Charleston Southern University

Ethics Paper:

The Good Hacker?

Alena Durel

Procedural Programming

Dr. Sean Hayes

September 14, 2020

Merriam-Webster dictionary defines a hacker in two ways, “an expert at programming and solving problems with a computer” or, “a person who illegally gains access to and sometimes tampers with information in a computer system”. While these designations show two different meanings of the word hacker, both are accurate. Meanwhile, the cultural definition of “hacker” more often than not holds an illegal connotation. Yet, not all hackers are immoral or unethical. Hackers are often split into three groups: whitehats, who do not take part in illegal activities, blackhats, who do, and grayhats, who fall somewhere in the middle. However, can you really be a grayhat hacker? According to Roger Grimes, author of *Hacking the Hacker: Learn from the Experts Who Take Down Hackers*, “Grayhats are blackhats. You either do illegal stuff or you don’t. Rob a bank and I’ll call you a bank robber no matter what you do with the money.” (*Hacking the Hacker*, pg. 4). Hacking is an important skill that can be used to find flaws within systems that make them vulnerable to blackhats. There is a definitive line between good and bad hackers; when and how you are hacking. Breaking into a system when you don’t have permission or hacking with malicious intent are signs of a blackhat hacker.

System-cracking is only ever ethical if a company or individual has given you explicit permission to hack into a system that they own. Hacking another person or group should never be for fun, even if there is no theft or breach of confidentiality. There are websites, such as tryhackme.com, that give people a place to learn and have fun. While some might think that it is acceptable to hack for fun as long as you are not harming anyone, it is important to remember 1 Corinthians 1:23-24, “[23]‘I have the right to do anything,’ you say–but not everything is beneficial. ‘I have the right to do anything’–but not everything is constructive. [24]No one should seek their own good, but the good of others.” Just because you have the power to do something, it does not mean that you should or that it is beneficial.

If a vulnerability in a company’s system is found by a penetration tester, they should report it so that the issue can be resolved. Meanwhile, if a company is offering some form of payment in exchange for finding security flaws, then a hacker should report any vulnerabilities found to the company. If the company does not respond, the hacker has a responsibility to continue attempting to contact them through any means they can. In an article by CNBC, “Ethical Hacking: Are Companies Ready?”, an ethical hacker found a security flaw in United Airlines’ network after they launched a bug bounty program. When he received no response from the program’s email address, he reached out on LinkedIn. Finally, he brought the issue to the CNBC, who alerted United Airlines and the hole was fixed. While this seems like a lot of effort to report a single hole, a major vulnerability left in a system could compromise the private information of the company and its clients. Luke 6:31 reads, “Do to others as you would have them do to you.” If another hacker found the flaw in the system and did not persist to receive a response from the system’s owner, it could be your information that is stolen.

Even though hacking should not be “just for fun”, there should still be attempts to reach out to a company if a hole is found while hacking for pleasure. However, even if no harm is intended, companies might be wary of a hacker who is finding flaws in their security and might believe that you are trying to infiltrate the system and steal information. Companies might also be wary of programs like the one implemented by United Airlines because “these people work as freelancers under no contract, potentially causing issues around confidentiality and whether the company’s security flaws will remain a secret.” (“Ethical Hacking: Are Companies Ready?”).

Overall, hacking should only be used under ethical circumstances with permission from the individual or company being hacked and should never be purely for pleasure. In addition, if any holes are found while hacking, they should be reported so that they can be resolved.

Works Cited

Grimes, Roger A. *Hacking the Hacker: Learn from the Experts Who Take down Hackers*. Wiley, 2017.

"Hacker." *Merriam-Webster*, Merriam-Webster, www.merriam-webster.com/dictionary/hacker.

Kharpal, Arjun. "Ethical Hacking: Are Companies Ready?" *CNBC*, CNBC, 19 June 2015, www.cnbc.com/2015/06/17/are-companies-still-scared-of-white-hat-hackers.html.

"New International Version." *Bible Gateway*, www.biblegateway.com.