

Tim Klein

03/19/2023

Professor Duvall

CYSE 201S

## Article Review 2

### “Elder Scam” Risk Profiles: Individual and Situational Factors of Younger and Older Age Groups’ Fraud Victimization

As online access and applications continue to integrate themselves into daily life, methods of exploitation also increase. While no one is truly safe from being targeted, people over the age of 60 are targeted at a disproportionately higher rate. This article is focused on cyber victimization and seeks to identify and study the social and psychological factors which contribute to the increased risk of being victimized online. This study seeks to better understand why the elderly are at a greater risk so that cyber policies and law may be adapted to better protect those most often victimized. The report mentions that collecting data on how often this age group of 60 year olds and up is difficult due to several factors like online fraud is not reported most of the time due to reasons of personal embarrassment but also potential fears of losing their personal autonomy over life choices. Self report studies give inconsistent results and feedback to the researchers. Researchers also interviewed different people who had been targeted by cyber crime to find similar connecting factors like how if the elderly person did not have any close family or friends then they were much more likely to be successfully scammed. The studies

were subjective in nature and relied upon self reporting and interviews mixed with demographic analysis. The individuals studied were separated into different groups largely based on age and whether they had been targeted for cyber crime. This article in a nutshell could be a textbook example study for cyber victimization studies and profiling. The article dissects how behavior in relation to online activities brings in additional risk factors and how the exploitation happens. Protecting our elderly population against cyber crime is extremely important due to how they are essentially the most vulnerable demographic for financial cyber crimes. Many are emotionally manipulated or coerced into giving over their finances which have taken a lifetime to build up. With the Baby Boomer generation heading into retirement age there is a huge demographic of the population which is increasingly at risk. By combining the understanding of what factors make the elderly vulnerable and which specific behaviors increase that risk then plans and education can be provided in the short term. Long term new technologies and methods may be created based on this research to provide better cybersecurity to a very vulnerable demographic.

#### [View of Designing Predictive Models for Cybercrime Investigation in Iraq](#)

Predictive analysis or PA, as the article refers to it, carries great importance in the future of cybersecurity because it seeks to solve the forthmost issue with the field, the constantly evolving and high paced online world. This article focuses upon the cyber crime vulnerabilities of modern day Iraq and its population. As the electronic device per capita metric increases the rates of cyber crime skyrocket with it. The population is targeted through these devices and predictive analysis seeks to find solutions through the right understanding and application of algorithms. The study researched through a combination of a literature review and

documentation review of a variety of separate studies. By analyzing the data yielded from global collective research on increasing a population's cyber security and studying how each algorithmic option operates for a future team to use the data to come up with a solution. The problem which the study is created around, how a developing society can increase its cyber security, shows how a social system is reacting to the need for cyber security in order to engage with a modern world. From the end user, the individual, to the collective population what protection systems may be implemented to create a more secure online environment. This information is critical to not only the people of Iraq, who fight the problem of being a developing online country against a well established cyber crime system, but to any other developing country which is seeking solutions to fighting cyber crime. The article concludes that since cyber security is such a large problem it requires a highly multidisciplinary approach. There needs to be the resources, systems, and political will in order to get the ball rolling. Predictive modeling shows the potential problems which may be faced and the understanding that AI predictive modeling and self troubleshooting are the options being looked at for developing nations to get security up to speed in the highly competitive online world.