Cyber Crimes: Nobody Is SAFE

Taylor Lincoln

February 25, 2013

IT 103-007

"By placing this statement on my webpage, I certify that I have read and understand the GMU Honor Code on http://oai.gmu.edu/honor-code/ . I am fully aware of the following sections of the Honor Code: Extent of the Honor Code, Responsibility of the Student and Penalty. In addition, I have received permission from the copyright holder for any copyrighted material that is displayed on my site. This includes quoting extensive amounts of text, any material copied directly from a web page and graphics/pictures that are copyrighted. This project or subject material has not been used in another class by me or any other student. Finally, I certify that this site is not for commercial purposes, which is a violation of the George Mason Responsible Use of Computing (RUC) Policy posted on http://universitypolicy.gmu.edu/1301gen.html web site."

Introduction

Picture this! You're on your favorite shoe store's website and you find the perfect pair. They aren't too pricy, and they come in your size too. What do you do? You select your size, the color, and add the pair of shoes to your shopping bag. Then you run to get your handy dandy debit card. As you type your information into those blank boxes, you never think twice. Your fingers and 20/20 vision work as one to complete your order. Meanwhile, John Doe, a well trained hacker and identity thief, has copied every number and word submitted into those now filled boxes. He has your address, name, and your card information, but at least you got those shoes! Though this is a just one of many ways someone can steal someone's information, it occurs every day and can happen to anyone.

Background

Cyber crimes, according to B4USurf, an organization dedicated to promoting a safe and legal digital world, are any illegal actions directed by revenue of security and computer systems (B4USurf, 2012). In a simpler explanation, any criminal act while sitting behind a computer screen and a keyboard is considered a cyber crime. There are five categories of computer crime, piracy, financial, hacking, cyber-terrorism, online pornography, and in-school (B4USurf, 2012).

Online piracy, or music theft, is the "infringement of copyright on a commercial scale" **(**IFPI, 2007**).** Piracy includes counterfeits, bootlegs, and Internet piracy (creative Internet piracy content). The financial side of cyber crimes proves that hackers can do just about anything they want. ID theft and fraud are the most common crime of the cyber world. Because the use of the Internet piracy is increasing by the second, it's becoming easier to steal someone's credit card information and even harder to catch the thief (B4USurf, 2012).

As for cyber-terrorism, FBI defines it as “the premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against noncombatant targets by sub national groups or clandestine agents” (Krasavin, 2001). In schools, cyber-crime exists. In Downingtown, PA, a group of hackers stole almost $700k from the Downingtown School Districts bank account. Though returned, the thieves are still at large (Craig, 2013). Students hack into virtual grade books and can change their earned “F” to an “A”. Becoming a victim of a cyber crime puts one in a weird position. A computer can be used as the target of a cyber-offense, for example, a virus through spam (Robinson, 2001). Computers can be used as the primary tools for the cyber-crime, for example, child pornography, fraud, and the sale of illegal substances and goods online (Robinson,2001).

The Internet piracy, the ATM machine, and someone’s tuition could all be at risk without the slightest hint or suspicion because cyber crimes occur behind a computer, and today everyone is behind a computer.

Legal Consequences of Hacking

“[Most hackers,] by the time they reach a certain age, [are either in jail or very rich,]” states a detective of Systems Solutions Group. Jonathan James hacked into NASA causing them to shut down their network for 3wks, which cost them $41k. James was later suspected of a wave of network attacks in 2008. Not wanting to be convicted for crimes he did not obligate, he committed suicide the same year. (Goyal, 2012)

Albert Gonzales collected almost 200 million credit card and ATM machine numbers. Along with health insurance cards and fake passports, Gonzalez’s crimes totaled in over $4 million stolen. He was later sentenced to 20 years in prison, for hacking into TJX Companies and

Heartland Payment. (Suddath, 2009) Crimes committed behind computers are not always given a huge jail sentence, if caught.

Kevin Minick, the best hacker in world, began hacking computers when he was twelve years old. He moved onto the LA Bus System causing him to never pay for another bus fee. He is known for hacking the FBI, DEC, IBM, Motorola, Nokia, Sun Microsystems and Siemen. When freed from prison after 5 year sentence, he created his own security company, Mitnick Security (Goyal, 2012)

In 2011, McAfee, a security software company, informed 72 victims of the world's largest cyber-attack. The victims included the United Nations, the United States, and the International Olympic Committee (Gilbert, 2011).

With every crime, there comes a law. In 2004, the Computer Software Privacy and Control Act was created. This law made it "it unlawful for any person to transmit to a protected computer owned and operated by another person" (HG.org, 2013). The law also prevents any person of collecting and transferring personal information about an owner or operator. The Fraudulent Online Identity Sanction Act, introduced in 2004, is a copyright law if a person knowingly provided materially false contact information in making or maintaining the registration of a domain name used for violation (HG.org, 2013).

Prevention

Cyber Crimes Watch states that 25% of cyber crime remains unsolved. (CCW, 2013) As hi-tech as the world is today, removing all electronics from one's home is like removing them off the face the earth. Americans especially, are so pruned and glued to the use of technology that safety becomes the last step in purchasing merchandise online and when inserting their card into the ATM machine. So how does one protect their information? How does one protect their family?

According to B4USurf, "One can start by making their passwords more difficult". Hackers are people too, crossing all ages, they know about the" first name-birthday". Trying more upper case with lower case passwords could put at a lower risk for

Firewalls protect computers from intruders. They are "walls" that block the outsiders from getting into your computer.

When the Internet piracy is not in use, disconnect it. When the Internet piracy I connected, your computer is at risk, especially when you're are not monitoring it. Your shared files are vulnerable and accessible to hackers. "Do NOT open spam mail or emails that have an unfamiliar sender" (B4USurf, 2010). In May of 2005, "ILOVEYOU", or the "Love Letter", attacked over millions of personal computers through an email system. Created in the Philippines', "ILOVEYOU" traveled to Hong Kong, then to Europe, and finally the US (Kane, 2009). "When using anti-virus software, keep it up-to-date" **(**B4USurf, 2010)**.** Recent software makes an effective protector. The many ways that one can protect their computer can go a long way. By protect the computer you protect your children from pedophiles, your bank information, your house, and your life.

Conclusion

Though not all people are victims to cyber crimes, they are still at risk. Crimes by computer vary, and they don't always occur behind the computer, but they executed by computer. The hacker's identity is ranged between 12 years young to 67years old. The hacker could live three continents away from its victim, and they wouldn't even know they were being hacked. Crimes done behind the computer are the 21st century's problem. With the technology increasing, criminals don’t have to rob banks, nor do they have to be outside in order to commit any crime. They have everything they need on their lap. Their weapons aren’t guns anymore; they attack with mouse cursors and passwords.

References

B4USurf.org. (2012). *Tips on Protecting Your Computer*. Retrieved from http://www.b4usurf.org/index.php?page=tips-on-protecting-your-computer

❖ This reference is reliable because it is an organization that specializes in cyber-crimes and how to prevent cyber crimes.

Craig , F. C. (2013, April 13). Downingtown area school district recovers $665,000 from apparent cyber attack. *The Tribune-Review* , Retrieved from http://triblive.com/news/allegheny/3835809-74/district-downingtown-bank?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed: alltribstories (TribLIVE News)

❖ This reference reports the incident in which I used to support my claim of cyber crimes in schools

Gilbert, D. (2011, August 01). *World's largest cyber crime uncovered*. Retrieved from http://www.trustedreviews.com/news/world-s-largest-cyber-crime-uncovered

❖ This review reports the world's largest cyber crime, bringing light to government issued systems being hacked.

Goyal, K. G. (n.d.). Top hackers of the world. (2012). *World Top 10*, Retrieved from http://worldtop10.net/top-10-hackers-of-the-world/

❖ This is a reliable source because it is a ".net" and it provides information about the top ten hackers in the world.

HG.org. (2012). *Computer crime law.* Retrieved from http://www.hg.org/computer-crime.html,

(International Federation of the Phonographic Industry. (2007, October). *Why is piracy illegal?* Retrieved from http://www.ifpi.org/content/section_views/why_is_piracy_illegal.html

❖ This is a reliable source because it is a ".org" and it provides information about piracy.

Kane, M. (2009, May 4). ‘*I Love You E-mail Worm Invades Pcs*. Retrieved from http://web.archive.org/web/20081227123742/http:/news.zdnet.com/2100-9595_22-107318.html?legacy=zdnn

- This is a reliable source because it provides infromation about a popular global virus that affected multiple countries.

Krasavin, S. “What Is Cyber-terrorism*?* (2001, March 20) Web. 14 Apr. 2013. Retrieved from http://www.crime-research.org/library/Cyber-terrorism.htm

- This is a reliable source because it clearly defines cyber terrorism.

Liu, S., & Cheng, B. (2009). Cyberattacks: Why, what, who, and how. IT Professional Magazine, 11(3), 14-21. doi: http://dx.doi.org/10.1109/MITP.2009.46

- This is a reliable source because it was written by representatives of the US National Library of Medicine and the Computer Sciences Corporation.

Robinson, J. "Internet as the scene of crime". (2001). Forensic Accounting Review and Computer Security Digest, 17(8), 5-8. Retrieved from http://search.proquest.com/docview/197255673?accountid=14541

- This is a reliable source because it states what role computers play in cyber-crimes.

Suddath, C. (2009, August 19). Master Hacker Albert Gonzalez. Retrieved from http://www.time.com/time/business/article/0,8599,1917345,00.html

- This is a reliable source because it discusses the famous hacker Albert Gonzalez.