Cybercrime, Censorship, Perception and Bypassing Controls: An Exploratory Study

Ibrahim Baggili[1], Moza Al Shamlan[2], Bedoor Al Jabri[2], and Ayesha Al Zaabi[2]

[1] Tagliatela College of Engineering, Department of Electrical and Computer Engineering and Computer Science, University of New Haven, CT
Ibaggili@newhaven.edu
[2] Zayed University, College of Technological Innovation
Advanced Cyber Forensics Research Laboratory
m80001612@zu.ac.ae, {budur44,ayesha.alzaabi}@hotmail.com

Abstract. Countries have employed the Internet proxy as a censorship mechanism for various reasons. Concurrently, cyber criminal activities continue to rise. This research explores peoples' engagement in bypassing the Internet proxy and if it is related to cyber criminal engagement. Through an experimental design, participants were randomly assigned to three groups. Using manipulation paragraphs, in the first group (Group 1), a positive view on the Internet proxy was presented. In the second group (Group 2), a negative view on the Internet proxy was presented. The third group (Group 3) was used as the control group, where the participants' view of the Internet proxy was not manipulated. All three groups were asked to self-report their rate of proxy bypass (SRPBE) and cybercrime engagement (CCI). The results indicated a significant positive correlation between self-reported cyber criminal engagement and self-reported proxy bypass engagement. The results also showed that individuals with more knowledge in computers are more likely to bypass the Internet proxy. However, individuals with better knowledge in computers are not necessarily the ones that are more likely to commit cyber criminal activities. The results were inconclusive on whether or not the manipulation paragraphs used had an effect on the participants' view of the Internet Proxy.

Keywords: Cybercrime, psychology, censorship, Internet proxy, UAE.

1 Introduction

With time the Internet continues to grow. More users today are engaged in the World Wide Web and are actively infused with this technology. The Internet World Stats website reveals the number of increasing Internet surfers in different regions of the world. Data also reveals that there are about fifty seven million surfers in the Middle East alone. In the case of the United Arab Emirates (UAE), it was determined that it has the fifth highest number of Internet users amongst other Middle Eastern countries [1]. Furthermore, it is one out of a number of countries that applies an Internet proxy to censor Internet content.

The reasons behind the employment of an Internet proxy may vary. In the UAE, the purpose could range from religious, to social, to political reasons [2]. One of these

M. Rogers and K.C. Seigfried-Spellar (Eds.): ICDF2C 2012, LNICST 114, pp. 91–108, 2013.

reasons could also be to prevent cyber criminals from accessing and downloading hacking and exploitation tools. For example, when attempting to visit the website http://remote-exploit.org, a website that contains software that could be used for malicious purposes, we find that the Internet Proxy in the UAE prohibits access to such a website. If a primary reason for censoring Internet content is to prohibit users that are actively engaged in cybercrime from downloading hacking tools and content, it becomes important to investigate the relationship between bypassing the Internet proxy and cybercrime engagement.

Internet censorship remains a topic of debate despite the many reasons behind why an Internet proxy is applied. In the UAE for instance, Sheikh Abdulla Bin Zayed, Minister of Information and Culture is in favor of an open Internet, for he states that the UAE's Internet Service Providers should not block access to websites because every citizen is entitled to knowledge and learning [3].

Due to the restricted Internet access in the UAE, it is hypothesized that users may engage in ways to bypass the Internet proxy. The purpose and intentions behind such user activity is yet to be empirically examined. Understanding this relationship can shed light on the effectiveness of the Internet proxy, and whether it is fulfilling the purpose of evading cyber criminals from accessing illegal content.

2 Problem Statement

One of the reasons of employing an Internet proxy is to not only censor illegal content, but also to curb cyber criminal engagement. Currently, there is no formal published research that studies the relationship between cyber criminal engagement and proxy bypass engagement. It is important to study this relationship in order to validate the productivity of the Internet proxy.

3 Research Questions and Hypotheses

In this study, the researchers attempted to answer the following questions:

- Is there a relationship between Self Reported Proxy Bypass (SRPB) and cybercrime engagement?
- Is there a relationship between the level of knowledge in computers and SRPB?
- Can respondents be manipulated using manipulation paragraphs to affect their perception of the employment of an Internet proxy?

To answer the abovementioned questions three major hypotheses were formulated:

- H1: There is a positive correlation between self-reported cybercrime (CCI) and self-reported proxy bypass engagement (SRPB).
- H2: Individuals with better knowledge in computers are more likely to bypass the Internet proxy and engage in cybercrime.
- H3: Decreasing the positive perception of the Internet proxy increases self reported cybercrime and proxy bypass engagement.