Reviewing the computer hacking industry

Science, Computer Science

As the world becomes more and more reliant on computers the computer hacking industry is greatly rising. With people such as Kevin Mitnick, who is known as a “ computer terrorist” (Kjochaiche 1), computerized information isn’t safe any more. Kevin is known as “ the most high-profiled computer criminal and responsible for more havoc in the computer world today.”(1) He considered this a fun and easy task. He got caught and thrown into prison, but once he got out nothing changed. Kevin stated that as long as the technology is there it just calls to people to break into it. Computer hackers usually start off young, thinking that it is nothing but a little harmless fun. But as they get older, they realize it has turned into an addiction. The definition of a hacker according to the Hacker’s Dictionary, “ a person who enjoys exploring the details of programmable systems and how to stretch their capabilities.”(Hackers 1) “ The Internet is just another playing field.” (Kjochaiche 3) “ Hackers regard hacking as a game in which their mind is up against that of the system designers.” (Hackers 3) The Internet allows the hackers to take files, programs, passwords, and other information from users that are using it. They use this as a tool to make it easier to beat “ the system”. There are three major types of hackers, one with good intentions but gets slapped in the face due to the bad reputation of others, there are the hackers with bad intentions, and there are the hackers that fit in between. The bad hacker category is the largest by far. “ A bad hacker’s motives are to punish someone or retaliate against the owner of a computer system.”

Computer terrorists fall under this category. Some bad hackers may also hack just to challenge the programmer. The hacker feels that if they can

break into it then they are much more superior than the person who actually wrote the software. They can feel so superior that they might enter a virus to eliminate a program that was not worthy of their abilities. One of the other many goals of a hacker is to steal passwords. Hackers can steal your password about four different ways. Intercepting your password through email is " not that difficult."(How are they getting my password? 1) This is by far the easiest method because all they have to do is take the email as it is being sent to you. Hackers can also use a program called a password cracker to actually learn you password. There are two types of theses but both have their own problems.

The first " checks every password possible from the entry site." (1) The second uses a program that goes in and reads the passwords off. The problem with both is that you have to " get the cracker into the site, undetected"(1) You also must cover you trail. Some prefer the manual method first. " There are actually lists of 100(or more) most-used passwords."(2) Hackers have reported that, " a simple password that appears in the English dictionary will take about an hour or less for a hacker to crack."(4) " This is not considered a long time to a hacker."(Brian 2) Third, they use what is called web spoofing. This is the most dangerous because they see what every you are doing. They can get you passwords plus any other information you might have. This web spoofing is caused by a middle man who can redirect information from your page, to his page, to the page you were sending the information to.

“ The middle man sees all.”(How are they getting my password? 3) This is above all the easiest way to get any information that they might want or need. The last method is through Java. Through a program they can hack into a computers hard drive through your Java program. That is why if you can avoid keeping your passwords on your hard drive do it. Some people keep their passwords on three by five cards and store them which is allot safer. The best method to securing yourself is always backing up files. That way if a virus or hacker crashes you computer you will safe. Another very safe method is to change your password often and don’t use the same password for everything. “ If they already know another one of your passwords, they ‘ ll try them first.”(How are they getting my password? 2) Consider rotating your passwords, just make sure they are not available on you hard drive.

In the long run it will be safer to go throughout the trouble than find out that someone is using your passwords to get into things. This can be dangerous in that Hackers supply their work with peoples money by buying stuff with other peoples credit cards. They can do this by using the same technique as getting a password. They use web spoofing to look at the peoples credit card numbers while they type them in. Rule #1, on the Internet nothing is secure, even if it says it is…(4) This is considered the golden rule of the safety on the Internet. Many people swear that the Internet is safe but there is always that little chance that someone could be watching. Today many major Internet companies are allowing users to order then about 5 minutes later the company calls you back and you transfer your credit card number over the phone, which is safer than over the Internet. There is a bigger threat of

getting your number taken over secured Internet sites than over the telephone.(Hackers 1) The novice computer hacker usually doesnt try anything as challenging as credit card fraud of password stealing. They usually are just pranksters looking for a good time. They are the ones who often release computer viruses. Viruses are the leading threat amongst the Internet.(Espy, 6) These viruses are dangerous because they can erase, or change files, or can even disable the computers that access the site. These viruses are starting to become more of a nuisance and cause corruption.

They recent release of the love bug virus is a good example of this. It is suspected that a young adult had released this just to see its effects. This virus steals the passwords and deletes certain information of your machine. This type of virus also was created to spread from one person to all of the people in their computer address book throughout their email. They computer specialists working for the government have to learn how to solve this problem. Good hackers do exist also, they are the ones who work for the government. They are the ones who use their knowledge to try to stop to bad hackers from striking again. Their knowledge is used to try and outsmart the enemy. (Kjochaiche, 5) Their job is to try and predict what kind of viruses will be made as well as the existing viruses. They try to get in the mind of their evil adversaries.(5) They learn to explore what is going on in the hackers brain. Good hackers try to eliminated viruses and find was to stop people from uploading them. Their goals are to write software to prevent such occurrences. They are hired by companies to find safety measures that will help the company. Web servers are introducing new software that was used to be hacker-proof.(Orman, 2) These good hackers are essential for the

survival of technology and the Internet. (Dellert, 4) Hackers will be around no matter what happens. There will always be loop holes that the hacker can break into. There will always be the man who thinks he can rein over technology.(5) It is a constant war between good and evil.

The government and other companies will spend millions and millions each year. This what people pay for in their taxes. Every one suffers from this problem. There are underground hacker groups that hack for fun. Because they are underground police and government agents cannot track them down. There is a certain respect between each of the hackers. You dont rat someone out even if they are your enemy.(3) All hackers are linked together even though they never meet each other personally. Your work sort of represents yourself.

On an occasion you might even have a team of hackers working together. This is very uncommon but can happen especially when the job is to big for one man and it needs to completed right away. But with the group of hackers comes different views and often the hacker relationship(1) doesnt work out. More often than not the hackers are soloists.(Kjochaiche, 6) It is proven that when hackers work together they get caught more often. Hackers will always do their work just like doctors will always treat patience. With the growth of technology comes new threats, and new problems. This will continue to be on the rise due to advances in the world.(Hackers, 3) Millions and millions of dollars will be put to end this but this will not work because new ways of hacking will always be made.