

# Behavioral Factors Affecting Internet Abuse in the Workplace – An Empirical Investigation

**Irene M.Y. Woon**

National University of Singapore  
iwoon@comp.nus.edu.sg

**Loo Geok Pee**

National University of Singapore  
peelooge@comp.nus.edu.sg

## ABSTRACT

Internet abuse in the workplace refers to employee's use of Internet provided by the organization for non-work-related purpose. It has not only resulted in productivity loss, bandwidth waste and legal liability, it also exposed organizations' information systems to a host of new security threats. To gain a better understanding of the factors influencing Internet abuse behavior in the workplace, this study applied the Theory of Interpersonal Behavior proposed by Triandis and investigated the effects of job satisfaction, affect, social factors, perceived consequences, habit and facilitating conditions on Internet abuse intention and behavior. Results indicated that all factors are significant at 0.05 level. Affect, social factors and habit have the greatest influence on Internet abuse intention and behavior. An interesting result is that employees with higher level of job satisfaction have a more positive affect towards Internet abuse. Implications for Internet security management are discussed.

## Keywords

Internet security, Internet abuse, Triandis' theory of interpersonal behavior, job satisfaction, social factors, perceived consequences, habit, facilitating conditions.

## INTRODUCTION

Organizations are increasingly using Internet as a tool for meeting their business needs. As a result, Internet access for office workers has become commonplace. Despite its myriad use, a pervasive problem associated with Internet use by employees is its potential for abuse. In this research, "Internet abuse" refers to employees' use of Internet for non-work-related purpose. Although some researchers have considered non-work-related Internet use as a form of self-directed, experiential learning (Belanger and Van Slyke, 2000), its consequences, such as bandwidth waste and legal liability cannot be ignored. More importantly, Internet abuse has exposed organizations' information systems (IS) to a host of new security threats that put organizations at risk. The CSI/FBI 2003 survey report showed that Internet connection is increasingly cited as a frequent point of attack (78%) and, among others, virus (82%) is the most cited form of attack.

Recent literature on Internet abuse has focused on identifying technical measures (Josyula, 1997), modifying user behavior (McBride, 2000), proposing Internet use policy (Siau, Nah and Teng, 2002), educating user (Case and Young, 2002), understanding the role of moral dimensions (Lee, Lee and Kim, 2003) and identifying antecedents (Galletta and Polak, 2003). Our study contributes to this growing body of knowledge by examining Internet abuse in the workplace from a sociological and psychological perspective using Triandis' Theory of Interpersonal Behavior (TIB). Specifically, we attempt to answer the research question: *"What is the relative significance of jobs satisfaction, affect, social factors, perceived consequences, habit and facilitating conditions in explaining and predicting employee Internet abuse intention and behavior?"*

Our contribution to theory and practice is two-fold: First, this is the first study that we are aware of to empirically examine habit as an antecedent of employee Internet abuse behavior. Research has showed that habitual behavior leads to continued behavior of the same type (Aarts, Verplanken and van Knippenberg, 1998). In the context of Internet abuse, it is important to consider habit because Internet abuse is a "continuing" behavior. When a particular behavior repeatedly occurs, the influence of habit increases while that of behavioral intention decreases (Triandis, 1980). Its exclusion may lead to false conclusions concerning the impact of other attitudinal variables. Second, our results provide practitioners with insights into how the problem of Internet abuse can be adequately managed. Managers and IT departments can channel their time, effort and other valuable resource into effective mechanisms.

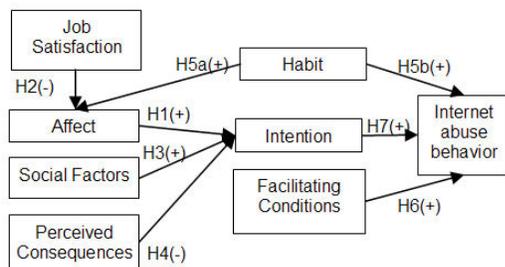
## THEORETICAL BACKGROUND

Previous studies had applied Theory of Planned Behavior (TPB) to investigate antecedents of Internet abuse (e.g. Lee et al., 2003; Galletta and Polak, 2003). In this study, we employ the TIB which is a part of the Triandis Model of Subjective Culture and Social Behavior (Triandis, 1980). Although TPB has been widely used for understanding a variety of unethical human behaviors (e.g. Chang, 1998; Leonard and Cronan, 2001) and several meta-analyses have supported its strong predictive

power (e.g. Sutton, 1998), we consider TIB to be more comprehensive than TPB in that it contains all components of TPB and includes two additional aspects: *habit* and *affect*. In particular, researchers (e.g. Bamberg and Schmidt, 2003) have found that the inclusion of habit increases the predictive power of TIB over TPB. Hence, we expect TIB to perform better than TPB in explaining and predicting Internet abuse.

## RESEARCH MODEL AND HYPOTHESES

Figure 1 presents our research model. It consists of seven factors based on TIB: *affect*, *social factors*, *perceived consequences*, *habit*, *facilitating conditions*, *intention* and *behavior*. Motivated by Galletta and Polak's (2003) study which showed that *job satisfaction* is a significant predictor of Internet abuse, we incorporate it into our model to improve its explanatory power.



**Figure 1. Factors influencing Employee Internet Abuse**

**Affect** – Affect refers to individual's pure emotion of joy, elation, pleasure, depression, distaste, discontentment, or hatred with respect to a particular behavior. Cheung and Chang (2001) found that affect is significant in predicting Internet usage intention. However, in a study on software piracy, Limayem, Khalifa and Chin (1999) reported an insignificant effect. One possible reason may be that their measure of affect combined both cognitive (e.g. unethical, valuable) and affective elements of attitude (e.g. exciting) which introduced additional bias or random error into the measurement of the construct (Goodhue, 1988). In keeping with Triandis, we assessed the affective component through *affect* and the cognitive component through *perceived consequences*. We therefore hypothesize that: (H1) *There is a positive relationship between employees' level of positive affect towards Internet abuse and employees' intention to abuse Internet.*

**Job Satisfaction** – Job satisfaction is a cluster of evaluative feelings about the job (Spector, 1985). Galletta and Polak (2003) showed that job satisfaction is a significant factor affecting Internet abuse. They attributed this phenomenon to employee's detachment with aspects of their job and desire to disengage by substituting other activities. Employees with poor job satisfaction may feel that they are being treated poorly and taken advantage of and as a result, they tend have more reasons to justify their Internet abuse behavior and are more likely to overcome any negative emotional feelings towards the behavior (Mangione and Quinn, 1975). Hence, we posit

that: (H2) *There is a negative relationship between employees' level of job satisfaction and employee's affect towards Internet abuse behavior.*

**Social Factors** – Social factors refer to the individual's internalization of the reference group's subjective culture, and specific interpersonal agreements that the individual has made with others, in specific social situations (Triandis, 1980). Previous studies on Internet abuse (e.g. Lee et al., 2003) had assessed and found the link between social norms and intention to be significant. Therefore we hypothesize that: (H3) *There is a positive relationship between supportive social factors and employees' intention to abuse Internet.*

**Perceived Consequences** – According to Triandis (1980), each act is perceived as having potential outcomes that have positive or negative value, together with a probability that the outcome will occur. This definition is consistent with the expectancy theory of motivation and general deterrence theory, which suggest that highly visible detective activity has the desirable effect of deterring future computer abusers. Backhouse and Dhillon (1995) established that countermeasures such as security policy can also significantly reduce criminal intention or abuse behavior. In the context of Internet usage, measures such as Internet use policy and monitoring are commonly used against Internet abuse. Therefore, we hypothesize that (H4) *There is a negative relationship between undesirable perceived consequences of Internet abuse and employees' intention to abuse Internet.*

**Habit** – Habit refers to situation-behavior sequences that are or have become automatic and occurs without self-instruction, cognition and deliberation in response to specific cues in the environment (Triandis, 1980). It is a function of individual's past experience and ability to perform a specific behavior and act. Researchers have found that habit is a good predictor of future behavior (e.g. Orbell, Hodgkins and Sheeran, 1997). Hence, we postulate that: (H5a) *There is a positive relationship between employee's habit of abusing Internet and level of positive affect towards Internet abuse.* (H5b) *There is a positive relationship between employee's habit of abusing Internet and Internet abuse behavior.*

**Facilitating Conditions** – Triandis (1980) defined facilitating conditions as objective factors in the environment that several judges or observers can agree make a behavior easy to perform. Facilitating conditions are important in that individuals with intention of accomplishing a certain act may be unable to do so because his/her environment prevents the act from being performed. Consistent with Triandis, we hypothesize: (H6) *There is a positive relationship between the extent to which facilitating conditions of Internet abuse exists and employee's Internet abuse behavior.*

**Intention** – Intention represents an individual's conscious plan or self-instruction to carry out a behavior (Triandis,

1980). It is characterized by a subjective probability dimension linking the individual with the behavior and it indicates how much effort one is willing to try and to invest to abuse Internet. Intention is considered to be an accurate predictor of actual behavior in many studies (e.g. Harrison, Mykytyn and Rienenschneider, 1997). Therefore, we purport that: (H7) *There is a positive relationship between employees' intention to abuse Internet and Internet abuse behavior.*

**Behavior** – In this study, behavior refers to employees' actual act of using Internet provided by the organization for non-work-related purpose. It depends directly on the factors *habit, facilitating conditions* and *intention*.

## RESEARCH METHODOLOGY

**Instrument Development** – A step-by-step process recommended by Churchill (1979) was used to develop the instrument for this study. During item generation, we reviewed validated measures to generate an initial list of items. Pretest Interviews were then conducted with experienced observers to assess the face and content validity of proposed items. We also used the belief elicitation process (Fishbein et al., 2001) to identify additional items. Subsequent to interviews, the sorting routine (Moore and Benbasat, 1991) was employed to assess the convergent and discriminant validity of instrument. Two sorting rounds were conducted and all items achieve high item placement ratio of at least 0.8.

**Data Collection** – Data was collected from employees of various organizations. 239 responses were collected and 25 incomplete responses were eliminated, leaving 214 for data analysis. Most respondents were holding professional/technical positions (81.8%), aged between 20 and 39 (94.4%) and have more than 5 years of experience in using computers (99%) and Internet (94.4%).

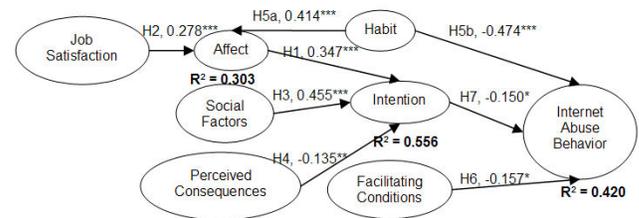
## DATA ANALYSIS AND RESULTS

Partial Least Square with PLS-Graph version 2.91 and bootstrap resampling method (100 resamples) were used to assess the proposed framework. In our study, the factors *affect, habit, intention* and *behavior* are reflective and the factors *job satisfaction, perceived consequences, facilitating conditions* and *social factors* are formative (Falk and Miller, 1992).

**Test of Measurement Model** – For reflective constructs, internal consistency was measured using Cronbach's alpha reliability coefficient. All constructs except *behavior* have scores above the recommended level of 0.70 (Nunnally, 1978). Three tests were used to assess convergent validity: a) item reliability, b) composite reliability and c) average variance extracted (AVE) of each construct. Results showed that with exception to *behavior*, all item and composite reliabilities are above the recommended level of 0.70 and all AVEs are above 0.5. Two tests were used to assess discriminant validity: a) factor analysis and b) item correlations. Four factors were extracted. With exception to the factor *behavior*, all

item loadings on stipulated constructs are greater than or close to the required 0.5 and all eigenvalues are around one (Hair, Anderson, Tatham and Black, 1998). The item correlation matrix showed that the discriminant validities of all scales except *behavior* are adequate.

For formative constructs, absolute values of item weights were examined to determine the relative contribution of items constituting the construct. Results showed that: a) coworkers and contingent rewards contribute most to individual's job satisfaction, b) friends and IT department are significant social factors with regard to Internet abuse, c) warning/reprimands and convenience are the two most important consequences perceived by the employee and d) lack of productivity measurement and disciplinary measures with respect to Internet abuse are the main facilitating conditions of employee Internet abuse.



**Figure 2. Results of Test of Structural Model**

\*Significant at  $p < 0.05$  (One-tailed T-value: 2.6, df: 208); \*\* significant at  $p < 0.01$  (One-tailed T-value: 2.344); \*\*\*significant at  $p < 0.0005$  (One-tailed T-value: 3.338)

**Test of Structural Model** – Statistical significance of loadings ( $R^2$ ) and path coefficients were assessed. The results of structural model analysis are presented in Figure 2. All paths are significant at 0.05 level with six out of eight paths significant at 0.01 level. *Affect, social factors* and *perceived consequences* explained 55.7% of the variance in intention. This suggests that TIB has greater explanatory power over TPB for intention in the context of employee Internet abuse. Falk and Miller (1992) suggested 10% as an indication of substantive explanatory power. Our research model, thus, possesses high predictive validity for Internet abuse intention.

Supporting our hypothesis, *affect* (H1) and *social factors* (H3) influence intention positively, *perceived consequences* influences intention (H4) negatively and *habit* (H5a) influences *affect* positively. Contrary to expectations, three constructs: *habit* (H5b), *facilitating conditions* (H6) and *intention* (H7) affect *behavior* negatively while *job satisfaction* influences *affect* positively (H2).

**Follow-up** – After data analysis, follow-up e-mails were sent to respondents to help us gain further insights into data. This feedback is incorporated into our discussion.

## DISCUSSION AND CONCLUSION

Results indicated that *habit* has a significantly positive effect on *affect* (H5a). Hence, it is important to prevent Internet abuse from turning habitual by first limiting the

chances that employees can abuse their Internet access so as to manage their affect towards it. For example, a clearly articulated Internet policy notifying employees about the potential consequences may reduce their intention to abuse Internet, as suggested by the results.

Results also showed that employees abuse their Internet access for convenience and to spice up work life. However, they are also worried about affecting work productivity. This suggests that implementing productivity measurement may be effective in limiting and reducing Internet abuse. However, the management should be aware of its negative effects on aspects such as job commitment and be careful not to overexert it.

We found *social factors* to be the most significant factor relating to employees' intention to abuse Internet (H3). Specifically, friends, families, coworkers and the organization's IT department have greatest effects on intention. This shows that Internet abuse intention is likely to be under normative control. Interestingly, immediate supervisors and top management have less influence than the IT department. This is consistent with a) Rational-legal Authority of Weber's theory of Bureaucracy, which suggests that legitimate domination in organization rests on rational grounds and on a belief in the legality of enacted rules and the right of those elevated to authority under such rules to issues commands; and b) Power-Dependency Theory, which suggests that people, groups, and organizations have power to the extent that they have access to alternate sources of a valued resource, and the extent to which they control resources valued by others in the network. As Internet is an IT-related behavior, employees may perceive that IT department has the rational-legal authority and power to monitor, control and assess their Internet usage. This suggests that despite common practice, top management and immediate supervisors are not always the best persons to advocate proper Internet use in organizations.

Contrary to expectation, when Internet abuse turns *habitual*, employees reported lower level of abuse *behavior* (H6b). One possible source of this apparent incongruity may be inherent in the self-report measure of behavior. Due to the illicit nature of the behavior in question, respondents may be unwilling to report the truth possibly due to social desirability bias (Elliott, 1984) and self-presentation bias (Gaes, Kalle and Tedeschi, 1978). Also, respondents may have failed to report their actual behavior accurately when it turned habitual. Indeed, follow-up results indicated that as many as 31% are only half-willing in reporting their actual behavior and 81% are able to report their behavior with only 50% accuracy. Future research may consider the use of unobtrusive observation via access logs. The main problems with unobtrusive measures, however, are ethical issues involving informed consent and invasion of privacy.

It is interesting to see that Internet abuse *intention* is found to be negatively related to *behavior* (H7). As the measure of behavior demonstrated low reliability,

measurement artifact may have attenuated the relationship between intention and behavior (Fishbein and Ajzen, 1973). Researchers have also showed that intentions do not always lead to successful enactment of the behavior and suggested that the relationship between intention and behavior may be more complex (e.g. Sutton, 1998). Being a normatively-controlled behavior, Internet abuse is expected to have weaker intention-behavior correlation as it is initiated and pursued because of pressures external to self (Orbell, Hodgkins, Sheeran, 1997). Further research and improvement on measurements are necessary before we start questioning the merit of previous research that assumed intention to be indicative of behavior.

Results showed that employees with high level of *job satisfaction* have more positive *affect* towards Internet abuse (H2). In the follow-up study, some respondents revealed that they perceive the use of Internet for non-work-related purpose as a form of fringe benefit that can help relieve work stress. We suggest that aspects of job can be adjusted to allow an acceptable degree of personal use while effectively and efficiently managing the associated security risks with Internet policy.

*Facilitating conditions* are negatively related to Internet abuse *behavior* (H6). Our result is consistent with Lee, et al. (2003) and Galletta and Polak (2003). Lee et al. explained that this may indicate the inappropriate operation of policies and systems instead of inherent uselessness of controls. Galletta and Polak reasoned that a) Internet use policy may be lacking in both legal and behavioral grounding; b) workplace privacy is insignificant because Internet abuse does not always involve graphics; and c) definitions for productivity measurement and monitoring are not restrictive enough. This may explain the pervasiveness of Internet abuse despite extensive efforts and money spent on drafting Internet use policy and installing monitoring systems.

This study examined the sociological and psychological factors affecting employee Internet abuse in organizations using TIB. To increase the theoretical validity of the model and provide further causal understanding, future research should consider a longitudinal approach towards data acquisition. We hope that this study will help organizations in crafting judicious security policies that will benefit both the employee and the organization.

## REFERENCES

1. Aarts, H., Verplanken, B. and van Knippenberg, A. (1998) Predicting behavior from actions in the past: Repeated decision making or a matter of habit? *Journal of Applied Social Psychology*, 28, 1356-1375.
2. Backhouse J. and Dhillon G. (1995) Managing computer crime: a research outlook, *Computers & Security*, 14, 7, 645-651.
3. Bamberg, S. and Schmidt, P. (2003) Incentives, morality or habit? Predicting students' car use for

- university routes with models of Ajzen, Schwartz and Triandis, *Environment and Behavior*, 35, 264-285.
4. Belanger, F. and Slyke, C. V. (2000) End-user learning through application play, *Information Technology, Learning, and Performance Journal*, 18, 1, 61-70.
  5. Case, C. J., and Young, K. S. (2002) Employee Internet management: Current business practices and outcomes, *CyberPsychology & Behavior*, 5, 355-361.
  6. Chang, M. K. (1998) Predicting Unethical Behavior: A Comparison of the Theory of reasoned action and the Theory of planned behavior, *Journal of Business Ethics*, 17, 16, 1825-1834.
  7. Cheung W. and Chang M. K. (2001) Determinants of the intention to use Internet/WWW at work: a confirmatory study, *Information & Management*, 39, 1-14.
  8. Churchill, G.A. (1979) A paradigm for developing better measures of marketing constructs, *Journal of Marketing*, XVI, 64-73.
  9. Falk, R. F. and Miller N. B. (1992) A primer for soft modeling, Akron, Ohio: University of Akron Press.
  10. Fishbein, M. and Ajzen, I. (1973) Attitudes toward objects as predictors of single and multiple behavior criteria, *Psychological Review*, 81, 59-74.
  11. Fishbein, M., Triandis, H. C., Kanfer, F. H., Becker, M., Middlestadt, S. E. and Eichler, A. (2001) Factors influencing behavior and behavior change, *Handbook of health psychology*, Mahwah, NJ: Lawrence Erlbaum, 3-17.
  12. Gaes, G. G., Kalle, R. J. and Tedeschi, J. I. (1978) Impression management in the forced compliance situation: Two studies using the bogus pipeline, *Journal of Experimental Social Psychology*, 9, 491-501.
  13. Galletta D. F. and Polak P. (2003) An Empirical Investigation of Antecedents of Internet Abuse in the Workplace, *Proceedings of the 2nd Annual Workshop on HCI Research in MIS*, Seattle, WA, 12-13.
  14. Goodhue, D. L. (1988) IS attitudes: towards theoretical and definitional clarity, *Data Base*, Fall/Winter, 6-15.
  15. Hair, J. F., Anderson, R. E., Tatham, R. L. and Black, W. C. (1998) *Multivariate Data Analysis*, 5th Ed, Prentice-Hall: Upper Saddle River.
  16. Harrison, D. A., Mykytyn, P. P. Jr, and Rienenschneider, C. K. (1997) Executive decisions about IT adoption in small business: Theory and empirical tests, *Information Systems Research*, A *Journal of the Institute of Management Sciences*, June, 8, 2, 171-195.
  17. Huizinga, D. and Elliott, D. S. (1983) Self-report measures of delinquency and crime: Methodological issues and comparative findings. Report No. 30, National Youth Survey, Boulder, Co: Behavioral Research Institute.
  18. Lee, Y., Lee, Z., Kim, Y. (2003) *Personal Web Usage in the Workplace: A Guide to Effective Human Resources Management*, Information Science Press, (ed) Anandarajan, M. and Simmers, C. Part II, *Personal Web Usage in Organizations*.
  19. Leonard, L. N. K. and Cronan, T. P. (2001) Illegal, inappropriate and unethical behavior in an Information Technology context: A study to explain influences, *Journal of the Association for Information Systems*, 1, 12, 1-31.
  20. Limayem, M., Khalifa, M., Chin, W. W. (1999) Factors motivating software piracy: a longitudinal study, *International Conference on Information Systems*, Charlotte, United States, 124-131.
  21. Mangione, T. W. and Quinn, R. P. (1975) Dissatisfaction, counterproductive behavior and drug use at work, *Journal of Applied Psychology*, 60, 1, 114-116.
  22. McBride, P. (2000) Develop secure Internet practices, *Internet Security Advisor*, 18-25.
  23. Moore, G. C., Benbasat, I. (1991) Development of an instrument to measure perceptions of adopting Information Technology innovation" *Information Systems Research*, 2, 192-222.
  24. Nayeem, I., Rangachari, A., Trent, J. and Josyula, R. R. (1997) A flexible security system for using Internet content, *Software, IEEE*, 14, 15, 52-59.
  25. Nunnally, J. C. (1978) *Psychometric Theory*, 2nd ed., McGraw-Hill Book Company, New York.
  26. Orbell, S., Hodgkins, S. and Sheeran, P. (1997), Implementation intentions and the Theory of Planned Behavior, *Personality and Social Psychology Bulletin*, 23, 9, 953-962.
  27. Siau K., Nah F., Teng, L. (2002) Acceptable Internet policy, *Communications of the ACM*, 45, 1, 75-79.
  28. Spector, P. E. (1985) Measurement of human service staff job satisfaction: Development of the job satisfaction survey, *American Journal of Community Psychology*, 13, 693-713.
  29. Sutton, S. (1998) Predicting and explaining intentions and behavior: How well are we doing? *Journal of Applied Social Psychology*, 18, 15, 1317-1338.
  30. Triandis, H. C. (1979) Values, attitudes, and interpersonal behavior, (ed.) E. How, Jr., *Nebraska symposium on motivation*, 27, 195-259, Lincoln, NE: University of Nebraska Press.