Chapter 1
Predicting Cyber Security Behaviors Through Psychosocial and Demographic Conditions During COVID-19

Mololuwa Oluseyi Arogbodo
Bournemouth University, UK

Vasilis Katos
Bournemouth University, UK

ABSTRACT

This research examines the influence of demographic conditions on those psychosocial conditions resulting from the pandemic to predict cyber security behaviors. Multiple linear and logistical regression models showed that addicted users who barely worked from home before the pandemic are more likely to exhibit risky cyber security behaviors, which is also similar for lonely users who barely worked from home to predict internet addiction. One interesting finding is that addicted female users were found to be more susceptible to cyberattacks. The implications and recommendations focused on therapeutic interventions, social change, awareness campaigns, and so forth. The limitation of this study is also covered, and possible future research areas are recommended.

INTRODUCTION

The United Kingdom (UK) formally declared its first lockdown on the 23rd of March 2020 due to the rapid spread of Covid-19. The outbreak of coronavirus and the enormous lockdown measures have significantly changed people's way of living. When people were told to remain at home and maintain physical distancing, the lives of all citizens were affected. Humans are naturally social creatures, meaning that we all rely on social interactions to survive (Young, 2008). For months, people were neither able to go to work/school nor hang out with friends occasionally. What was unexpected was that the UK had over

DOI: 10.4018/978-1-6684-9018-1.ch001

3 lockdowns due to the pandemic, each with varying levels of restrictions (Zhou & Kan, 2020). Two years on, people's lives are not the way they used to be pre-pandemic, and the pandemic is still not over.

Due to the nature of humans, the observed lockdown regulations resulted to a mental and psychological breakdown of citizens. During this period, there has been an enormous increase in cyber-crime with criminals taking advantage of people's fears, resulting in Covid-19 being classed as the biggest threat to cyber security at the time (Panda Security, 2020). The rapid growth of the pandemic had severe impacts on living including mental and financial consequences. In a report by IBM (2020), the shift to work from home (WFH) model was found to have increased the average cost of a data breach by $137,000. Within the UK alone, reports claim that over £1.3 billion was lost to cybercrime activities between 1st of January and 31st of July 2021 (Scroxton, 2021).

More recently, Meyer (2022) states that British taxpayers could lose at least £4 billion of Covid-19 support funds to fraudsters and mistakes. These financial impacts and damage to victims highlights the relevance of psychosocial factors contributing to cyber security during the current crisis. The pandemic has undoubtedly changed the way people use technology, and there is evidence of people increasing their use of digital devices during the lockdown. While the adoption of new technology signifies growth among the population (Feldmann et al., 2020; Király et al., 2020), a major concern is the increased rate of problematic internet use (PIU) and internet addiction (Cellini et al., 2020; Garfinn, 2020).

Similarly, the pandemic along with its stay-at-home restrictions has cause people to feel depressed and lonely, the inability to participate in social gatherings caused people to get their social satisfaction online. Research conducted by Deutrom et al. (2021) highlighted the relationship between these two social factors. It also added Life satisfaction and how all three can be used to predict security behaviour during the pandemic. This current research follows on by examining the effect of demographic conditions in the existing predictions to give a more detailed insight on the cause of these behaviors. Considering that the effects of the pandemic are long-term and the increased demand for remote work, the findings of the research could be used to provide guidance for the new post-pandemic norm, or even similar future crises.

Aims

The primary aim of this research is to identify the demographic characteristics that affect psycho-social behaviors in predicting cyber security behaviors.

Research Objectives

- To review the existing literature on the overview of Covid-19, the lockdowns, and its effects particularly within the UK.
- To examine the status of cybersecurity before and during the pandemic. This gives room for comparisons, and effective analysis of the pandemic on cybersecurity sector in UK.
- To highlight the psychosocial impacts of the pandemic and its effect on cyber security industry in the UK.
- To analyze the already existing data acquired during the pandemic and create effective combinations and find statistically significant data of psychosocial and demographic factors.
- To create multiple regression models and determine its relevance to the stated hypothesis.
- To interpret the current findings and provided recommendations for businesses and government on how to minimise the effect of similar current/future events.