order to educate users of information and communication systems on possible threats, vulnerabilities and countermeasures that can be taken to minimize these risks.

Certain Notorious Black-Hat Hackers and Their Hacks

This chapter will explore three notorious black-hat hackers who pulled off some of the largest and most incredible hacks of all time. The hacks pulled by these black-hat hackers, their actions in cyberspace, how they were apprehended by the authorities, and the mistakes that led to their capture, etc. will be discussed here. For the remainder of this paper, the term ‘hacker’ will be used to identify or describe a black-hat hacker or cybercriminal. In this paper, the cyber actions of the hackers Jeanson James Ancheta, Kevin Poulsen, and Albert Gonzalez are studied.

Jeanson James Ancheta

Selecting certain hackers out of the numerous known destructive hackers for this study was difficult, but placing Jeanson James Ancheta within the top-ranked hackers is not surprising as he was the first person to be accused of controlling a large number of hacked computers.

Ancheta was a high school dropout who invented ‘rxbot’ – a software robot program also known as a bot. Bots or software robots are malicious software created to take over the control of a computer remotely by a third party (Pegg, 2016). With this software, Ancheta took over a large number of computers connected to the Internet under his control. These networks where the computers are connected with malicious bot programs are called botnets. Ancheta used a botnet to send spam and connection requests to online servers by launching spam distributed denial of service (DDoS) attacks. Even though these computers were involved in these sorts of criminal activities, the real owners of these computers would never know what took place. Ancheta started building his botnet in June 2004 and his collection included two military sites as well (FBI, 2006).

After his success in creating a large botnet, Ancheta hosted a website to sell or rent infected computers for other hackers and in this website, he listed guidelines on how to use bots and estimations about how many botnets someone would need to crash a corporate website, etc. The rate he charged for his bots were four cents apiece and a client needed to rent or purchase a minimum of ten thousand bots. According to the Federal Bureau of Investigation (FBI), when they finally caught up with him, Ancheta was successful in conducting business with ten clients. ‘SoBe’ was a teen from Florida who joined with Ancheta in August 2004 and helped him to grow the number in his botnet up to four-hundred-thousand computers. Using his botnet, he made nearly $60,000 by joining as an affiliate for online advertising. Ancheta got paid every time an owner of a computer in the botnet had to download adware and visited the advertisement. He earned all that money in just under six months (FBI, 2006).

The FBI got the scent of Ancheta after seeing the price list in his website. The FBI nick-named him the ‘Zombie King’ as the computers he hacked and controlled perfectly matched the concept of zombies. FBI agents got to him by posting in an online chat room asking for Ancheta’s help in launching an attack using his bots. In the chat room, he bragged about making a thousand dollars within just two weeks with his botnets and he made a deal with the undercover agents for two-thousand bots. He finalized the deal by saying that two-thousand bots were “enough to drop a site”. As a result of this undercover operation, the FBI seized his computer in December 2004 and disabled his server in May 2005. Ancheta was arrested in November 2005 and pleaded guilty to federal charges of hijacking computers for profit. He was the first person to plead guilty to this crime. After the trial, he was sentenced to fifty-seven months in prison followed by supervised release. He was also ordered to make restitution for damages caused to the two military sites which he had added to the computer collection in his nationwide botnet (FBI, 2006).

Kevin Poulsen

Among notorious hackers, the man named as ‘the Hannibal Lecter of Computer Crime’, Kevin Poulsen is one of the most talked about due to the steep turn he took in his career. Before the nickname given him by the FBI, he was known in the world of hackers as ‘Dark Dante’. He can be called one of the luckiest hackers of all time. In 1988, when he was just twenty-three years of age, Poulsen was successful in hacking into a federal computer network. After gaining illegal access, he started to poke around the file regarding the investigation of the president of the Philippines, Ferdinand Marcos. This was the hack that cost him his invisibility over the Internet.

After realizing that the FBI has caught scent of him, Poulsen fled for his freedom. Unlike most outlaws, Poulsen managed to stay untouched for seventeen months. Even during this period of laying-low, he was not the type of person who could keep quiet. He hacked into FBI servers and revealed wiretaps that had been set up for mobsters, foreign politicians, and the American Civil Liberties Union (Lammle, 2011). The hack he was most notorious for is the one he pulled on KIIS FM, a Los Angeles-based radio station, to win a brand-new Porsche 944 S2 and $20,000 in cash (Poulsen, 2017). Poulsen hacked into all the phone lines connected to this radio station and jammed them so that no one else could call the radio station until he became the 102nd called and won the grand price. To accomplish this feat, Poulsen engaged the help of some of his disciples such as Ronald Austin and Justin Peterson, and got them to work with him (Soylent Communications, 2014).

Poulsen's dance of mischief came to an end after a television show broadcast by NBC network called Unsolved Mysteries caught wind of him and featured an episode based on him and his hacks. This turned out to be the final blow to end the destruction caused by Dark Dante. While the episode was on air, telephone lines opened to get tips from civilians got blocked. It was not difficult for anyone to figure out the cause behind that block. Broadcasting this episode and educating the people in the US about this most-wanted cyber-criminal, led to Poulsen's arrest. Even having been one of the FBI's most wanted criminals, Poulsen could not be prosecuted for any major charges. Prior to his hearing, however, he was incarcerated in a federal facility for five years without bail until the FBI could build a case against him since he was too deeply involved in the national secrets by hacking into classified information, before being released to serve his court sentence (Littman, 1993).

Once having being considered as one of the most-wanted criminals, Poulsen can also be considered the most reformed hacker of all time. After his release, he took a completely different path and went on to become a journalist and a cyber-security consultant. He is also famous for helping to find seven-hundred-and-forty-four sex offenders who were phishing for underage victims using social media such as MySpace (Lammle, 2011).

Albert Gonzalez

There are two main reasons why people explore the darkness of hacking. One reason is the curiosity or the excitement which they get from breaking the law, and the other reason, which is the most addictive reason, is monetary gain. When it comes to cyber-crimes resulting in financial damages, the name Albert Gonzalez is ranked at the top with the largest cyber-crime of all time, even though he eventually had to pay his dues with twenty years in prison, a $25,000 fine, and restitution for the losses caused in the companies which he hacked. Before looking at the prosecution and punishment of Gonzalez, it is required to understand the actual crime he was accused of (Verini, 2010).

Gonzalez was a twelve year-old boy when he bought his first computer out of his own money. One day, while downloading some content, he accidentally downloaded a computer virus and had to call the computer technician to fix the issue. That planted the seed of curiosity about computer security in his mind. This interest that came out of the blue, led to his dive in the advanced science of computer and cyber-security. At age fourteen, Gonzalez was paid a visit by an FBI agent, because he had hacked into the National Aeronautics and Space Administration (NASA) Agency's database. According to Gonzalez's best friend, the person responsible for providing Gonzalez with the packet sniffing tool which he used in his crime was Stephan Watt (Verini, 2010).

Before being the mastermind of the largest cyber-crime of all time, Gonzalez started his career in a smaller scale scam, which was caught by the police in 2003. One night, a detective who was undercover investigating a string of car thefts, accidently noticed a random person who looked a little suspicious. The detective followed him to an automated teller machine (ATM) and pretended to withdraw money from a different ATM while observing the suspicious character. Gonzalez inserted an ATM card and withdrew a few hundred-dollar bills. Instead of stopping after using one card, he pulled out one card after the other. Since it was close to midnight, his plan was to withdraw money from the ATM until the cards reached their limits for that particular day and to use them again once their limits reset after 12:00am. The detective took Gonzalez into custody, and it was not until he was interrogated by the police that they came to know that he was Albert Gonzalez, who was in an administrative position in a website called 'shadowcrew.com', which was one of the black-market sites for illegal products and stolen credit card information. This information made the story of Gonzalez take a new and unexpected turn when the Secret Service came into play (Verini, 2010).

The Secret Service of United Stated was investigating about credit card and identity theft and even had a special task force dedicated to the task. When they got to know that a person associated with 'Shadow Crew' was in custody, they saw a golden opportunity to bring 'Shadow Crew' down. When the proposal to work as a confidential informant for the Secret Service in exchange for his freedom and a salary of $75,000 was offered, Gonzalez accepted the deal without any hesitation. His job was to lure the users of that website to a virtual private network (VPN), claiming that it was a safe channel. This VPN, of course, was wire-tapped by the Secret Service. With the help of Gonzalez, the Secret Service was able to bring down twenty-eight members of 'Shadow Crew' who were involved in dealing stolen credit card information. This mission, which ended in 2008, was code named 'Mission Farewell'.

After that, Gonzalez moved to Miami, but unbeknownst to the Secret Service, while serving his country, he had also laid out a master plan. While conducting a war-driven expedition along Miami highways and other locations to find poorly protected wireless networks, he also found some well-known retailers. Among them, he spotted a company called TJX. Together with his crew of misfits, Gonzalez connected to the local network of TJX. It was only a matter of time until they made their way up to the corporate network in Massachusetts. Gonzalez now needed a way to get the data from the transactions happening in the network. For that, he turned to his best mate, Stephan Watt, who equipped him with the packet sniffing tool. With that, Gonzalez and his crew could get their hands on all the transaction data from the network including credit card information. He used the SQL Injection technique to extract information from company databases. After retrieving that data, he stored it in two servers he had rented in Ukraine and in Latvia. When he finally got caught, there was information about 16.3 million credit and debit cards stored in the Latvian server, and about twenty-seven-point-five million cards in the server in Ukraine. In order to sell this information, he joined forces with a Ukrainian black-market credit card dealer called Maksym ‘Maksik’ Yastremskiy. When he received the information from Gonzalez, he would distribute them to other small scale black-market credit and debit card dealers for e-Gold, web money, and even for normal bank transactions in to Eastern European bank accounts. The whistle was blown on their perfect fairytale when Yastremskiy was arrested in Turkey in 2007 from the leads the authorities got about the hack on Dave and Buster’s company. In his computers, they found large amounts of data which was linked to the e-mail address ‘soupnazi@efnet.ru’. ‘Soup Nazi’, which was an early nickname used by Gonzalez, gave away the hacker who Yastremskiy was in cohorts with: Albert Gonzalez. This information dropped the final nail on the coffin of Gonzalez’s arrest and prosecution, and he was sentenced to the lengthiest punishment ever given to a cyber-criminal, which is 20 years imprisonment, by also taking into consideration his plotting and planning other cyber-crimes even while working as a confidential informant for the Secret Service (Verini, 2010).

Lessons Learned

There are a few lessons that can be learned from studying these hackers and their hacks. First, it can be seen that digitized information can be easily shared and communicated with others, but limiting its access to a select few is a difficult task in today’s heavily interconnected world. Thus, unless one is absolutely certain that a certain piece of information needs to be shared they should refrain from sharing it on the Internet or on any network. One should diligently follow best practices in creating passwords, etc., follow proper protocol and procedures when sharing information and refrain from trying to cut corners to make their task at hand easier. Security always comes at a cost, and if a required security standard has been established, then the users of that system should comply with that standard and all it entails. One should refrain from clicking on unnecessary or unfamiliar buttons and links, etc. and if it is required, one should always validate certificates or other credentials before performing such actions.

Further, looking at the reasons why these hackers got caught can also provide guidance on behavior in cyberspace. For instance, Ancheta got caught not due to any technical issue, lack of skill, or a misstep in his hacking methods. Instead, it was his psychological reaction to brag about his achievements, along with publicly marketing his malicious work in order to earn a few extra bucks that led to his destruction. When looking at how Gonzalez got captured, it can once again be seen that his need to sign his work by using his previous nickname in the e-mail address which he used for dealings with other criminals, led to his downfall. In fact, this need for taking credit for their work, making their mark, and the behavior resulting from such psychological acclaim is something common not only to most criminal masterminds, but also to people in general. Thus, it can be seen that watching one’s step is more important in cyberspace than advertising one’s achievements, whereabouts, and habitual patterns.

Conclusion

In conclusion it can be seen that any user of an information and communication system needs information security education and awareness so that they may know the security risks they are taking, and device a security plan to suit the risk, as well as to be able to safeguard their information assets and protect them from perceived threats. A complete and thorough education in information security covering all security domains will only be required for students of computer or information science, and IT professionals and software engineers who design and develop software programs, applications, and information and communication systems. Yet, any person who uses such a system should have a basic understanding and awareness of information security before publicly publishing their information in any such system or network. Thus, it can be concluded that just as important as it is to give a basic IT skills education to students of many different subject fields and people of many different professions, it is also important – perhaps to even a greater extent – to give them an information security education to provide the basic understanding and awareness of information security. If unable to prevent information security breaches and attacks, this will at least help all users of information and communication systems to at least minimize the damage of such a breach or an attack, and thereby protect the majority of their information assets.

References

Bishop, M. *Computer Security – Art and Science*. Boston, MA: Addison-Wesley.

FBI. (2006). *The case of the Zombie King*. Retrieved from https://archives.fbi.gov/archives/news/stories/2006/may/botnet050806

Fernando, S. (2014). *Internal Control of Secure Information and Communication Practices through Detection of User Behavioral Patterns* (pp. 2-3). Niigata, Japan: Nagaoka University of Technology.

Gonzalez, J.J. and Sawicka, A. (2002). A framework for human factors in information security. *Proceedings of 2002 World Scientific and Enginieering Academic Society International Conference on Information Security*. Rio de Janeiro, Brazil.

Harris, S. and Maymi, F. (2016). *CISSP All-in-One Exam Guide* (7th Ed.), New York, NY: McGraw-Hill Education.

ISO/IEC 270001. (2005). *Information technology – Security techniques – Information security management systems – Requirements*. Geneva, Switzerland: ISO.

Lacey, D. (2009). *Managing the Human Factor in Information Security: How to win over staff and influence business*. West Sussex, England: Wiley.

Lammle, R. (2011). Four famous hackers who got caught. *Mental Floss*. Retrieved from http://mentalfloss.com/article/26767/4-famous-hackers-who-got-caught

Littman, J. (1993). The last hacker. *Los Angeles Times*. Retrieved from http://articles.latimes.com/1993-09-12/magazine/tm-34163_1_kevin-poulsen/5

Pegg, D. (2016). Twenty five most notorious hackers to ever get caught. *List25*. Retrieved from http://list25.com/25-most-notorious-hackers-to-ever-get-caught/

Poulsen, K. (2017). About the Author. *Kingpin: How one hacker took over the billion-dollar cybercrime underground*. Retrieved from https://www.kingpin.cc/about/

Schneier, B. (2008). *The psychology of security*. Retrieved from http://www.schneier.com/essay-155.html

Soylent Communications. (2014). *Kevin Poulsen*. Retrieved from http://www.nndb.com/people/453/000022387/

Verini, J. (2010). The great cyberheist. *The New York Times Magazine*. Retrieved from http://www.nytimes.com/2010/11/14/magazine/14Hacker-t.html

Williams, B.R. (2011). Do it differently. *Journal of Information Systems Security Association* 9(5), (p. 6).