How a hacker's mind can help security specialists:

An analysis of psychology in unethical hackers and the uses of this data to prevent cyber-attacks

Elizabeth Simpkins

Engl 211

Professor Nolan

Fall 2024

Abstract

Security from cyber-threats has become more important in the ever-evolving age of technology that we live in today. The best way to make our technology more secure is to understand why and how unethical hackers think about forming an attack. Research into the psychology of an unethical hacker has become limited due to lack of support and the recent use of AI by unethical hackers. There is still importance in this research; however, because being able to understand an unethical hacker more can help cyber-specialists follow similar movements in order to prevent attacks. Therefore, I propose to review the existing research of the motivations and thoughts behind a hacker's actions and how, based on that, cybersecurity specialists can develop better security methods and better target places where hackers may attack. Many proposed theories behind unethical hackers have been made, including a very important one called the depersonalized obedience theory. Other major research projects like honeyspys that track an unethical hacker's psychological movements through an attack have been made. Other sources of data including personal interviews with past unethical hackers have uncovered the concept of nerve control in unethical hackers. This research is not complete, however, due to the continued increase in cyber-attacks. By continuing to understand and work with unethical hackers, cyber-specialists will be able to determine types of deterrence that can prevent unethical hackers from committing more cyber-attacks in the future.

Introduction

In a world where technology is increasingly needed to complete everyday tasks, it is essential that devices stay protected from cyber-attacks in order to stay reliable and keep society functioning. However, research has shown that alongside the advancement of technology, the rate of successful attacks has likewise increased (Chng, et al., 2022). Therefore, beyond just engaging in a technology race, the drive and motivation behind these attacks need to be understood to keep up and find new mitigating techniques. If a cybersecurity specialist can understand why a hacker attacks in the first place and what allows them to go through with attacks, a lot of people and companies could be saved from having their data stolen. Research is needed to understand why they take certain paths in their infiltrations (Silic & Lowry, 2021), and this research could provide more methods of dealing with cyber-crimes and limiting the spread of them. **Therefore, I propose to review the existing research of the motivations and thoughts behind a hacker's actions and how, based on that, cybersecurity specialists can develop better security methods and better target places where hackers may attack.**

An Overview of Ethical Versus Unethical Hackers

Hackers did not start out as a malicious majority; they were typically people who just wanted to see how a computer worked and how it could be manipulated. People with curious intentions were originally called hackers, while their malicious counterparts were called crackers. The name hacker has been generalized to encompass all computer savvy people who can hack into a system (Guo, 2016). Ethical hackers will get paid to use their curiosity and technical skills to hack into systems, to help companies who have vulnerable systems. These are

not all set, or fixed categories, however. The types of behaviors and traits that can accumulate in an ethical hacker, also known as a white hat hacker, are present in figure 1, and show what leads to a gray or black hat hacker. Hackers can shift categories from ethical to unethical, such as gray and black hat hackers, if they have malicious intentions in using their skills.

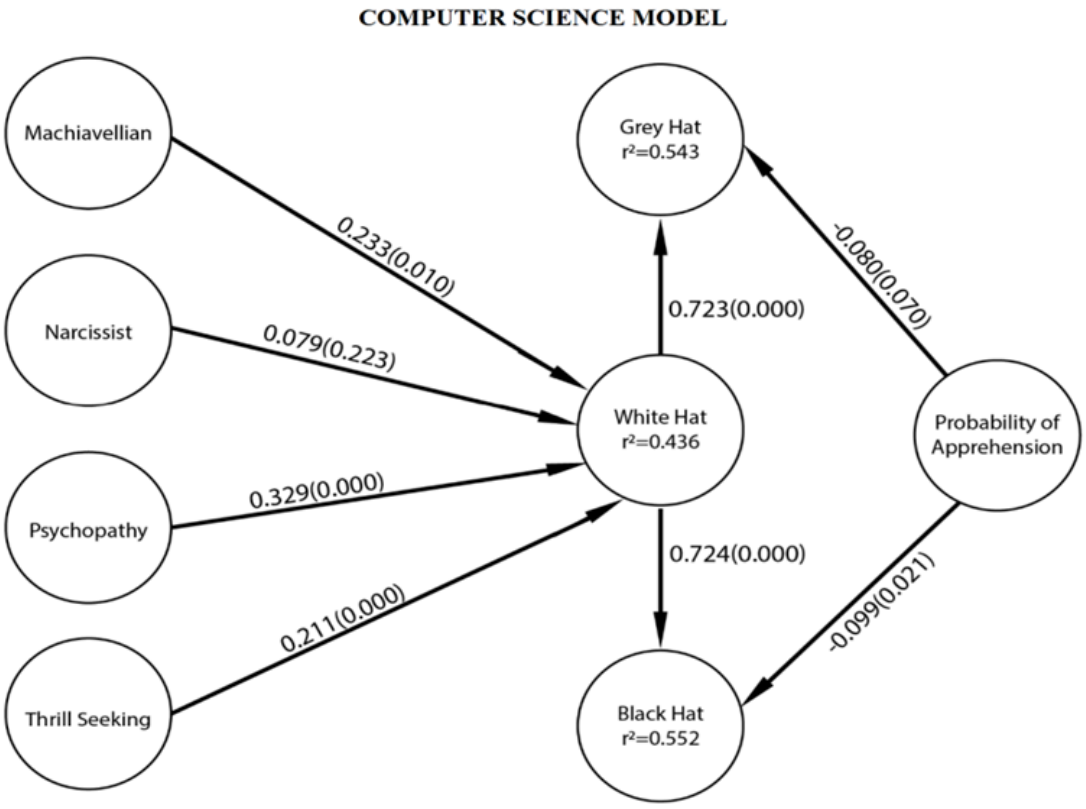

Figure 1: (Gaia, et al., 2021). This diagram shows the characteristics and traits that can lead an ethical hacker to unethical hacking behaviors.

Who and Where Unethical Hackers Target

The types of vulnerable people and specific times of the year that hackers look for

Unethical hackers will typically target people who have little knowledge about computer security. These people have little concern for it due to stress or fear, or are unaware of the enormity of attacks during specific times of the year. People nowadays can be flooded with typical phishing and click bait scams. Phishing can be email or text messages containing links in order to gain information from the target. Click bait scams can be false advertisement links or deceiving headlines that take the target to a site with completely different topics, meant to get targets to click on the link or insert information. These scams were very popular during COVID. People fell for many phishing, clickbait, and the new vishing scam, due to fear of wanting answers and getting vaccines (Chng., et al., 2022). Vishing is an AI modified version of phishing in which a voice can be duplicated and sent to a target to get information. Elections and large political events can also be targets for hackers as well, especially hacktivists who want political justice (Chng., et al., 2022). Events like these can be targeted by hackers by creating false content. An example would be AI generated Deepfakes, which can format facial features and put someone else's face on another's in a video or picture. A hacktivist, for example, could use this to control what that face people are seeing is saying. This has been used for false presidential speeches in order to stir up controversy and possibly support for hacktivists' cause. Other times of the year that can attract hackers are holidays. This is due to distractions such as shopping and browsing the internet for the holidays. This leads to people not paying much attention to clickbait, phishing, or even malware on card machines.

Critical infrastructures and Vulnerable Network Connection

The attack of Target's card machines opened peoples eyes to many places that an unethical hacker can get into a network. In 2014, Target announced that all shoppers going back to 2012 have had their information exposed due to the attack (McMullen, Sanchez, & Reilly-Allen, 2016). This attack was an example that made security a key issue to protect all parts of a network. The hackers got in through the HVAC portal using a phishing attack, not directly through the card machines. Hackers will move laterally through a network by entering through other doors other than their specific target, or just to see what all is open (McMullen, Sanchez, & Reilly-Allen, 2016). The hackers were able to google how Target was connected to their HVAC vendor portal, which shows the value that the internet can have for a hacker. This attack in particular was huge to a lot of people because it showed that technology, even if it isn't a valuable data storage machine, has to be protected in order to keep other things on the same network safe.

Why Do Unethical Hackers Hack?

Behaviors of unethical hackers

Unethical hackers can be hard to categorize due to little research into the psychology behind unethical hackers. Some general motivations behind these hackers have been collected, however. Unethical hackers typically have certain motivations in common such as financial gain, curiosity, revenge, fame, fun, belief, or impulses of sorts (Chng, et al., 2022). The reason that these motivations can be hard to determine is because most hackers are not actually caught. High

profile malicious hackers that have been caught seem to present similar behaviors such as a history of criminality, abuse, anti-social personalities, and commonalities to psychopaths (Gaia, et al., 2021). Hackers that stay in the unethical realm of hacking will experience psychopath behaviors due to their low anxiety and stress levels while committing crimes online. Communities of unethical hacker groups like hacktivists, which typically have political goals, will influence each other to commit cyber-attacks (Gaia, 2021). The rush and curiosity behind an attack can fuel an unethical hacker's drive to commit more attacks, especially when the stakes are low for getting caught.

Theories Behind Unethical Hacker Motivations

Some of the most important factors that can help an unethical hacker focus on their goal and continue to commit cyber-crimes can be summed up through several theories. One theory, called the depersonalized obedience theory, focuses on the virtual environment that an unethical hacker will put themselves in. This helps them focus on the code on the screen during an attack, rather than the person they are harming on the other end (Chng, et al., 2022; Guo, 2016). When an unethical hacker commits an attack, they may not worry about who they are harming because they can't physically see the damage. They may also feel like they aren't doing any harm, since their attacks are digital. This lack of empathy leads into another theory called the cognitive distortion theory. This is where an unethical hacker will convince themselves that their actions are not harmful, but rather can be accomplishments according to other unethical hackers (Silic & Lowry, 2021). These mindsets can be dangerous, especially if an unethical hacker can get into and take control of something very important, like a card machine or a car's electronics.

Another theory is Bevron's theory of flow which is the development of skills due to a connection between technology and the hacker. This connection makes them feel they have the control and curiosity to fulfill the extent of their abilities that makes them excited and happy (Chng, et al., 2022). Unethical hackers will develop their skills in order to continuously feel the rush of getting into a system and obtaining their goals. A key theory that explains why unethical hackers are willing to risk everything to commit cyber-crimes, is the Broken Windows theory. This theory explains that there is little risk for unethical hackers to get caught or face high punishments, due to little lawful concern for minor hacks and attacks (Silic & Lowry, 2021).

Some theories can be connected to unethical hackers, but they are not able to be applied to them due to the differences in location and processes. One well-known theory that has been applied to street criminals is the General strain theory. There is significance in this theory because it cannot be applied to unethical hackers. Since unethical hackers develop their own motivations to commit crimes, they have completely different ways that help them choose to commit cyber-crimes compared to street crimes (Silic & Lowry, 2021). Another theory that has little effect on unethical hackers is deterrence theory. Deterrence is the ability of consequences to deter current or possible convicted criminals from committing the same or similar crimes. Unethical hackers generally have little deterrence, because the consequences and stakes are low for small virtual crimes. This causes hackers to have low anxiety about commiting crimes (Gaia, et al., 2021). It is common for low level attacks to go unnoticed or unenforced, due to the enormity and little harm of them.

One last general theory behind unethical hackers is one that can apply to the majority of criminals. This is the fact that crime follows where the money goes (Jordan & Taylor, 2003). While not all unethical hackers' intentions may be financial gains, like vengeful or thrillful motivations, money is a large driving factor in small cyber-crimes. This is why places like stores, banks, businesses, and any other places that have money flow need to have security all across their network.

Nerve control

A key factor in unethical hackers being able to commit cyber-crimes is their ability to control their nerves. Even in an isolated environment, the intensity and lack of an ability to control nerves can lead to an unethical hacker moving away from crimes. Therefore, the need for low anxiety levels is required for a successful unethical hacker (Silic & Lowry, 2021). Hacking groups can put pressure on other members to control their nerves to become successful. In unethical hacking, nerve control is not only required but impressive to other hackers as well (Silic & Lowry, 2021). Referring back to the depersonalized obedience theory, unethical hackers will not be able to see their victims in most cases. This lowers their stress and manages their nerves because they may have little guilt for a victim they can't see.

In several interviews with past unethical hackers, the hackers defend their attacks by stating that their reasoning would often outweigh the costs, due to little consequences for minor cyber-crimes (Silic & Lowry). Other unethical hackers stated that crimes they committed were easy due to little risk and the ability to control their nerves. Some stated that compared to worse crimes on the street, their minor crimes seemed like they were not affecting anyone (Silic &

Lowry, 2021). Due to current low-stake consequences for minor cyber-crimes, the number of attacks has skyrocketed. Unethical hackers are not able to see their victims most of the time, and feel that they are not harming anyone. An unethical hacker's isolation from people and nerve control can create a dangerous hacker with little remorse due to the low risk factors against them.

Generalizations and stereotyping

Due to the common household name of a hacker, all hackers are seen to be malicious in their intentions, and therefore are all dangerous. This is not the case, however, because there are hackers working for the defensive side called gray or white hat hackers. Generalizations about hackers are due to unintentional exposures of a victim's personal information (Guo, 2016). When hackers were becoming a new type of criminal in the early 2000s, the mass media would make unethical hackers sound all powerful and all malicious. In reality, however, unethical hackers typically gain very little, even though the attacks were often (Jordan & Taylor, 2003). This statistic still applies today, since there are more low-level unethical hacker attacks with little gains compared to widespread attacks. Stereotyping all hackers can eventually lead to the aggravation of hackers, and creation of more malicious attacks (Guo, 2016). Ethical or gray hat hackers can even get controversy due to the fact that their job is to break into a network to see if it has vulnerabilities. With a limit on what a hacker can do, and the addition of constant stereotypes, a hacker may want to feed into the generalizations in order to prove a point.

Insider Threats

Insider threats are people who currently or used to work for a company, and are causing harm to that company through data leakage. Insider threats come in all shapes and forms, and are not all malicious in intent. Many insider threats are due to the lack of training and knowledge for security. This can lead to costs and leakages of information for the company. However, these threats can also be intentional and may be based on revenge or financial gains through the release of company secrets or customer information (Gaia, 2021). Insider threats could be people who previously had been ethical hackers and switched sides due to some sort of motivating factor. These factors can include things like money, justice, or curiosity in seeing how much they can hack into and steal.

How Knowing These Unethical Hacker Traits Can Help cyber-specialists

Mapping their movements through Honeypots and Honeyspys

Unethical hackers are able to be watched and studied through the use of honeypots and honeyspy systems. Honeypots are fake networks that attract unethical hackers to hack into them. Their movements are traced as they move through the network. In figure 2, the use of a honeyspy system is used. A honeyspy tracks an unethical hacker's behaviors and psychological preferences based on certain choices, in order to determine how unethical hackers think. A cybersecurity specialist can use this to map an unethical hacker's moves through reused coding and anticipate their outcomes, in order to protect other systems (Chng, et al., 2022). Unethical hackers typically

move laterally, as in from system to system, rather than directly towards their intended target, in order to gain as much information and data as possible.

A cyber-team can use defense in depth, which is creating a security system that has many layers. This secures each step of an unethical hacker's movements in order to make it harder for infiltration. By also narrowing down locations where hackers target, according to specific honeypots and honeyspys, cybersecurity specialists can secure higher targeted places (McMullen, Sanchez, & Reilly-Allen, 2016).

Limitations of unethical hacker research

The use of AI has made the practice of honeypot supervision difficult, however. Since AI repeats its processes over and over until it gets a working attack or code correct, an unethical hacker is not using the same methods every time. This has increased the difficulty of a cybersecurity specialist's job with these sophisticated attacks. Through the use of defensive AI, however, and more research into decisions made by hackers and AI systems, the defensive side can keep up with the attacks.

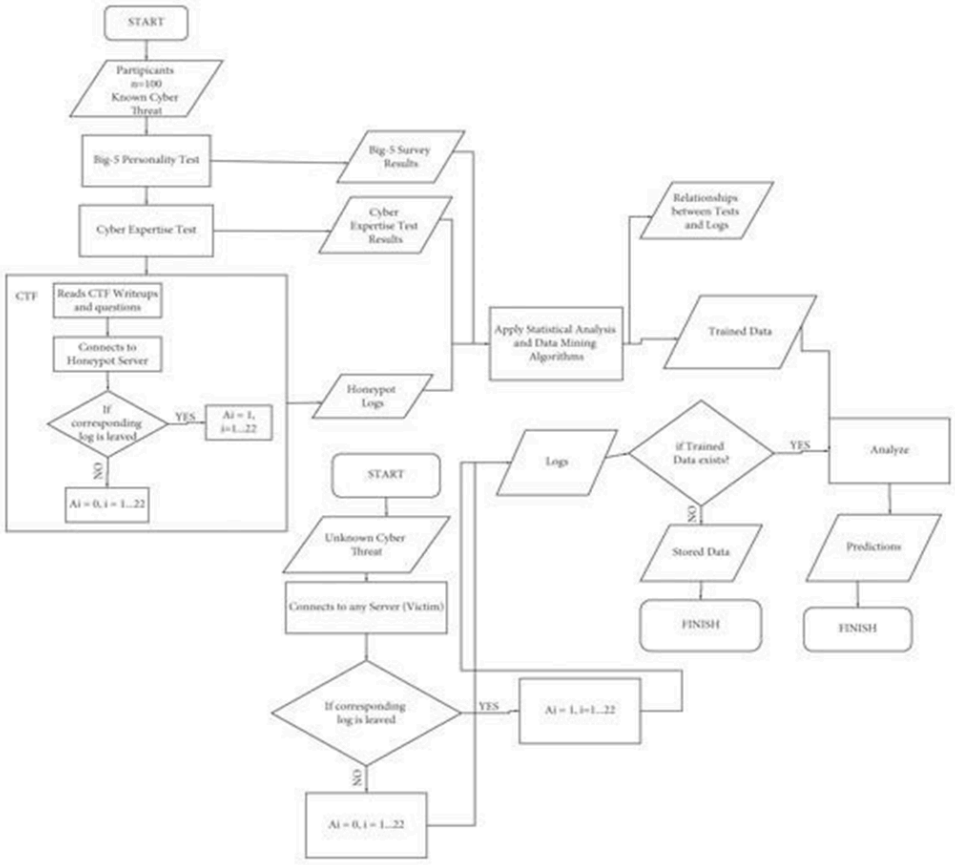

Figure 2: (Odemis, Yucel, & Koltuksuz, 2022). This is a diagram of the process that a hacker can take moving through a honeyspy system, in which the hacker's psychological decisions are recorded and studied.

How attacks can expose vulnerabilities and help customers

Hackers may use their skills in a way that is illegal, but for the greater good. This is seen in a case discussed on a Ted Talk when Kyle Lovett found a vulnerability on a wireless router company's product. He was ignored in his request and later a group of hackers infiltrated the vulnerability. The hackers used the infiltration to send out a warning message, seen in figure 3, to

all that were affected by the vulnerability and how to fix the problem (Elazari, 2014). These types of hackers broke the law by hacking into the systems, but they did it to help the people who were vulnerable, because the company would not fix their product. Therefore, while some illegal attacks can be malicious and harmful, some can be for the greater good of helping cybersecurity specialists. Since these hackers prevented a serious attack on their own, cyber specialists and the company did not have to deal with a malicious attack. Therefore, malicious hackers can be stopped by other hackers as well. This is why understanding a hacker is so important.

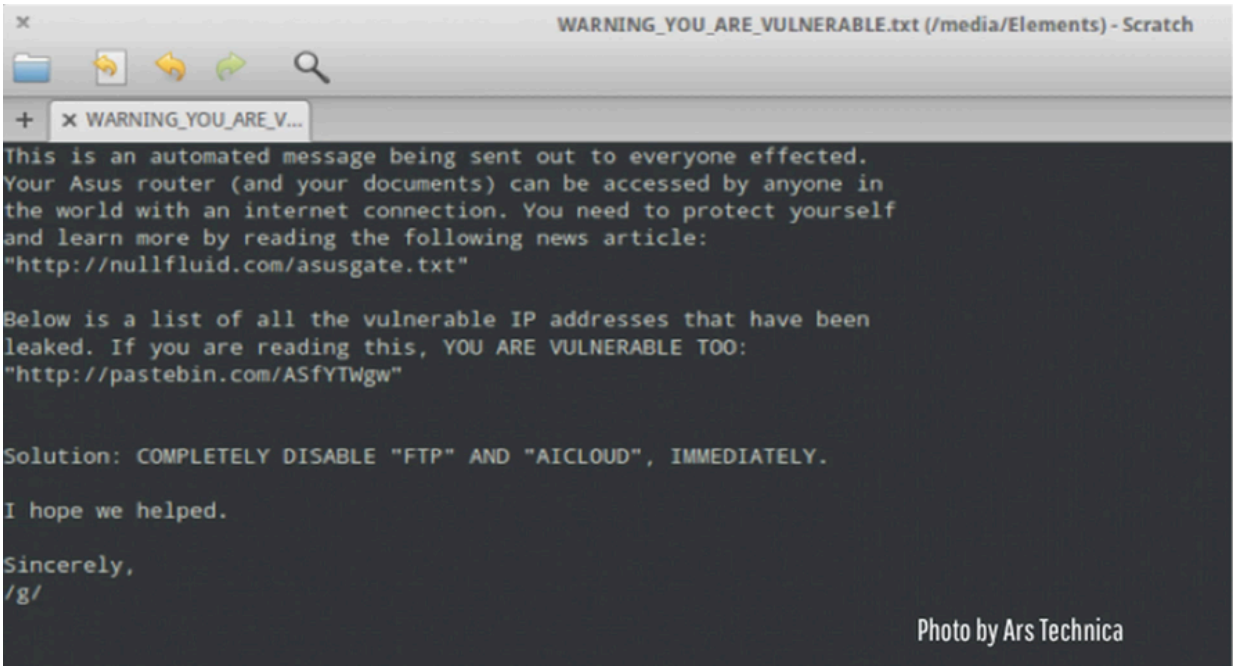

Figure 3: (Elazari, 2014). This screenshot shows the message that vulnerable users received from the hacker group if they were affected by the wireless router bug.

Updated research needed and possible deterrence for unethical hackers

Research into the psychology of unethical hackers is needed for cyber specialists to use this data to make deterrence methods for unethical hackers. This research is currently limited, which means that security specialists have a limited view of why an unethical hacker operates (Silic & Lowry, 2021). These points of data can be hard to test, because unethical hackers are typically not caught. The ones that change sides to ethical hackers don't always ride the same line as other hackers who were able to control their nerves enough to commit more malicious unethical crimes. The line between different types of hackers, their intentions, rate of recurring offenses, severity, and methods is another topic that needs more research into. Cyber-specialists have to prioritize attacks, based on these factors, especially with the increase in attacks (Chng, et al., 2022). More research into the nerve controlling aspect of unethical hackers is also needed. The removal of nerve control can be made by cyber specialists in order to create a deterrence. (Silic & Lowry, 2021). This, in turn, could possibly lower the cyber-crime rates that keep increasing.

Conclusion

The key quality in unethical hackers seems to be their nerve control, and researchers have begun to study their movements through the use of honeyspy systems, which can continue to be used to collect more data on unethical hackers and their thought processes, and through different theories applied to explain why an unethical hacker might behave in certain ways. More research, however, is needed to better understand how unethical hackers can continuously come up with new attacks and control their nerves as risks get higher in more malicious attacks.

Deterrence factors can also be put into place to help raise risk levels for unethical hackers in order to control cyber-crime rates. The development of AI in cyber-attacks also makes this data more difficult to collect, due to its ability to automate attacks without an unethical hacker's use of code. Another question arises with this use as well, how has an unethical hacker's mindset been altered to the use of AI? More education on the topic at hand, or even an interview with a cyber-specialist dealing with psychology of unethical hackers, would have been beneficial in getting more information about hackers. This research, however, can be used as a general guiding tool for continuing to understand unethical hackers, help prevent major attacks, and even work with hackers to build a better online world.

References

Chng, S., Lu, H.Y., Kumar, A., & Yau, D. (2022). Hacker types, motivations and strategies: A comprehensive framework. Computers in Human Behavior Reports, 5. https://doi.org/10.1016/j.chbr.2022.100167

Elazari, K. [Keren Elazari]. (2024, March). *Hackers: The internet's immune system*. [video]. TED. https://www.ted.com/talks/keren_elazari_hackers_the_internet_s_immune_system?referrer=playlist-who_are_the_hackers&subtitle=en

Gaia, J., Sanders, G. L., Sanders, S. P., Upadhyaya, S., Wang, X., & Yoo, C. W. (2021). Dark traits and hacking potential. Journal of Organizational Psychology, 21(3), 23–46. https://doi.org/10.33423/jop.v21i3.4307

Guo, B. (2016). Why hackers become crackers—An analysis of conflicts faced by hackers. *Public Administration Research*, *5*(1), 29-36. https://pdfs.semanticscholar.org/b4b9/1526081203190e5623063c08db5fc4e6849f.pdf

Jordan, T., & Taylor, P. (2003). A sociology of hackers. In Wall, D.S. (Ed.). (2003). Cyberspace Crime (1st ed. Pp 757 - 780). Routledge. https://doi.org/10.4324/9781315199627

McMullen, D. A., Sanchez, M. H., & Reilly-Allen, M. O. (2016). Target security: A case study of how hackers hit the jackpot at the expense of customers. Review of Business & Finance Studies, 7(2), 41-50. https://ssrn.com/abstract=2801762

Odemis, M., Yucel, C., & Koltuksuz, A. (January 27, 2022). Detecting user behavior in Cyber Threat Intelligence: Development of honeypsy system. WILEY Hindawi 2022(1), 1-28. https://doi.org/10.1155/2022/7620125

Silic, M., & Lowry, P.B. (2021). Breaking bad in cyberspace: Understanding why and how Black Hat Hackers manage their nerves to commit their virtual crimes. Inf Syst Front 23, 329–341. https://doi.org/10.1007/s10796-019-09949-3