Cybersecurity and Online Privacy: Impact of Content Filtering and Blacklisting on Cyber Security and Online Privacy

Information Communication Technology has taken over the majority of personal day to day activities such as shopping, working, and gaming. The increased reliance on information technology has left the society prone to significant security challenges on their IT infrastructure. Events such as network outages, virus attacks, data compromise, and hacking have increased proportionally to the number of mobile, application and data networks. Cyber security is the protection of computers, applications, networks and data from unauthorized users for alteration or destruction (Graham, Howard and Olson 1). Online privacy defines an entitlement to confidentiality in storage, processing, sharing and display of personal information on the internet. With the extensive use of ICT infrastructure by individuals, organizations and governments, massive amounts of information are collected, processed and stored on these systems. This includes confidential information and critical process information being transferred or stored across networks or in storage in network devices (Singer and Friedman 7). The increasing threat and sophistication of cyber-attacks demands a continuous and evolutionary process for guarantee protection of critical personal and business information as well as mitigate any national security challenges that may rely on ICT systems (Cavelty 2). New users of ICT infrastructure ought to be aware of the potential threats posed by this platform and some rudimentary mitigation steps in case of an attack. Further, novice users must also know of using technology platforms that match their skills and authorization.

In this study, the author pursues to understand the impact of content filtering and blacklisting on cyber security and online privacy. In the course of this project, the author expects to examine and critically analyze diverse cyber security threats, understand their sources, causes, applicable mitigation measures and the success of these measures. Particularly, the author also expects to gain a greater understanding of the filtering and

blacklisting methods commonly used in ICT, evaluate their contribution to reducing the threat and suggest probable improvements that can reduce user exposure. The prevailing assumption in this study is blacklisting, and filtering is most applied approaches to ensuring online privacy and reducing cyber security threats. In the assessment of the challenge, the study will use two parallel systems with one running with filters and blacklists enabled while the other will run unprotected. Measurements for the number of virus attacks, network outages, the amount of spam traffic and unauthorized system access will be taken from both systems for comparison through a side-by-side technical evaluation to determine the effectiveness of content filters and blacklists.

The view of the writer is that the use of filters and blacklists on known sources of malicious traffic is an effective way of reducing cyber-attacks and improving online privacy. When the respective apparatuses are used correctly, the rates and exposure to cyber-attacks will drop. The study will seek to convince readers that;

a. The use of suitable security applications ensures that all inbound and outbound traffic is vetted and authenticated before access is granted.
b. The use of network management applications is an effective way for filtering and control of network traffic.
c. User awareness is crucial in the protection of network content.
d. Ethical standards for use of technology systems.

A critical consideration of these points will enable readers to understand the types of threats posed by cyber-attacks and the most applicable tools for handling of such threats. It will also highlight the critical role played by individual users above the measures taken by network experts in ensuring that the networks and transit data remains secure (Kaiser n. pag.). Further,

it will also enlighten users on the acceptable standards in interaction with technology platforms.

In the study, I wish to work with my Information Technology professor. My choice of a mentor is informed on their knowledgeability on the theoretical and technical aspects of technology. The professor is also among the most respectable and experienced members of the faculty in matters technology. These traits will be essential in providing guidance and direction in new areas as well as an expert opinion on the study, the progress and the results obtained. The anticipated duration of the study is two months – first two months of the semester – that will cover both the research and writing of the project thesis. The first six weeks will be used in preparation for the research, implementation of the study and assessment of the obtained results. In the last two weeks, the thesis outlining the findings, conclusions and recommendations will be prepared. To accomplish the objectives of the study, I will require;

i. Two computers
ii. Internet connection
iii. Network management applications
iv. Blacklisting applications

The references for the study will be books, journal and news articles on the subject of cybersecurity and online privacy. The references will be identified through context filtered searches from the university's library resources. I will also seek help from my mentor on items they find might be useful for the study.

Works Cited

Cavelty, Myriam Dunn. "Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities." *Sci Eng Ethics* (2014): 701 - 715. Print.

Graham, James, Richard Howard and Ryan Olson. *Cyber Security Essentials*. Boca Raton, FL: Auerbach Publications, 2011. Print.

Kaiser, Michael. *It's Data Privacy Day, and Consumers Are Concerned About Their Online Privacy*. 28 January 2016. Online. 29 January 2016. <https://staysafeonline.org/blog/its-data-privacy-day-and-consumers-are-concerned-about-their-online-privacy/>.

Singer, P W and Allan Friedman. *Cybersecurity: What Everyone Needs to Know*. Oxford: Oxford University Press, 2014. Print.