Michael Nicholson

2/11/19

CSCI 235 ~ Dr. Hayes

Can Hacking be Ethical?

The first instance of hacking took place in the late 1870s when switchboard operators hired by the Bell Telephone Company purposely misdirected, disconnected, and pranked telephone calls by innocent customers (Clarke 2). Nowadays, hacking is a necessary security concern for anyone who owns technology and especially for companies who stores their customers' sensitive data. The term "computer hacker" carries a negative connotation with it, but a computer hacker, in the eyes of Brian Harvey, is simply someone who lives and breathes computers (Harvey). The misconception with the term hacker is that many people see hackers as the bad guys when most of the times hackers are the good guys protecting us from widespread data leaks every day. The term for malicious hackers is "crackers" (Clarke 2). These are the people that are breaching the databases of companies using direct denial of service attacks on companies. With this negative association that hacking has, the question arises. Is hacking ethical?

There are two types of hackers. White hat hackers and black hat hackers. This seems to create a clear divide between what is good and what isn't, but the argument on whether hacking is ethical is not as clear cut as it seems. In most cases, if the hacker has honest intentions and is just trying to help a person, company, or a government out will not face trouble. If a hacker does find a vulnerability in a system, they should privately disclose the vulnerability to the developers or security team of the company. This gives them time to fix the problem and doesn't give them any reason to pursue any legal actions against you. If the company does not address the issue

even though you tried contacting them in multiple ways, then tell the media about the problem. This may cause backlash, but if it is to keep customers and the company safe, then it is ethical. In the situations of Yosi Dahan and United Airlines both, the company and hacker acted in a civil manner and the problem was resolved, but in the case of Allan Dumanhug, the company didn't reply with the appropriate response. If a hacker tells a company about a system vulnerability, the company should address the situation by patching it and thanking the hacker. They should be thankful that it wasn't a black hat hacker that found the vulnerability first. On the other hand, the company at question has no idea whether the hacker is genuine or not, so they have every right to be suspicious. I think that instead of accusing a hacker of being malicious they should question the hacker and try their best to work with them.

System-cracking is essentially looking for a backdoor into a program to exploit it and cause it to do tasks it isn't supposed to do normally. An example of this would be cracking Sony Vegas to make the free trial last forever. If a person is doing this and contacting the developers about the problem, then it is ethical. Doing it for educational purposes, in my opinion, is fine, but you shouldn't share the program, steal data, or breach any confidential data. Just like hacking there tends to be a clear line for whether the activity is ethical or not, but there is always a grey area when it comes to doing it for fun or educational purposes.

Hacking and cracking are necessary to keeping security breaches at a minimum. If done ethically, they are great ways to keep the world more cyber safe. In the future, if you find a security vulnerability or a way to crack in system remind yourself of the Bible verse Luke 6:31, "Do to others as you would have them do to you." If you would be okay with what you are doing to someone else's program or software to be done to you, then your actions will more than likely be ethical.

Sources:

Title: A Brief History of Hacking... | Authors: Zuley Clarke, James Clawson, Maria Cordell

http://steel.lcc.gatech.edu/~mcordell/lcc6316/Hacker%20Group%20Project%20FINAL.pdf

Title: What is a Hacker? | Author: Brian Harvey

https://people.eecs.berkeley.edu/~bh/hacker.html

Title: History & Impact of Hacking: Final Paper | Author: HistoryOfComputing

https://courses.cs.washington.edu/courses/csep590a/06au/projects/hacking.pdf

Title: How to Handle Security Vulnerability Reports | Author: Mary Branscombe

https://www.cio.com/article/3157698/security/how-to-handle-security-vulnerability-reports.html