Caroline Rae Strickland

Doctor Melissa Walburn

Law of Cyberspace

30 November 2015

The Good, the Bad, and the Ugly world of Hacking

When you hear the word hacker what comes to mind? Truth is there is no right or wrong answer to what a hacker can or could possibly be. To some people a hacker might be a term we use for someone who is dangerous, someone who breaches government systems and throws the world to all a chaos. To other hackers might just be a way to get a head of life and save some time or money doing do it yourself (DIY) projects or study tips as study hacks and short cuts. In other words being a so-called a hacker can moreover be a compliment or an insult depending on use.

In this particular research paper I would like to go into details of what it means to be a hacker in the cyber world. I will first go into details of what type of hackers are found in cyber space, then I will break the world of hacker into three categories. The good, as in what are the benefits to being a hacker or having a hacker on your side. The next section will be the bad and the disadvantages you face being a hacker and having the bad fortune of being hacked. Lastly I will describe the ugly statistics of cybercrimes associated with being a hacker or being hacked and steps you can take to protect yourself from being a victim. In conclusion I will restate all main topics and explain my personal opinion on the life of hacking. I will state if I am guilty of hacking or if I'm completely against it. Let's get started.

So what are the benefits of being a hacker or having a hacker network with you on the internet? Some unmistakable benefits to being a hacker is for personal use personal and gain. Being a hacker can help you connect to the community of inventors and likeminded people. If being a hacker means you enjoy tinkering with the cyber world imagine the benefits you could have on technology.

In a case study on Thecon.Ro called Growth Hacking Practices in a startup, the benefiters of being a hacker were traditional marketing. This case study examined the development of using hacker skills for marketing to avoid spending any funds the end results of this case study was " hacking techniques applies by this marketing company tends to forward more online content than its competitors."

Another benefits of being a hacker in 2015, you can print your ideas or concepts in 3D! If you someone with great ideas and are a savvy hacker try visiting websites such as Metrix Create:Space, Logo Electromechanical, and Hackerbot Labs. These are a few of many places a hacker can go to expand their mind and experience there cyber world on a whole new level. Lastly being a hacker doesn't just mean developing new technology or crashing the internet, being a hacker may mean creating short cuts to make life easier. Such as simple cyber short cuts such as saving work on the computer or re programing your computer for more effecting run time.

First let's redefine what a good hacker is. According to bright hug a good hacker is also known as an Ethical hacker. "Ethical hackers are network and computer experts who track a security system to help the computer systems owners." In simple relations an ethical hacker can help a lot in business and technology security analysis. According to bright hub the benefits to having a hacker work for you are "Compliance documentation with respect to legal regulations,

standards and parameters, supporting arguments for information technology activities and projects in the future, Know-how transfer, Building awareness at all levels, Prevention to provide for indirect and direct cost savings as time goes on, Detail the testing process and Create their plan and then share it with stakeholders.

Now for the scary part. What happens to you when you're a hacker and things go poorly and you get caught doing something that most people in society would consider unethical. According to wonder how to, the legal consequences of hacking are "prosecuted by the federal law enforcement. Surprisingly, the secret service is the lead agency." Generally FBI Cyber Crime Task Forces are located locality to better pinpoint hackers who are doing illegal activities. Most hackers are caught by bragging about their achievements.

"Although federal law makes it a felony to do more than $5,000 damage, the general rule is the FBI won't even get involved in cases that involve less than $100,000 in damages. Note that the key word here is "damages". This has nothing to do with how much the hacker gets away with, but rather how much damage is done to the individual or business."

FBI Cyber Crime Task agencies in the U.S. prosecute hacking cases using two principal federal statutes; "U.S. Title 18 Section 1029 and 1030." According to a OLR research report back in June 28th in 2012 they expand on degrees of computer crimes ranging from one degree to five degrees, one degree being the worst case scenario and fifth degree being the best case scenario and the least amount of penalty. The amount of damage or harm required and their penalties.

For 1st degree you must "Damage to or the value of the property or computer services is over $10,000" your penalty for a 1st degree computer crime a prosecuted with a B felony be up to

twenty years in prison, a fine up to $15,000 or both. For 2nd degree you must "Damage to or the value of the property or computer services is over $5,000" the penalty for a 2nd degree computer crime is a prosecuted with a C felony up to 10 years in prison, a fine up to $10,000 or both. For a 3 degree computer crime there are two possible reasons to amount to damage. You must "Damage to or the value of the property or computer services is over $1,000 and Reckless conduct that creates a risk of serious physical injury to another person". A penalty for a 3rd degree is a prosecuted with a D felony, up to five years in prison and fine up to $5000 or both.

For a 4th degree computer crime you must "Damage to or the value of the property or computer services is over $500". The penalty for a 4th degree is a prosecuted with an A misdemeanor and up to one year in prison, a fine of up to $2000 or both. Last but not least for a 5th degree computer crime you must "Damage to or the value of the property or computer services, if any, is $500 or less". You are then penalized with a B misdemeanor, six months in prison, fine up to $1000 or both.

So as you can see there are server consequences to hacking unethically and you should be aware of the dangers to being a hacking. You should also be aware of what a hacker can do to you so you can recognize the signs of being a victim so you can get help. I will be referring to Connecticut law and regulations for examples of what hackers are capable of doing.

"1. Temporarily or permanently remove, halt, or disable computer data, programs, or software; 2. Cause a computer to malfunction; 3. Alter or erase computer data, programs, or software; 4. Create or alter a financial instrument or an electronic funds transfer; 5. Cause physical injury to another's property; 6. make or cause to be made an unauthorized copy of computer data, programs, or software residing in, communicated by, or produced by a computer or computer network; or &) falsify or forge email information or other routing information in

any manner in connection with the transmission of unsolicited bulk email through or into the computer network of an electronic mail service provider or its subscribers." Some other crimes hackers are proficient of undertaking is terrorist attacks on civilian population, structures of government or public safety. Hackers are also known for taking personal identity much like when someone steals credit card information or hacks into an ATM for personal information.

If you believe that someone has partaken in hacking unethically there steps you can do to prevent or future crimes. These steps would include you to file a civil action for (1) a temporary or permanent order preventing the activity; (2) restitution; or (3) appointment of a receiver.

Wrapping up I would like to shine a light on hacking court cases and give some examples of real cases where hacking situations have occurred. And although I have mentioned some things you can do to protect and prevent yourself from being hacked I would like to go deeper on how you can truly secure yourself for the future. According to Wired these are the most controversial hacking cases of the past decade. In 2011 Aaron Swartz is a CFAA prosecution internet activist. In 2011 Swartz "allegedly connecting to an MIT network downloaded 2.7 million academic papers that were freely available to any campus visitor through the JSTOR service."

So why is this a big deal if anyone can get these papers for free? According to the justice department Swartz violated terms of serves by downloading documents with intent of distributing them off campus. Swartz was prosecuted with four felony counts and then later increased to 13 counts due to the fact he had downloaded these files on different days created separate counts. Potentially Swartz was faced with 6 months years in prison and fined up to $1 million. Unfortunately three months before Swartz trial he committed suicide.

Andrew Auernheimer was a self-declared internet troll to which the government had out for along with his friend Daniel Spitler. In 2011 Auernheimer and Spitler "discovered a hole in AT&T's website that allowed them to obtain the email addresses of AT&T iPad users. When iPad users accessed AT&T's website, the site recognized their device ID and displayed their email address." Spitler and Auernheimer wrote a plan to yield about 120,000 email addresses by manipulating the comportment of thousands of ipads.

The government concluded that accessing AT&T unprotected emails was considered criminal hacking therefore Auernheimer was prosecuted and sentenced to three and a half years in prison. However his attorney won on his appeal and challenged the government that accessing data on a public website is not qualified as hacking. The issue has yet been resolved.

Finally we have Fidel Salinas. A 28 year old who identify as " Anonymous, faced what may be the most schizophrenic hacking prosecution of all time: In 2012, he was charged with 44 felony counts of computer fraud and abuse, each one carrying a potential 10-year prison sentence." If you do the math, that is 440 years of prison. The goal for this overzealous punishment was to make an examples of hackers. Salina had basically been charged each time he simply entered text in an unnamed victim website. By the end of 2014 most of the charges had been drooped and reduced to a single misdemeanor with six months of prison time and a $10,600.

As you can conclude hacking can be some serious business and also very had to control. I feel that the government took very strong approaches to eliminating hacking by making examples of people and giving them sever punishment to scare other from hacking. I do feel with the case of Aaron Swartz's CFAA prosecution the government should have learned that "hackers" are people to and making an example of them so to speak and lead to the demise of a

human begin who in my mind didn't do any criminal injustice. Perhaps eliminated the middle man of distributing information but anybody who visited MIT campus had access to the very same information he extracted. Also JSTOR didn't pursue a complaint. I truly believe the government made Swartz's a victim and abused their power in attempt to stop hacking.

So how can you better protect yourself? According to learning English these are nine ways to protect yourself from hackers online. First and foremost make you passwords more unique so they are harder to hack. Unique passwords would include "upper and lower case letters, numbers and special characters. They should be at least eight characters in length. They should also not spell out words easy for hackers to find, like your pet's name or the name of a family member." You should also change your password often and don't use the same passwords for all your sites.

Something else that is often over looked is your clearing your history, you might also look at your google setting and disabling saved password. Do not use free wi-fi! Why you ask, hacker now have found a way to stream through free wi-fi because user don't need a password to connect to wireless networks. Subsequently hackers bug your computers, its important pay attention to email attachment, "If someone sends you a file or a website you did not ask for, it is best to not click on it.

Also try your best not to use public computers, they are easily filled with viruses and thumb drives that can spread viruses across computers and networks. You should train yourself to use HTTPS also known as "hyper-text transfer protocol secure." HTTPS adds encryptions creating an extra layer security. HTTPS is another way of telling whether or not attachments to emails are authentic or not.

So in conclusion of the good, the bad and the ugly. I would say being a hacker is only determined to be for good or bad based on their usage and outcome.is it ethical or is it cheating or stealing in some way? I believe that hacking can be very beneficial and if used wisely completely safe. I feel that you can use hacking to invent new technology and help promote businesses.

As far as a bad hacking I don't believe that punishing a person an obsessive amount is how the government should regulate. I believe using 1st degree to 5th degree of computer crimes is a reasonable grid on pin pointing fare punishment. It's always tricky regulating anything in cyber space. You could put more eyes on what people do but then people feel exposed and that the government is in barking on their privacy.

So I'm not sure on the solutions for regulating hackers in cyberspace but as mentioned before there are simple way to prevent yourself from being hacked and I feel that, that's a great place to start. It's easy to see how hacking can be ugly. It can be ugly in the way someone is using the inner webs to hurt people and cause sever damage to the public , much like what you would see in a movie and a hacker turns the intersection light from green to red to cause obstruction or when someone hacks into a bank to extract electronic bills. I also feel that the government can become ugly when regulating.

References

Advantages and Potential Dangers of Ethical Hacking. (n.d.). Retrieved December 1, 2015, from http://www.brighthub.com/internet/security-privacy/articles/77412.aspx

Growth Hacking Practices In A Start-Up: A Case Study On Thecon.Ro. (n.d.). Retrieved December 1, 2015, from https://ideas.repec.org/a/ddj/fserec/y2014p212-216.html

The Legal Consequences of Hacking. (n.d.). Retrieved December 1, 2015, from http://null-byte.wonderhowto.com/forum/legal-consequences-hacking-0153914/

The Legal Consequences of Hacking. (n.d.). Retrieved December 1, 2015, from http://null-byte.wonderhowto.com/forum/legal-consequences-hacking-0153914/

PENALTIES FOR COMPUTER HACKING. (n.d.). Retrieved December 1, 2015, from https://www.cga.ct.gov/2012/rpt/2012-R-0254.htm

The Most Controversial Hacking Cases of the Past Decade. (n.d.). Retrieved December 1, 2015, from http://www.wired.com/2015/10/cfaa-computer-fraud-abuse-act-most-controversial-computer-hacking-cases/

Nine Ways to Protect Yourself from Hackers Online. (n.d.). Retrieved December 1, 2015, from http://learningenglish.voanews.com/content/nine-ways-to-protect-yourself-from-hackers-online/2655600.html