Cybercrime and Covid-19

By

Lonell J, Riddick

Submitted in partial completion for CRJS 215

Department of Sociology and Criminal Justice

Old Dominion University

Introduction

Whenever there is a lock, there is always a person out there trying to pick the lock or trying to break in. Cybercrimes is any criminal activities carried out using computers or the internet. Cybercrimes are important to everyone because people are using technology more often and hackers is always looking to take advantage of innocent people. Cybercrimes can be prevented by learning more info about it. The first thing, I will talk about is the current examples in society of cybercrimes. Then, I will discuss how has this problem/issue been studied in the past. In addition, I will discuss what are the common themes that emerge from the reviewed collection of literature. Next, does the criminological literature support or provide evidence of utilizing any particular criminological theory. The last thing I will discuss is any programs, initiatives, or policies exist to address the issues. The reason why I want to research this is because many people may not be aware cybercrimes and how dangerous or how much of a setback it can be for people or companies. In this paper I want to bring to attention cybercrimes affecting people and how hackers why hackers are getting more prevalent. I want to introduce you to cybercrime and covid-19 effects it has on cybercrimes in this research paper.

Current Example in society

Cybercrimes have definitely been represented in popular media. Cybercrimes are usually describing the type of attack used on a person or on the company. Social media spreads this info very quickly and make people more aware. For example, back in 2013 target had a major data breach and the news helped spread more info about it. This breach costed target millions and it was caused by phishing scams from emails. The people responsible for this was arrested However, in some instances cybercriminals can use the media as an exploit. People has used social media to set up scams, threat, or bully people, harassing people, and stalking other people online. For example, people being on social media more because of covid. These people see links on Instagram and those links ended up hacking you account.

Review of Literature

This problem has been studied in the past. It was studied in the past by collecting data from the past and looking at it. This usually looked for anything that stood out in that data. Cybercrimes have definitely been on the rise over years and the covid effects it has on people. According to Kranenbarg (2018) “computer hacking incidents recorded in Dutch police registration data has tripled between 2007 and 2017”. Kranenbarg looked at cybercrimes and regular crimes and tried to differentiate the two. He found that the person how commits the crime who has a partner is less likely to commit one. He also stated employment and enrollment are not related to each other when it comes to cybercrimes.

Cioban looked at the differences with adolescents’ deviance and cyber deviance. And found that they are somewhat related to a certain extent. Cioban looked at the behaviors. Hawdon looked at cybercrimes to see if they went up because of covid-19. Because of the lock down that happened in 2020, everyone was using computers more often. According to Hawdon (2020) “The change in our daily routines appears to have resulted in an abrupt drop in street crimes. However, the shift to the digital world undoubtedly creates new opportunities and platforms for motivated offenders to engage in various illegal activities.”. Hawdon also stated that “This shift should increase the number of suitable targets, as millions of people are confined to their homes and forced to work, study, and socialize online”.

Monteith also looked at the behaviors and cyber crime in while in the pandemic. According to Monteith findings “Human factors are a central component of cybersecurity as individual behaviors, personality traits, online activities, and attitudes to technology impact vulnerability.”. He also talked about it cybercrimes can have financial consequences. The OVC people looked at tech abuse with in the covid-19 pandemic. They worked with communities, agencies, and technology companies to gather data on this. According to the OVC people (Respondents reported an increase in every type of tech abuse during the pandemic. Mirroring findings about the most frequent kinds of tech abuse overall, harassment, limiting access, and surveillance were reported to have greater increases than impersonation.).

Research Themes

Some of the common things I saw when looking at the sources is that the trends for cybercrimes seem to go up over times. Another thing I saw is that every single one of my sources had crimes or acts for cybercrimes. The behavior people may have had something to do with cybercrimes as well. Cybercrimes in these sources looked at people’s behavior caused by cybercrimes in the mist of covid. Some of the challenges that these have face is that some of the data that was used had a lot of variables to it or some of the data collected from people may or not be true. For most of these sources since covid is a new topic and the data collect could be irrelevant if the pandemic gets under control and it is limited to a certain extent. The cybersecurity aspect on it will probably stay relevant even if covid became irrelevant. I think the methods the researchers used are pretty good and the overall collection of data is good.

Crime Theory

I think that the criminological literature provides evidence of utilizing any particular criminological theory The types of crime theories I saw while looking at the info was rational choice theory, self-control theory, strain theory, routine theory, and social learning theories. Some of the academic disciples that are involved in all of these are sociology and psychology. You can understand the problem better by analyzing the evidence they present in the research. The most prominent theories in this kind of research are routine activity theory, self-control theories, and social learning theory.

CJ policy and Implications

Some of the programs, initiatives, or policies exist to address the issue discussed wanted to bring this to attention to people and provide service to people. Some of them even used introduced plans for people and support them in some cases. The goal of the programs is to reduce and prevent any cybercrimes happening to anyone. The programs are usually implemented by government agencies and are funded by the government as well. Some of the programs used was doctoral programs by schools too. They are evaluated by studying the behavior people had and the technology people use to commit cybercrimes. The policies as a whole seem to be effective. They are different from previous crime control strategies because they actually rely on the technical side of things and people also need to have training in technical side of things.

Review/Report summary

In conclusion, I talked about cybercrimes and how cybercrimes are getting more prominent in these cases. I reviewed the current examples in society dealing with cybercrimes while covid is in effect. Then I looked at the problem/issue been studied in the past with cybercrimes during the covid. Moreover, I took a look at some of the common themes that emerge from the reviewed collection of literature from all of my sources. The last thing I also reviewed is the criminological literature support or provide evidence of utilizing any particular criminological theory and the programs, initiatives, or policies exist to address the issues.

References

Kranenbarg, M et al. (2018). Cyber-Offending and Traditional Offending over the Life-Course: an Empirical Comparison. Retrieved from

https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6428311/

Cioban, S et al. (2021). Adolescent Deviance and Cyber-Deviance. A Systematic Literature Review. Retrieved from

https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8546304/

Hawdon, H et al. (2020). Cybercrime in America amid COVID-19: the Initial Results from a Natural Experiment. Retrieved from

https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7286417/

OVC (2021). Tech Abuse in the Pandemic & Beyond: Reflections from the Field. Retrieved from

https://ovc.ojp.gov/library/publications/tech-abuse-pandemic-beyond-reflections-field

Monteith, S et al. (2021). Increasing Cybercrime Since the Pandemic: Concerns for Psychiatry. Retrieved from

https://link.springer.com/article/10.1007/s11920-021-01228-w