Talk to me, and take care: Unleashing the power of word of mouth to increase cyber safety.

Dipakkumar P Pravin
University of North Texas
Dipakkumar.Pravin@unt.edu

M A Shariful Amin
University of North Texas
mashariful.amin @unt.edu

Extended Abstract

Over the last 30 years, significant technological advancements have transformed the digital society we live in, influencing every aspect of our lives. These changes have resulted in increased interaction with our digital community, known as the "cybervillage," but have also introduced the potential for real-life compromises. Despite the satisfaction of our inherent needs through these advancements, we lack the corresponding awareness of the associated threats, leading to inadequate safety measures even with government and industry-led cybersecurity awareness efforts. We integrated Theory of Reasoned Action Approach with the UK based *MINDSPACE* concept to develop a conceptual research model. Thus, this study proposes the utilization of "Trusted Cyber Messengers" to directly communicate threat awareness and mitigation measures to individuals in their personal networks, with the aim of creating a safer cybervillage. The findings of this study will serve to develop effective strategies for promoting cybersecurity awareness through word-of-mouth channels, contributing to the overall goal of mitigating risks associated with the use of digital technologies.

Introduction

Despite the internet's 3 decades of widespread prevalence among a large percentage of the US (and world) population, the incidents of cybercrimes continue to grow (Zagaris, 2019; Amin and Pravin, 2021). This is as if, either no one is aware of the crimes, or they do not know what to do. The governments around the world are aware of the situation and have launched a variety of awareness campaigns (van Steen et. al) in the hope that the awareness will lead to appropriate actions, but there is no evidence that this is the case (van Steen et. Al., 2020; Bada et. Al., 2019).

In 2022, FBIs, (ic3.gov) Internet Crime Complaint Center's reported a total of 800, 944 complaints that is 2,194 every day, and one every 39 seconds! The total victim losses in 2022 it was $10.3 billion. These numbers are staggering by themselves while the actual pain and stress felt by the victims would be impossible to know. The top 10 crimes by victim loss per the report are as follows: (1) Phishing/Vishing/Smishing/Pharming. (2) Non-Payment/Non-Delivery, (3) Extortion, (4) Personal Data Breach, (5) Spoofing, (6) Business Email/ Email Account Compromise, (7) Confidence Fraud/Romance, (8) Identity Theft, (9) Harassment/Threat of Violence, (10) Overpayment. We believe the incidents from categories (1) (4) (5) (6) & (8) can be drastically reduced by increasing the awareness of the crimes' prevalence, ways to recognize it and knowledge of actions to be taken.

We believe it is time to use the word of mouth from "Trusted Cyber Messengers" to take the awareness message directly & in-person to induce actions. A Cyber Messenger knows/learns effective practices to stay safe online and then they teach the same to a few selected people in their own sphere of influence. Thus, such a campaign is more direct and personal, and it imparts not just awareness but demonstrates actions to be taken and demands/requests action from the target. "Trusted Messengers" have been used effectively in the healthcare context (Asfaw et al., 2019; Kritz, 2020; Phase 3, n.d.), we want to understand if we use "Trusted Cyber Messengers", will it be effective in the cybersecurity context. Therefore, in this

study we investigate the existing theories that help in understanding the required characteristics of the trusted cyber messengers' effectiveness to induce action through awareness.

Model Development

The primary goal of cyber security awareness programs is to influence the safe online behavior and proper adoption of the online platform (Koh et al., 2019; Burns & Roberts, 2013). As per Rogers (1985) effective influencing requires more than just educating people about what they should and should not do such as firstly, they need to understand and agree that the data is important, secondly, they need to understand how they should react, and finally, be prepared to face many other consequences or demands (Witte, 1993).

The 17 "awareness campaigns" studied by van Steen (van Steen et. Al. 2020) are focused on providing static messaging to the general public without any specific follow through to measure campaign's effectiveness or campaign's ability to bring actions from the targeted population. Another reason for ineffectiveness of awareness campaigns is that they may be perceived as "impersonal and so general as to apply to any audience" (Wilson M. & Hash J, 2003, NIST 800-53).

There are multiple models of behavior theory and models that have been applied in the cybersecurity. For instance, the Theory of Planned Behavior (TPB) (Burns and Roberts, 2013), Deterrence Theory (DT), Protection Motivation Theory (PMT) (Vance et al., 2012), the Health Belief Model (HBM) (Davinson and Sillence, 2010) and Threat Avoidance Theory (Liang, 2010). To be effective in changing vulnerable behaviors and lower cyber-security threat the attitude towards cyber messenger is critical (Dolan, 2010). Currently, little is known about the users' attitude towards cyber messenger and improving cyber messenger effective communication with users to enhance cybersecurity threats (Coventry et al., 2014).

Affecting a user's behavior is a difficult endeavor for anybody let alone society or even government except in emergency through a fiat or stringent law. A study from UK Cabinet Office's Institute for Government (Dolan, 2010) reports "we set out nine of the most robust (non-coercive) influences on our behaviour, captured in a simple mnemonic – MINDSPACE – which can be used as a quick checklist when making policy. "The factors are as follows: Messenger (trust the message based on who is delivering it); Incentive (direct benefit), Norms (what others do); Defaults (go with the flow); Salience (novel & relevant; Priming (unconscious cues); Affect (emotional association); Commitment (keep public promises), Ego (act to feel better). Part of our motivation for TCM comes from this study. We believe our Trusted Cyber Messenger based approach will influence at least these factors: Messenger; Norms, Salience, Priming, Affect & Commitment.

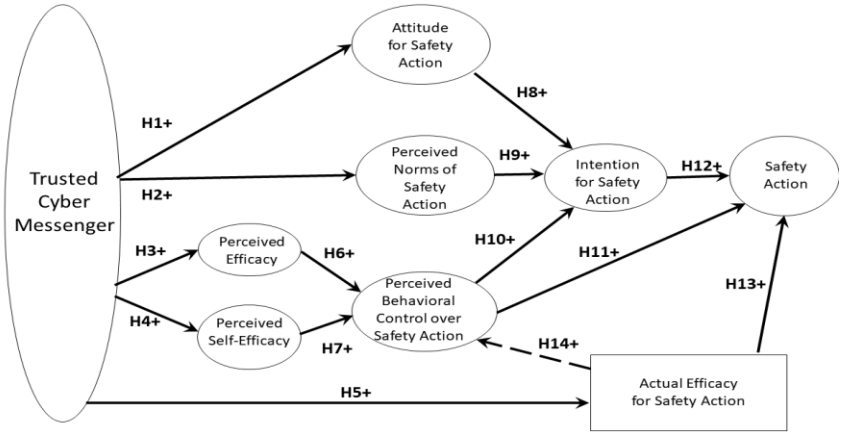

Figure-1: Conceptual Research Model: Trusted Cyber Messenger (TCM) an individual inducing safety actions by the target individual.

We have built our research model by compacting some constructs in the Theory of Reasoned Action Approach (TRAA) (Fishbein & Ajzen, 2010; Fishbein, 1979). Our approach is to be in-person to influence a target's Attitude towards action, Perceived Norm, Perceived Behavioral Control (thru Perceived Action Efficacy and Perceived Self Efficacy) and Actual Efficacy (by imparting new skills and abilities).

Support for the effectiveness of TCM idea comes from these observations (Bada et. al., 2019) (A) Helping people form new thought patterns (and habits) works, (B) A trusted messenger is more likely to be aligned with the target's cultural and societal norms, (C) Many of the government awareness campaigns do not have accompanying helpline, which TCM provides due to the existing relationship, and (D) According to Protection Motivation Theory, target's action would depend on their appraisal of threat and self-efficacy.

Expected Contributions

This study will provide both theoretical and practical contributions to the area of "how to change cybersecurity safety practices of populations from various demographics." From a theoretical perspective, our paper will provide a conceptual model to understand the role of trusted cyber messenger in cybersecurity information dissemination and effectiveness of such a method. From a practical point of view, our analysis will lead to the creation of a new model to explain effective role of trusted cyber messenger.

References

Asfaw, S., Morankar, S., Abera, M., Mamo, A., Abebe, L., Bergen, N., ... & Labonté, R. 2019. Talking health: trusted health messengers and effective ways of delivering health messages for rural mothers in Southwest Ethiopia. Archives of Public Health, 77(1), 1-8.

Amin, M. A., Pravin, D., & Dipakkumar, P. (2021). Trusted Cyber Messengers: Spreading Awareness to Induce Actions.

Bada, M., Sasse, A. M., & Nurse, J. R. 2019. Cyber security awareness campaigns: Why do they fail to change behaviour?. *arXiv preprint arXiv*:1901.02672.

Burns, S., & Roberts, L. 2013. Applying the theory of planned behaviour to predicting online safety behaviour. *Crime Prevention and Community Safety*, 15(1), 48-64.

Davinson, N & Sillence, E 2010. It won't happen to me: Promoting secure behaviour among internet users. *Computers in Human Behavior* 26(6):1739-1747.

Dolan P., Hallsworth, M., Halpern, D., King,D., Vlaev, I.: MINDSPACE Influencing behaviour through public policy, Institute for Government, Cabinet Office, (2010). http://www.instituteforgovernment.org.uk/sites/default/files/publications/MINDSPACE.pdf

Fishbein, M. & Ajzen, I. (2010). Predicting and changing behavior: The Reasoned Action Approach. New York: Taylor & Francis.

FBI, IC3.GOV. 2019. https://ic3.gov/Media/PDF/AnnualReport/2019_IC3Report.pdf

Glaser, C. L. (2011). Deterrence of cyber-attacks and US national security. The George Washington University Cyber Security Policy and Research Institute.

Koh, B., Hann, I. H., & Raghunathan, S. 2019. Digitization of music: consumer adoption amidst piracy, unbundling, and rebundling. MIS Quarterly, 43(1), 23-45.

Liang, H., & Xue, Y. L. 2010. Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the association for information systems*, 11(7), 1.

Kritz, F. (2020, December 24). 'Trusted messengers, Trusted Messages': How to Overcome Vaccine Hesitancy. Retrieved February 20, 2021, from https://www.npr.org/sections/health-shots/2020/12/24/948776228/trusted-messengers-trusted-messages-how-to-overcome-vaccine-hesitancy.

Rogers, R. W. 1975. A protection motivation theory of fear appeals and attitude change1. *The journal of* psychology, 91(1), 93-114.

Vance, A., Siponen, M., & Pahnila, S. 2012. Motivating IS security compliance: insights from habit and protection motivation theory. *Information & Management*, 49(3-4), 190-198.

van Steen, T., Norris, E., Atha, K., & Joinson, A. 2020. What (if any) behaviour change techniques do government-led cybersecurity awareness campaigns use. *Journal of Cybersecurity*, 6(1), tyaa019.

Wilson, M. & Hash, J. NIST [800-53] NIST: Building an Information Technology Security Awareness and Training Program. Computer Security Division Information Technology Laboratory. October 2003. http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf

Zagaris, B. 2019. Cybercrime and Fraud. IELR, 35, 351.