**Hacking in Society: An Annotated Bibliography**

Génesis M. Ojeda Rosa

Department of Education, English: Interamerican University of Puerto Rico

GEEN 1203: English Communication III

Professor: Monique Guidicelli Resto

December 1, 2022

**Hacking in Society**

**Content**

Hacking has been present in society since technology has been developing. Cybercrime is a big issue in society due to what it affects. The objective of the study is to instruct society of cybercriminals. The research focuses on three questions. This are what are the types of hacking, how does hacking affect society and how can the crime of hacking be minimized. It was concluded that the principal type of hacking is malware with its subdivisions, viruses, trojans and ransomware. Hacking has an effect in society that can be both negative and positive. It affects economically and it creates victims. Its impact is more negative than positive now due to the increasing cybercrime. The crime of hacking can be minimized by a 99% primarily by using a two-factor authentication method. The methods used in the research is quantitative. Some limitations can be the reduced report of cybercrime victims and the sincerity of the sample in the secondary data extracted. Some future research questions that can be developed by this research can include the effect of the emerging cryptocurrency in hacking and technologies that are arisen to implement in the hacking system.

**Introduction**

**Significance of the Problem**

Efforts are made to combat the increasing cybercrime by the FBI (Mayer, 2021), but there is more cybercrime emerging than it is being eradicated (Films Media Group, 2018).

**Summary of the Problem**

Hacking is a big problem in society economically and psychologically (Burt, 2021). In 2021, cyberattacks increased by a 50% (Kaspersky, 2022). Ransomware is rising in Puerto Rico drastically (Primera Hora, 2022). Many victims of cybercrime experience negative impact in their lives, the most common effects being anxiety and anger (Palassis, Speelman, Pookley, 2021).

**Problem Statement**

Hacking in the world is a social problem that is present in the daily lives of people, but it isn’t created the sufficient awareness of it. Less than 20% of society use good anti-hack features (Check Point, 2022).

**Nature of the Study**

The research is focused primarily on three questions: the different types of hacking, the effects of hacking in society and how can the crime of hacking be minimized.

**Purpose of the Study**

The purpose of the study is to educate society of the dangers of cybercriminals and how to minimize and prevent these attacks.

**Conceptual Framework**

The impact of cybercrime in the world economically costs more than $68,493,180 per hour and it continues to increase drastically every day (Microsoft, 2022). 99% of cybercrime can be prevented (Kaspersky, 2022). The methodology used in the research is quantitative.

**Key Terms**

White hat hackers find vulnerabilities in a system and fix it (Chng, Lu, Kumar, Yau, 2022). Black hat hackers find or create vulnerabilities in a system and gain information of a target (Summers, 2013). Malware is a software that is infected, and it contaminates a user’s device (Microsoft, 2022).

**Assumptions, Limitations, Scope, and Delimitations**

Limitations and potential weaknesses in the research may include reduced information of Puerto Ricans victims of cybercrime, the honesty of the participants in the studies conducted used to strengthen the research, and the reduced information of the psychological impact on victims o0f cybercrime.

**Significance of the Study**

The study applies to the world, due to the information it portrays. It can add knowledge of cybercriminals personally and professionally due to everyone having the possibility to encounter a cybercrime at least once in a live time. The research brings a positive social change because it educates society on the dangers and how to prevent cybercrime.

**Summary**

Hacking is a problem that society faces daily, but more awareness needs to be created of the situation. Hacking comes in many forms, but they all have a negative effect on society. The minimization of hacking can be done by updating a person’s device, using strong and different passwords for every account, educating society on how to prevent being hacked and many other ways.

**Literature Review**

**Historical and Theorical Background**

Hacking has an impact on society. This impact is mostly negative, due to hackers taking advantage of others ignorance in technology (Koyun, Hanabi, 2017). The world economy is affected drastically, being more than 1billion per month that is spent on cybercrime (Microsoft, 2022). Victims of cybercrime show significant changes in their daily lives after their devices were hacked (Palassis, Speelman, Pookley, 2021). The organization is done by a thematic approach. The principal theme is cybercrime with the subthemes being cybercriminals, economy, victims, security, and prevention. The content displayed is from websites that are certified to have good and reliable sources.

**Cybercrime**

***Cybercriminals***

Cybercriminals are intelligent in the themes of technology due to how they engage in problem solving. They create mind maps that help them to envision the objective. (Films Media Group, 2018) Hackers engage in creativity to develop their tools to do their job. New hackers are validated and welcomed to the industry, making them feel comfortable as they share their ideas and are constantly supported by experienced hackers. (Chng, Lu, Kumar, Yau, 2022).

***Economy***

Economically society is impacted drastically. The world approximately spends more than $6,000,000,000 yearly on trying to minimize cyberattacks that occur daily (Microsoft, 2022). Society is impacted by this, directly or indirectly in some manner. Many cyberattacks to individuals or companies are motivated by economic purposes, and mostly all these attacks request a sum of money to stop the hacking (Films Media Group, 2018).

***Victims***

Cybercrime victims may develop severe psychological problems when their devices are hacked. Their privacy was invaded, and their conduct changes due to this. Their social interactions are affected, as well as patterns are developed as coping strategies to manage with the struggle (Palassis, Speelman, Pooley, 2021).

***Security and Prevention***

Only 1% of hacking can’t be prevented, but the other 99% can be prevented if the correct tools are used that are provided by companies, that are mostly free of use forever (Microsoft, 2022). Prevention can help determine if a person is hacked or not.

**Quality of Literature**

The best sources that were found and compiled were the Palassis, Speelman and Pooley study of victimization, the Microsoft study of cybercrime in a minute, the Schicks, Weijer, Leukfeltdt and Rutger study of the capabilities of cybercriminals and Summers study of how hackers think. All these sources accomplish their purposes of the study, as well as it complies with the structure of a well-done research. Everything is presented in a simplistic, but sufficient information for the researcher to understand and analyze the problem, possible solutions and results of it.

**Relevance of Literature to Study**

It adds knowledge to the researcher about the topics of cybercrime and how it can be applied in the daily lives of society. It can educate society and minimize the delict of hacking, influencing long term of spending less money on cybercriminals and attending other important matters that are happening in the world now (Burt, 2021).

**Relevance of Literature to Each Other**

***Cybercriminals***

Chngs and Lau’s, Summers and the Films Media Group studies conclude that hacker motivations are for personal gain. Their research also points out that hackers are brilliant people that know a lot of technology. All their study state that there are good and bad hackers. Chngs and Lau’s and Films Media Group use a quantitative method to conduct their studies, while Summers a qualitative method. Chngs and Lau’s and Films Media Group differ in the types of hackers. Chngs and Lau’s study points out that they are 13 types of hackers, while Films Media Group states 10. Although they differ from how many types of hackers are there, it covers all the principal hackers. These sources are relevant to each other due to the information talking about cybercriminals and their doings.

***Economic Impact***

Burt, Check Point, Kaspersky, and Microsoft studies all conclude that cyber-attacks affect the world economy. Their cost of cybercrime in the world ranges from 1 billion to more than 6 billion. All their research is made in the quantitative method. Check Point and Kaspersky are live maps of cybercrime, but they both differ in the most attacked country now. Kaspersky states that it’s the United States, while Check Point Russia. Burt and Microsoft are in accordance with the economic impact on society. These sources are relevant due to the information stated of the impact hackers have in society.

***Victims***

Primera Hora and Palassis, Speelman and Pooleys studies all conclude that victims suffer consequences. Both are in accordance with the impact that cybercrime has on victims directly or indirectly. In Primera Horas study, the impact was economical and indirectly, while in Palassis, Speelman and Pooleys study was psychological and directly. Although their research differs from the impact, it acknowledges both impacts the same way. Both use the qualitative method to conduct their studies. These sources are relevant due to the importance of helping the victims of cybercriminals and the consequences it has on society.

***Security and Prevention***

Kaspersky and Mayers studies conclude that security and prevention is necessary to stop cybercriminals from doing more damage to society. Mayers approach is that is necessary to implement more white hat hackers, while Kaspersky differs and states that is necessary to educate and reinforce the existent software’s. Although they both differ on the ideas on how to minimize the crime of hacking, their ideas are valid and correct. Both use a quantitative method to conduct their research. These sources are relevant due to the importance of protection and prevention to minimize the conduct of hacking in society.

**Summary**

Cybercrime keeps increasing on the daily affecting their targets economically and psychologically. There are many types of hackers, but they can be differentiated by their works. Security and prevention play an important role in the fight of cybercrime. Cybercriminals are intelligent people when it comes to technology and developing ideas. Teamwork is essential in their group, as well as problem solving.

**Methods**

**Introduction**

Cybercrime is increasing in an alarming state, bringing consequences (Microsoft, 2022). These consequences are seen in the economy as well as the victim’s psychology (Summers, 2013). The different types of hacking, the effects of hacking in society and how can the crime of hacking be minimized are the purpose of the research. The method used to analyze the data is quantitative. The data used was secondary data provided by certified studies.

**Methodological Approach**

The data collection was made from internet resources. It was chosen that the data collection was going to be from internet resources due to the vast content of cybercrime that is being displayed on the internet.

**Methods of Data Collection**

The methodological approach of the research paper is quantitative. This approach was chosen because it was the most appropriate for the content that is presented on the research. The research questions are more inclined to be answered in a quantitative than a qualitative method.

**Methods of Data Analysis**

The methods of data analysis are exploratory. An exploratory analysis connects data and establishes a relationship between it to find meaning in something. It was used Excel as a tool to certify the calculations made with the data, as well as dictionaries from the internet to explore terms. It wasn’t used the method qualitative or the mix method, due to the quantitative method being the most adequate for this research.

**Conclusion**

The method used in the research is quantitative. This method was used because the research questions are more oriented to be answered in the quantitative method. Some tools used to analyze the data was Excel and dictionaries from the internet.

**Results and Discussions**

**Results**

Hacking has had consequences in people’s lives, whether it has been positive or negative, its present. These consequences create an impact, being the purpose on the research to educate people on this influence. The three questions established on the research paper were what the different types of hacking are, what are the effects of hacking in society, and how can the crime of hacking be minimized. The results were that there are a lot of different types of hacking, but the most common type is malware (Chng, Lu, Yau, 2022). The effects on society can be both positive and negative, but its more negative (Mayers, 2021). The crime of hacking can be minimized by using features that prevent hacking, as well as reporting any issues to the FBI or the ICCC (Summers, 2013).

**What are the Types of hacking?**

It was concluded that the result of the question of the types of hacking is that there are a lot of hacking types, but the most common one is malware (Chng, Lu, Yau, 2022). Malware a type of malicious software is the principal hacking type and it’s divided by sub sections, being the most common types that can be encountered are viruses, trojans, worms and ransomwares (Microsoft, 2022). Malware is the easiest way to install a malicious software in a target’s device, this being why it’s the most common type (Check Point, 2022). The ignorance of people in the types of hacking can also be cataloged as why is the most common type, because some type of malware that can pose as a real and safe software and most people don’t know how to distinguish the difference of a real and fake site, thus being hacked by a black hat hacker (Summers, 2013).

**What are the Effects of the Types of Hacking?**

It was concluded that the result of the question of the effects of hacking in society can be positive and negative. On the positive side, it can be found the white hat hackers. These ethical hackers help to strengthen the system, helping society economically They prevent information or data from being hacked or fix and encounter hackers doings (Mayer, 2021). On the negative side, it can be found the black hat hackers, who affect society economically and psychologically. It was concluded that 50% of cyberattacks increased in 2021 since 2019 due to the covid-19 outbreak (Kaspersky, 2022). Everyone was working in their homes, leading to many vulnerabilities being exploited by hackers due to the poor security they had, affecting people and companies economically (Films Media Group, 2018). Psychologically it was established that victims of cybercrime may go through a negative effect on their lives. They can develop anxiety and anger issues. They can also experience some unhealthy coping strategies to prevent a cyberattacks in the future. All of this affects them at their workplace, in their family and friend circle as well as internally as a person (Palassis, Speelman, Pookley, 2021).

**How can the Crime of Hacking be Minimized?**

It was concluded that the result of the question of how the crime can be minimized can be with the act of before, during and the aftermath of the hacking. It’s important to highlight that no one is 100% safe from being hacked, but it can be minimized. Before any hacking threat, it is crucial to make sure a user’s account it strengthens with a multistep authentication and a strong and different password for each account. This will help secure an account, being less probable to being hacked than an account that doesn’t have the necessary security to prevent these attacks (Kaspersky, 2022). 99% of these hacking attacks were preventable by only using two step authentication features (Burt, 2021). 19% of society use these strong features, leading the 81% of people being vulnerable to being hacked (Kaspersky, 2022). During the attack and aftermath, it’s important to stay calm and contact the ICCC (Internet Crime Complaint Center) or the FBI (Federal Bureau of Investigation) and report any incident that is happening to the device (Palassis, Speelman, Pooley, 2021). Always maintaining the device up to date will also prevent cybercriminals from hacking a device so easily (Kaspersky, 2022).

**Analysis**

The results found in the research can be compared to several investigations and articles that are seen today. Ransomware is increasing in Puerto Rico rapidly today (Primera Hora, 2022). This can be compared to the research question number one. Ransomware is a type of hacking derived by malware. Its increase is due to the security vulnerabilities and ignorance of people with dealing with hacking problems (Summers, 2013). The AutoExpresso ransomware affected all the civilians in Puerto Rico economically and psychologically (Rosario, 2022). This can be compared to the research question number two. How society is affected negatively by cybercriminals in this case both economical and psychological. Both examples can be applied to research question number three. Prevention an action during and in the aftermath of the hacking can prevent more hackings from occurring. These three questions are comparable in a similar way with each other and with what happens daily in the world. Some limitations and weaknesses that the research could include is the limited information of the victims of cybercrime in general from any country and specifically in Puerto Rico. Honesty in members of all the secondary sources gathered can always be questioned. The strengths are the sources from where it was collected. All the sources provided sufficient and comported information. Some future research questions that can be developed based on the research findings can be how the new type of crypto currency affects the hacking methods, what new technologies are being developed and implemented to encounter cybercriminals and how hacker’s groups can be minimized.

**References**

Burt, T. (2021). Russian cyberattacks pose greater risk to governments and other insights from our annual report. Microsoft On the Issues. <https://blogs.microsoft.com/on-the-issues/2021/10/07/digital-defense-report-2021/>

Check point: Live cyber threat map. (2022) Live Cyber Threat Map | Check Point. (n.d.). <https://threatmap.checkpoint.com/>

Chng, S., Lu, H. Y., A, & Yau, D (2022 January) Hacker types, motivations, and strategies: A comprehensive framework. Computers in Human Behavior Reports. https://www.sciencedirect.com/science/article/pii/S245195882200001

Films Media Group. (2018). Dark web: Fighting cybercrime. Films On Demand. <https://fod.infobase.com/PortalPlaylists.aspx?wID=103691&xtid=207055>.

Kaspersky, K. (2022, September 30). What is cybercrime? how to protect yourself from Cybercrime. www.kaspersky.com. <https://www.kaspersky.com/resource-center/threats/what-is-cybercrime>

Kaspersky. (2022). Kaspersky cyberthreat real-time map. MAP. <https://cybermap.kaspersky.com/>

Koyun, A., & Hanabi, E. A. (2017, June 6). Social Engineering Attacks. Isparta; Suleyman Demirel University. https://www.jmest.org/wp-content/uploads/JMESTN42352270.pdf

Mayer, J. (2021, March 8). Government hacking. HeinOnline. <https://heinonline.org/HOL/LandingPage?handle=hein.journals%2Fylr127&amp;div=15&amp;id=&amp;page=>

Microsoft. (2022, August 1). Cyberthreat Minute: The scale and scope of worldwide cybercrime in 60 seconds. Security Insider. https://www.microsoft.com/en-us/security/business/security-insider/anatomy-of-an-external-attack-surface/cyberthreat-minute/

Microsoft. (2022). What is a cyberattack? Microsoft Security. <https://www.microsoft.com/en-us/security/business/security-101/what-is-a-cyberattack>

Palassis, A., Speelman, & Pooley, F. (2021, October). An exploration of the psychological impact of hacking victimization. ResearchGate | Find and share research. (PDF) An Exploration of the Psychological Impact of Hacking Victimization (researchgate.net)

Primera Hora. (2022, October 1). ¡cuidado! FBI advierte Sobre Secuestro de Datos en Puerto Rico. Primera Hora. https://www.primerahora.com/noticias/profugos/shows/cuidado-fbi-advierte-sobre-secuestro-de-datos-en-puerto-rico-279377/?utm\_medium=Social&amp;utm\_source=Facebook#Echobox=1664716790

Rosario, F. (2022, May 1). *Para largo los problemas del AutoExpreso tras el hackeo.* Primera Hora. <https://www.primerahora.com/noticias/gobierno-politica/notas/piden-amnistia-en-pago-de-deuda-en-peaje-por-hackeo-en-autoexpreso/>

Summers, Timothy (2013, September 18). How hackers think: A study of cybersecurity experts and their mental models. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract\_id=2326634