Article review 2 : ***Assessing the Credibility of Cyber Adversaries***

Assessing the
Credibility of Cyber A

Aiyianna Herndon

The major topic of this article was about being heuristic which is when humans look for guidance all the time and a way they look is by going on the Internet. Gaining relationships and social dynamics are huge topics that are talked about. A hypothesis that the author had was the more technology we have the more cybercrime we will have. As technology grows we see that more people using technology makes them more of a target for hackers. In class we discussed many topics and some of those topics are discussed in this article are gaining trust, deception, phishing, and learning human behavior.

Relativism was a huge topic in this article which is a Principles of Social Science topic. Being said talking about the political system like emails being hacked and turned into threats against the US. As well as the votes not being counted and the 2016 election being hacked by Russians. In addition to that we also had social media spreading the word for political rallies. Political laws against technology has increased because of so many hackers are not just hurting the little people but using political personal.

Cyberspace is a huge influence on behavioral dynamics and economic decisions. The research used shows how cybercrime is overseen against Internet citizens as deception. Cybercrime will decrease if we had less technology. The cybercrime is caused by hackers which are also known as cyber actors. These cyber actors are focusing on human behavior on the Internet. These cyber actors often look at someone's social behavior and those whom are looking for help or want attention from others. With that information they will gain a person's trust so they can get any data off their computer. The Author states that humans should focus on prevention strategies to protect citizens against phishing. In addition to that they think Instagram, Twitter, Facebook, video chats and many more social apps and sites are reasons why people have became easy targets.

In this article the research is based on Understanding Online Credibility, Prominence-interpretation, Cognitive Heuristics, and Characteristics. The author used multiple methods of data and research that shows how Social Network formed overtime which give others the conception that a user has an authentic account. Research show the different characteristics like Information characteristics, User Characteristics, and Interaction Characteristics which all falls down to gaining trust. Cyber actors with malice intent often use strategies like growing relationships, interacting and communicating with randoms to make them look authentic. But in all actuality they are phishing and profiling you to get your personal information.

Concepts discussed in class like phishing, deception, and trust are referenced many times in this article. Phishing in ways such as Identity fraud and making fake accounts on Social media sites and sending scam emails. Deceptions such as using false Wi-Fi Names and IP Addresses that could be similar to the common ones around you but in all actuality it is totally different. Hackers also collect your post, comments, photos, and even your searches together to use against you. These threats can be verbal or nonverbal and can harm you in many ways. So being predictable and sharing too much info on the Internet makes you an easy target.

An idea given was to limit to use of Internet to citizens. This gives people the question, "Does limiting access to certain communities reduce cybercrime?". Places like Northern Europe and North America are open to anyone being on the internet. While others are limiting the public to the use of the Internet or just forbid their citizens of such. All of this is a part ethical Neutrality in the world.

By the end of the article you will realize that cybercrime and social sciences are intertwined. The most common way is the Internet, and it is when cyber actors profile you. Hackers often use the things shared on Social media to learn about you so that they can gain further knowledge. With that knowledge they then use that against you to steal important information and documents such as passwords. This is an example of cybercrime and learning human behavior are connected.