



**INVESTIGATION ON FACTORS INFLUENCING  
CYBERSLACKING AND INTERNET ABUSIVE  
BEHAVIOR**

By

**Shampa Rani Das**

**ID: 151-35-1009**

This Report Presented in Partial Fulfillment of the Requirements for the  
Degree of Bachelor of Science in Software Engineering

DEPARTMENT of SOFTWARE ENGINEERING  
DAFFODIL INTERNATIONAL UNIVERSITY

FALL 2018

## **APPROVAL**

This is an analysis of MIS (Management Information System): A case study of Investigation on factors influencing cyberslacking and internet abusive behavior thesis is submitted by Shampa Rani Das to the Department of Software Engineering, Daffodil International University, has been accepted as partial fulfillment of the requirements for the degree of Bachelor of Science and approved as to style contents.

## **BOARD OF EXAMINERS**

---

Dr. Touhid Bhuiyan Head

Professor & Head

Department of Software Engineering

Faculty of Science and Information Technology

Daffodil International University

---

Examiner

Internal

---

Examiner

Internal

---

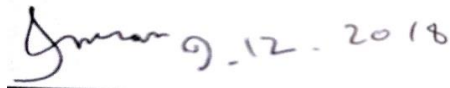
Examiner

External

## THESIS DECLARATION

I hereby declare that, this thesis report is done by me under the supervision of Dr. Imran Mahmud, Assistant Professor & Associate Director (Research), Department of Software Engineering, Daffodil International University, in partial fulfillment my original work. I am also declaring that neither this thesis nor any part therefore has been submitted else here for the award of Bachelor or any degree.

### Supervised by



---

Dr. Imran Mahmud

Assistant Professor & Associate Director (Research)

Department of Software Engineering

Daffodil International University

### Submitted by



---

Shampa Rani Das

ID: 151-35-1009

Department of Software Engineering

Daffodil International University

## **ACKNOWLEDGEMENT**

Foremost, I am thankful to God for my wellbeing and that's why I am completed my research procedure. Then I am grateful to my research supervisor, Dr. Imran Mahmud who guided me throughout the whole research activities. Besides my supervisor, I would love to thank the rest of my research committee: Ms. Samia Nasrin, Ms. Tapushe Rabaya Toma, Ms. Farzana Sadia and Ms. Fatama Binta Rafiq for their encouragement and insightful comments. After that I would like to thank Md. Nadir Bin Ali, Joint Director of IT, Daffodil International University who helped me during survey of my research. I wish to express my special thanks to Professor Dr. Touhid Bhuiyan, Head of the Faculty for providing all the necessary facilities for the research purpose. I am also thankful to all the lecturers, Department of Software Engineering who sincerely guided me at my difficulty. I am grateful to my parents for their unconditional support and encouragement. I am thankful to my friend who supported me throughout this venture.

## TABLE OF CONTENTS

<b>APPROVAL</b>	i
<b>THESIS DECLARATION</b>	ii
<b>ACKNOWLEDGEMENT</b>	iii
<b>TABLE OF CONTENTS</b>	iv
<b>LIST OF TABLES</b>	v
<b>LIST OF FIGURES</b>	vi
<b>LIST OF ABBREVIATIONS</b>	vii
<b>ABSTRACT</b>	Viii, ix
<b>CHAPTER 1: INTRODUCTION</b>	
1.1 Background	1-2
1.2 Motivation of the Research	2-3
1.3 Problem Statement	3
1.4 Research Questions	3
1.5 Research Objectives	3
1.6 Research Scope	4
1.7 Thesis Organization	4
<b>CHAPTER 2: LITERATURE REVIEW</b>	
2.1 Previous Literature	4-5
2.2 Previous Literature on cyberslacking	5-6
2.3 Previous Literature on Abusive Behavior	6
2.4 Research Gap	6-12
2.5 Hypothesis Development	12-14
2.5.1 Self-esteem	12
2.5.2 Private Demand	12
2.5.3 Rules and Regulations	13
2.5.4 Cyberslacking	13
2.6 Summary	14
<b>CHAPTER 3: RESEARCH METHODOLOGY</b>	
3.1 Questionnaire Design	14-16
3.2 Sample Size and Questionnaire Distribution	17
3.3 Demographic information	17-21
3.4 Summary	21
<b>CHAPTER 4: RESULTS AND DISCUSSION</b>	
4.1 Data Analysis Technique	21
4.2 Measurement Model	21-23
4.3 Structural Model	24-26
4.4 Summary	26
<b>CHAPTER 5: CONCLUSIONS AND RECOMMENDATIONS</b>	
5.1 Findings and Contributions	26-28
5.2 Limitations	28
5.2 Recommendations for Future Works	28-29
<b>REFERENCES</b>	29-35

## LIST OF TABLES

Table 1. Information of Research Gap	6-12
Table 2. Demographic profile of survey respondents	18
Table 3. Frequency table of survey respondents	18-19
Table 4. Frequency table of Gender	19
Table 5. Frequency table of Marital Status	20
Table 6. Frequency table of Education Level	20
Table 7. Frequency table of Routinized Internet Use (RIU)	20-21
Table 8. Convergent Reliability and Validity	22
Table 9. Discriminant validity	23
Table 10. Mean, STDEV, T-Values, P-Values	24
Table 11. Effect size calculation result	25

## LIST OF FIGURES

Figure 1. Research Model	14
Figure 2. Composite Reliability graph	22
Figure 3. Average Variance Extracted (AVE) graph	23
Figure 4. Our final research model validating using data from the survey	25
Figure 5. f Square graph	26

## LIST OF ABBREVIATIONS

### Abbreviation

SE

PD

RR

C

AI

### Explanation

Self-Esteem

Private Demand

Rules and Regulations

Cyberslacking

Abuse Intention



## **ABSTRACT**

In this research, we investigated the influence of individual factors and organizational factors in a one platform; these factors are motives of cyberslacking and internet abuse intention. According to the source of Daffodil International University's IT, they revealed that cyberslacking behavior is existed in this organization. Several times peoples in this organization visited various online newspaper, entertainment, transportation sites and so on. Another survey by International Data Corp (IDC), 30 to 40% of internet access was spent on non-work related browsing, and a tremendous 60% of all online purchases were made during working hours. It exposed that 70% of all web traffic to Internet mature websites occurs during the work hours of 9am-5pm. 58% of industrial spying was done by current or former employees. 48% of large companies blamed their worst security breaches on employees. 46% of the one thousand largest companies globally utilized IM (Instant Message) as a daily communications tool. 64% of employees said they use the Internet for personal interest during working hours. 37% of workers said they surf the Web constantly at work. 77.7% of major U.S. companies keep tabs on employees by checking their e-mail, Internet, phone calls, computer files, or by videotaping them at work. 63% of companies monitored workers Internet connections and 47% store and review employee e-mail. 27% of companies said that they've fired employees for misuse of office e-mail or Internet connections, and 65% report some disciplinary measure for those offenses. 90% of employees feel the Internet can be addictive, and 41 percent admit to personal surfing at work for more than three hours per week. 60% of Security Breaches occurred within the Company – behind the Firewall. 25% of corporate Internet traffic was considered to be

“unrelated to work”. 30-40% of lost productivity was accounted for by cyber-slacking. 32.6% of workers surfed the net with no specific objective; men were twice as likely as women. Some estimates disclosed that computer crime may cost as much as \$50 billion per year. Around 80% of computer crime was committed by “insiders” and they managed to steal \$100 million by some estimates; \$1 billion by others. The average fraud inflicted a loss of about \$110,000 per corporate/organization victim, and \$15,000 to each individual victim. In here, data were collected through a survey questionnaire. We used SPSS and SmartPLS 3 to analyze the data collected; and also SEM (Structural Equation Modeling) that is helpful in confirming the model of research studies involving latent variables. This research explores the impacts of both individual and organizational factors on cyberslacking and internet abuse intention among employees who are already directly or indirectly connected to IT sectors’, as most of the previous research has focused on these factors individually. We employ both theoretical and practical contributions in this paper. The results supported all of the hypothesized relationships among individual factors, organizational factors, cyberslacking and internet abuse intention. Our proposed model was empirically tested and contributed to an augmentative body of knowledge about the influential factors on cyberslacking as well as internet abuse intention. Above all, we discuss the results as to know how the present study expands on previous research, and based on limitations future directions research are indicated.

# CHAPTER 1

## INTRODUCTION

### 1.1 Background

People are enlarging use internet for both private and professional demands day by day. Employees who abuse internet privileges at workplace have become a major concern in today's world. Surveyed IT managers on average estimated that each employee is using the internet for personal use for 5.9 hours a week and after multiplying these numbers by the average American hourly salary, Websense came up with the figure of \$178 billion (19 JUL 2005, [www.infoworld.com](http://www.infoworld.com)). A survey by the International Data Corporation (Snapshot Spy, 2008) stated that internet access at work was exhausted on non-work related activities till that time 40 percent and also 60 percent of all online purchases are made during laboring hours. Researchers (Lim & Chen, 2009) investigated that gender differences in cyberslacking found that men cyberslacked more frequently and also for longer periods than women (<http://businessbarbados.com/trending/entrepreneurship/cyberslacking-in-your-workplace/>). According to Bock and Ho (2009), the usage of internet to fulfill the private demands was directly influenced by habits. In a survey, it was initiated that employees exhausted at least one hour on non-work related operations in a day regularly, especially for private demands (Vitak et al., 2011). Regarding the amount of time spent doing internet deviance activities, (Restubog et al., 2011) reported that approximately 30%-50% of Internet consumption at work is non-work-related which was caused annual losses as much as \$1 billion. Individuals were more curious about violating cybersecurity than whimsical as well as righteous people which was noticeable by McBride et al. (2012). About 60% of

online purchases were actually made during office hours which are not-work related (StaffMonitoring.com, 2013). People having elevated private demands did more cyberloafing (Konig and Caner de la Guardia, 2014). In fact, Salary.com found that surfing the internet is one of the biggest culprits in 2017. Forbes revealed that 64 percent of employees visit non-work related websites every day at work (<https://www.forbes.com/sites/cherylsnappconner/2012/07/17/employees-really-do-waste-time-at-work/#560befa15e6d>). According to human resources, Employees spent between one and three hours a day surfing the web on personal business at work (January 11, 2018). A study exposed that perceived consequences, affect and social factors were significant to intention to cyberloafing except for private demands (Kian et al., 2017). This study disclosed that conflict between individuals and organizations as well as rules and regulations of an organization affected employees' internet frauds in private sector (Soudabeh and Niloofar, 2015). The study published that Self-esteem significantly influenced employees' internet addictions and on the consequences this addiction significantly influenced employees' abuse intention at the workplace (Jengchung et al., 2008). High self-esteem people are more confident and benefited than low self-esteem people; and these low self-esteem peoples are remain depressed and less confident which has a great impact in all of their lives for both high and low self-esteem (Rosenberg, 1965). This study enhanced that habitual internet use may play a role in cyberslacking behavior (Jessica et al., 2011). According to the statistics of salary.com 34 percent wasted maximum 30 minutes, 24 percent wasted 30-60 minutes, 11 percent wasted several hours on a daily basis at the workplace for personal desire (Aaron, 2013). An individual having higher level of morality is refer to less abuse intention (jongwoo et al., 2016).

## **1.2 Motivation of the Research**

Our study aimed to investigate and empirically validate how individual (self-esteem and private demand) and organizational factors (rules and regulations) effected on cyberslacking which leads to intent of internet abuse. From previous theoretical aspect, we desired to explore the impact of these variables and that's why we developed a theoretical research model.

## **1.3 Problem Statement**

A research problem is an area of concern in the existing knowledge that points to the need for further understanding and investigation. As we said before, the previous researchers have paid concentration on individual and also organizational factors individually; and these factors have impact on cyberslacking and sometimes these cyberslacking is the cause of intention to abuse the internet at the workplace (Jengchung et al., 2008; Jessica et al., 2011; Soudabeh and Niloofar, 2015; jongwoo et al., 2016; Kian et al., 2017). Individual factors have a great impact on doing internet deception (Soudabeh and Niloofar, 2015). We got to know about limited research on individual and organizational factors simultaneously.

## **1.4 Research Questions**

The research question is following to test the impact of individual and organizational factors on cyberslacking intention as well as examine the impact of cyberslacking factors on abuse intention,

☞ **RQ1:** What are the factors that influence cyberslacking intention?

☞ **RQ2:** Is there any relationship between cyberslacking and abuse intention?

We developed a theoretical research model that focused on the influential factors of cyberslacking and abuse intention to inquire about the research questions'. We also did survey among IT related peoples' to examine the model. After a thorough literature review, we developed hypotheses.

## **1.5 Research Objective**

As a result, our objectives are

- ☞ To find out the factors that influence cyberslacking intention
- ☞ To investigate the relationship between cyberslacking and abuse intention

## **1.6 Research Scope**

We identified the research gap. Based on this gap, we chose a few factors which were used moderately in different literatures. Then we integrated a research model that included two factors which are individual and organizational that influenced cyberslacking along with abuse intention at the workplace. After that we collected data through a survey from targeted respondents and examined all the data through SPSS and SmartPLS3. Above all, we got our desired results that was supported all the hypothesis of our research model.

## **1.7 Thesis Organization**

In the following, we first discussed about literature including the research gap. Second, we addressed research methodology along with hypothesis and research model. Third, we mentioned results and discussions. We then discussed the conclusions and recommendations containing findings, limitations and future directions.

## CHAPTER 2

### LITERATURE REVIEW

#### 2.1 Previous literature

A study assessed that most of the cyberloafing empirical studies did by developed countries (Shafaat and Truptimayee, 2016). Higher levels of private demands will be positively associated with higher levels of employees' intention to use the Internet for cyberloafing (Kian et al., 2017). This research estimated that employees' intention on cyberslacking behavior has a great impact on public organization than for a private organization (Zill-e-Huma et al., 2017). The study (Coker, 2011) revealed that cyberloafing has a positive impact on worker productivity. The research stated that employees might avoid their organizational duties due to the usage of internet for private perspectives at the workplace (Hunik, 2012). A research estimated that UK businesses were lost £1.4m every week as employees tried to access popular Big Brother game show for ten weeks from their offices (<https://www.computerweekly.com/feature/Dealing-with-staff-Internet-abuse>). A study (Pruthikrai et al., 2004) developed a measurement model based on personal web usage at work. Nowadays internet access become more available as a social networking site so that employees often desired to browse it for entertainment or personal purposes during working hours (Shafaat and Truptimayee, 2016). According to (Jengchung et al., 2008) Low self-esteem online users easily addicted to use internet than high self-esteem online users. From employees' perspectives, Private demands had obvious impact on cyberloafing (Konig and Caner de la Guardia, 2014). Organization's rules and regulations should be

more exact otherwise people will explicate these by their own understanding by which organization may face a great problems (Soudabeh and Niloofar, 2015).

## **2.2 Previous research on cyberslacking**

Cyberslacking is a severe threat to any organization. According to (Phillips and Reddie, 2007; Jessica et al., 2011; Soudabeh and Niloofar, 2015) cyberslacking (also known as cyberloafing) referred as non-work (such as personal purposes, internet browsing and so on) related activities during office hours through internet and mobile technology which causes loss in revenue of an organization. Research announced that 1,000 internet user employees could lose up to \$35 million in productivity annually from just an hour of daily web surfing of a company (StaffMonitoring.com, 2017). Higher levels of intention to cyberloaf will lead to higher levels of actual cyberloafing behavior (Kian et al., 2017). The statistics of salary.com disclosed that 64 percent employees do cyberslacking during office hours (Aaron, 2012) in a day. An employee who earns \$ 40,000 in a year leads to a \$ 5,000 damage for his/her company by wasting an hour of the working time on the internet (Özkalp et al., 2012). 70 percent of all Internet porn traffic occurs from the workplace that means one in five employees' access adult sites at work ([https://www.shrm.org/hr-today/news/hr-magazine/pages/cms\\_006514.aspx](https://www.shrm.org/hr-today/news/hr-magazine/pages/cms_006514.aspx)).

## **2.3 Previous research on Abusive Behavior**

While internet is always available, then the employees tend to misuse the organization's internet, they don't realize the consequences associated with exploiting the privilege. UK companies were lost up to £2.5m each year due to non-work-related surfing by CIPD



(Chartered Institute of Personnel Development)

(<https://www.computerweekly.com/feature/Dealing-with-staff-Internet-abuse>). Research indicated that during work most popular non-work related activities were instant messages, online shopping, blogging and so on among employees (Madden, 2009). From personal perspectives employees spent between one and three hours a day surfing the web during working time (<https://www.thebalancecareers.com/surfing-the-web-at-work-1919261>). A study disclosed that the internet was used unnecessarily for browsing different SNS at work (<https://thebroodle.com/internet/internet-abuse-at-the-workplace-and-its-consequences/>).

## 2.4 Research Gap

In the following table 1 we provided the information of research gap and based on this gap we continued our research.

Table 1. Information of Research Gap

Year	Author	IV	DV	Research Gap
2004	KIMBERLY, and CARL	Policy, training, rehabilitation	Internet abuse	Limited research on individual and organizational factors together, and also the relationship between cyberslacking and abuse intention.
2008	Jengchung, Charlie, Hsiao-Han	External Locus of Control, Low Self Esteem, High Gratifications of Internet Use, High Perceptions of the Existence of Internet Use Policy, Internet Addiction, High Perceptions of the Existence of Electronic Monitoring Systems	Internet abuse	
2010	Ibrahim, Alok	Gender, age, income, usage profile, usage pattern	Internet (usage profile and pattern)	

2011	Jessica, Julia and Robert	Demographics, Job dissatisfaction, External control, Internet job utility, Routinized use of Internet, Job characteristics	cyberslacking
2012	Hunik	Role ambiguity, role conflict, role overload, internet experience	cyberloafing
2013	Cornelius, Mariette	Personal internet use at work, private demands, border strength	Cyberslacking
2015	Hasmida, Zauwiyah, Mazni, Maimun	Gender, age, problematic internet use, habit, external locus of control, organizational justice	Use of internet
2015	Hosseini, Daraei & Mostafa	Sanctions, past enforcement, detection	Strict rules & regulations against Cyber loafing
2015	Hemin, Aggeliki	emailing activities of PIU, browsing activities of PIU, and online financial activities of PIU	perceived injustice (i.e., procedural justice and distributional justice), role ambiguity and role conflict, perceived organizational security policy (i.e., existence of the policy and enforcement of the policy), self-control, perceived benefit, social norm, habit and demographic factors (i.e., age and gender)

2015	Kwanghyun, MariaKwiyoung, Nahyun	Age, gender, education, organizational justice, empowerment, emotional stability	cyberloaf
2015	Vimala	Age, gender, status, ethnicity, internet frequency	Cyber-bullying
2015	Soudabeh, Niloofer	Rules & regulations, culture, economical & political condition, Environmental & external factors	cyberbullying
2015	Rebecca	Defamation, harassment, Invasion privacy and breach of confidence	Cyberbullying
2015	OK-Hee, Kyeong, Yang- Sook	Age, gender, religious, affiliation, education level, job experience, marital status	Violence, abuse
2015	Nafsika, Constantinos	Age, country of origin	Cyberbullying, school bullying
2015	Tracy, Catherine	Age, gender, ethnicity, School grade	cyberbullying
2016	Xian, Joan, Dongping, Haiyan	Gender, age, socio- economic status, family functioning, school type, effortful control, anger, shyness, frustration,	PIU,DPA
2016	Jongwoo, Eun,  Richard	Liberty, facilitation, goal  conductiveness, morality,  abuse morality affect	Abuse intention
2016	Farah, Ghinwa,  Hicham, Nada,  Latife, Aline,  Lydia	Insomnia, Self-esteem,  Anxiety, depression and  stress	Internet  addiction
2016	Andrzej, Mateusz,	Age, gender	problematic internet use

	Agnieszka, Lukasz		
2016	Apoorva, Manoj, and P. Marimuthu	Age, duration of internet use,	Internet use, interpersonal interaction, leisure activities
2016	Bhavna	Rapid globalization, low cost of mobile phones, easy internet access, psychological perverts, financial cause	cybercrime
2016	Koay, Patrick, Chew	Perceived consequences, social factors, habit, affect, Behavioral intention, facilitating conditions, internet addiction, job productivity	Cyberloafing
2016	Ebru, Suna	Gender, duration of internet use, personality, neuroticism, psychoticism, romantic appeal, physical appearance, user opinion,	Problematic internet use
2016	Ahu	Psychological problem, belief, fears, career goals, behaviors, insecurity, organization culture, leadership, job satisfaction	Bullying
2016	Francisco, Joyce	Age, sex, year of study, parental educational attainment	Problematic Internet Use
2016	Yousef, Morten, Petter,	Gender, age, work schedule, position in job,	Bullying, physical

	Khaldoun, Espen, Hein, Rita		aggression, verbal aggression	
2017	Lee	Human Behavior	Cybersecurity, internet addiction	
2017	Aminah, Zoharah	Age, gender, behavior	Cyber loafing	
2017	Zill-e- Huma, saddam, Ramayah, Muhammad Imran	Gender, educational level, type of Organization, work experience, facilitating condition, behavior, habit, intention, social influences	Cyberloafing	
2017	Kian, Patrick, Kok	Habit, intention, social factors, private demands, Facilitating condition, age, gender, Severity of negative consequences , affect, work performance, job stress	Cyberloafing	
2017	Shafaat and Truptimayee	Attitude, opportunities, addiction, professional experience	Cyberloafing	
2017	Pinar, Mine, Umit, Ozlem	Profession, marital status, social lives, working time, age	Workplace bullying perception	

2017	Laconi, Vigouroux, Lafuente, Chabrol	Personality traits, defense mechanism, coping styles, depressive symptoms, self-esteem	PIU
2017	Howard	Country region, social condition, social norms, political conflict, ,country income level	Child abuse
2017	Mehdi	Metacognitions, distress intolerance, emotional dysregulation	PIU
2017	Brandon, Kiersten, Linda	anxiety, hopelessness, job stress	Workplace bullying, Bullying support, coworker support
2018	Seonyoung, Jiyeon	Authentic Leadership, Relationship-oriented culture	Workplace Bullying
2018	Elena, Immaculada, Vicente, Rosario, Izabela	Age, gender, Lower level of social and emotional competencies, lower self-management and motivation, lower responsible decision making	Abuse of technology
2018	Han, Zin, Jie, Rathindra	Age, gender, internet experience, less motivation, less beneficial at work, weak self-control	Internet abuse
2018	M.Rajalakshmi, B.Naresh	Organizational justice, psychological contract, Organizational culture, Organizational structure	workplace bullying

## **2.5 Hypothesis Development**

### **2.5.1 Self-Esteem**

Self-esteem influence the employees' internet addiction which causes internet abuse intention at work (Jengchung et al., 2008). It means self-esteem has a significant relationship with abuse intention. Therefore it is obvious that higher level of self-esteem will lead to higher level of cyberslacking which means cyberslacking is related with self-esteem. Thus, we hypothesize

**H1:** Self-esteem has a positive impact on cyberslacking.

### **2.5.2 Private Demand**

The willingness to engage in internet misuse of internet during office hour's referred by cyberloafing (Lee et al., 2005) which is based on an individual's personal perspectives. The result of a study expressed that private demand had a positive impact on cyberloafing (Kian et al., 2017). It is indicated that private demand has an effective relationship with personal internet use which leads cyberslacking. So, we therefore propose the following

**H2:** Private demand has a positive impact on cyberslacking.

### **2.5.3 Rules and Regulations**

A research disclosed that organization's rules and regulations had significant impact on doing internet deception (Soudabeh and Niloofar, 2015). It also stated that it is illogical to fight for the law of cybercrimes that means we must enforce the law against organization's rules and regulations. Then the employees may get to know that how they will conduct their activities during working hour at their office. If rules and regulations against cyberloafing is strict, then cyberloafing intention will be less (Hosseini et al., 2015). So we

understand that we may reduce cyberslacking motive during office hours through enforcing appropriate rules and regulations; and also providing training how to do their official activities. That's why, we propose

**H3:** Rules and regulations has a positive impact on cyberslacking.

### 2.5.4 Cyberslacking

The statistics of salary.com indicated that in every single day 69 percent employees do cyberslacking at work (Aaron, 2013). 6% of UK based worker spent more than one hour of their working day on social media sites (<https://www.interaction.uk.com/insight/the-rise-of-cyber-slacking/>). Intention was the significant factor for actual cyberloafing behavior (Kian et al., 2017). A survey reported that 21% – 31% admitted to sending company confidential information including financial or product data to recipients outside the company by email among 800 workers (StaffMonitoring.com, 2017). This can be hypothesized as follows

**H4:** Cyberslacking has a positive impact on abuse intention.

By combining all these hypotheses proposed so far, Figure 1 illustrates our research model.

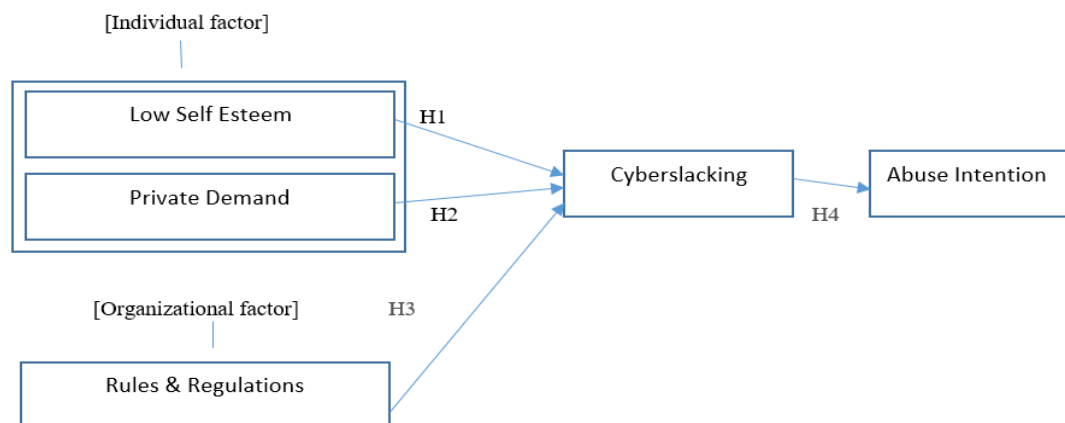


Figure 1. The Research Model



## **2.6 Summary**

Our Study is motivated by the need for research focusing on both individual and organizational factors, particularly factors related to cyberslacking and abuse intention of internet at work. We tried to demonstrate our hypothesized research model. We supposed the positive impact of this individual and organizational factors on cyberslacking as well as abuse intention.

## CHAPTER 3

### RESEARCH METHODOLOGY

#### 3.1 Questionnaire Design

This research devoted the quantitative approach to meet the required objectives. The measurement items were all measured from the published literature. IT related persons were selected as the targeted population due to their higher usage of internet at work. To evaluate our model, we collected questions from several research papers (Rosenberg, 1965; Jessica et al., 2011; Konig and Caner de la Guardia, 2014; Soudabeh and Niloofar, 2015; jongwoo et al., 2016) which helped to make a structured survey questionnaire. We had two factors, one is individual factor and the other is organizational factor by which we examined our research model. Individual factor contained self-esteem and private demand; and organizational factor included rules and regulations of an organization. We tried to find out the impact of these factors on cyberslacking as well as abuse intention. That's why we tested the model empirically.

Self-esteem (Rosenberg,1965) was examined using a four point Likert scale format which contains ranging from strongly disagree to strongly agree consisting of ten items which are “On the whole, I am not satisfied with myself”, “At times I think I am not good at all”, “I feel that I do not have number of good qualities”, “I am not able to do things as well as most other people”, “I feel I do not have much to be proud of”, “I certainly feel useless at times”, “I feel that I'm not a person of worth, at least on an equal plane with others”, “I wish I could have more respect for myself”, “All in all, I am inclined to feel that I am a failure” and “I do not take a positive attitude toward myself”.

Private demand was surveyed using the scale adopted from (Konig and Caner de la Guardia, 2014) which is made of five items measured in a seven point Likert scale format ranging from strongly disagree to strongly agree. The included items are “I have many private demands”, “My private demands require much of my time”, “I have the impression I am not paying sufficient attention to my private obligations”, “It would be good if I had more time for my private obligations” and “I have to rush in order to meet all my private obligations”.

Rules and regulations were investigated from (Soudabeh and Niloofar, 2015) using a seven point Likert scale format which is ranging from strongly disagree to strongly agree. It contained five items which are “Ambiguity and contradiction in rules and regulations”, “Lack of timely revision and modification of regulations”, “Lack of law enforcement”, “Undue law enforcement” and “Tolerance and indulgence”.

Cyberslacking was identified from (Jessica et al., 2011) and measured it using binary variables where “0” means respondents did not do the questioned tasks at work and on the other hand “1” means respondents did the questioned tasks while they at work. The questioned nine items are “sending emails”, IM (Instant messages)”, “Texts”, “Visiting a SNS (Social Networking Sites)”, “Watching video”, “Writing blogs”, “Reading blogs”, “Playing video games” and “Shopping”.

We included a scenario based questionnaire to investigate the internet abuse intention. The scenario was “You work for an IT firm; and for last five years, you managed several projects. You are always dedicated to your work but unfortunately you are not appreciated with all of your successful aspects. Your salary increment is totally off for last two years. On the other hand, your rival is always credited without doing successful

perspectives as well as his/her salary increment is going on day by day. All on a sudden, your rival is promoted for higher designation but you are not. These situations are humiliating for you. You also hear a rumor that the firm may be fired you soon. If you want, then you may take revenge against the company because of your high liberty. From your past experience, you know that you can access several confidential files/documents easily. The security control situation at the company is poor. You know all of the confidential information of your company and also know how to destroy all of those information without leaving any evidence”. Abuse intention was measured using the scale from (Jongwoo et al., 2016) consisting of three items with response options varying from strongly disagree to strongly agree in the seven point Likert scale format. The included items are “I intended to abuse the systems”, “I predict I will abuse the systems” and “I plan to abuse the systems”.

### **3.2 Sample Size and Questionnaire Distribution**

We distributed 200 questionnaire among targeted people and also tried to reach them through online based questionnaire but we received responses from only 106 respondents. We used G power software to calculate the minimum sample size. According to G power software we needed 119 responses to make the research model significant. The questionnaire consists of two sections. The first section exhaled the demographic data; the second section was focused on items to measure the constructs of our research model.

### 3.3 Demographic Information

This study provides several notable contributions. The demographic of the respondents tabulated in Table 2 were derived from descriptive analysis. It empirically examined the impact of targeted peoples (IT related teachers and employees) selected demographic factors which are age, gender, marital status, educational level and routinized internet use (riu) that significantly influence the cyberslacking and internet abuse intention. Here, almost all the peoples having more than 6 years internet usage experience. The final data is comprised of 70 males (66%) and 36 females (34%) (see in table 4); 66 unmarried (62.3%) and 40 married (37.7%) (see in table 5); education level contained diploma (1.9%), bachelor (37.7%), masters (54.7%) and PhD (5.7%) (see in table 6). According to (Lim and Chen, 2012), men more engaged in cyberslacking behavior than women at work. A majority of the respondents are of the consequences age group of 21 to 30 years (60.3%), 31 to 40 years (30%), 41 to 50 years (7.4%) and more than 50 years (0.9%) (see in table 3). The amount of routinized internet use is “Less often” (1.9%), “Every few day” (4.7%), “Once a day” (6.6%), “Several times” (34.0%) and “Constantly” (50.0%). Routinized internet users are used internet on a regular basis (see in table 7).

Table 2. Demographic profile of survey respondents

	age	gender	Marital_status	Education_level	riu
Valid	106	106	106	106	103
Missing	0	0	0	0	3

Table 3. Frequency table of survey respondents

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	21	1	.9	.9	.9
		22	1	.9	1.9
		23	4	3.8	5.7
		24	6	5.7	11.3
		25	13	12.3	23.6
		26	7	6.6	30.2
		27	8	7.5	37.7
		28	8	7.5	45.3
		29	7	6.6	51.9
		30	9	8.5	60.4
		31	2	1.9	62.3
		32	7	6.6	68.9
		33	1	.9	69.8
		34	1	.9	70.8
		35	4	3.8	74.5
		36	5	4.7	79.2
		37	3	2.8	82.1
		38	5	4.7	86.8
		39	1	.9	87.7
		40	3	2.8	90.6

41	1	.9	.9	91.5
42	4	3.8	3.8	95.3
43	1	.9	.9	96.2
45	1	.9	.9	97.2
48	1	.9	.9	98.1
50	1	.9	.9	99.1
65	1	.9	.9	100.0
Total	106	100.0	100.0	

Table 4. Frequency table of Gender

	Frequency	Percent	Valid Percent	Cumulative Percent
Male	70	66.0	66.0	66.0
Female	36	34.0	34.0	100.0
Total	106	100.0	100.0	

Table 5. Frequency table of Marital Status

	Frequency	Percent	Valid Percent	Cumulative Percent
Unmarried	66	62.3	62.3	62.3
Married	40	37.7	37.7	100.0
	106	100.0	100.0	

Table 6. Frequency table of Education Level

	Frequency	Percent	Valid Percent	Cumulative Percent
Diploma	2	1.9	1.9	1.9
Bachelor	40	37.7	37.7	39.6
Masters	58	54.7	54.7	94.3
Phd	6	5.7	5.7	100.0
	106	100.0	100.0	

Table 7. Frequency table of Routinized Internet Use (RIU)

	Frequency	Percent	Valid Percent	Cumulative Percent
Less often	2	1.9	1.9	1.9
Every few day	5	4.7	4.9	6.8
Once a day	7	6.6	6.8	13.6
Several times	36	34.0	35.0	48.5
Constantly	53	50.0	51.5	100.0
Total	103	97.2	100.0	
Missing	3	2.8		
Total System	106	100.0		



### **3.4 Summary**

The questionnaire approach focuses on the factors related to cyberslacking and internet abuse intention along with their relationships. This approach helps us to find out how all the factors are interacted with each other. All the factors (individual and organizational) have positive impact on the other factor (cyberslacking and abuse intent).

## CHAPTER 4

### RESULTS AND DISCUSSIONS

#### 4.1 Data Analysis Technique

Data was collected as a structured questionnaire. We used the Partial Least Squares (PLS) analysis using the SmartPLS 3.0 software and also SPSS (<https://en.wikipedia.org/wiki/SPSS>) to evaluate the hypothesized paths in the research model. We used PLS because of its suitability to test the model.

#### 4.2 Measurement Model

We assessed the measurement model that examined two types of validity, one is convergent reliability and validity; and then the other is discriminant validity.

Table 8. Convergent Reliability and Validity

	<b>Composite Reliability (CR)</b>	<b>Average Variance Extracted (AVE)</b>
<b>ai</b>	0.923	0.800
<b>c2</b>	1.000	1.000
<b>pd</b>	0.884	0.656
<b>rr</b>	0.875	0.586
<b>se</b>	0.758	0.517

Note: ai=abuse intention; c2=cyberslacking2;pd=private demand;rr=rules and regulations; se=self-esteem.

Convergent validity assessed through loading the items, composite reliability of each scale and average variance extracted (AVE) for each construct (Gholami et al., 2013; Zill-

e-Huma et al., 2017). The composite reliabilities (CR) were all higher than 0.7 (Hair et al., 2016) and the AVE were also higher than 0.5 (Fornell and Larcker, 1981) as suggested in the literature (see Table 8 and also Figure 2, Figure 3).

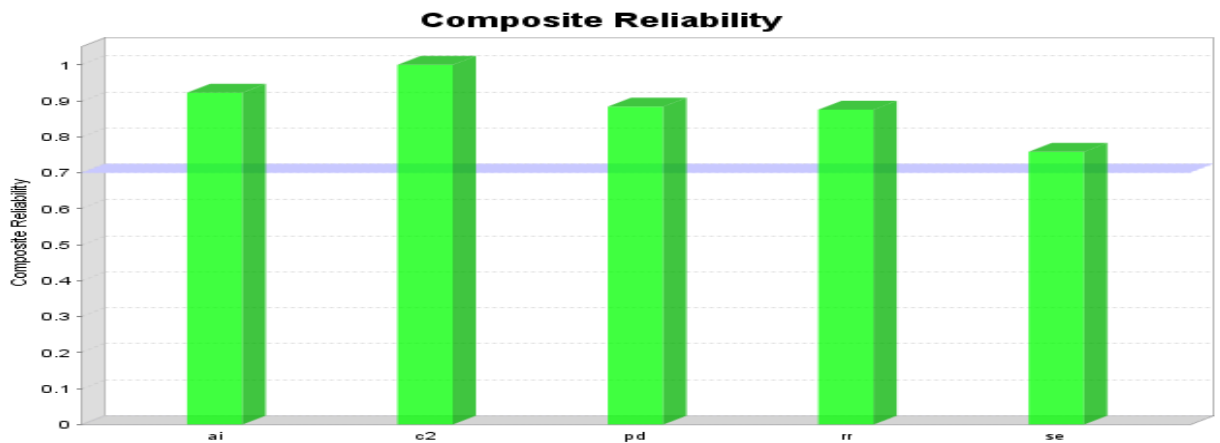


Figure 2. Composite Reliability graph

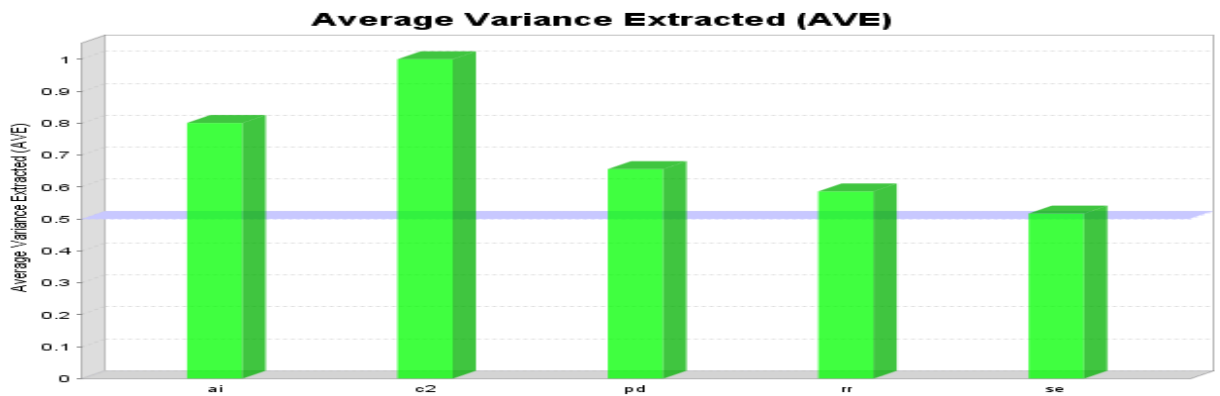


Figure 3. Average Variance Extracted (AVE) graph

Table 9. Discriminant Validity

	ai	c2	pd	rr	se
ai	<b>0.895</b>				
c2	0.173	<b>1.000</b>			
pd	0.092	0.252	<b>0.810</b>		
rr	0.129	0.180	0.314	<b>0.766</b>	
se	0.094	0.348	0.220	0.079	<b>0.719</b>

Note: The diagonal represents the square root of average variance extracted (AVE) while the other entries represents squared correlation.

The discriminant validity of the measures (the degree to which items differentiate among constructs or measure distinct concepts) was examined by following the (Fornell and Larcker, 1981) criterion of comparing the correlations between constructs and the square root of the average variance extracted for that construct (see Table 9). All the values on the diagonals were greater than the corresponding row and column values indicating the measures were discriminant.

### 4.3 Structural Model

We identified the basic measures to report the Mean, STDEV, T-Values, P-Values (see table 10) and effect sizes ( $f^2$ ) (see table 111 and figure 5).

Table 10. Mean, STDEV, T-Values, P-Values

	<b>Original Sample (O)</b>	<b>T Statistics ( O/STDEV )</b>	<b>P Values</b>	<b>Remark</b>
<b>se -&gt; c2</b>	0.306	3.263	0.001	Supported
<b>pd -&gt; c2</b>	0.150	1.756	0.080	Supported
<b>rr -&gt; c2</b>	0.108	0.912	0.362	Not supported
<b>c2 -&gt; ai</b>	0.173	2.190	0.029	Supported

Here, 0.02 to 0.1 =small, 0.15 to 0.35=medium, < 0.35=high

Our final research model validation using data from the survey is given in Figure 4.

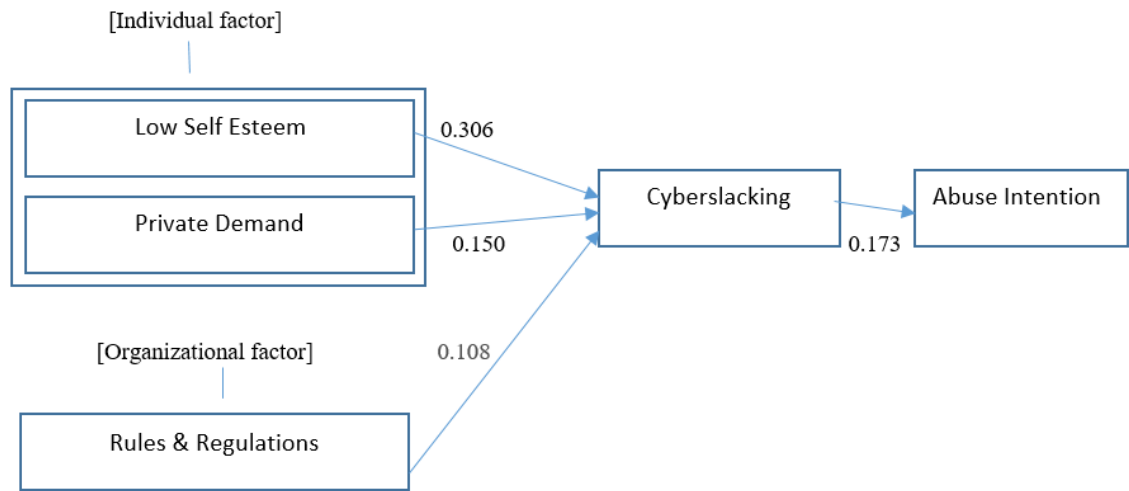


Figure 4. Our final research model validating using data from the survey

Table 11. Effect size calculation result

Hypothesis	Relationship	value	effect size
H1	se->c2	0.107	small
H2	pd->c2	0.023	small
H3	rr->c2	0.013	no effect
H4	c2->ai	0.031	small

\*\*p<0.01, \*<0.05

To determine effect strength, we calculated  $f^2$  values. Table 11 shows that se, pd have small effect on c2. Result also indicates, c2 has small effect on ai and rr has no effect on c2.

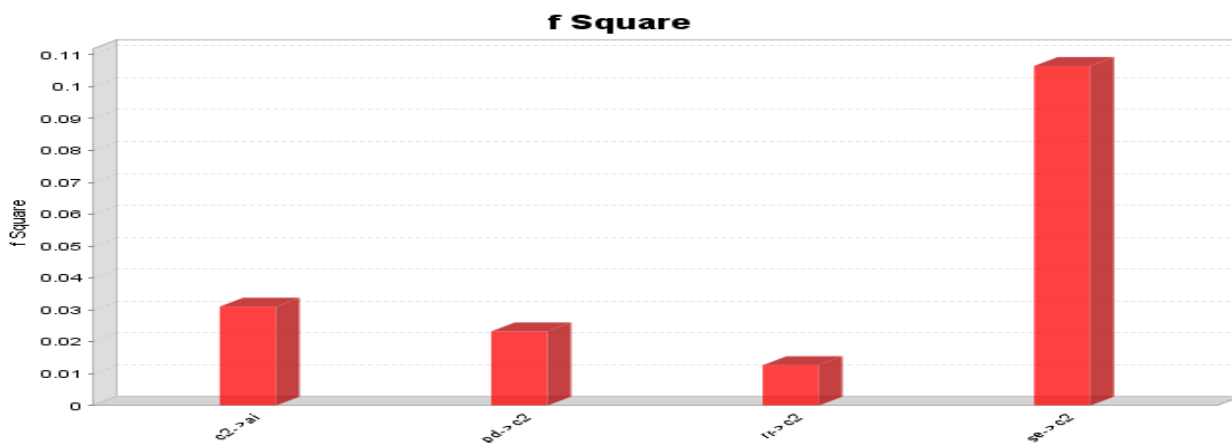


Figure 5. f Square graph

#### 4.4 Summary

This analyzed data benefits researchers by offering a more precise understanding about our research model. Finally the result confirms the significant positive impact of individual and organizational factors on cyberslacking and abuse intention.

## CHAPTER 5

### CONCLUSIONS AND RECOMMENDATIONS

#### 5.1 Findings and Contributions

The research goal of this study was to investigate the impact of various factors on cyberslacking and abuse intention. We understood and validated both individual and organizational factors and processes within an insider abuse context is crucial in the prevention of internet abuse. We identified that how individual factors and organizational factors affect cyberslacking and internet abuse intent. We developed an integrated internet abuse model that incorporates the individual factors and organizational factors that incorporates emotion.

#### Relation between self-esteem and cyberslacking

These findings indicate that self-esteem considers to investigate the internet abusive behavior. 85 percent world's population experienced low self-esteem and this study was conducted by a medical professional (<https://www.forbes.com/sites/ashleystahl/2016/05/11/how-self-worth-affects-your-salary/>). This study points out that self-esteem has a positive influence on cyberslacking.

#### Relation between private demand and cyberslacking

We find out that private demand have significant impact on using internet at work for personal reasons. There is a relationship between private demand and counter-productive activities. The result of the present study suggests that private demand has a positive influence on cyberslacking.

### Relation between rules and regulations, and cyber slacking

An organization must implement precise rules and regulations to prevent internet abuse at the workplace. A study (Soudabeh and Niloofar, 2015) stated that internet abuse can be reduced through implementing precise rules. These findings suggest that rules and regulations has a positive influence on cyberslacking. If any organization's rules and regulations do not consider the awareness of internet use policy then it may lead to many internet abuse vulnerabilities. The existence of internet use policy helps to commit limited amount of internet abuse (Jengchung et al., 2008).

### Relationship between cyberslacking and abuse intention

Cyberslacking behavior influences to do internet abuse. A study (Munir and Maruf, 2016) estimated that employees' intention to use the internet for personal use at work has a positive effect on cyberloafing behavior. In regards to consequences of cyberslacking, it was found that cyberslacking has a significant relationship with internet abuse intention.

Previous studies suggested that identify the current limitations in the general of understanding how individual and organizational factors affect internet abuse intent because of cyberslacking at the workplace. Our insights into relationship between cyberslacking and abuse intent provide further opportunities to improve practice. Cyberslacking directly affects the abuse intent and a few individual and organizational factors affect this cyberslacking behavior.



## **5.2 Limitations**

There are several limitations to be acknowledged. Our targeted sample was very small and all of them are not responded properly. We received limited data from respondents. Result might differ in case of large sample size. We focused on limited number of factors from individual and organizational factors. We collected data from IT related teachers and employees.

## **5.3 Recommendations for Future Works**

Future research should be directed toward examining technological infrastructure, personal factors and organizational factors in a one research. We would like to work with more samples and add more factors including emotional factors with more specific research model. Further research might be concentrated on students who are connected or did job in IT farms.

We may reduce cyberslacking behavior through several activities such as monitoring software, application and website restriction, applying accurate organization's rules and regulations, and so on. We may fight against cyberslacking through Monitoring the software that helps to provide us every history (which applications are being used, what documents are being altered or created or deleted, who is logging into where etc.) of an employee at work. Organization must restrict access to websites and applications which are not related with work. Organization may allow a certain amount of recreation during employees off time at work. All the employees' must know about their organization's rules and regulations.

## REFERENCES

- A.Gouveia, Wasting Time at Work Survey, 2012 (<https://www.sfgate.com/jobs/salary/article/2013-Wasting-Time-at-Work-Survey-4374026.php>)
- A.Gouveia, 2013 Wasting Time at Work Survey (<https://www.sfgate.com/jobs/salary/article/2013-Wasting-Time-at-Work-Survey-4374026.php>)
- Ahmad, A., & Omar, Z. (2017). Age and gender differences in employee cyberloafing behavior.
- Arora, B. (2013). Cyber Crimes Schemes and Behaviors. *Journal of Advanced Research in Computer Science and Software Engineering Research*, 3(5).
- Akman, I., & Mishra, A. (2010). Gender, age and income differences in internet usage among employees in organizations. *Computers in Human Behavior*, 26(3), 482-490.
- Akbari, M. (2017). Metacognitions or distress intolerance: The mediating role in the relationship between emotional dysregulation and problematic internet use. *Addictive behaviors reports*, 6, 128-133.
- Attell, B. K., Brown, K. K., & Treiber, L. A. (2017). Workplace bullying, perceived job stressors, and psychological distress: Gender and race differences in the stress process. *Social science research*, 65, 210-221.
- Antoniadou, N., & Kokkinos, C. M. (2015). Cyber and school bullying: Same or different phenomena?. *Aggression and violent behavior*, 25, 363-372.
- Bock, G. W., & Ho, S. L. (2009). Non-work related computing (NWRC). *Communications of the ACM*, 52, 124-128.

- Balakrishnan, V. (2015). Cyberbullying among young adults in Malaysia: The roles of gender, age and Internet frequency. *Computers in Human Behavior*, 46, 149-157.
- Chen, J. V., Chen, C. C., & Yang, H. H. (2008). An empirical evaluation of key factors contributing to internet abuse in the workplace. *Industrial Management & Data Systems*, 108(1), 87-106.
- Coker, B. L. (2011). Freedom to surf: the positive effects of workplace Internet leisure browsing. *New Technology, Work and Employment*, 26(3), 238-247.
- Cho, O. H., Cha, K. S., & Yoo, Y. S. (2015). Awareness and attitudes towards violence and abuse among emergency nurses. *Asian nursing research*, 9(3), 213-218.
- Cudo, A., Dobosz, M., Jarzabek-Cudo, A., & Basaj, Ł. (2016). Problematic Internet use and intrapersonal and interpersonal attitudes in adolescents. *Postępy Psychiatrii i Neurologii*, 25(3), 159-178.
- Duru, P., Ocaktan, M. E., Çelen, Ü., & Örsal, Ö. (2018). The effect of workplace bullying perception on psychological symptoms: a structural equation approach. *Safety and health at work*, 9(2), 210-215.
- Dubowitz, H. (2017). Child sexual abuse and exploitation—A global glimpse. *Child abuse & neglect*, 66, 2-8.
- Fornell, C., & Larcker, D. F. (1981). Structural equation models with unobservable variables and measurement error: Algebra and statistics. *Journal of marketing research*, 382-388.
- Gholami, R., Sulaiman, A. B., Ramayah, T., & Molla, A. (2013). Senior managers' perception on green information systems (IS) adoption and environmental performance: Results from a field survey. *Information & Management*, 50(7), 431-438.

- Hussain, S., & Parida, T. (2017). Exploring cyberloafing behavior in South-central Ethiopia: A close look at Madda Walabu University. *Journal of Media and Communication Studies*, 9(2), 10-16.
- Hassan, H. M., Reza, D. M., & Farkhad, M. A. A. (2015). An experimental study of influential elements on cyberloafing from general deterrence theory perspective case study: Tehran subway organization. *International Business Research*, 8(3), 91.
- Huma, Z. E., Hussain, S., Thurasamy, R., & Malik, M. I. (2017). Determinants of cyberloafing: A comparative study of a public and private sector organization. *Internet Research*, 27(1), 97-117.
- Hair Jr, J. F., Hult, G. T. M., Ringle, C., & Sarstedt, M. (2016). *A primer on partial least squares structural equation modeling (PLS-SEM)*. Sage Publications.
- Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*, 3(7), e00346.
- Hassan, H. M., Reza, D. M., & Farkhad, M. A. A. (2015). An experimental study of influential elements on cyberloafing from general deterrence theory perspective case study: Tehran subway organization. *International Business Research*, 8(3), 91.
- Jamaluddin, H., Ahmad, Z., Alias, M., & Simun, M. (2015). Personal Internet use: The use of personal mobile devices at the workplace. *Procedia-Social and Behavioral Sciences*, 172, 495-502.
- Jiang, H., & Tsohou, A. (2015, May). The Same Antecedents Do Not Fit All Activities: An Activity-specific Model of Personal Internet Use in Workplace. In *ECIS*.

- Jaradat, Y., Nielsen, M. B., Kristensen, P., Nijem, K., Bjertness, E., Stigum, H., & Bast-Pettersen, R. (2016). Workplace aggression, psychological distress, and job satisfaction among Palestinian nurses: A cross-sectional study. *Applied nursing research, 32*, 190-198.
- König, C. J., & De La Guardia, M. E. C. (2014). Exploring the positive side of personal internet use at work: Does it help in managing the border between work and nonwork?. *Computers in Human Behavior, 30*, 355-360.
- K Koay, Y., Soh, P. C. H., & Chew, K. W. (2017). Antecedents and consequences of cyberloafing: Evidence from the Malaysian ICT industry. *First Monday, 22*(3).
- Koay, K. Y., Soh, P. C. H., & Chew, K. W. (2017). Do employees' private demands lead to cyberloafing? The mediating role of job stress. *Management Research Review, 40*(9), 1025-1038.
- Kim, J. J., Park, E. H. E., & Baskerville, R. L. (2016). A model of emotion and computer abuse. *Information & Management, 53*(1), 91-108.
- Kim, K., Triana, M., Chung, K., & Oh, N. (2015). When do employees cyberloaf? An interactionist perspective examining individual differences, justice, and empowerment.
- Karabulut, A. T. (2016). Bullying: harmful and hidden behavior in organizations. *Procedia-Social and Behavioral Sciences, 229*, 4-11.
- Lim, V. K., & Chen, D. J. (2012). Cyberloafing at the workplace: gain or drain on work?. *Behaviour & Information Technology, 31*(4), 343-353.
- Lee, O. K., Lim, K. H., & Wong, W. M. (2005, January). Why employees do non-work-related computing: an exploratory investigation through multiple theoretical perspectives. In *System Sciences, 2005. HICSS'05. Proceedings of the 38th Annual Hawaii International Conference on* (pp. 185c-185c). IEEE.

- Li, X., Newman, J., Li, D., & Zhang, H. (2016). Temperament and adolescent problematic Internet use: The mediating role of deviant peer affiliation. *Computers in Human Behavior*, 60, 342-350.
- Lai, F. T. T., & Kwan, J. L. Y. (2017). The presence of heavy Internet using peers is protective of the risk of problematic Internet use (PIU) in adolescents when the amount of use increases. *Children and Youth Services Review*, 73, 74-78.
- McBride, M., Carter, L., & Warkentin, M. (2012). Exploring the role of individual employee characteristics and personality on employee compliance with cybersecurity policies. RTI International-Institute for Homeland Security Solutions.
- Mahatanankoon, P., Anandarajan, M., & Igbaria, M. (2004). Development of a measure of personal web usage in the workplace. *CyberPsychology & Behavior*, 7(1), 93-104.
- Mashi, M. S., & Salimon, M. G. (2016). Consideration of future consequences as an antecedent of employee cyberloafing behavior among selected working adults Nigeria. *International Journal of Business and Technopreneurship*, 6(2), 319-334.
- Madden, M. (2009). *The audience for online video-sharing sites shoots up*. Washington, DC: Pew Internet & American Life Project.
- Nasaescu, E., Marín-López, I., Llorent, V. J., Ortega-Ruiz, R., & Zych, I. (2018). Abuse of technology in adolescence and its relation to social and emotional competencies, emotions in online communication, and bullying. *Computers in Human Behavior*, 88, 114-120.
- Özkalp, E., Aydoğan, U. ve Tekeli, S. (2012). A New Phenomenon on Organizational Behavior And Deviant Work Life: His Virtual Cyberloafing) And The Effects On Business Relationships, *Journal of Cement Employer*, 26 (2): 18-33.

- Phillips, J. G., & Reddie, L. (2007). Decisional style and self-reported email use in the workplace. *Computers in Human Behavior*, 23(5), 2414-2428.
- Rosenberg, M. (1965). *Self-esteem scale*.
- RuningSawitri, H. S. (2012). Role of Internet experience in moderating influence of work stressor on cyberloafing. *Procedia-Social and Behavioral Sciences*, 57, 320-324.
- Rajalakshmi, M., & Naresh, B. (2018). Influence of psychological contract on workplace bullying. *Aggression and violent behavior*.
- Simon Lloyd D. Restubog, Patrick Raymund James M. Garcia, Lemuel S. Toledano, Rajiv K. Amarnani, Laramie R. Tolentino, Robert L. Tang. 2011. Yielding to (cyber)-temptation: Exploring the buffering role of self-control in the relationship between organizational justice and cyberloafing behavior in the workplace. *Journal of Research in Personality* 45, 247-251. [CrossRef]
- Ong, R. (2015). Cyber-bullying and young people: How Hong Kong keeps the new playground safe. *Computer Law & Security Review*, 31(5), 668-678.
- Öztürk, E., & Özmen, S. K. (2016). The relationship of self-perception, personality and high school type with the level of problematic internet use in adolescents. *Computers in Human Behavior*, 65, 501-507.
- Shrivastava, A., Sharma, M. K., & Marimuthu, P. (2016). Internet use at workplaces and its effects on working style in indian context: An exploration. *Indian journal of occupational and environmental medicine*, 20(2), 88.
- Tehrani, N. (2016). Extraversion, neuroticism and secondary trauma in Internet child abuse investigators. *Occupational medicine*, 66(5), 403-407.

- Tang, K., Qu, X., Li, C., & Tan, S. (2018). Childhood sexual abuse, risky sexual behaviors and adverse reproductive health outcomes among Chinese college students. *Child abuse & neglect, 84*, 123-130.
- Vahdati, S., & Yasini, N. (2015). Factors affecting internet frauds in private sector: A case study in cyberspace surveillance and scam monitoring agency of Iran. *Computers in Human Behavior, 51*, 180-187.
- Vitak, J., Crouse, J., & LaRose, R. (2011). Personal Internet use at work: Understanding cyberslacking. *Computers in Human Behavior, 27*(5), 1751-1759.
- Young, K. S., & Case, C. J. (2004). Internet abuse in the workplace: new trends in risk management. *CyberPsychology & Behavior, 7*(1), 105-111.
- Younes, F., Halawi, G., Jabbour, H., El Osta, N., Karam, L., Hajj, A., & Khabbaz, L. R. (2016). Internet addiction and relationships with insomnia, anxiety, depression, stress and self-esteem in university students: a cross-sectional designed study. *PloS one, 11*(9), e0161126.
- Yeik, K. K., Soh, P. C. H., & Wai, C. K. A Proposed Conceptual Model of Internet Use, Addiction and Job Productivity in Malaysia.
- Yun, S., & Kang, J. (2018). Influencing factors and consequences of workplace bullying among nurses: a structural equation modeling. *Asian nursing research, 12*(1), 26-33.
- Waasdorp, T. E., & Bradshaw, C. P. (2015). The overlap between cyberbullying and traditional bullying. *Journal of Adolescent Health, 56*(5), 483-488.