**Chapter 4: Rise of the Trolls**

**By**

**Natnael Kebede**



**University of Dallas**

**2020**

This Paper Submitted in Partial Fulfillment of the Requirements for

CYBS 7359 – Penetration Testing and Vulnerability Assessment

Spring 2020

Presented to Dr. Renita Murimi

1. Research the distribution of cybersecurity incidents.

The distribution of cybersecurity incidents has been a significant concern. Some of the areas the widespread are notable include the following:

* The health of the U.S. economy: cybersecurity is strongly tied to the health of the U.S. economy. Due to this, malicious cyberattacks could cause chaos in the financial industry. In fact, The World Economic Forum estimated that cybersecurity incidents could cost as much as $3 trillion by 2020 (Kesan, n.d.).
* National security: cybersecurity is also strongly tied to national security. Critical infrastructures from power to transportation continue to be great attractions for incidents, with most of these systems being vulnerable to cyberattacks. We have seen ransomware attacks and shut down of these systems, leaving a nation in a dangerous situation (Kesan, n.d.).
* Private sectors: cyber incidents have been spreading in the private sector as well and have become inevitable. The incidents are caused by exploiting various vulnerabilities that reside in physical security, information systems, and people (Kesan, n.d.).
* Reputation: The distribution of cybersecurity incidents continues to be a prime cause of possible damage to reputation. This case has been evident in most company’s stocks going down, and their business slowing down following an attack (Kesan, n.d.).
* Various types of losses: The spread of cybersecurity incidents is usually followed by property damage, loss of income, loss of wages, fines, and penalties. Additionally, other costs are also paid by the victim company for violating regulation due to a cyber incident (Kesan, n.d.).

1. How does influence play a role in the hacker’s ideology and in that of the cybersecurity analyst?

Influence plays a role in the hacker’s ideology by allowing the individual to execute his or her evil plan for a personal gain or to commit a crime such as stealing sensitive information against a targeted victim user.

On the other hand, influence also plays a role in the cybersecurity analyst’s ideology. This case is possible by allowing the professional to identify, detect, and analyze biased harmful communications using known cybersecurity methodologies and take a resolution mechanism against these harmful intentions.

1. What is an account takeover?

An account takeover is a technique used by hackers who appear as fans and trick targeted users to click on links so that they can access these users’ computers. Once they get access, they can uncover personal secrets, or take over the users’ social media, compromising their account entirely. The hackers can also leak personal files to a media outlet. This scenario can result in the victim user losing his or her job, being hated by family members, and losing online supporters. That is, an account takeover can also result in the users’ audiences unfollowing the compromised account due to the fear of being hacked themselves.

1. What is the Turing test? What are social media bots? How are they passing the Turing test?

The Turing test is a challenge that was developed by Alan Turing to assess whether a specific machine can communicate and exhibit intelligent behavior equivalent to, or indistinguishable from, that of a live person.

Social media bots are programs that are defined by a computer algorithm to produce personas and content on social media applications that replicate a real human. They often perform with the goal of influencing the course of discussions and/or the opinions of audiences.

According to the author, social media bots are passing the Turing test since they can emulate real people. That is, the bots can create bogus accounts that mimic the conversations of a target audience around the world. Additionally, some bots can even automate spamming accounts that replicate the same message/s at a specific interval.

References

Kesan, J. (n.d.). Analyzing Cyber Incidents from a Risk Assessment Perspective. Retrieved from https://ciri.illinois.edu/sites/default/files/Seminar%20Slides\_Cyber%20Insurance%20Risk%20Assessment\_%20092617.pdf