**Security anxiety**

<https://www.sciencedirect.com/science/article/pii/S0747563215300698>

**Survey**

<https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2328022/pdf/canfamphys00201-0076.pdf>

**Security awareness**

“According to Ng, Kankanhalli, and Xu (2009), information security education including security education, security training, and security awareness programs will influence users to become more security conscious.”

<https://d1wqtxts1xzle7.cloudfront.net/46834988/Information_Security_Awareness_Campaign_20160627-30002-134m17f-libre.pdf?1467048018=&response-content-disposition=inline%3B+filename%3DInformation_Security_Awareness_Campaign.pdf&Expires=1695008557&Signature=FTLNQAwKoe4~W8Zueld2kwJoy2oUeaOIWEcjpjo2t3CYz2gstuLe0Y1jMq0Rd5joXDDdyBIYcLx7U9g-V3a9-lONlB50UDzaF724DzrlFzdKHgPW-Zlr0BLGFJyDo7sURv4f983wammLPHOEy2ET23h920jkrgNOMsmQMLPpX266iwft39yg3ChyPLlMz6okHQ~ZLhlD9SjOcAZiywXtqeC-TyKiG4G33q09ihD1ul-d5zrq1rKVSb2eS~4TMfO-6yhpQswuLs3OXQbTryHsnJVR1AWPgj3j4p1BOYqH74P8ecfWZ4snRLpL~xgfT0qKZYRTrtArHOxt3SLOs6-5HQ__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA>

In this article, the author aims to create an effective security awareness campaign by considering the application of healthcare and environmental safety awareness. Security awareness is defined as “the extent to which every member of staff understands the importance of information security, the levels of information security appropriate to the organization, their individual security responsibilities, and acts accordingly” in this article. According to the author, this definition best describes security awareness in relation to behavior. Therefore, by this definition, an individual who is aware of information security exhibits behavior that reflects this awareness.

The author highlights the important difference between healthcare awareness and security awareness. Firstly, being ignorant of health-related awareness campaigns usually affects only one person. However, ignoring information security awareness not only affects the individual, but the whole network of computers they are connected to and consequently their organization. Additionally, participants of healthcare campaigns are usually a population of the general public. On the other hand, participants of information security awareness are employees of an organization.

The article analyses the success of the Information-Motivation-Behavioral model in relation to HIV and AIDS. This model is based on the belief that an individual’s behavior is based on the extent to which they are well informed and motivated to perform or change a behavior. The author concluded, based on research on related work, that the IMB model is more effective at producing desired behavior in comparison to campaigns that are based purely on knowledge. As it relates to information security, the IMB model can be implemented by providing avenues for individuals to gain knowledge about information security. These include but are not limited to presentations, magazines, etc. Furthermore, an effective IMB information security campaign should motivate individuals to behave according to the organization’s policies. However, this should be done by ensuring that employees are aware of the benefits of practicing information security behavior. A focus on employee benefits rather than strict “do’s and don’ts” will be more effective at creating positive behavioral changes. Individuals can also be motivated on a social level by making the campaign more social through more informal and discussion-based meetings that prioritize conversation over one-way communication.

Normative feedback, also referred to as normative social norms, has proven to be effective in environmental awareness as it relates to recycling. According to the author, this method involves “(1) procedural knowledge that gives information about when, how and where to recycle? (2) Impact knowledge that refers to an individual’s belief about the consequences of recycling and (3) normative knowledge is the belief about behaviors of others.”

In case of information security campaigns, descriptive and injunctive social norms (normative knowledge) can be induced in the campaigns by describing the acceptable information security behavior and by giving examples of the colleagues in the organization who perform information security conscious behavior so that the audience are motivated in adopting information security behavior. To implement this method in information security campaigns, the author states that it is important for the campaign to include social interaction. He suggests that leaflets should be distributed with figures of the improved information security environment of other organizations and improvements in their colleague’s performance in relation to information security as well. Additionally, he suggests that it should highlight how information security behaviors have benefitted other organizations as well as their colleagues. According to him, this knowledge of other’s behavior causes normative belief which can then change the behavior of the employees of an organization.

Conclusively, the author proposed a model that focuses on normative knowledge in collaboration with the IMB model. In this model, the normative knowledge replaces the information component of the IMB model to create an effective security awareness campaign.

<https://connections-qj.org/system/files/3401_tasevski_awareness.pdf>

This article dives into cybersecurity awareness in Macedonia, analyzing existing campaigns, activities, and strategies, and then providing recommendations on how these campaigns can be improved for end-users. This article will be useful in my research as it can provide a basis on which a new cybersecurity awareness campaign can be created effectively. According to the article, current security awareness programs aim to “prevent exposure on Internet, hate speech, network security, secure passwords, hacking, etc” by providing “tips, guides on websites, caravans, posters, interactive videos, etc.”. Further analysis on current initiatives revealed that participants believed that education on topics such as “: increasing security – which sites are not safe; cyber attacks and statistics; hate speech on the Internet; social networking privacy awareness; abuse of personal information; secure usage of mobile phones; etc” is necessary. The authors recommended that Information Technology Foundation for Education (HITSA) should be used as a basis for increasing information security awareness in Macedonia. They state that in doing this, it is important to highlight the weakest link in cybersecurity; the end-user. By doing this, a cybersecurity culture can be developed which can be followed by awareness, education, training, and campaigns. Based on this, they stated that interdisciplinary training would be valuable in aiding the nation to deal with the emerging cybersecurity threats. Along with this, they state that continuous training should be implemented to equip professionals to face evolving technology and consequent threats.

\*\*\* <https://iopscience.iop.org/article/10.1088/1757-899X/263/4/042043/pdf>

This article is based on a survey conducted inTamil Nadu by that focuses on security threats including “email, virus, phishing, fake advertisement, popup windows and other attacks in the internet.” This article is useful for this study as it can provide a basis on how to effectively measure cybersecurity awareness among the participants in the study. The study was done by conducting a survey among college students, one hundred from five different cities. Their survey focused on different topics including user ID and password awareness, home computer protection, installation and updating of firewall and antivirus software, and awareness of viruses. Their analysis of the survey results considered users’ awareness of virus attacks from unknown sources, “email/Message phishing, password attacks, and threats for publishing personal details in social networking sites” (misuse of social networking sites).

<https://www.researchgate.net/profile/Margit-Scholl/publication/357166000_The_Current_State_of_Information_Security_Awarenes_in_German_SMEs/links/61bf2175a6251b553acc3c5c/The-Current-State-of-Information-Security-Awarenes-in-German-SMEs.pdf>

**Motivation**

\*\*\* <http://jise.org/Volume23/n4/JISEv23n4p407.pdf>

This article examines factors that motivate college students’ information security behaviors. The Protection Motivation Theory (PMT), integrated with social norms and habit factors are used as the framework for this study. This study will be useful in the current behavior as it can provide a basis for which participants’ motivation to perform secure habits is examined. **LOOK INTO PMT.** Security habits can be defined as “learned sequences of acts that become automatic responses to specific situations which may be functional in obtaining certain goals or end states” (Verplanken, Aarts and Van Knippenberg 1997; Limayem, Hirt and Cheung 2003). The performance of these habits requires little minimal mental effort and attention and are therefore performed almost automatically. By extension, security behavior can be defined by a continuous practice of security habits. Constructs for the design of the study include: “perceived vulnerability, perceived severity, response efficacy, response costs, and self efficacy, which are variables derived from PMT and subjective norm construct to measure the affect of a student’s intention to practice information security.” The study was conducted by surveying students from a university in South Korea and included a questionnaire that measured all items using a seven-point Likert scale, with responses ranging from “strongly disagree” to “strongly agree.” The study yielded results that were both reliable and valid based on t-values and composite reliability and thus proposed a research model based on PMT, including subject norm and habit factors

“The results of this study revealed that PMT is a valuable model for predicting students' information security behaviors. Particularly, response efficacy and self-efficacy were found to have a strong impact on students’ intentions to practice information security. These results suggest that students will make more of an effort to apply information security and thus experience high levels of confidence in doing so when their efforts are perceived as being effective and practicable. Conversely, response cost has a negative impact and perceived vulnerability has no significant impact on motivation to practice information security. Although security behaviors may first begin due to awareness of external threat or the surrounding pressure on information security, motivation towards information protection becomes routine and habitual over time based on the experiences of that repeated behavior”

**Protection Motivation Theory (PMT)**

<https://www.mdpi.com/1805742>

<https://www.sciencedirect.com/science/article/pii/S0747563215000539>

**LOOK AT HITSA**