Did you know that 45 percent of cyber-attacks target small businesses? In this paper the first journal that was used was “Fighting cybercrime: A review of the Irish experience”. This journal was written by Catherine friend, Larraine Bowman Grieve, and Jennifer Kavanagh, they are all from the University of Ireland; this was published through July 2 – December 2020. The second journal that was used in this paper Is “rising trend of phishing attacks on corporate organization in cross river state, Nigeria”. This journal was written by John Thompson Opka from the University of Calabar, Benjamin Okorie from the University of Nigeria and Joseph Egidi Igbi from the University of Calabar. In these journals I will cover how the topic relates to the principles of the social sciences, the study’s research questions or hypotheses, and the types of research methods used. Additionally, I will cover the types of data and analysis done, how concepts discussed in class relate to the article, how the topic relates to the challenges, concerns, and contributions of marginalized groups, and the overall contributions of the studies to society.

The first article that was used was “Fighting cybercrime: A review of the Irish experience”. In this journal it relates to social science by showing how the Ireland crime legislation deal with cybercrime. For example, they deal with cyber crime by creating certain laws to lower the chances of cybercrime. One law that they have is called “Criminal Damage Act 1991”. This was supposed to cover property damage and data access, but it had a limited understanding motive, permission, and scope of property damage. The next thing that was put into place was theft and fraud act 2001, this covered data access and focused as an extending warranty. The journal stated that “it maintained ambiguous definitions of computer and operate and ignored mixed crimes”. The third thing that was put into places was “offences relating to information systems act” 2017. This introduced the term information systems an updated data

definition and acknowledge the intent of harm. The text stated that “it extended the scope of the attacks, the scope of data transmission, elements of social engineering and machine tools to do so well furthering corporate liability in data attacks”. The next thing that will be considered is the research question or hypothesis. The first research question is how is current cybercrime-related legislation perceived and utilized by digital security experts in Ireland? The second research question is what recommendations can be made to improve cybercrime related legislation in Ireland? The method that was used was a survey, this short qualitative survey was given to people online to professional digital working groups in Ireland through the first author’s twitter and LinkedIn accounts. The survey asked basic questions like “how does your work connect technology-related crime”, “do you/ your categorized collaborate with any other organization in approaching technology-related crimes”, and “where do you see the development of legislation against technology-related crime moving to in the future”? The data was qualitative analyzed using a thematic approach. The way that this journal connects with some of the thing that we learned is by showing how they use experiments, case studies, and surveys to determine the rate of these things happening and how they can go about fixing it. This topic relates to the concern of marginalized groups by showing how the legislative branch in Ireland is dealing with this problem of cybercrime. The overall contribution of this study is giving the government and the people a better understanding on why these things happened and what is put in place to stop people from doing these things.

The second journal that was used was “rising trend of phishing attacks on corporate organization in cross river state, Nigeria”. This journal is related to social science by showing how Nigeria have been dealing with phishing scandals. Nigeria has dealt with phishing scandals by carrying out case study like the study that Saudi, Ismail, Tamil, and indris carried out in 2007.

When they did this study it showed that the people knew about phishing scandals but they had a lack of knowledge on the topic. Another study that Yeboah-Boateng and Amanor did was a study on phishing, smishing, and vishing attacks against mobile devices in Ghana. This showed that men are more vulnerable to phishing attacks, because they tend to trust cyber space more than women. The type of research methods that were use was surveys that the cross-river state, Nigeria made. The data that was collected was qualitative data that was elicited using the in-depth interview guide. The article had this to say about the in-depth interview guide, “it is rich and insightful”. This connects with the content that we spoke about in class by showing the Nigerians use surveys to determine where they should go from here. This shows the challenges, concerns, and contributions of marginalized groups by showing how the effect that it has on the society in Nigeria. The overall contribution of this journal is to give us a better understanding on what phishing is, and how to stop it from happening to us.

In conclusion these two journals are a great source of information for on how people in other countries handle on cybercrime. In the first journal they talked about how the Irish fought against the cyberattacks. The second journal was about how in Nigeria they had a real big problem with phishing. After reading these two article I have learned how I can take control of this problem so it does not happen to me.