

# Factors Influencing the Cyberslacking Behavior and Internet Abusive Intention in Academic Settings: A Structural Equation Modeling Approach

Shampa Rani Das, Mohammad Hassan Seif, Imran Mahmud and  
Ali Vafaei-Zadeh

**Abstract---** *In this study, a new research model is proposed to evaluate the abusive intention of cyberslacking behavior among the employees of a company. Cyberslacking can be considered as the non-productive behavior where the employees get engaged in personal activities in internet during office hours leaving their assigned activities behind. This behavior creates psychological effect on the employees and productivity gets diminished as a result. The aims of this study were firstly to find out the factors that influence cyberslacking behavior and secondly to examine whether there exists any relationship between cyberslacking behavior and internet abusive intention. In our model, low self-esteem, private demand and rules and regulations have direct impact on cyberslacking behavior and 4 hypotheses were developed accordingly. Data was collected from 106 academics from two different universities through survey questionnaire. SPSS v.21 was used to calculate the frequency of demographic questionnaire and Smart PLS v.3.0 was employed to test the hypotheses. According to the result, both the self-esteem and private demand had significant effect but rules and regulations did not have significant effect on cyberslacking behavior. Most importantly, our newly proposed model established the relationship between cyber-slacking and abuse intention and the hypothesis resulted significant.*

**Keywords---** *Cyberslacking, Structural Equation, Internet Abusive.*

---

## I. INTRODUCTION

Cyberslacking is defined as the utilization of electronic devices connected through internet technology, i.e., computers, mobile etc. at the workplace where users get engaged with the activities which are not related to assigned tasks. In other words, it can be considered as the leisure browsing in internet during work hours for personal reasons [1]. The problem of cyberslacking at workplace is on the rise now a day. Cyberslacking can lead to shirk the performance of the employees at the workplace. Typical cyberslacking activities include browsing social media, surfing porn sites, online shopping, gambling, gaming etc. [2].

Due to the ease availability of internet at the workplace, the employees tend to misuse the facilities without realizing the consequences. Few years ago, UK companies lost almost £2.5m each year due to these undesired leisure surfing by CIPD (Chartered Institute of Personnel Development). As per the research, most popular unassigned activities performed by employees are instant messages, online shopping, blogging etc. [3]

---

*Shampa Rani Das, Department of Software Engineering, Daffodil International University, Dhaka, Bangladesh.  
Mohammad Hassan Seif, Associate Professor, Department of Educational Science, Payame Noor University, Tehran, Iran.  
Imran Mahmud, Department of Information Technology & Management, Daffodil International University, Dhaka, Bangladesh.  
Ali Vafaei-Zadeh, Graduate School of Business, Universiti Sains Malaysia, Penang, Malaysia.*

Eight years ago, a survey was first conducted by a magazine which revealed that employees spend about 1.44 hours surfing the internet for personal enjoyment [4]. At the same time, it was also reported that employees find it difficult to focus on their assigned tasks after the weekend. In addition, they used to feel unfit and their productivity declined as a result.

Recently, [5] has found that employees waste 20–24% of their work time due to cyberslacking behavior. According to a survey carried out in India, on an average participant remain busy for 1.55 hours in browsing social networking sites, 1.44 hours in recreational sites, 1.46 hours in knowledge sharing and 1 hour in bill payments in each working day.

Previously, reference [6] reported that these unassigned activities consume 30–50% of work hours and the total annual loss of productivity was measured about \$1 billion. Besides, employees are observed to spend one to three hours per day in web surfing for leisure activities during working hours [7]. Interestingly, [8] conducted a survey on 1,000 employees of a company. The loss of productivity was examined around \$35 million annually due to just an hour of cyberslacking behavior by employees during office hours.

Most of the studies indicate that the consequences of cyberslacking behavior can become a serious issue. Therefore, the companies should take steps against the employees' cyberslacking behavior for 3 reasons. Firstly, cyberslacking during office hours consumes internet bandwidth and it becomes totally wasted. Secondly, there could be legal implications for the company when employees exploit business assets for personal purposes. Lastly, there exists a fear of declining productivity.

The previous researchers conducted their research on individual and organizational factors separately. These factors made impact on cyberslacking behavior due to intention of abusing the internet at the workplace [9], [1], [5]. As a result, these studies approached, firstly, low self-esteem and private demand from individual point of view. And secondly the result approached rules and regulations from organizational perspectives. Again, according to [9], internet abuse is considered as an extension of internet addiction. So, certainly a research gap exists and it is required to test the possible relationship between cyberslacking behavior and internet abusive intention at the workplace during office hours. Thus, the following research questions will be analyzed in this paper:

RQ1: What are the factors that influence cyberslacking behavior?

RQ2: Is there any effect of cyberslacking behavior in internet abusive intention?

## **II. RESEARCH MODEL DEVELOPMENT**

Our proposed model argues that self-esteem (SE) influence the employees' internet addiction which causes internet abuse intention at work [9]. It means self-esteem has a significant relationship with abusive intention. Therefore, it is obvious that more self-esteem will lead to higher cyberslacking (CS). So, it also can be stated that cyberslacking is related with low self-esteem (LSE). Thus, we hypothesize:

H1: Low self-esteem has a positive impact on cyberslacking behavior.

Again, the willingness to engage in internet misuse during office hours was referred by cyber-loading [10] which

was based on user perspectives. The result of the study expressed that private demand (PD) had a positive impact on cyber-loafing [5]. As a result, it can be argued that private demand has an effective relationship with personal internet use which leads to cyber-slacking. Therefore, the following hypothesis is proposed:

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

Further, a research disclosed that organization's rules and regulations (RR) had significant impact on internet deception [11]. If rules and regulations are strictly imposed against cyber-loafing, the less intention will be observed [12]. So, it is clear that cyberslacking motive can be reduced during office hours through enforcing appropriate rules and regulations. In addition, training on how to do the official activities efficiently can add advantages. So, the following hypothesis is projected:

H3: Rules and regulations have a positive impact on cyberslacking.

Furthermore, many factors can encourage the employees to become an abuser of online activities. We can take short-term comfort, excitement, distraction [13] etc. for example. So, it would be imperative to examine whether internet abuse intention (AI) is the result of serious cyberslacking problems from an individual perspective. So, it can be hypnotized that:

H4: cyberslacking has a positive impact on abuse intention.

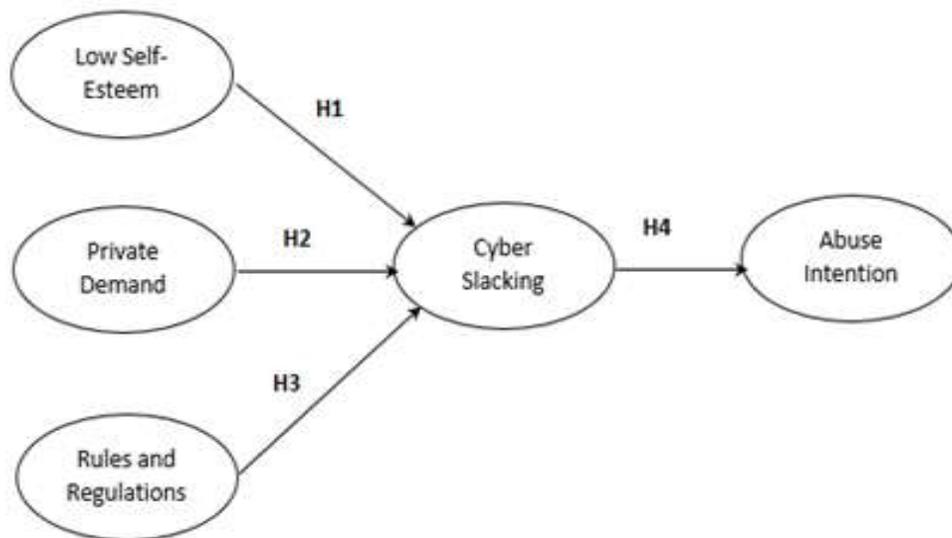


Figure 1: Research Model

### III. RESEARCH METHOD

#### *Data Collection Procedure and Respondents' Profile*

In order to study more on cyberslacking and abusive intention, an empirical survey was conducted among academic and non-academic staffs to validate the proposed model. Therefore, 200 questionnaires were distributed among the academic and non-academic staffs of two private universities namely Daffodil International University and Stamford University in Bangladesh where 106 usable questionnaires were received

from the survey.

Table 1: Demographic Information

	<i>Frequency</i>	<i>Percentage</i>
<b>Gender</b>		
<b>Male</b>	70	66.0
<b>Female</b>	36	34.0
<b>Age</b>		
<b>20- 30</b>	64	60.3
<b>31-40</b>	32	30.0
<b>41-50</b>	9	8.3
<b>50 above</b>	1	0.9
<b>Marital status</b>		
<b>Unmarried</b>	66	62.3
<b>Married</b>	40	37.7
<b>Education</b>		
<b>Diploma</b>	2	1.9
<b>Bachelor</b>	40	37.7
<b>Masters</b>	58	54.7
<b>PhD</b>	6	5.7

The demographic of the respondents are tabulated in Table 1 which was derived from descriptive analysis. It was examined that demographic factors i.e. age, gender, marital status, educational level and routinized internet use (riu) significantly influence the cyberslacking and internet abuse intention among the targeted peoples (IT related teachers and employees). In the survey, most of the respondents have more than 6 years of internet usage experience. The final data is comprised of the following factors such as 70 males (66%) and 36 females (34%), 66 unmarried (62.3%) and 40 married (37.7%), education level contained diploma (1.9%), bachelor (37.7%), masters (54.7%) and PhD (5.7%). The respondents belong to the 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%). 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%). To be noted, routinized internet users use internet on a regular basis.

### ***Measurement Items***

To measure the relationship among the variables, items were adapted from the established literature. Items for low self-esteem was adapted from Chen et al. (2008) [9], private demand was adapted from [5], rules and regulations was adapted from [11]. cyberslacking was identified from and measured using binary variables ‘0’ and ‘1’. The ‘0’ indicates that the respondents did not perform questioned tasks at working hours. On the other hand, ‘1’ specifies that the respondents did the questioned tasks during work time. 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’ using internet.

We developed a scenario based on the provided questionnaire to investigate the internet abuse intention among the employees. The scenario is described below;

“Suppose, you work in an IT company and you have successfully completed several projects in the last five years. In addition, you are always very dedicated to your tasks as assigned by your supervisors. Unfortunately, you

are not appreciated well from concerned authority for your successful efforts. Besides, you did not receive salary increment in the last two years even of your utmost sincerity and dedication towards the assigned tasks. On the other hand, your colleagues are always credited without so much successful efforts and salary gets incremented regularly. Suddenly, your competitor gets promoted whereas you were not considered. These situations are humiliating for you for sure. You also hear a rumor that the company might release you soon for no reason. Therefore, you have the options to take the revenge against the company because of your high liberty within the company. From your past experience, you know that you can access several confidential files and documents easily. Most importantly, the security control system of the company is too poor to identify anyone. You know all of the confidential information of your company and also know how to make maximum damage out of it without leaving any trace”. This abuse intention was measured using the scale derived from [14] 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”.

SPSS v.21 was used to calculate the frequency of demographic questionnaire and SmartPLS V3.0 was employed to test the hypotheses (relationship between the variables) by following the research papers [15],[16].

#### IV. RESULTS AND ANALYSIS

We assessed the measurement model that examined two types of validities namely convergent reliability and validity and discriminant validity. Convergent validity was assessed through composite reliability of each scale and average variance extracted (AVE) for each construct. The composite reliabilities (CR) were found to be higher than 0.7 and the AVE were also higher than 0.5 [17] as suggested in the literature (see table 2).

Table 2: AVE and CR

	<i>Composite Reliability</i>	<i>AVE</i>
AI	0.923	0.800
CS	1.000	1.000
PD	0.884	0.656
RR	0.875	0.586
LSE	0.758	0.517

Table 3: Discriminant Validity

	<i>AI</i>	<i>CS</i>	<i>PD</i>	<i>RR</i>	<i>LSE</i>
AI	<b>0.895</b>				
CS	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>	
LSE	0.094	0.348	0.220	0.079	<b>0.719</b>

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

The discriminant validity (the degree to which items differentiate among constructs) was examined by

the following the [18] criterion of comparing the correlations between constructs and the square root of the average variance extracted for that construct (see table 3). All the values on the diagonals are greater than the corresponding row and column values indicating that the measures are discriminant.

Table 4: Path Co-efficient and T Statistics

		<i>Path Co-efficient</i>	<i>T Statistics</i>	<i>Remark</i>
<b>H1</b>	<b>LSE -&gt; CS</b>	0.306	3.263	Supported
<b>H2</b>	<b>PD -&gt; CS</b>	0.160	1.856	Supported
<b>H2</b>	<b>RR -&gt; CS</b>	0.108	0.912	Not supported
<b>H4</b>	<b>CS -&gt; AI</b>	0.173	2.190	Supported

The t-values were evaluated using the bootstrap routine with 5,000 samples [19] to analysis the path coefficients of the research model. Among the four hypotheses, three of our hypotheses are found to be significant. Regarding H1, we can confirm a significant relationship between low self-esteem and cyberslacking behavior (H1 supported,  $b = 0.306$ ,  $p < 0.05$ ). Furthermore, results also reveal that a significant relationship is observed between private demand and cyberslacking behavior (H2 is supported,  $b = 0.160$ ,  $p < 0.05$ ). In terms of the outcome of cyberslacking behavior, there is strong relationship with abusive intention (H4 is supported,  $b = 0.173$ ,  $p < 0.05$ ). However, no significant relationship was found for organizational rules and regulations and cyberslacking behavior ( $b = 0.108$ ,  $p > 0.05$ ). So, our hypothesis H3 is not supported.

## V. DISCUSSION

Based on the research of [9], we conceptualized the relationship between low self-esteem and cyberslacking behavior and low effect was found between the variables in our result. Therefore, the result remains consistent with the previous research of [9]. Previously [5], [20] investigated the relationship of private demand with personal internet use. Our result also confirms that the private demand has low effect on cyberslacking behavior. Even though organizational rules and regulations for internet usage has no effect over cyber-slack, many practitioners suggested that the company's internet usage policy should be re-evaluated after discussion with directors, managers, in-house computer experts, and company attorneys. These policies should also be clear to all employees. In addition, the rules and regulations of the company should be strict. Otherwise, employees might have tendency to breach the rules and to take undue advantages. Most importantly, our newly proposed relationship between cyberslacking and abuse intention was significant and established.

## VI. IMPLICATIONS

A company might face obstacles to develop an effective management system without addressing this cyberslacking behavior with adequate attention. Moreover, managers must be able to handle the critical situations to facilitate their company's success. Through developing employees' awareness of the consequences of cyberslacking activities, some degree of self-restraint can be achieved. The problem could be linked to performance related adverse outcomes like missed deadlines, negative employee evaluations etc. Managers can reduce cyberslacking by adopting several measures, such as monitoring of activities in the network, blocking access to certain websites, checking applications installed on company computers, checking the type of data that employees collect, and how they are stored. Besides, software can be installed that enables

control and remote management of computers from the administrator or employer level. Without effective monitoring system, employees who are addicted to the internet might show some abusive internet behavior. As a pre-emptive measure, employees should also be allowed to take short breaks and a certain amount of time off from the workplace to reduce the boredom and monotony of regular works. The measurement, in turn, could lead to better productivity.

## VII. CONCLUSION

Similar to other research works, this study is also not free from few limitations. Firstly, this research is conducted among the employees of two different private universities of Bangladesh. Moreover, it is a cross sectional study and a longitudinal study might confirm a different result. Secondly, generalizability of this research may be constrained among employees from academia whereas the results might vary in different industry settings. Finally, we assessed the intention of abuse rather than actual abusive behavior. These limitations will be addressed in our future study.

## REFERENCES

- [1] J. Vitak, J. Crouse, and R. Larose, "Personal Internet use at work: Understanding cyberslacking," *Comput. Human Behav.*, vol. 27, no. 5, pp. 1751–1759, 2011.
- [2] N. P. Rana, E. Slade, S. Kitching, and Y. K. Dwivedi, "The IT way of loafing in class: Extending the theory of planned behavior (TPB) to understand students' cyberslacking intentions," *Comput. Human Behav.*, vol. 101, no. October 2018, pp. 114–123, 2019.
- [3] M. Madden, "The Audience for Online Video- Sharing Sites Shoots Up The share of online adults who watch videos on video-sharing," 2009.
- [4] S.L.D. Restubog, K.L. Scott, and T.J. Zagenczyk, "When Distress Hits Home : The Role of Contextual Factors and Psychological Distress in Predicting Employees' Responses to Abusive Supervision," vol. 96, no. 4, pp. 713–729, 2011.
- [5] Kian Yeik Koay, Patrick Chin-Hooi Soh and Kok Wai Chew, "Antecedents and consequences of cyberloafing: Evidence from the Malaysian ICT industry", *First Monday*, Volume 22, Number 3, 6 March 2017.
- [6] Daniel Bukszpan. "The highest grossing children's movies of all-time", 2011. Retrieved from <https://www.cnn.com/2011/04/14/The-Highest-Grossing-Childrens-Movies-of-All-Time.html>
- [7] S.M. Heathfield, "How (and why) to Foster Employee satisfaction," May 12, 2019. Retrieved from <https://www.thebalancecareers.com/employee-satisfaction-1918014>
- [8] Stats, October 24, 2017. Retrieved from <https://staffmonitoring.com/p32/stats.htm>
- [9] J.V Chen and C.C. Chen, "An empirical evaluation of key factors contributing to internet abuse in the workplace," vol. 108, no. 1, pp. 87–106, 2007.
- [10] One-Ki Daniel, Lim, Kai H, Wong Wing Man, "Why employees do non-work-related computing: an exploratory investigation through multiple theoretical perspectives", *Proceedings of the Annual Hawaii International Conference on System Sciences*, pp. 185c-185c, 2005.
- [11] S. Vahdati and N. Yasini, "Computers in Human Behavior Factors affecting internet frauds in private sector : A case study in Cyberspace Surveillance and Scam Monitoring Agency of Iran q," *Comput. Human Behav.*, vol. 51, pp. 180–187, 2015.
- [12] H.M. Hassan, D.M. Reza, and M.A. Farkhad, "An Experimental Study of Influential Elements on Cyberloafing from General Deterrence Theory Perspective Case Study : Tehran Subway Organization," vol. 8, no. 3, pp. 91–98, 2015.
- [13] Rewarch, "Internet addiction - time to be taken seriously?" vol. 8, no. 5, pp. 413–418, 2000.
- [14] J. Jonathan, E. Hee, E. Park, and R.L. Baskerville, "Information & Management A model of emotion and computer abuse," vol. 53, pp. 91–108, 2016.
- [15] Mahmud, T. Ramayah, and S. Kurnia, "To use or not to use : Modelling end user grumbling as user resistance in pre-implementation stage of enterprise resource planning system," *Inf. Syst.*, vol. 69, pp. 164–179, 2017.

- [16] T.R. Toma, "Satisfaction and its impact on revisit intention and word of newspaper reading satisfaction and its impact," no. September 2018, 2019.
- [17] J.F. Hair, J.J. Risher, and C.M. Ringle, "When to use and how to report the results of PLS-SEM," vol. 31, no. 1, pp. 2–24, 2018.
- [18] T.H.E. Algebra, O.F. Factor, and S. Modeling. "Unobservable Variables and Measurement Error : *Algebra and Statistics*," vol. XVIII, no. August, pp. 382–388, 1981.
- [19] C.M. Ringle and R.R. Sinkovics, "The use of partial least squares path modeling in international marketing," vol. 20, no. 2009, pp. 277–319, 2004.
- [20] C.J. König, M.E. Caner, and D. Guardia. "Computers in Human Behavior Exploring the positive side of personal internet use at work : *Does it help in managing the border between work and nonwork?*" vol. 30, pp. 355–360, 2014.