**Security anxiety**

<https://www.sciencedirect.com/science/article/pii/S0747563215300698> (1)

It is common knowledge that everyone’s data can be vulnerable, and this may lead to fear and anxiety. This article aims to determine the anxiety and stress that is associated with the possibilities of internet hacking. The study utilized an online survey with a sample of 304 adult participants. The article reported that a recent Pew research poll of 607 Americans revealed that 91% of respondents are concerned that they have lost control over the collection and use of their electronic data are collected (Kedmey, 2014, November 12). More than half of respondents reported feeling insecure about sharing private data on social media, through instant/text messaging, or email (Madden, 2014, November 12). Additionally, the poll revealed that older adults are more likely to perceive technologies such as social media and instant messaging as insecure. Another Pew poll, of 498 adults, found that most respondents do not feel confident that their data are being protected by the government or private industry (Madden & Rainie, 2015, May 20). These results are consistent with a recent global survey of more than 23,000 people in 24 countries, finding that two-thirds of the sample reported being more concerned about online privacy than they were a year ago (Centre for International Governance Innovation & IPSOS, 2014, November 14). These concerns lead to an inevitable growing recognition of the importance of better internet security behavior. (Nazareth & Choi, 2015). “The Pew poll found that 6 in 10 respondents indicated an interest to do more to protect the privacy of their personal information online (Madden, 2014, November 12).” This study focused on two research questions, namely: “1) Are people's perceptions of the scope and impact of data breaches associated with emotional distress, such as stress or anxiety? And 2) Does securing one's online accounts help alleviate stress or anxiety associated with these data breaches?” The study found that “ratings of data breach anxiety were somewhat higher than that of resting anxiety. (worry, anxiety or stress reported at the beginning of the survey).

<https://journal.uii.ac.id/inCAF/article/view/27411/14689> (2)

This study aimed to test the relationship between perceived threat and anxiety on coping behaviors (protective action, seeking help, avoidance) of e-banking users in Kebumen Regency. One hundred and twenty one research samples were obtained by distributing questionnaires via a google form for this study. The questionnaire five variables including:

* Perceived Threat - Anxiety felt by internet users because they have no resources to face the threat - Chen & Zahedi(2016)
* Internet Anxiety - A condition of an individual who has concerns and anxiety within him/herself while using an internet. Anxiety means fears of losing valuable personal data - Wachyudy & Sumiyana(2017)
* Protective Actions - Individuals’ action to protect themselves from attack or threat in facing problems - Chen & Zahedi(2016)
* Seeking Help - The condition of individuals who request the assistance by looking for information or advice about the threats or problems encountered - Chen & Zahedi(2016)
* Avoidance - The condition of individuals who prefer avoiding internet security threat rather than facing it - Chen & Zahedi(2016)

Results showed that perceived threat and internet anxiety influenced the coping behaviors or e-banking users. The findings did not show any effect of perceived threat on avoidance.

<https://www.sciencedirect.com/science/article/pii/S0747563205000397?casa_token=EGQHpBhnKn8AAAAA:UT_2TzWH-7yP5aZRcRb2vY9b0Zx2KD9V9ZZB47X3DvcEKQZnhdwyA7TVyhALcMY8_GSu3fP8uQ> (3)

This paper examined the results of a study that investigated the relationship between Internet identification, Internet anxiety and Internet use.

A scale was developed to measure Internet anxiety and was based on a scale designed to measure computer anxiety ([Brosnan and Thorpe, 2001](https://www.sciencedirect.com/science/article/pii/S0747563205000397?casa_token=EGQHpBhnKn8AAAAA:UT_2TzWH-7yP5aZRcRb2vY9b0Zx2KD9V9ZZB47X3DvcEKQZnhdwyA7TVyhALcMY8_GSu3fP8uQ#bib5), [Thorpe and Brosnan, 2001](https://www.sciencedirect.com/science/article/pii/S0747563205000397?casa_token=EGQHpBhnKn8AAAAA:UT_2TzWH-7yP5aZRcRb2vY9b0Zx2KD9V9ZZB47X3DvcEKQZnhdwyA7TVyhALcMY8_GSu3fP8uQ#bib37)). The students were asked six questions (shown below) and answered using a five-point Likert Scale (Cronbach *α* = 0.77).

* 1. I always feel anxious when using the Internet.
* 2. I go out of my way to avoid using the Internet.
* 3. It is easy for me to use the Internet.
* 4. It is important for me to be able to use the Internet.
* 5. My anxiety about using the Internet bothers me.
* 6. I am more anxious about using the Internet than I should be.

**Security awareness**

<https://www.researchgate.net/publication/220849938_Information_Security_Awareness_Campaign_An_Alternate_Approach> (4)

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> (5)

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> (6)

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 on 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> (7)

topics used in the study include passwords, phishing (and related areas), data protection etc, social engineering, manipulation, etc., apps, software, etc., security in the home office, data protection in the cloud as well as in the context of customers and suppliers, messenger services, secure transmission, storage, encryption, etc., information classification.

<https://www.sciencedirect.com/science/article/pii/S0747563215000539> (8)

This study aims to examine the effect of knowledge in information security on the detection of intrusions in a simple network. A simplified Intrusion Detection System (IDS) was developed to allow for the examination of how individuals with or without knowledge in cyber security detect malicious events and declare an attack based on a sequence of network events. Results indicated that more knowledge in cyber security facilitated the correct detection of malicious events and decreased the false classification of benign events as malicious. The study involved fifty-five novice participants and twenty security professionals. A short questionnaire was created to differentiate between these two populations. This questionnaire assessed domain knowledge through questions on network and information security, evaluating two independent dimensions: theoretical knowledge (participants’ familiarity with the definition of technical terms, cyber-attacks and the use of network security tools) and practical knowledge (working experience – by stating years of experience and level of interaction with an IDS). An IDS-tool was used to present scenarios, with a new event appearing on screen every ten seconds. Participants classified each event as attack or no-attack as they appeared. Following this, participants determined if the entire network scenario represented a cyber-attack and stated their confidence in their answer.

The study found that 100% of the experts had theoretical knowledge compared to 36% of the novices, though a relatively high proportion of novices (85%) knew the right definition of phishing attacks (possible attributed to the fact that phishing attacks target end-users, compared to a DoS attack for example, that targets a network). Results revealed that the experts “classified a significantly larger proportion of the malicious network events as threats and a significantly lower proportion of benign events as threats compared to novices.” Based on the results, the authors concluded that analysts should be trained to quickly learn and adapt to novel and dynamic environments. Also, they state that “considering the increasing number of personal networks that end-users deploy by themselves (e.g., home network), the growing number and variety of devices connected to these networks (e.g., computers, smartphones, tablets, media smart-TV, etc.) and their complexity, intrusion detection can become a concern of many end-users without extensive domain knowledge in information and network security.”

<https://www.scielo.org.za/scielo.php?pid=S2077-72132017000100007&script=sci_arttext> (9)

The research presented in this article aimed to assess the levels of CSA among students at a private tertiary education institution in South Africa. A questionnaire tested students in terms of four variables: cybersecurity knowledge; self-perception of cybersecurity skills, actual cybersecurity skills and behaviour; and cybersecurity attitudes. The questionnaire included six sections:

* section 1: The student's demographic information
* section 2: the student's online usage
* section 3: the student's cybersecurity knowledge
* section 4: the student's self-perception of cybersecurity skills
* section 5: the student's actual cybersecurity skills and behaviour
* section 6: the student's cybersecurity attitudes.

The study found that increasing cybersecurity awareness can decrease the number of victims of cybercrime. The author stated that there is a need for targeted security awareness intervention to address shortcomings, and that generic awareness campaigns are no longer sufficient. The author suggests that an assessment of the target population would be beneficial to identify the population’s shortcomings before designing the security awareness campaign.

<https://www.researchgate.net/profile/Lukasz-Wiechetek/publication/339273589_Cyber_Security_Awareness_Knowledge_and_Behavior_A_Comparative_Study/links/5e46d7d9458515072d9db266/Cyber-Security-Awareness-Knowledge-and-Behavior-A-Comparative-Study.pdf> (10)

This research examines the correlation between cyber security awareness, knowledge, and practices involving protection tools among individuals in four specific countries: Israel, Slovenia, Poland, and Turkey. The findings indicate that while internet users generally display sufficient awareness of cyber threats, they tend to employ only basic protective measures, often relatively common, simple, and straightforward in nature. Moreover, the study reveals a direct link between a deeper understanding of cyber concepts and heightened awareness, regardless of respondent gender or country of origin.

<https://www.researchgate.net/profile/Bibhu-Dash-5/publication/362112009_Prevention_of_Phishing_Attacks_Using_AI-Based_Cybersecurity_Awareness_Training/links/62d6e554593dae2f6a28d4e0/Prevention-of-Phishing-Attacks-Using-AI-Based-Cybersecurity-Awareness-Training.pdf> (11)

The progression of machine learning has empowered its effectiveness in evading cyber-attacks, indicating a growing necessity for enhanced cybersecurity awareness utilizing AI. This research paper describes how awareness regarding AI-based cyber security can lead to a decrease in phishing attacks. Consequently, the paper highlights the efficacy of AI-driven cyber security awareness training and its potential impact on mitigating cyber-attacks.

Brad (2021) indicates that AI technologies have significant results in avoiding most phishing attacks. This paper highlights AI’s fast response time and ability to learn over time by learning from its mistakes allows it to understand attack patterns including new attacks that humans may not understand. These factors have been proven to be essential in effectively avoiding phishing attacks according to the author.

<http://www.imrjournal.org/uploads/1/4/2/8/14286482/imr-v14n2art1.pdf> (12)

Following the guidelines recommended by the National Institute of Standards and Technology, this document aims to outline the essential elements of a comprehensive program that trains, tests, measures and enhances an organization’s cybersecurity to defend against phishing attack.

<https://www.tandfonline.com/doi/pdf/10.1080/15332861.2010.487415?casa_token=yJfhjE1RHukAAAAA:gEf76ESyQA9DcPmDkmUvpiSwH2cyOjnj-881qxnS74SJIDmplHCDrMBpAdj-eHwV6hll_Eg_mIDo> (13)

This article presents the results of a study to determine the impact of a cyber threat education and awareness intervention on changes in user security behavior. It is concluded that when users were educated of the threats to e-commerce and trained about proper security practices, their behavior could be changed to enhance online security for themselves and the firms where they are employed.

<https://www.researchgate.net/profile/Hussain-Aldawood/publication/330293734_Educating_and_Raising_Awareness_on_Cyber_Security_Social_Engineering_A_Literature_Review/links/5d9ae3c192851c2f70f21bf8/Educating-and-Raising-Awareness-on-Cyber-Security-Social-Engineering-A-Literature-Review.pdf> (14)

The author of this article defines social engineering as “the practice of taking advantage of human weaknesses through manipulation to accomplish a malicious goal.” According to the article, one of the most straightforward solutions to safeguard victims from social engineering attacks is through effective training and education programs. As such, the paper details how innovative information security education programs can effectively increase user/employee awareness and ultimately reduce cyber security incidents.

The road to providing training and awareness programs is fraught with challenges arising from many factors including business, social, constitutional, organizational, economical, and personal environments. Security training and information security awareness programs include techniques of simulations, serious games, virtual labs, and themed awareness videos and modules. However, these modern training techniques have their own limitations in enhancing employee preparedness.

<https://www.mdpi.com/1999-5903/11/3/73> (15)

This study highlights pitfalls and ongoing issues that organizations encounter in the process of developing the human knowledge to protect from social engineering attacks. Enhancing information security training and awareness programs can help organizations achieve better results against social engineering techniques.

<https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=d12af7f9216518bca25183edb47d5ef6a478c135> (16)

In this paper, we will show the need for security awareness programs in schools, universities, governments, and private organizations in the Middle East by presenting results of several security awareness studies conducted among students and professionals in UAE in 2010. This includes a comprehensive wireless security survey in which thousands of access points were detected in Dubai and Sharjah most of which are either unprotected or employ weak types of protection.

**Motivation**

\*\*\* <http://jise.org/Volume23/n4/JISEv23n4p407.pdf> (17)

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.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 effect 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> (18)

This article is based on a study that examined the factors influencing government employees’ cybersecurity behavior in Malaysia by analyzing the responses of four hundred and forty-six participants who completed an online poll. “The findings suggest that highly motivated employees with high severity, vulnerability, response efficacy, and self-efficacy exercise cybersecurity. Incorporating the users’ perceptions of vulnerability and severity facilitates behavioral change and increases the understanding of cybersecurity behavior’s role in addressing cybersecurity threats—particularly the impact of the threat response in predicting the cybersecurity behavior of government employees.” Based on these results, the author of the study concluded that “The rising usage of tablets and smartphones for personal and financial information underscores the need for more information security research focusing on cybersecurity behavior.”

<http://www.edfoundation.org/index.htm>

<https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-50.pdf> (19)l