Antecedent, Consequences, and Policies View of Cyberloafing among the Employees

Mohommad M.Dmour, Hanif S.Bakar, Mohammad R.Hamzah
No28, Jalan Maju 8, Taman Kemjuan, Kangar Perlis 01000
mohmmaddmour24@gmail.com

Abstract. As the Internet has brought a lot of benefits to the work the Internet also creates new problems that were not found before as the cyberloafing. The cyberloafing defined as an activity involving the use of smart mobile and computers devices at the workplace for personal purpose activity by employees. In this paper, the researcher going to show some the demographic areas and the factors that effect on the employees’ attraction to cyberloafing from the previous studies have been shown consciences of cyberloafing in both of employees and organization. Finally, this paper will present some of the strategies to control and reduce the cyberloafing in the organizations.

1. Introduction

The Internet has become a very important aspect of our life today’s and has changed people’s lifestyle in ways which were unexpected before, especially in the work. Where the Internet is available at work and used by employees and employers offers great possibilities for organizations, for instance, increase the speed of communication in the organization as well as with their client (Yogun, 2015), and it reduces the distances between the employees where they can work far from their work sites, and they can work in teams with the employees in a different place in the world (Stone, Krueger, & Takach, 2017). However, the Internet creates some problems that were not have been there before such as the cyberbullying, sexting, hacker, cyberloafing. This research will focus on cyberloafing phenomenon among the employees.

There are many terms to express cyberloafing such as cyberslacking, or personal Internet usage, this terms and other similar terms defined as the voluntary act of employee using the Internet access for personal purpose activity during the work hours distracting the employee from work tasks and unproductive work time (Lim, 2002). With the wide development of Internet access using mobile, laptop and tablet, the definition of cyberloafing continues to evolve and change in the modern research such as an activity involving the use of smart mobile and computers devices at the workplace for personal purpose activity by employees (Jandaghi, Alvani, Matin, & Fakheri, 2015).

Cyberloafing can be considered as a counterproductive work behavior an umbrella term for behaviors that harm, waste of the employees’ time at work, and even have the potential to harm the organizations (Leonard, Chukwuemeka, & Emmanuel, 2018; Mercado, Giordano, & Dilchert, 2017; Pindel, Kraicevska, & Spector, 2018; Varghese & Barber, 2017), and threatens employment security (Al-Shuaibi, Subramaniam, & Mohd-Shamsudin, 2014). Previous studied on the misuse of the Internet indicated that cyberloafing is prevalent in organizations and causing significant financial losses. For example, according to Mysammy (2013) in the United States showed there is 61 percent of United
States employees engage in doing non-work related activities during working hours, resulting in a monetary loss almost US$ 4,500 per employee and productivity loss worth US$ 178 billion annually. In a follow-up study, Jandaghi et al. (2015) shown that the phenomenon of cyberloafing in the US costs is $183 billion annually. In the recent statistics by Staffmonitoring (2017) shown that a company with 1,000 Internet users could lose upwards of $35 million in productivity annually from just an hour of daily web surfing by employees. If this statistic showed the right scenario at work, the organizations will eventually end up with productivity and performance losses. In addition, Cyberloafing causes an increase in support costs for IT, decreased productivity, wasting of time, company resources, reduce the productive and introduced hazards over security threats and damage to the reputation of the organization (Al-Shuaibi, Shamsedin, & Subramaniam, 2013; Leonard et al., 2018; Saidin, Iskandar, & Dahlan, 2017; Sheikh, Atashgah, & Adibzadegan, 2015).

On the other hand, some researchers considered the cyberloafing as a beneficial activity for the employees for taking rest, stress reduction, self-development and refresh their mind for back to work and give a good performance for their organizations (Baturay & Toker, 2015; Lim & Chen, 2012). Likewise, the cyberloafing might lead to enhancing the learning environment, flexibility, creativity, and increase innovation (Derin & Gökçe, 2016). However, some managers ignore the physical and psychological benefits of job interruption and their positive impact on employee productivity. Lim and Chen (2012) found that browsing has a positive impact on employee emotions. Internet browsing provides an informal learning method, reduces stress, and promotes improved time management (Coker, 2011). In addition, the work breaks such as Internet surfing breaks can play an important role in the mental and physical well-being of workers and contribute positively to productivity (Cambo, Avrahami, & Lee, 2017). Dursun, Donmez, and Akbulut (2018) stated there are some types of cyberloafing that can even be considered as a facilitator for relaxation and self-development of employees.

2. Demographics of Cyberloafing

Because of the development of technology, cyberloafing is possible to be done regardless of occupation. A lot of studies report that a large number of sample to measure the cyberloafing (Aktibulut, Dönmez, & Dursun, 2017; Andreassen, Torsheim, & Pallesen, 2014; Cheng, Li, Zhai, & Pallesen, 2014; Dursun et al., 2018; Gökçeçarslan, Mumcu, Haşlaman, & Çevik, 2016; B. Lee, 2017; Lim & Chen, 2012). One of these studies found that 65% of employees reported using the Internet for personal purpose during the work (Cheng et al., 2014). Some of the studies found the young workers are more likely to do cyberloafing behavior (Çınar & Karcioğlu, 2015; Sheikh et al., 2015; Varghese & Barber, 2017). On the other hand, Ahmad and Omar (2017); Rahimmia and Mazidi (2015); Yan and Yang (2014) found age has no significant difference in the prevalence of cyberloafing.

Several researchers investigated the relationship of the experience and skill of usage Internet with the cyberloafing and they found the individuals who have experience and skill usage Internet more likely and spend more time on the cyberloafing activities than individuals who have less experience and skill of usage Internet (Baturay & Toker, 2015; Mercado et al., 2017). On the other hand, Li, Luo, Zhang, and Sarathy (2017) found there is no significant difference between the experience of using the Internet and the cyberloafing.

In another study investigating the relationship between education level and cyberloafing found there is a negative relationship between the education level and the cyberloafing behavior, which the employees with higher education showing lower levels of cyberloafing (Rahimmia & Mazidi, 2015; Sheikh et al., 2015). On the other hand, the recent study by Mercado, Giordano, and Dilchert (2017) found there is a positive relationship between education and the cyberloafing behavior, signifying that more educated individuals engaged in greater cyberloafing. Another study by Andreassen, Torsheim, and Pallesen (2014) stated that high-level of managers were the highest offenders of cyberloafing in spite of their negative attitudes toward cyberloafing behaviors. This may be because the of employees with higher statuses have more access to the tools to cyberloafing (for example, iPhones, Tablets,
laptops, PC) which make them able to commit cyberloafing at higher levels more than the individuals at the lower or normal levels of an organization.

Interestingly, several researchers investigated the relationship between gender and cyberloafing and they found the males are more likely to spend more time on the cyberloafing activities than females (Ahmad & Omar, 2017; Baturay & Toker, 2015; Özcan, Gökçearslan, & Yüksel, 2017; Schings, 2014; Sheikh et al., 2015; Varghese & Barber, 2017; Yılmaz, Yılmaz, Öztürk, Sezer, & Karademir, 2015). On the other hand, Rahimnia and Mazidi (2015) found the females are more likely to commit cyberloafing than males. However, recent studies disclose that gender differences may vary consistently with the characteristics and kind of the cyberloafing activities (Akbulut et al., 2017; Dursun et al., 2018; Keser, Kavuk, & Numanoglu, 2016).

3. Antecedent of cyberloafing

The previous study investigates many of the factors that influence the cyberloafing such as boredom, stress, internet addiction, ability to hide, habit, personality traits, organization justice, and job demand.

The boredom at work has been shown to increase cyberloafing behavior (Mercado et al., 2017; Wan, Downey, & Stough, 2014). A cyberloafing may help the employees to pass free time or keep them committed to something during work time when they do not have work to do (Jandaghi et al., 2015). In these situations, cyberloafing can be a counter-boredom activity because it restores the boring situation at work to include more interesting components (Pindek et al., 2018). In addition, employees may use cyberloafing as a strategy to relieve stress. There are some studies that have shown that cyberloafing negatively affects the work stress (Andreassen et al., 2014; Blanchard & Henle, 2008; Lim, 2002; Yeik, Soh, & Chew, 2017a).

There is another factor that has been identified as contributing factor to cyberloafing which is the addiction to the Internet which has been shown to increase cyberloafing (Keser et al., 2016; Yan & Yang, 2014; Yaşar & Yurdugül, 2013). Yaşar and Yurdugül (2013) found the Internet addiction construct as one of the reasons that lead to cyberloafing activities. In another study by Keser et al. (2016) found the male Internet addiction level was higher than female. There are many researchers who have been investigating the relationship between the ability to hide with the cyberloafing (Askew et al., 2014; Mercado et al., 2017; Saidin et al., 2017; Sheikh et al., 2015). The ability to hide cyberloafing refers to the employee's ability to hide her or his activity on the Internet from her or his supervisors and colleagues based on conditions in her or his work environment (Saidin et al., 2017). Motivated by Askew et al. (2014) study shown the ability to hide cyberloafing is a significant predictor of cyberloafing. Mercado et al. (2017) found that the employees’ ability to hide cyberloafing shown a strong positive relationship with cyberloafing.

The cyberloafing also influenced by employees’ habit of using the Internet for personal purpose. Previous studies have shown that the habit has a strong predictive power of cyberloafing (Betts & Setterstrom, 2014; Jamaluddin, Ahmad, Alias, & Simun, 2015). In addition, the habit found to have a significant interaction effect on cyberloafing (Son & Park, 2016; Yeik, Soh, & Chew, 2017b). In a study by Huma, Hussain, Thurasamy, and Imran Malik (2017) found the employees in private organizations usually have less influence of habit over cyberloafing behavior than employees in public organizations.

One of the important factors that had been studied is the relationship between personality traits and cyberloafing behavior. Several studies found there is a relationship between personality traits and cyberloafing (Jia, Jia, & Karau, 2013; Lepp, Li, Barkley, & Salehi-Esfahani, 2015; Varghese & Barber, 2017; Yan & Yang, 2014). Recent studies have shown that personality traits of agreeableness have negatively related to cyberloafing (Andreassen et al., 2014; Jia et al., 2013; Varghese & Barber, 2017). Likewise, some of the studies present there is a negative relation between conscientiousness and cyberloafing (Andreassen et al., 2014; Kim, Triana, Chung, & Oh, 2015; Varghese & Barber, 2017). The fundamental desire to maintain and improve performance is likely to deter individuals who have a reputation for engaging in deviant behaviors such as cyberloafing. Similarly, employees who agree will demonstrate cooperative and trustworthy behavior.
On the other hand, there are some studies examine the relationship between openness and cyberloafing, and they found the openness has positively related with cyberloafing (Jia et al., 2013; Jia & Jia, 2015). Similarity, the traits extraversion and neuroticism have been positively related to cyberloafing (Andreassen et al., 2014; Varghese & Barber, 2017). Employees who have a high level of neuroticism tend to have emotional instability and anxiety (Varghese & Barber, 2017). Therefore, it is likely that these employees adopt adaptation strategies that can be avoided by nature, which may include the cyberloafing to avoid the work (Andreassen et al., 2014). The need to be in socially stimulating environments may encourage them to search for social networking sites or other online entertainment resources by cyberloafing (Varghese & Barber, 2017).

Another important factor that has an effect on cyberloafing is procrastination. While the researchers considered that procrastination is the most important personality traits that are positively related to the behavior of cyberloafing (O’Neill, Hambley, & Chatellier, 2014; Yan & Yang, 2014). In the other word, the employees they have a high level of procrastination they will be more likely to engage to cyberloafing actives although they are away from doing the organization task by using the Internet for personal purpose.

One of the important factors that have been the effect on the cyberloafing is the norms or social influences at the work (Askew, Buchner, Taing, Ilie, Baure & Coovwet, 2014; Mohd-shamsudin, Kura, & Alshuaib, 2014; Sheikh et al., 2015). Cyberloafing by co-workers indicates that behavior is acceptable which affects whether or not an individual participates in observable behavior (Askew et al., 2014). Askew et al. (2014) found also an individual is more likely to cyberloafing if there is a norm within the organization or in her or his working group that it is acceptable to deal with personal work online during working hours, and if that is strongly discouraged in the work, the employees will be less likely to be attracted to cyberloafing. Organizational policies, sanctions, and IT tracks have been found to prevent the cyberloafing (Andreassen et al., 2014). However, other research by Askew et al. (2014) supports that employees will do cyberloafing if they are confident that they will not get caught.

Organization justice has been related to increases the cyberloafing behaviors (Li, Luo, Zhang, & Sarathy, 2014; Li et al., 2017; Lim, 2002). The employees will do cyberloafing for a response to the perceived injustice in the workplace (Krishnan & Lim, 2010). Studies suggested that if the employees feel unfairly treated by organizations, they feel resentful and angry, they will be likely to seek revenge against the organization (Li et al., 2017; Son & Park, 2016). The result of this, employees will seek to engage in cyberloafing behaviors by performing low-quality work or working less.

Job demands considered as an important factor that has an effect on cyberloafing, there are many previous studies had investigated the relationship between the job demands and the cyberloafing (Al-Shuaibi, Shamsudin, & Subramaniam, 2014; Charoensukmongkol, 2014; Jandaghi et al., 2015). Al-Shuaibi et al (2014) proposition that the job demands will lead to stress in employees and it will increase the employees’ propensity to engage in cyberloafing behavior at the workplace. Charoensukmongkol (2014) found that job demands will positively be related to the intensity of social media usage at work. It means if the employees have low work demands the possibility of engaging in cyberloafing behavior is higher. This is because of the spare time of the employees. Therefore, when the employees don’t have enough work to do, they will engage in cyberloafing behavior to pass the time.

4. Consequences of Cyberloafing
The previous study had not focused on the consequences of cyberloafing as they focused on factors that effect on cyberloafing, hence it is less common (Jandaghi et al., 2015). The cyberloafing can lead to lose employee’s time and reduce job performance and productivity (Ugrin, Pearson, & Nickle, 2018), and increase the risk of information security breaches (Hadlington & Parsons, 2017). According to Ahmad and Omar (2017) act the cyberloafing is considered to be counterproductive because the participation of the employees in cyberloafing activities leads to effective in a negative
way to performance and efficiency. However, the cyberloafing has a beneficial effect for both employees and the organizations (Hartijasti, 2016).

Cyberloafing leads to the low performance of tasks by the loss of working time and productivity (Al-Shuaibi, Subramaniam, et al., 2014; Jandaghi et al., 2015). In this regard, the time spent in the cyberloafing is the time it would have been spent on the work, and any loss of working time is expected to be translated as lost productivity. In the study by Ugrin and Pearson (2013) shown the employees spend 60-80% of their time during the work hours on websites that have nothing to do with their tasks and responsibilities, reducing organizational performance. However, when the performance appraisal is perceived favorably by the employees, they are less likely to engage in cyberloafing behavior at work (Al-Shuaibi et al., 2013).

On another hand, the cyberloafing only effects on the performance of tasks in certain cases (Jandaghi et al., 2015). Sometimes the employees use the Internet for personal purpose when they have free time and do not have a task to do. This indicates that cyberloafing does not affect the loss of production in some cases. Indicates that each employee has a certain level of work they aspire to and puts enough work to get to this standard and engage to cyberloafing with some of the time leftovers. If this perspective is true, there must be a positive relationship between cyberloafing and task performance (Jandaghi et al., 2015).

Some previous study had investigated the relationship between the employment security with the cyberloafing especially in Jordan (Al-Shuaibi et al., 2013; Al-Shuaibi, Subramaniam, et al., 2014). The result from previous research when employees look at employment security positively, they are less likely to do the cyberloafing during the work (Al-Shuaibi et al., 2013; Al-Shuaibi, Subramaniam, et al., 2014). In the other word, because of the unemployment rate in Jordan is 18.5% (Tradingeconomics, 2018), the employees try to not do any bad behavior at work that may be the reason for being kicked out of work, because there is potential replacement that makes it easier to get the employees out of a company. For instance, some companies such as Hewlett-Packard and Xerox warn employees not to use the Internet for personal activity during work time, but the employees ignore the warning, many employees violated this policy, and some have even fired employees as a result (Jandaghi et al., 2015; Piscotty, Martindell, & Karim, 2016).

Though there are policies in the organizations, security tools are important to prevent employees from cyberloafing. However, employees who engaged in cyberloafing had significantly lower information security awareness and thus increases the risk of information security breaches (Hadlington & Parsons, 2017). There are many organizations that allow their employees to use their own electronic devices, like tablets and smartphones, for access to organization data (Lee, Warkentin, Crossler, & Otondo, 2016). Employees may use their devices to get access to the Internet without using organization's networks via their mobile data networks. In this situation, the organization manager needs to adopt security strategies and monitoring, such as tracking e-mail messages, blocking websites, and reviewing the browsing history (Harris & Patten, 2014).

There are many organizations that have used many strategies to control the cyberloafing behavior such as using a personal device, texting, data streaming, and voice messages (Baturay & Toker, 2015; Moody & Siponen, 2013). Organizations may use mobile device management systems to control and monitor almost all the functions of employee’s devices and to collect private data (Lee et al., 2016). However, it is hard to know the security risks faced by employees without having real knowledge about a security concept of information stored on their smartphones (Lee et al., 2016). Using smartphones at work and daily life may increase the risk of attacks (Lee et al., 2016). Although a smartphone is a personal property, it can be used by employees to access personal information and work information in accordance with the strategy of bring-your-own-device (Lee et al., 2016). Many organizations have confirmed that using smartphones to access organization databases lead to reduces operating costs (Harris & Patten, 2014; Lee et al., 2016). Therefore, about 75% of large organizations allow employees to access to the organization’s system by personal smartphone, many of these smartphones lack security application or even passwords that can protect from potential risks (Harris & Patten, 2014). There should be a secure system to protect the organization’s information and save
the working time when the employees connect their smartphones to the system directly or through the
desktop computer in the organization.

Most of the employers consider the cyberloafing as negative behavior and lead to production losses
(Andreassen et al., 2014). In the other side, there are some of the employees who considered the
cyberloafing as positive behavior (J-Ho & Ramayah, 2016). Actually, the cyberloafing positively
benefits both of the employers and employees (Baturay & Toker, 2015; Derin & Gökçe, 2016). Where
the employees can take rest, stress reduction, self-development and refresh their mind for back to work
and give a good result for their organizations (Baturay & Toker, 2015; Lim & Chen, 2012). Likewise,
the cyberloafing might lead to enhancing the learning environment, flexibility, creativity, and increase
the innovators (Derin & Gökçe, 2016). Therefore, organizations should not ignore or underestimate
the advantages of cyberloafing.

However, some managers ignore the physical and psychological benefits of job interruption
and their positive impact on employee productivity. Lim and Chen (2012) found that while
browsing had a positive impact on employee emotions. Internet browsing provides an informal
learning method, reduces stress, and promotes time management improvement (Coker, 2011). In
addition, a work break such as Internet surfing can play an important role in the mental and
physical well-being of workers and contribute positively to productivity (Cambo et al., 2017).
Dursun et al. (2018) stated there are some types of cyberloafing that can even be considered as a
facilitator for relaxation and self-development of employees.

5. Policies and Anti-Cyberloafing

Today, most of the organizations use policies and strategies for reducing the effect of cyberloafing in
the workplace and increase the productivity such as monitoring or blocking some of the website
(Baturay & Toker, 2015; Moody & Siponen, 2013). According to Glassman, Prosch, and Shao (2015),
the Internet monitoring and filtering software industry has grown exponentially with revenue of $ 1.18
billion in 2012. As J-Ho and Ramayah (2016) refer to the organizations needs to use policies which
might control and reduce the cyberloafing actives from the employee's intention, and the employers
and manager must give awards to employees who follow the rules. The study by Hadlington and
Parsons (2017) shown the employees who stated that their organization had a policy were less likely to
show a problem with the cyberloafing behavior. Hence, the organizations use many mechanisms to
reduce and control the cyberloafing, including prevention strategies, organizational control, and
monitoring strategies (Piscotty et al., 2016).

5.1. Organizational control

Organizational control has related with some terms such as policy control, system control, managerial
control, and behavior control and this terms represent the potential actions used to control employees
behavior and involve them in complying with institution policies and objectives (Piscotty et al., 2016).
Generally, the employees follow the organizational rules and policies when managers or employers are
forcing them to follow that, and when employees are aware that sanctions are in place (Rahimnia &
Mazidi, 2015; Son & Park, 2016). This strategy is based on employing many types of sanctions and
applying these sanctions to employees who violate the rules (Cheng et al., 2014).
If employees realize that there is a punishment in work and that punishers will apply them in practice
on others who commit or violate a regulatory policy, they will avoid a repetition of unwanted behavior
(Piscotty et al., 2016). The manager can control or reduce the behavior of unwanted employees by
making them expect different punishments if they continue to use the Internet for the personal purpose
during working time (Cheng et al., 2014). Although effective strategies must be in work to control the
misuse of the Internet in the workplace, including the punishment strategy and control strategy to
control the phenomenon of cyberloafing, supervisors should be close to employees, understand their
behavior, monitor and apply sanctions if they occur to any violations (Piscotty et al., 2016).

5.2. Electronic Monitoring Strategy
A study in the UK showed that computer users spend about 31.4 hours monthly surfing the Internet and 5.4 hours using their mobile devices to surf the web (Ofcom, 2015). In the same report shown people use a smartphone 61% more than desktop, where smartphones provide people with the freedom to browse wherever they are (Ofcom, 2015). Nevertheless, despite the many advantages associated with the use of e-mail and Internet tools, misuse the Internet at work has created legal challenges and new financial in the organizations (Dursun et al., 2018). Organizations have a lot of concerns about the cyberloafing by their employees and therefore some of the organizations adopt electronic monitoring strategy to protect their business to reduce or prevent potential risks to online services at work from employees (Piscotty et al., 2016).

Some concerns about the misuse of personal information of employees when employers monitor their employees' Internet activities including storing employee data and retrieving data for occasional review to ensure employee productivity and to avoid any financial liability that employees by “cyberloafing monitoring strategy” in terms of changing the work environment and worker behavior (Gökçearslan, Muncu, Haşlaman & Çevik , 2016). Additional concerns are focused on making employees feel discomfort, although organizational managers can monitor employees when they use the organization’s resources, as computers and other devices (Glassman et al., 2015). The monitoring and punishment for the employee who does cyberloafing activities may offend to employees by causing them to feel undervalued and distrusted. Consequently, their job satisfaction and morale may be affected (Son & Park, 2016). Sarpong and Rees (2014) investigated the concerns, discomfort, and employees' stress due to the use of the monitoring system during working hours and found that electronic monitoring is not all bad or all good; it is value-neutral and offers a win-win situation. However, the organizations need to use policy which might control and reduce cyberloafing activities (J-Ho & Ramayah, 2016). Therefore, the balance is important between the monitoring system and the privacy of the employee (Lee et al., 2016).

Ugrin and Pearson (2013) noted that use different deterrence models can serve as a deterrent to cyberloafing, but there are no specific data that show how individual and organizational controls are used to stop the misuse of the Internet by employees. Organizational managers need to identify the types of cyberloafing and know what types are more frequent to monitor or control it (Askew et al., 2014).  

5.3. Prevention Strategy

Many organizations have a strategy to control employee policy violations (Eivazi, 2011). The prevention strategy is important to deter employee policy violations. The use of technology may help in the development of a business, but technology can cause employers to lose their reputation and their customers because of employee abuse of technology in the workplace (Eivazi, 2011). Therefore, the prevention strategy is important at work.

Organizational managers should follow some steps to start an effective preventive strategy. The first step is to make sure that online policy contains clear points about the organization's policies and rules (Glassman et al., 2015). It is difficult for employers to assess the risks faced by employees without real knowledge of the concept of security. Therefore, managers must be trained to identify security risks and threats that may be related to regulatory policy violations (Bartariya & Rastogi, 2016; Drouvelis & Nosenzo, 2012). Employees also need security training and experience before they can identify the risks of using an online service in the workplace (Glassman et al., 2015).  

6. Conclusion

This conceptual paper attempts to explain the factors that effect on the employees to be attracted to cyberloafing behavior during the work hours. As to provide some of the consequence of cyberloafing and show the benefits of cyberloafing for both employees and organizations. In addition, suggest some solutions that have been shown in the previous study.  

References
[1] Ahmad, A., & Omar, Z. (2017). Age and Gender Differences in Employee Cyberloafing Behavior, (1995), 24–28.

[2] Akbulut, Y., Dönmez, O., & Dursun, Ö. Ö. (2017). Cyberloafing and social desirability bias among students and employees. Computers in Human Behavior, 72, 87–95. https://doi.org/10.1016/j.chb.2017.02.043

[3] Al-Shuaibi, A., Shamsudin, F. M., & Subramaniam, C. (2014). Exploring the Theoretical Link between Characteristic in a Job and Cyberloafing Using Job Demands Resource Theory. The 13th International Conference of the Asia Chapter of Academy of Human Resource Development.

[4] Al-Shuaibi, A., Shamsudin, F., & Subramaniam, C. (2013). Do Human Resource Management Practices Matter in Reducing Cyberloafing At Work: Evidence From Jordan. Journal of WEI Business and Economics, 2(2), 1–11.

[5] Al-Shuaibi, A., Subramaniam, C., & Mohd-Shamsudin, F. (2014). The Mediating Influence of Job Satisfaction on the Relationship between HR Practices and Cyberdeviance. Journal of Marketing and Management, 5(1), 105–119. Retrieved from http://wv9lq5ld3p.search.serialsolutions.com.library.capella.edu/?ctx_ver=Z39.88-2004&ctx_enc=info:ofi/enc:UTF-8&rfri_id=info:sid/ProQ%253Aaibglobal&rf_val_fmt=info:ofi/fmt:kev:mtx:journal&rf.genre=article&rf.title=Journal+of+Marketing+and+Management&

[6] Andreassen, C. S., Torsheim, T., & Pallesen, S. (2014). Predictors of use of social network sites at work - a specific type of cyberloafing. Journal of Computer-Mediated Communication, 19(4), 906–921. https://doi.org/10.1111/jcc4.12085

[7] Askew, K., Buckner, J. E., Taing, M. U., Ilie, A., Bauer, J. A., & Coover, M. D. (2014). Explaining cyberloafing: The role of the theory of planned behavior. Computers in Human Behavior, 36, 510–519. https://doi.org/10.1016/j.chb.2014.04.006

[8] Bartariya, S., & Rastogi, A. (2016). Security in Wireless Sensor Networks: Attacks and Solutions. International Journal of Advanced Research in Computer and Communication Engineering, 5(3), 214–220. https://doi.org/10.17148/IJARCE.2016.5352

[9] Baturay, M. H., & Toker, S. (2015). An investigation of the impact of demographics on cyberloafing from an educational setting angle. Computers in Human Behavior, 50, 358–366. https://doi.org/10.1016/j.chb.2015.03.081

[10] Betts, T., & Setterstrom, A. (2014). Explaining cyberloafing through a theoretical integration of theory of interpersonal behavior and theory of organizational justice. Organizational and End User Computing, 26(4), 23–42. Retrieved from https://books.google.com/books?hl=en&lr=&id=gYwtDWAAQBAJ&oi=fnd&pg=PA144&dq=Explaining+cyberloafing+through+a+theoretical+integration+of+theory+of+interpersonal+behavior+and+theory+of+organizational+justice”&ots=YNgYUQkbsa&sig=jd76DCLTV8NH9EJAEumn

[11] Blanchard, A. L., & Henle, C. A. (2008). Correlates of different forms of cyberloafing: The role of norms and external locus of control. Computers in Human Behavior, 24(3), 1067–1084. https://doi.org/10.1016/j.chb.2007.03.008

[12] Cambo, S., Avrahami, D., & Lee, M. (2017). BreakSense: Combining Physiological and Location Sensing to Promote Mobility during Work-Breaks. Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems - CHI ’17, (December), 3595–3607. https://doi.org/10.1145/3025453.3026021

[13] Charoensukmongkol, P. (2014). Effects of support and job demands on social media use and work outcomes. Computers in Human Behavior, 36, 340–349. https://doi.org/10.1016/j.chb.2014.03.061

[14] Cheng, L., Li, W., Zhai, Q., & Smyth, R. (2014). Understanding personal use of the Internet at work: An integrated model of neutralization techniques and general deterrence theory. Computers in Human Behavior, 38, 220–228. https://doi.org/10.1016/j.chb.2014.05.043
[15] Çınar, O., & Karcioğlu, F. (2015). The Relationship between Cyber Loafing and Organizational Citizenship Behavior: A Survey Study in Erzurum/Turkey. *Procedia - Social and Behavioral Sciences, 207*, 444–453. https://doi.org/10.1016/j.sbspro.2015.10.114

[16] Coker, B. L. S. (2011). Freedom to Surf: The Positive Effects of Workplace Internet Leisure Browsing. *New Technology, Work, and Employment, 26*(3), 238–247. https://doi.org/10.1111/j.1468-005X.2011.00272.x

[17] Derin, N., & Gökçe, S. G. (2016). Are Cyberloafers Also Innovators?: A Study on the Relationship between Cyberloafing and Innovative Work Behavior. *Procedia - Social and Behavioral Sciences, 235*, 694–700. https://doi.org/10.1016/j.sbspro.2016.11.070

[18] Drouvelis, M., & Nosenzo, D. (2012). GROUP IDENTITY AND LEADING-BY-EXAMPLE. Econstor.

[19] Dursun, O. O., Donmez, O., & Akbulut, Y. (2018). Predictors of Cyberloafing among Preservice Information Technology Teachers. *CONTEMPORARY EDUCATIONAL TECHNOLOGY, 9*(1), 22–41.

[20] Eivazi, K. (2011). Computer use monitoring and privacy at work. *Computer Law and Security Review, 27*(5), 516–523. https://doi.org/10.1016/j.clsr.2011.07.003

[21] Glassman, J., Prosch, M., & Shao, B. B. M. (2015). To monitor or not to monitor: Effectiveness of a cyberloafing countermeasure. *Information and Management, 52*(2), 170–182. https://doi.org/10.1016/j.im.2014.08.001

[22] Gökçearslan, Ş., Mumcu, F. K., Haslaman, T., & Çevik, Y. D. (2016). Modelling smartphone addiction: The role of smartphone usage, self-regulation, general self-efficacy and cyberloafing in university students. *Computers in Human Behavior, 63*, 639–649. https://doi.org/10.1016/j.chb.2016.05.091

[23] Hadlington, L., & Parsons, K. (2017). Can Cyberloafing and Internet Addiction Affect Organizational Information Security? *Cyberpsychology, Behavior, and Social Networking, 20*(9), 1–5. https://doi.org/10.1089/cyber.2017.0239

[24] Harris, M., & Patten, K. (2014). Mobile device security considerations for small- and medium-sized enterprise business mobility. *Information Management & Computer Security, 22*(1), 97–114. https://doi.org/10.1108/IMCS-03-2013-0019

[25] Hartijasti, Y. (2016). Is serious internet deviance a problem in Indonesian workplace? *Asian Journal of Information and Communications, 8*(2), 96–107.

[26] Huma, Z., Hussain, S., Thurasamy, R., & Imran Malik, M. (2017). Determinants of cyberloafing: a comparative study of a public and private sector organization. *Emerald Insight, 27*(1), 97–117. https://doi.org/http://dx.doi.org/10.1108/VINE-10-2013-0063

[27] J-Ho, S., & Ramayah, T. (2016). The Good, Bad and Ugly Sides of Internet Usage in the Workplace. *Journal of Business and Social Review in Emerging Economies, 2*(2), 159–165.

[28] 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. https://doi.org/10.1016/j.sbspro.2015.01.391

[29] Jandaghi, G., Alvani, S. M., Matin, H. Z., & Fakheri, S. (2015). Cyberloafing Management in Organizations. *Iranian Journal of Management Studies (IJMS), 8*(3), 335–349.

[30] Jia, H., Jia, R., & Karau, S. (2013). Cyberloafing and personality: The impact of the Big Five traits and workplace situational factors. *Journal of Leadership and Organizational Studies, 20*(3), 358–365. https://doi.org/10.1177/1548051813488208

[31] Jia, R., & Jia, H. (2015). An individual trait-based investigation of employee cyberloafing. *Journal of Information Technology Management, XXVI*(1), 58–71.

[32] Keser, H., Kavuk, M., & Numanoglu, G. (2016). The relationship between Cyber-Loafing and internet addiction. *Cyprot Journal of Educational Sciences, 11*(1), 37–42.

[33] Kim, K., Triana, M. D. C., Chung, K., & Oh, N. (2015). WHEN DO EMPLOYEES CYBERLOAF? AN INTERACTIONIST PERSPECTIVE EXAMINING PERSONALITY, JUSTICE, AND EMPOWERMENT. *HUMAN RESOURCE MANAGEMENT, 10*(1), 1–18.
[34] Krishnan, S., & Lim, V. K. G. (2010). Moderating Effects of Extroversion and Neuroticism on Sleep Deprivation and Cyberloafing. PACIS 2010 Proceedings, 1020–1031. Retrieved from http://aisel.aisnet.org/pacis2010/100/

[35] Lee, B. (2017). Explaining Cyber Deviance among School-Aged Youth. Springer, 11(2), 563–584. https://doi.org/10.1007/s12187-017-9450-2

[36] Lee, J., Warkentin, M., Crossler, R., & Otondo, R. (2016). Implications of Monitoring Mechanisms on Bring Your Own Device Adoption. Journal of Computer Information Systems, 57(4), 309–318. https://doi.org/10.1080/08874417.2016.1184032

[37] Leonard, N., Chukwuemeka, E., & Emmanuel, N. (2018). ABUSIVE SUPERVISION AND ORGANIZATIONAL CYNICISM AS PREDICTORS OF CYBER-LOAFING AMONG FEDERAL CIVIL SERVICE EMPLOYEES IN ANAMBRA STATE, NIGERIA, 1(2), 19–36. https://doi.org/10.5281/zenodo.1172162

[38] Lepp, A., Li, J., Barkley, J. E., & Salehi-Esfahani, S. (2015). Exploring the relationships between college students’ cell phone use, personality and leisure. Computers in Human Behavior, 43, 210–219. https://doi.org/10.1016/j.chb.2014.11.006

[39] Li, H., Luo, R., Zhang, J., & Sarathy, R. (2014). Understanding internet abuses at work using extended rational choice theory. 20th Americas Conference on Information Systems, AMCIS 2014, 1–7.

[40] Li, H., Luo, X., Zhang, J., & Sarathy, R. (2017). Self-control, organizational context, and rational choice in Internet abuses at work. Information and Management, (September), 1–10. https://doi.org/10.1016/j.im.2017.09.002

[41] Lim, V. K. G. (2002). The IT way of loafing on the job: Cyberloafing, neutralizing and organizational justice. Journal of Organizational Behavior, 23(5), 675–694. https://doi.org/10.1002/job.161

[42] Lim, V. K. G., & Chen, D. J. Q. (2012). Cyberloafing at the workplace: Gain or drain on work? Behaviour and Information Technology, 31(4), 343–353. https://doi.org/10.1080/01449290903353054

[43] Mercado, B. K., Giordano, C., & Dilchert, S. (2017). A Meta-Analytic Investigation of Cyberloafing. Emerald Insight. https://doi.org/10.1108/CDI-08-2017-0142

[44] Mohd-shamsudin, F., Kura, K., & Alshuaib, A. (2014). Understanding the antecedents of cyberdeviance at work: A proposed framework. Proceedings of 6th International Conference of Education and Information Management, 6.

[45] Moody, G. D., & Siponen, M. (2013). Using the theory of interpersonal behavior to explain non-work-related personal use of the Internet at work. Information and Management, 50(6), 322–335. https://doi.org/10.1016/j.im.2013.04.005

[46] MySammy. (2013). Cyberloafing Infographic | Personal Internet Use at Work Infographic | MySammy. Retrieved February 26, 2018, from https://www.mysammy.com/cyberloafing-personal-internet-use-at-work-infographic

[47] O’Neill, T. A., Hambley, L. A., & Chatellier, G. S. (2014). Cyberslacking, engagement, and personality in distributed work environments. Computers in Human Behavior, 40, 152–160. https://doi.org/10.1016/j.chb.2014.08.005

[48] Ofcom. (2015). The communications market report. Retrieved April 7, 2018, from https://www.ofcom.org.uk/research-and-data

[49] Özcan, S., Gökçearslan, Ş., & Yüksel, A. (2017). An investigation of the relationship between cyberloafing and academic motivation among university students. Küreselleşen Dünyada Eğitim, (November), 733–742. https://doi.org/10.14527/9786053188407.52

[50] Pindek, S., Krajcevska, A., & Spector, P. E. (2018). Cyberloafing as a coping mechanism: Dealing with workplace boredom. Computers in Human Behavior, 86, 147–152. https://doi.org/10.1016/j.chb.2018.04.040

[51] Piscotty, R., Martindell, E., & Karim, M. (2016). Nurses’ Self-Reported Use of Social Media
and Mobile Devices in the Work Setting. *Line Journal of Nursing Informatics: OJNI*, 20(1). Retrieved from https://search.proquest.com/openview/e47dbe39cea42d1930fae7a00e85bc92/1?pq-origsite=gscholar&cbl=2034896

[52] Rahimnia, F., & Mazidi, A. R. K. (2015). Functions of control mechanisms in mitigating workplace loafing: Evidence from an Islamic society. *Computers in Human Behavior, 48*, 671–681. https://doi.org/10.1016/j.chb.2015.02.035

[53] Saidin, S. S., Iskandar, Y. H. P., & Dahlan, N. (2017). The Impact of Cyberloafing Towards Malaysia Employees’ Productivity: A Conceptual Framework. 2017 *International Conference on Electrical Engineering and Informatics (ICELTICs 2017)*, 5(1), 216–220.

[54] Sarpong, S., & Rees, D. (2014). Assessing the effects of “big brother” in a workplace: The case of WAST. *European Management Journal, 32*(2), 216–222. https://doi.org/10.1016/j.emj.2013.06.008

[55] Schings, S. (2014). Not All Web Activity at Work Is Detrimental. Retrieved March 18, 2018, from http://www.siop.org/Media/News/loafing.aspx

[56] Sheikh, A., Atashgah, M. S., & Adibzadegan, M. (2015). The antecedents of cyberloafing: A case study in an Iranian copper industry. *Computers in Human Behavior, 51*(PA), 172–179. https://doi.org/10.1016/j.chb.2015.04.042

[57] Son, J. Y., & Park, J. (2016). Procedural justice to enhance compliance with non-work-related computing (NWRC) rules: Its determinants and interaction with privacy concerns. *International Journal of Information Management, 36*(3), 309–321. https://doi.org/10.1016/j.ijinfomgt.2015.12.005

[58] Staffmonitoring. (2017). Office Slacker Stats. Retrieved August 2, 2018, from https://staffmonitoring.com/p32/stats.htm

[59] Stone, D. L., Krueger, D., & Takach, S. (2017). Social Issues Associated with the Internet at Work, 1(1).

[60] Tradingeconomics. (2018). Jordan Unemployment Rate | 2005-2018 | Data | Chart | Calendar | Forecast. Retrieved April 12, 2018, from https://tradingeconomics.com/jordan/unemployment-rate

[61] Ugrin, J. C., & Pearson, J. M. (2013). The effects of sanctions and stigmas on cyberloafing. *Computers in Human Behavior, 29*(3), 812–820. https://doi.org/10.1016/j.chb.2012.11.005

[62] Ugrin, J., Pearson, J., & Nickle, S. (2018). An Examination of the Relationship between Culture and Cyberloafing Using the Hofstede Model. *Journal of Internet Commerce, 17*(1), 1–18. https://doi.org/10.1080/15332861.2018.1424395

[63] Varghese, L., & Barber, L. K. (2017). A preliminary study exploring moderating effects of role stressors on the relationship between Big Five personality traits and workplace cyberloafing. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 11*(4). https://doi.org/10.5817/CP2017-4-4

[64] Wan, H. C., Downey, L. A., & Stough, C. (2014). Understanding non-work presenteeism: Relationships between emotional intelligence, boredom, procrastination and job stress. *Personality and Individual Differences, 65*, 86–90. https://doi.org/10.1016/j.paid.2014.01.018

[65] Yan, J., & Yang, J. (2014). Trait procrastination and compulsive Internet use as predictors of cyberloafing. *11th International Conference on Service Systems and Service Management, ICSSSM 2014 - Proceeding*, 7–10. https://doi.org/10.1109/ICSSSM.2014.6874119

[66] Yasar, S., & Yurdugul, H. (2013). The Investigation of Relation Between Cyberloafting Activities and Cyberloafing Behaviors in Higher Education. *Procedia - Social and Behavioral Sciences, 83*, 600–604. https://doi.org/10.1016/j.sbspro.2013.06.114

[67] Yeik, K. K., Soh, P. C.-H., & Chew, K. W. (2017a). Do employees’ private demands lead to cyberloafing? The mediating role of job stress. *Management Research Review, 40*(9), 1025–1038. https://doi.org/10.1108/MRR-11-2016-0252
[68] Yeik, K. K., Soh, P., & Chew, K. (2017b). Antecedents and consequences of cyberloafing: Evidence from the Malaysian ICT industry | Koay | First Monday. Peer-Review Journal On The Internet, 22(3), 1–18. https://doi.org/10.5210/fm.v21i13.CITATIONS

[69] Yılmaz, F., Yılmaz, R., Öztürk, H., Sezer, B., & Karademir, T. (2015). Cyberloafing as a barrier to the successful integration of information and communication technologies into teaching and learning environments. Computers in Human Behavior, 45, 290–298. https://doi.org/10.1016/j.chb.2014.12.023

[70] Yogun, A. (2015). Cyberloafing and Innovative Work Behavior Among Banking Sector Employees. International Journal of Business and Management Review, 3(10), 61–71.