Eric Smith

Mr. Richardi

CS Studio

5/17/19

The Dangers of Hacking and the Importance of Cyber Security

Over the years since the invention of the home computer and the creation of the world wide web, the public’s perception and understanding of the dangers of computer hacking have slowly progressed from mere fantasies such as those seen in *War Games* to the rising dangers of identity and information theft as seen in the wide-scale hack of Yahoo’s client base in 2016, when 3 billion yahoo accounts, which included information such as emails, monetary transactions and data, and other personal info, were breached and their information taken (Sobers). As more and more business and consumer interactions are taking place over the internet, so, too, are more crimes taking place over the internet and through computerized methods in order to take advantage of this new era online interactions. As a result, the role of cybersecurity in our digital society is becoming more and more vital as the impact of cybercrime is getting ever greater.

Firstly, to understand the full breadth of the effect of hacking and malicious web attacks on our current society, one must understand how cybercrime has grown over the last decade. According to Michael Lee from *ZDNet*, the Australian Computer Emergency Response Team (also known as AusCERT) reported a 296 percent increase in compromised host/computer notifications received by the organization over the period between 2007 and 2010, not to mention a doubling of reported websites hosting malware in the one year period between 2009 and 2010. This is for Australian web spaces alone, when looking at the United States it was seen that, in 2017, the yearly number of large-scale, targeted breaches reached a high of 130 cases per year with projected growth rate of 27 percent per year (Sobers). These are just the large scale attacks, the kind similar to Yahoo’s breach (though most in this category not quite so large) in which hundreds of thousands if not millions of users are affected with each breach, many without their knowing it. However, it is not just stolen information and identity theft that currently plagues our digital society, cryptojacking, or the theft of cryptocurrency from users whose accounts have been breached, and viruses hosted on malicious web pages and advertisements have caused billions of dollars in damages in 2017 alone, with $4 billion of that coming from the spread of the Wannacry virus, a ransomware attack which would encrypt important files and databases on infected computers to render them useless and then demand ransom payments in bitcoin in order to unlock these files for victims, to more than 400,000 machines (sober). This rampant increase in the severity and scale of cyber attacks in just 2017 alone illustrates the electronic issues our society now faces thanks to the growth of our electronic economy. In order to defend against these attacks, additionally, it is important for cyber security specialists to utilize the same tactics and strategies as the criminals they defend against in order to effectively combat cybercrime.

When using the term ‘hacking’, people generally look at the malicious cyber attacks mentioned previously, however, hacking, or the act of gaining unauthorized access to data in a system or a computer, is not a purely malicious action. Because the rising level of cybercrime and the growing abilities of cybercriminals, many (if not most) major online corporations (such as retailers, news sites, etc.) have employed cyber security experts whose main job is to search for vulnerabilities in their systems so that these weaknesses may be fixed before criminals breach their databases through this opening. These experts, dubbed “ethical hackers” by some, assist system developers in their goal of shoring up their defenses against hackers by locating any and all imperfections in the system and fixing them on a constant basis, at least for major corporations, so that systems and their openings are constantly changing and advancing to avoid the ever-analyzing gaze cybercriminals (Forbes Technology Council). These qualified “ethical” hackers are becoming more and more in demand for larger corporations with an online presence as the issue of malicious hacking gets progressively worse. The only issue with this morally sound method of preventing cyber attacks and breaches, however, lies within the ethical standings of allowing a person access to sensitive information through this type of probing, even while under supervision and contracts preventing them from using their knowledge for immoral purposes (“What is Ethical Hacking?”). In order to keep our information safe, we must trust these technicians with our sensitive data as the most effective way to prevent against cyber attacks is to do these kinds of structure tests, as worrying as that can be.

With cyber attacks on the rise and showing no signs of slowing down, it can be seen that cyber security is a must in our society and without it security breaches and stolen information on the internet would be impossible to avoid. However, in order to protect against cyber attacks cyber security experts must utilize malicious attacks and techniques in order to find the insecurities in a system, giving these “ethical” hackers access to vital and sometimes sensitive information that could be used for malicious attacks if these white hat security officials decide to work as black hat criminals. Despite this risk, ethical hacking is a must in order to keep systems and databases safe from attacks and the further development of cyber security tactics will lead to a safer future for the internet and the world that revolves around it.

Works Cited

Editors, Forbes Technology Council. “Ethics And Hacking: What You Need To Know.” *Forbes*, Forbes Magazine, 6 Mar. 2017, www.forbes.com/sites/forbestechcouncil/2017/03/06/ethics-and-hacking-what-you-need-to-know/#7b6fa93666d5.

Lee, Michael. “Is Cybercrime Replacing Physical Crime?” *ZDNet*, ZDNet, 5 Mar. 2012, www.zdnet.com/article/is-cybercrime-replacing-physical-crime/.

Sobers, Rob. “60 Must-Know Cybersecurity Statistics for 2019.” *Inside Out Security*, 17 Apr. 2019, www.varonis.com/blog/cybersecurity-statistics/.

“What Is Ethical Hacking.” *Maryville Online*, 14 Aug. 2018, online.maryville.edu/blog/ethical-hacking-and-morality-the-gray-area/.