JISSec 3(1) 2007

Journal of
Information System
Security

www.jissec.org

The Effect of Spam and Privacy Concerns on E-mail Users' Behavior

Insu Park[1], R. Sharman[1, 3], H. Raghav Rao[1, 2,] & S. Upadhyaya[2]

[1] Management Science and Systems, SUNY Buffalo, NY 14260
[2]Computer Science and Engineering, SUNY Buffalo, NY 14260

Abstract

This study aims to examine the effects of both spam and the resulting lack of privacy on users' behavior with respect to e-mail usage. This study reveals that spam e-mail triggers concerns about privacy and in turn, these privacy concerns influence the way users cope with spam or junk mails. Upon receiving spam e-mail, users predominantly exhibit two different behavioral patterns: usage-oriented (passive) and protection-oriented (proactive) behavior. For the purposes of this study, we used data obtained from Pew Internet Research. Logistic regression analysis was performed on the data (N=588) with the intention of examining how spam negatively affects e-mail usage and degrades life on the Internet. Our results show that: (1) e-mail users' spam experiences have a profound relationship with their privacy concerns; (2) privacy concerns help to mediate the relationship between the spam experience users' protective behavior; and (3) when concerned about privacy as the result of spam, e-mail users tend to exhibit both passive and proactive behaviors.

Keywords: privacy, spam e-mail, defense mechanism, usage-oriented behavior, protection-oriented behavior, mediation,

1. Introduction

E-mail has become one of the most popular Internet services for instant and convenient message delivery. Unfortunately, e-mail also enables the spread of unsolicited and unwanted spam mail (Neumann et al. 1997). Spam creates problems such as cost shifting, fraud, resource wastage, and the displacement of legitimate mail (Cournane et al. 2004). The proliferation of spam is also a potential threat to the credibility of e-mail as a reliable and efficient means of communication over the Internet. Further, the effect of spam on the infrastructure and conveniences provided by the Internet has augmented privacy concerns among e-mail users and has served to reduce users' welfare. According to the Pew Internet Report (Fallows 2003), 76% of the users who received spam responded that spam compromises their privacy[1].

Spam e-mail both directly and indirectly causes users to have privacy concerns[2] (Sipior et al. 2004). Privacy concerns that are derived from spam may be indirect as spam focuses users' attention on privacy when they receive spam mail. In addition, spam e-mail immediately raises concerns about privacy which are triggered by perceived harm when information is released by the offending party (Wathieu et al. 2005). The foregoing raises the research question: does the receipt of spam alert the user to privacy concerns? This issue has not been examined to any extent thus far, even though it is clear that there is a relationship between spam e-mail and privacy concerns. A study of the relationship between spam and privacy can also provide benefits to the information security field. That is, it may draw attention to the way in which spam e-mail can affect users' behavior with respect to their e-mail usage by alerting them to internal concerns about the circulation of their private information.

Users may consciously or unconsciously exhibit different behaviors that are defense or coping mechanisms that help them deal

[1] Privacy is defined as "the ability of the individual to control personally information about one's self (Stone et al. 1983: p. 460)." or "the claim of individuals, groups, or institutions ot determine for themselves when, how, and to what extent information abut them is communicated to others (Westin 1967: p. 7).

[2] Privacy concerns refer to an individual's subjective views of fairness within the context of information privacy(Campbell 1997). According to this definition, privacy concerns include individual's personal traits or general disposition to privacy invasion. The concerns for information privacy are affected by external conditions such as industry sectors, cultures, or regulatory laws (Malhotra et al. 2004).

with junk e-mail. For example, when they receive spam or junk e-mail, some users may be discouraged from using the Internet itself or they may harbor negative attitudes toward Internet e-mail, while others may solve the problem by using spam filters, changing e-mail addresses, ensuring that their e-mail address is not available easily on the Internet, etc. Although these different behaviors exhibited by users depend largely upon the their personal characteristics, or their preferences, their attitude can be largely affected by cognition, affection, or beliefs (Rosenberg et al. 1960) which may stem from a spam experience or because of privacy concerns.

This paper attempts to examine the effect of privacy concerns on user's behaviors after they have been exposed to spam e-mail. The contributions of this study are twofold. First, this study explains users' coping behavior with regard to spam e-mail in relation to privacy protection. By paying attention to the underlying psychological processes and motives, the current study also provides insight into how e-mail users behave while protecting their privacy. Second, this study provides a theoretical scheme for the users' behavior with regard to spam and privacy. In other words, this study explains the effect of spam e-mail and privacy concerns on users' behavior by using a psychometric approach.

This paper is organized as follows. The relevant literature on spam and privacy is discussed in Section 2. In Section 3, based on theoretical arguments, four hypotheses are proposed. The methodology for the analysis is contained in Section 4. Results and the summary analysis form the contents of Section 5. Finally, Section 6 discusses the implications of the findings for management policy and research on spam and privacy.

2. Backgroud

In this section, at the outset, we provide a general background on the effects of spam along with an overview of the related background literature. This section also includes a discussion of defense mechanisms and user behaviors, i.e. usage-oriented and protection-oriented behaviors.

2.1. Spam and Privacy

Spam is unsolicited electronic mail that most often comes in the form of commercial advertising (Cournane et al. 2004). According to the Federal Trade Commission[3], in the United States two out of three of these messages contain misleading information. Some consumers find unsolicited commercial e-mail - also known as "spam" - annoying and time consuming; others have lost money to bogus offers that arrived in their e-mail in-box. Companies have reported financial losses due to the costs of unwanted spam traffic. Judge et al. (2005) demonstrate in their work how spam detrimentally affects Internet use for company business.

In the economic context, spam cost European companies $2.8b in lost productivity alone. US based companies reported a loss of $20bn (Hinde 2003). This loss includes the time it takes people to delete the messages, the cost of buying larger mail servers and storage systems to cope with inboxes flooded with spam messages, and the cost of having staff unclog networks overloaded by spam. According to a report by MacAfee, entitled "MacAfee Americans and spam survey"[4] , spam is the prime technology time waster (49%) as compared to other technology-related annoyances including automated voice response systems (24%) and slow Internet connections (19%). This survey revealed that 49% of Americans spend more than 40 minutes per week deleting spam, while 14% reported that they spend as much as 3.5 hours a week - or 7½ days per annum - on this task.

Hinde (2002) states that spam e-mail has become a potent weapon for targeting unsuspecting consumers and stealing their money and identities. The new trend in spam, according Hinde (2002), is its ability to attract users to fraudulent schemes and to then victimize these unsuspecting users. Certain traits of spam, particularly the low cost and the ubiquity of e-mail usage, has made spam the best choice for Internet fraudsters and identity thieves. Previous research on privacy in this area has focused mainly on economic effects (Huberman et al. 2005; Odlyzko 2002) or the privacy trade-offs that individuals are willing to make in order to access specific services (Acquisti et al. 2003; Acquisti et al. 2005; Hann et al. 2004; Syverson 2003).

In much of the published literature that addresses the disparities between stated privacy attitudes and actions, the implicit assumption is that people have privacy concerns.

There is little research on the relationship between a user's behavior and spam e-mail as well as the mediating effect of privacy

[3] Federal Trade Commission, False Claims in Spam, April 30, 2003. Available from: http://www.ftc.gov/reports/spam/030429spamreport.pdf. [Accessed 25 December 2006].

[4] Federal Trade Commission, False Claims in Spam, April 30, 2003. Available from: http://www.ftc.gov/reports/spam/030429spamreport.pdf [Accessed 25 December 2006].

concerns on the relationship in an e-mail usage context. Understanding whether a user's behavior is affected by spam e-mail alone or if privacy concerns also play a role will allow us to design better systems to ensure a more satisfying experience for the user of e-mail systems. Studying this issue can also provide some insight into the major motivations behind e-mail users' coping behaviors. Regarding such behavior, previous research has only demonstrated the privacy paradox which is that users behave irrationally regarding private information. For example, Syverson (2003) shows that users place a high value on privacy while they paradoxically disregard their own privacy in exchange for meager benefits such as a free hamburger or a two dollar discount on groceries. In this paper, we establish that users exhibit both passive and active (dual) behaviors after a spam experience and especially if they have privacy concerns.

2.2. Defense Mechanisms

Individuals may have a series of reactions when they are personally confronted with anxiety-they develop a number of internal defense mechanisms to protect themselves from the unpleasant feelings of anxiety (de Board 1978). Anxiety not only arises from perceived external dangers, but it can also be experienced within the individual for no obvious reason (de Board 1978). This internal resistance called anxiety is often caused by past experiences, fears, or worries the individual has experienced (Wayne et al. 2001).

Defense mechanisms are habitual and unconscious strategies used to deny, distort, or counteract sources of anxiety and to help maintain an idealized self-image (Cramer et al. 1998). Defense mechanisms lie on the surface of human conduct and can be observed without the help of any explicit or standardized assessment procedure (Hentschel et al. 2004). In fact, they can be measured by automatic psychological processes that protect the individual from anxiety and from the awareness of internal or external stressors. E-mail-users, for example, are often unaware of these processes as they operate, even though defense mechanisms mediate the individual's reaction to emotional conflicts and internal and external stressors (p. 751)[5] . According to Holmes (1985) there are three central features of defense mechanisms: avoidance or reduction of negative emotional states, distortion of reality to various degrees, and the lack of conscious awareness in the use of defense mechanisms. Vasiliuk (1992) identifies the following four types of experience as antecedents to the reliance on defense mechanisms: stress, frustration, conflict, and crisis. Several or all of these four conditions can occur together. Even though psychoanalysis has traditionally focused on internal threats and conflicts, the fact that external dangers could trigger defense mechanisms has also been recognized (Draguns 2004).

Due to the foregoing characteristics, defense mechanisms have been used to examine individual reactions to organizational change (see Carnall 1986; Oldham et al. 1990; Ondrack 1974; Wayne et al. 2001). However, there is a lack of research on users' reactions to the Internet. Consider that defense mechanisms represent more an effort to confirm, adapt, or adjust to one's surroundings rather than an effort to influence and mould those surroundings to fit one's own desires and ideas. Thus, users will manifest behavior, as a result of receiving spam or having their privacy invaded, in various avoidant ways such as undoing, repression, denial, and so on. For example, the act of 'undoing' involves nullifying a distressing experience through a reverse action (Clark 1991). 'Repression' involves removing from one's consciousness painful or shameful experiences (Waldmann 2000); this process enables an individual to 'conveniently forget' their own undesirable and unethical behavior. On the other hand, 'denial' is a defense mechanism which a person may rely on in an attempt to protect him or herself from some painful or frightening information related to external reality (Breznitz 1983). E-mail users particularly choose avoidance tactics such as undoing or denial when coping with spam in an online context. For instance, users may try to use e-mail less frequently to avoid the annoyance or to protect their privacy.

2.3. User's Behaviors

Bovey and Hede (2001) claim that when users attempt to protect their privacy, their behaviors can be classified as either active or passive. Accordingly, we categorize users' behavior as being (a) usage-oriented (passive) or (b) protection-oriented (active). In the remainder of this section, we discuss these two behaviors. In particular, users may consciously or unconsciously use well-developed and habitual defense mechanisms to protect themselves from spam e-mail and from related anxieties. Users can also protect private information by reducing their e-mail usage or by simply avoiding it altogether. On the other hand, by reporting spam or using protection programs and

[5] American Psychiatric Association, Diagnostic and statistical manual of mental disorders. Washington, DC., The Association, 1994.

filters, they can aggressively counter spam mail. Post-spam behavior differs depending on the subject's previous spam experiences and privacy concerns.

The foregoing two behaviors are different in that usage behavior is a typical defense mechanism, while the second behavior is just defensiveness. According to Cramer (2004), the term defense mechanism is a theoretical construct that describes a cognitive operation whereas defensiveness is a more general term which refers to behaviors that protect the individual from anxiety, loss of self-esteem, or other disrupting emotions. Further, Cramer (2004) argues that a critical distinction between a defense mechanism and defensiveness is that the former is focused on an unconscious or conscious attitude, while the latter may be consciously recognized by the individual.

2.3.1. Usage-Oriented Behavior (UOB)

We use the term "usage-oriented behavior" to describe a behavior that relates to avoiding or reducing e-mail use-one that is a typical defense mechanism. Further, individuals are often unaware of these processes as they operate. Defense mechanisms mediate the individual's reaction to emotional conflicts and internal and external stressors[6]. Thus, the matter is, as Kraut (2005) mentions, not so much that dealing with junk e-mail or spam is no longer a mere nuisance, but also that it leads Internet users to have privacy concerns. As a result, users may try to avoid using e-mail on the Internet as an effective method because the spam or junk mail might be too difficult for them to protect themselves against.

2.3.2. Protection-Oriented Behavior (POB)

We use the term "protection-oriented behavior" to describe a more active response to spam which may include reporting spam to the e-mail provider and applying protection filters, or reporting spam to a consumer or government agency. In contrast to usage-oriented behavior in e-mail use, protection-oriented behavior represents the direct impact of spam, its impact on perceived privacy, and its impact on users' behavior. Thus, protection-oriented behavior is defined as a "user's positive defense behavior to protect their privacy from particular problems such as spam, hacking, etc.

[6] American Psychiatric Association, Diagnostic and statistical manual of mental disorders. Washington, DC., The Association, 1994.

The difference between usage-oriented and protection-oriented behavior is not only the degree to which a user's attitude towards privacy impingements are positive or negative but also, in contrast to usage-oriented behavior, it is the degree to which protection-oriented behavior actively (rather than passively) protects against spam.

In addition, protection-oriented behavior may depend on perceived privacy rather than spam because users may tend to give priority to protecting their private information rather than avoiding spam. A likely reason why spam is perceived to be more threatening than ever is because Internet users are beginning to recognize that spam is related to privacy intrusion. This study also assumes that users who know that junk mail or spam resulted from their Internet usage will more likely have privacy concerns. As a result, perceived privacy may provide mediating effects on the relationship between spam and protection-oriented behavior. That is, protection-oriented behavior may not be affected by spam directly.

2.3.3. Independence of Two Behaviors

Empirical and theoretical research shows that consumers often lack adequate information to make appropriate privacy-sensitive decisions and, even with sufficient information, they are likely to trade long-term privacy for short-term benefits (Acquisti et al. 2005). By contrast, however, users may exhibit active and passive (dual) behavior at the same time when protecting their privacy, assuming they have enough information about protection. Usage-oriented behavior and protection-oriented behavior are two different and exclusive strategies. If users conduct one of these behaviors, they do not engage in the other behavior, in general. That is, according to the definitions of the two behaviors as mentioned above, there is probably no overlap between usage and protection oriented behavior.

This dissimilarity is not only because users who discontinue e-mail usage do not have to take care of their e-mail. On the other hand, e-mail users who exhibit protection-oriented behavior use e-mail without considering a reduction in e-mail usage. Since the users acted to prevent their e-mail from attacks, they also would not consider e-mail as an alternative.

As stated above, the two behaviors (i.e., usage-oriented and protection-oriented behavior) that arise due to the receipt of spam are normally mutually exclusive. The rationale for this is that e-mail users who exhibit protection-oriented (active) behavior are unlikely to engage in usage-oriented (passive) behavior. This relationship between the two behaviors (i.e. usage-oriented and protection-oriented behavior) may be violated because of privacy concerns or the receipt of spam. For example, if a user engages in both usage-oriented (passive behavior) and protection-oriented (active) behavior, regardless of any other consideration, then we regard this behavior as dual behavior.

In this study, we use term "dual behavior" to refer to an action demonstrating two exclusive behaviors (both active and passive) at the same time. When users feel that their privacy is vulnerable, they would manifest dual behavior, even with perfect information.

3. Hypothesis

In this study, as part of Hypothesis 2 and 3, we explore the effect of a spam experience and privacy concerns on usage-oriented and protection-oriented behavior. In the latter part of this section, we examine e-mail users' behavior by exploring their dual behavior.

3.1. The Effect of Spam and Privacy on a Single Behavior

In this section, we present a causal model that affects "Usage-oriented Behavior" and "Protection-oriented Behavior." Figure 1 shows this study's conceptual model for the effect of spam and privacy concerns on a single behavior.

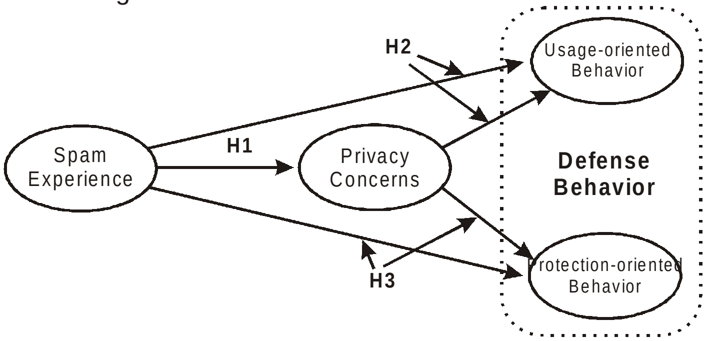

Figure 1. Conceptual Model for Hypothesis 1 to 3

As mentioned in our research question , we argue that a spam experience affects user's concerns about the privacy of their information. E-mail users believe that spam threatens their privacy. Most users fear that their personal information might fall into the hands of unscrupulous people, such as marketers, who will then intrude upon them with unwanted calls and messages or worse (Fahlman 2002). In a survey of attitudes to online privacy, Han and Maclauin (2003) found that a number of respondents labeled spam as a major privacy issue. In reality, spam is, indeed, a major privacy issue (Syverson 2003). While receiving spam can be a consequence of users' negligence in keeping their private information secure, it can also be the result of the illegal distribution of e-mail addresses. Therefore,

Hypothesis 1: T*he receipt of spam affects privacy concerns.*

Although users' experience with spam can cause many different behaviors in addition to defensive behavior. Since usage- and protection-oriented behaviors may be motivated by hierarchically different levels of stimuli, the exhibition of one of those two behaviors depends on the level of stimuli such as spam experience and privacy. Along with the effect of spam experience on usage-oriented behavior, privacy concerns mediate the relationship between spam experience and usage-oriented behavior. Protection-oriented behavior precedes usage-oriented behavior in the degree of intensity. As a result, Hypothesis 2 is as follows:

Hypothesis 2: *spam experience and privacy concerns affect users' usage-oriented behavior.*

Compared to usage-oriented behavior, protection-oriented behavior requires more effort from users because the behavior is more active and conscious. This means that users may not initiate the behavior without stimuli which seriously threatens them such as notification of fraud, warning of abuse of private information, and so on. One of the privacy concerns that can serve as an anxiety trigger is the recognition that private information can be abused by others. For example, without (implicit or explicit) agreements for other uses, privacy is violated if the merchant later uses personal information in a manner outside of the primary use (e.g., the merchant sells his customer list) or allows the information to be disclosed to a party as secondary use (Smith 2005). In summary, protection-oriented behavior will not be exhibited because of a spam experience but because of concern for privacy

Hypothesis 3: *user's experience with spam does not affect their protection-oriented behavior but privacy concerns do affect protection-oriented behavior.*

3.2. The Effect of Spam and Privacy on Dual Behavior

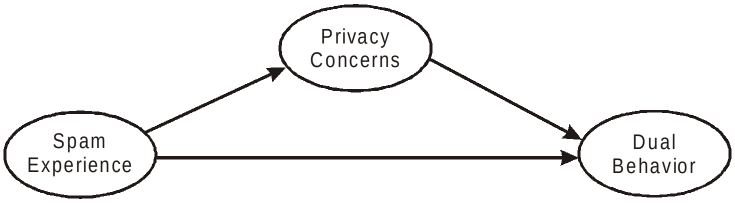

Figure 2. Conceptual Model for Hypothesis 4

Since usage-oriented behavior and protection- oriented behaviors are mutually independent and somewhat opposite, we assume that rational users would not exhibit both active and passive behavior at the same time. However, when users are annoyed, for example by a spam experience, they are apt to act irrationally by engaging in both active and passive behaviors. That is, if users consider spam e-mails as very bothersome, this spam experience could cause them to exhibit usage- and protection- oriented behaviors at the same time.

Furthermore, privacy concerns mediate the relationship between spam and the dual behavior. In other words, the users' dual behavior would be caused not only by the impact of the spam experience but also by privacy concerns. Therefore, we propose, Hypothesis 4:

Hypothesis 4: *Privacy mediates the relationship between the spam experience and a user's dual behavior*

4. Methodology

In this section, we present a methodology in terms of the data collection and the constructs that we have developed for this study.

4.1. Data Collection and Research Method

In order to test these four hypotheses, this study used 'The Pew Internet and American Life Project' data surveyed by the "Pew Internet Research Center" in 2003. The data was surveyed to determine Internet users' attitudes towards spam and the use of e-mail filtering from 6/10/03 to 7/3/03. Individuals who were 18 or older participated in the survey. This Pew survey data contained about 4000 responses that related to all Internet users. For this study, we filtered out 2,279 participants because they were e-mail users.

The sample was confined to people who have e-mail accounts and use e-mail every day. Of these 2,279 only 588 users were selected for analysis relating to Hypothesis 1, 2 and 3 as they corresponded to all e-mail users who had a spam experience; these users were also engaged in either protection-oriented or usage-oriented behavior but not both. From the set of 2,279 e-mail users, 1490 exhibited engaged in either protection-oriented or usage-oriented behavior or both and their responses were used to test Hypothesis 4.

4.2. Constructs

This study uses two different constructs as dependent variables: usage-oriented behavior and protection-oriented behavior.

4.2.1. Spam Experience

E-mail users experience spam or junk mail each time they log onto the Internet. The experience is measured by the number of spam mails received on a given day or the percentage of spam mail in relation to the total daily mail. In the Pew research questionnaire, spam experiences are measured by the following items: "Of all the e-mail you receive in your personal (account/accounts) on a typical day, what percentage are personal messages and what percentage are junk e-mail or spam." This construct was measured as a 7-point scale (1 implying "none" to 7 implying "81 % or more").

4.2.2. Perceived Privacy Concern on spam

Privacy is a uni-dimensional construct (Smith et al. 1996). However, in this study perceived privacy concern was captured in the original Pew research survey via a multiple choice question that asked users to respond to the question "which characteristics of spam affect their e-mail usage". The choices available to responders were: "spam has compromised users' privacy", "Deceptive or dishonest content", "Offensive or obscene content", "the amount of spam online", "the time it takes to deal with spam" and "it is unsolicited or you did not ask for it", and "the damage it can do to your computer". The responses were then encoded on a dichotomous scale (yes / no) based on whether the respondent chose the answer "spam has compromised users' privacy" or not.

4.2.3. Usage-Oriented Behavior

Usage-oriented behavior is defined by the construct referred to in the original Pew questionnaire as "reducing behavior caused by spam or junk mail". This construct consisted of two items: "Reduced your overall use of e-mail" and "Made you less trusting of e-mail in general".

These items capture intent rather than actual amount of reduction in e-mail usage. The construct 'usage-oriented behavior' is measured on a dichotomous scale based on the responses to the above two items. The construct, therefore, reflected the users' behaviors by measuring their responses on a dichotomous scale (yes/no). If a user had responded in the affirmative to at least one of the two items, then we encoded the usage-oriented behavior as "yes" (implying that the user engaged in usage-oriented behavior). A "no" was encoded for the usage-oriented construct when the response to both items in the Pew survey was in the negative.

4.2.4. Protection-Oriented Behavior

This construct reflects a user's positive defensive behavior as they attempt to protect their privacy from intrusions such as spam, hacking, and so on. According to Cramer (2004), protection-oriented behavior may be manifested as other mechanisms, such as acting differently than one feels, or suppressing a disturbing idea. In the original Pew survey participants were asked if they "Requested to be removed from a mailing list", "Reported it to your e-mail provider," and "Reported it to a consumer or government agency" after experiencing spam. The user was deemed to have engaged in protection-oriented behavior (active behavior) if the response to one or more of the above questions was in the affirmative. The remaining respondents were considered as not having engaged in protection-oriented behavior. This provided us data for encoding the variable on a dichotomous scale.

Causality among variables and the mediating effect of privacy was established using logistic regression (for more details on the procedure see Baron and Kenny (1986))

5. Analysis and results

The results and its analysis are presented in this section. The section is subdivided into four sections: the relationship between a spam experience and privacy concerns, the effect of privacy on defense behaviors (usage-oriented behavior and protection-oriented), and the effect of privacy concerns on dual behavior.

5.1. The Relationship between a Spam Experience and Privacy Concerns

First, to test the relationship between spam experience and privacy concerns, we analyzed this relationship by conducting a correlation and logistic regression analysis. Table 1 shows the correlation matrix among four variables. The result indicates that a spam experience statistically relates to privacy (0.072, *p*<0.01). Moreover, this relationship is also revealed in Table 2. The results show that when users have a spam experience, the probability that they are concerned about privacy is higher than it is with users who do not have an experience with spam mail. Therefore, Hypothesis 1 is supported.

variables	Spam	Privacy	Usage	Protect
Spam Experience	1			
Privacy	.072**	1		
Usage	.221**	.348**	1	
Protect	-.012	.081**	.174**	1

** Correlation is significant at the 0.01 level (2-tailed).

Table 1. Correlation Matrix

Independent variables	B	S.E.	Wald	df	Sig.	Exp(B)
Spam Experience	-.371	.148	6.316	1	.012	.690
Constant	1.223	.069	312.325	1	.000	3.396

Dependent variable: Privacy concerns

Model :Chi-square=6.132, p<0.05 df=1,

Table 2. Result of Logistic Regression

5.2. Effect of Privacy on Two Defense Behaviors

Given that a spam experience leads users to have privacy concerns, we analyzed the effects of each variable based on two behavior strategies. As a first step, we tested Hypothesis 2 as a means to reveal the presence of a relationship between a spam experience and privacy concerns and usage-oriented behavior. Then, we analyzed the relationship between two variables and protection-oriented behavior. Finally, the relationship between the two behaviors was tested.

5.2.1. Effect of privacy concern on usage-oriented behavior

We initially proposed that both the spam experience and privacy concerns would affect usage-oriented behavior in Hypothesis 2. To test Hypothesis 2, we used logistic regression analysis for the effect of privacy concerns and spam experience on usage-oriented behavior in the first step and the mediator role of privacy concern between a spam experience and usage-oriented behavior in the second step. Spam experience and privacy variables were coded as a dummy variable. The result is presented in Table 3.

Testing steps in mediation model	B	S.E.	Wald	df	Sig.	Exp(B)
Testing step 1 Outcome: Usage behavior Predictor: spam experience	-.818	.161	25.753	1	.000	.441
Testing step 2 Outcome: Privacy Predictor: spam experience	-.371	.148	6.316	1	.012	.690
Testing step 3 Outcome: Usage behavior Mediator: Privacy Predictor: Spam experience	-2.009	.181	123.276	1	.000	.134
	.763	.172	19.649	1	.000	2.145

Step 3 Model :Chi-square= 185.53, df=2, *p*<0.001.

Table 3. Testing mediator effects using Logistic Regression

When examining the results for step 3 in Table 3, the regression coefficient for spam experience was 0.763, which was significant at the conventional probability level (p<0.001). The regression coefficient for privacy was -2.009 (p<0.001), meaning that there was a significant relationship with usage-oriented behavior in the sample. Thus, the result supports Hypothesis 2 because usage-oriented behavior is related to an unconscious, psychologically-based attitude. Users experience this behavior when they have negative feelings about spam. As mentioned before, usage-oriented behavior is a strategy which can easily be used to cope with spam or junk e-mail.

In addition, with regard to the mediation effect, we explored whether a spam experience per se affects usage-oriented behavior. Table 3 contains the analysis necessary to examine this mediation hypothesis. Following the steps outlined earlier for testing mediation, we first established that a spam experience is the predictor and is related to usage-oriented behavior by conducting a logistic regression for usage-oriented behavior on the spam experience in Step 1. The regression coefficient (*b* =-0.818, *p*<0.01) associated with the effect of a spam experience on usage-oriented behavior was significant. Thus, the effect of spam experience on usage-oriented behavior is significant and the requirement for mediation in Step 1 is met (Baron et al. 1986).

To examine the relationship between a spam experience and privacy concerns, we conducted a logistic regression for privacy concern on the spam experience in Step 2. The regression coefficient (b=0.371, p<0.05) associated with this relation also was significant. To test whether privacy concern was related to usage-oriented behavior, we conducted a logistic regression for usage-oriented behavior simultaneously on both privacy concern and the spam experience variable in Step 3. The coefficient associated with the relationship between the privacy concern and usage-oriented behavior was significant (b=-2.009, p< .0001). This third regression equation also provided an estimate of the effect of spam experience on usage-oriented behavior in step 1. The effect of spam experience on usage-oriented behavior in step 3 was -0.763 with statistical significance in p< 0.01. Therefore, Hypothesis 2 was supported.

In summary, Table 3 shows that spam experience has its own affect on usage-oriented behavior and privacy concerns mediates between spam experience and usage behavior.

5.2.2. Effect of privacy concern on protection-oriented behavior

To test H2, a logistic regression analysis was conducted. We expected that spam experience does not affect protection-oriented behavior. Results from this model are reported in Table 4 which shows the result of the effect of a spam experience on protection-oriented behavior. The model is significant at the p<0.001 level (χ^2=20.739). The result in Table 4 also shows that spam experience does not affect protection-oriented behavior (b=0.175, p>0.1). This result may be because protection-oriented behavior is more positive so that users should consciously consider doing this behavior, in contrast to usage behavior.

We also see from Table 4 that privacy concerns affect protection-oriented behavior (b=-0.676, p<0.001). Therefore, the results from Table 4 support Hypothesis 3.

Testing steps in mediation model	B	S.E.	Wald	df	Sig.	Exp(B)
Spam experience (1)	.175	.151	1.331	1	.249	1.191
Privacy (1)	-.676	.158	18.311	1	.000	.509
Constant	-.979	.073	181.728	1	.000	.376
Chi-square= 20.739, df=2, P<0 .000.						

Reference: privacy =0, no privacy=1; Spam experience =0, no spam experience=1

Table 4. Logistic Regression

5.2.3. Effect of Privacy Concern on Dual Behavior

In this study, we assumed that a rational user would engage in only one type of behavior, either usage or protection-oriented behavior. These two behaviors can be substituted for a defensive attack on each other but, under normal circumstances, users seldom engage in two behaviors as an integrated behavior simultaneously. If a user adopts a protection oriented approach to block spam from their mail account, they would still use e-mail. On the other hand, if the user adopts usage behavior due to spam, they would not exhibit protective behavior. These are the two approaches a user adopts while dealing with spam. However, if they have privacy concerns from spam, they may start engaging in both active and passive behaviors.

According to the argument outlined above, we tested Hypothesis 4 by examining whether users selected both defensive behaviors when they perceived an impingement on their private information. In doing this, we created a new dependent variable "dual behavior" by combining usage- and protection-oriented behavior in existing data to fit within this analysis as follows. First, the defensive behaviors were integrated into one variable by being recoded as a binary variable (see Figure 3). If a user engaged in either usage or protection-oriented behavior, they would belong to quadrant Q1 or Q3, which in turn would indicate rational behavior. On the other hand, if the user displayed dual behavior, they would belong to quadrant Q2 (see Figure 3) which in turn would signify both active and passive behavior at the same time. Quadrant Q4 (Figure 3) was omitted in this study because this variable is binary in the analysis. We encode dual behavior as a binary variable. (Users who behave rationally, by either engaging in active [protection-oriented] or passive [usage-oriented] behavior but not both, are encoded with the value 0; and users who engage in both active (protection-oriented) and passive (usage-oriented) behavior at the same time are encoded with the value 1). It may be noted that the new variable (dual behavior) has a statistically different sample from that used for Hypothesis 3.

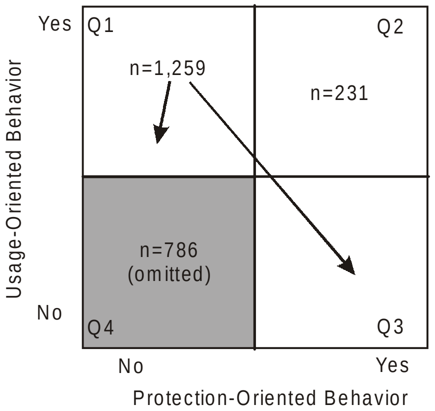

Figure 3: Data Gathering for Dual Behavior

Using this new variable as a dependent variable, we can determine the effects of privacy concerns on the rationality of user behavior. In other words, our hypothesis that privacy can make a user's dual behavior will be supported. We used Equation 1, 2, and 3 for logistic regression.

Step 1: Dual Behavior $= b_0 + b_1 Spam$.........................1)

Step 2: Privacy concerns = $b_0 + b_1 Spam$ .... 2)

Step 1: Dual Behavior $= b_0 + b_1 Spam + b_2 Privacy$........3)

Results are shown in Table 5. In this Table, for spam experiences at each step coefficients are 0.445 (p< 0.05), -0.371 (p< 0.05), and 0.008 (p>0.1) respectively. In addition, privacy concerns as mediator are -0.764 (p<0.01) in step 3. Results indicate that privacy concerns perfectly mediate the relationship between the spam experience and combination behavior. In step 3, the effect of spam experience on integrated behavior is not significant (*b*=0.008, *p*>0.1) which means that the effect of a spam experience on combination behavior is mediated by privacy concerns. In addition, the result of step 3 indicates that privacy concern plays a mediating role in the relationship between the spam experience and integrated behavior (b=-0.764, p<0.01).

In sum, users are more likely to conduct both behaviors at the same time when they perceive privacy concerns as a result of receiving spam or junk e-mail than when they do not have privacy concerns.

Although the result shows a low likelihood for conducting both behaviors (*Prob* =18.3%), we can conclude that privacy leads users to enact both behaviors. Therefore, Hypothesis 4 is supported.

Testing steps in mediation model	B	S.E.	Wald	df	Sig.	Exp(B)
Testing step 1						
Outcome: Dual behavior						
Predictor: Spam experience	.445	.209	4.522	1	.033	1.561
Testing step 2						
Outcome: Privacy						
Predictor: spam experience	-.371	.148	6.316	1	.012	.690
Testing step 3						
Outcome: Integrated behavior						
Mediator: Privacy	-.764	.291	6.908	1	.009	.466
Predictor: spam experience	.008	.043	.034	1	.854	1.008

Step 3 model: Chi-square= 8.157, df=2, P<0 .01.
Dependent variable:
Reference: privacy =0, no privacy=1; Spam experience =0, no spam experience=1

Table 5. Testing mediator effects using Logistic Regression

6. Discussion

In this study, we distinguish between two strategic behaviors that e-mail users can choose to use against spam and junk e-mails: usage-oriented and protection-oriented behavior. The purpose of this study was to explore mechanisms in relation to how users' experience with spam and their resulting privacy concerns may function in terms of two behaviors, i.e. the effect of a spam experience and privacy. The results revealed several key findings.

Primarily, our results showed that a spam experience has a relationship with privacy concerns. With regard to this relationship, usage-oriented behavior is affected by both spam experiences and privacy concerns. In addition, privacy has a partly mediating effect on the relationship between a spam experience and usage-oriented behavior.

Secondly, for protection oriented behavior which is a positive and proactive strategy against spam mail, spam experiences were not significant. However, when users who have such an experience feel that their privacy is being threatened, they adopt protection-oriented behavior.

Thirdly, the effect of a spam experience on both behaviors was a result of the mediation effect of privacy concerns. Results showed that users' behaviors to protect their mail from junk or spam mails are not because of an experience with spam but instead are due to privacy concerns.

We have structured the remainder of this concluding section into two sub-sections. In the first sub-section we discuss the implication of this research and in the second sub-section we discuss the limitations of this research and topics for further research.

This study has several implications for research and practice on privacy and spam mail. First and foremost, this study explains the use of defense mechanisms in users' privacy protection behavior. Psychoanalytic theory provides the conceptual framework for understanding unconscious or conscious processes that are simply described as thoughts and desires for the protection of one's privacy. By paying attention to the underlying psychological processes and motives, the current study responds to question of how e-mail users behave when they attempt to protect their privacy.

Second, this study presents a theoretical initiative for users' behavior with spam and privacy. There has been little research on an e-mail user's behavior for protecting their privacy and preventing spam e-mail. This study explains the role of spam e-mail and privacy concerns on users' behavior by using a psychological process.

Third, this study reveals that a spam experience has a limited impact on users' protection oriented behavior. Results show that a spam experience might have a significant effect only on passive behavior but not on active behavior. In practice, we assume that a spam experience may affect users' behavior, but the preliminary analysis shows that spam has a limited impact on behavior. Privacy has more of an impact on these behaviors by making users aware of risks from spam.

This study also reveals that an experience with spam has different effects according to users' behaviors. Regardless of the severity of the two behaviors, the spam experience affects usage oriented behavior but does not affect protection-oriented behavior. According to the characteristics of the two behaviors, a spam experience is related to passive behavior which is easy to enact without any physical efforts. That is, the experience with spam brings about privacy concerns more than it acts as a critical factor that causes users to attempt to protect their e-mail from spam or privacy attacks.

Finally, this result shows that privacy concerns lead users to resort to dual behavior. In practice, the concept of rational action is clearer in the field of economics than in psychology. This clarity is due to the fact that economics views rationality in terms of the choices it produces, whereas psychology views it in terms of the processes it employs (Simon 1982; Simon et al. 1986). The two different behaviors (usage-oriented and protection-oriented) are exclusive to each other so that it is enough for users to choose only one behavior to protect their e-mail.

The study shows that privacy is important in explaining users' dual behavior. Although it does not explicitly reveal that users are dual behavioral decision makers, the study demonstrates why users exhibit both behaviors to prevent spam or junk mails at the same time. If users are more concerned about privacy due to a spam experience, the user's behavior is likely to be highly dual. According to the study, dual behavior comes from extreme concerns for protecting private information, whereas spam experience is not a determinant which makes users act with dual behavior. However, as users experience more spam they are likely to perceive their private information as vulnerable to attack. Their perception of privacy concerns eventually leads them to adopt both approaches.

7. Conclusion

This study sheds light on the effect of spam experience, privacy concerns, and users' strategies for managing spam e-mail. The model shows that privacy plays a mediating role in the relationship between the spam experience and the users' behavior. Moreover, this study reveals that when users are faced with privacy concerns, they demonstrate dual behavior (i.e. both active and passive at the same time). We hope that this study will spur researchers to examine and amplify the potentially influential role of privacy and of users' behavior within other vulnerable online contexts.

This study has some limitations. Firstly, it uses secondary data which was collected by surveys for general Internet use and not for the purposes of the findings of this study. Secondly, with regard to the use of secondary data, measuring scales for variables were inconsistent with each other which makes the study's reliability low for a generalization of the results. We cannot say that the analysis is best for measuring dual behavior. This study can be treated as exploratory and as a means to define the need for a future study in this area.

References

Acquisti, A., and Grossklags, J., (2003), "Losses, Gains, and Hyperbolic Discounting: An Experimental Approach to Information Security Attitudes and Behaviors," 2nd Annual Workshop on Economics and Information Security Robert H. Smith School of Business, University of Maryland, MD.

Acquisti, A., and Grossklags, J., (2005), "Privacy and Rationality in Individual Decision Making," IEEE Security & Privacy, 3(1): 26-33.

Baron, R.M., and Kenny, D.A., (1986), "The Moderator-Mediator Variable Distinction in Social Psychological Research: Conceptual, Strategic, and Statistical Considerations," Journal of Personality and Social Psychology, 51(6): 1173.

Bovey, W.H., and Hede, A., (2001), "Resistance to organisational change: The role of defence mechanisms," Journal of Managerial Psychology, 16(7/8): 534.

Breznitz, S., (1983), The Denial of Stress International Universities Press, Inc, New York.

Campbell, A.J., (1997), "Relationship marketing in consumer markets: A comparison of managerial and consumer attitudes about information privacy," Journal of Direct Marketing, 11(3): 44.

Carnall, C.A., (1986), "Toward a Theory for the Evaluation of Organizational Change," Human Relations, 39(8): 745.

Clark, A.J., (1991), "The Indentification and Modification of Defense Mechanisms in Counseling," Journal of Counseling and Development : JCD, 69(3): 231.

Cournane, A., and Hunt, R., (2004), "An analysis of the tools used for the generation and prevention of spam," Computers & Security, 23(2): 154.

Cramer, P., (2004), "Stress, Autonomic Nervous System Reactivity, and Defense Mechanisms," in: Defense Mechanisms: Theoretical, Research, and Clinical Perspectives, U. Hentschel, G. Smith, J.G. Draguns and W. Ehlers (eds.), Elsevier, New York.

Cramer, P., and Block, J., (1998), "Preschool antecedents of defense mechanism use in young adults: A longitudinal study," Journal of Personality and Social Psychology, 74(1): 159.

de Board, R., (1978), The Psychoanalysis of Organisations Tavistock, London.

Dickinson, D., (2004), "An Architecture for Spam Regulation," Federal Communications Law Journal, 57(1): 129.

Draguns, J.G., (2004), "Defense Mechanisms in the clinic, the laboratory, and the social world: Toward closing the gaps," in: Defense Mechanisms: Theoretical, Research and Clinical Perspectives, U. Hentschel, G. Smith, J.G. Draguns and W. Ehlers (eds.), Elsevier, Boston, MA, pp. 3-41.

Fahlman, S.E., (2002), "Selling interrupt rights: a way to control unwanted e-mail and telephone calls," IBM System Journal, 41(4)

Fallows, D., (2003), "How It Is Hurting E-mail and Degrading Life on the Internet," Pew Internet & American Life Project, URL: http://www.pewInternet.org/report_display.asp?r=102.

Fenichel, O., (1945), The Psychoanlytic Theory of Neurosis Norton, New York.

Ghanea-Hercock, R., (2003), "Authentication with P2P Agents," BT Technology Journal, 21(4): 146.

Hann, I.-H., Roberts, J., Slaughter, S., and Fielding, R., (2004), "Economic Returns to Open Source Participation: A Panel Data Analysis," Third Annual Workshop on Economics of Information Security, University of Minnesota, MS.

Hansell, S., (2003), "Internet is losing ground in battle against spam," The New York Times. 2003, Apr. 22, , 1.

Hentschel, U., Juris G. Draguns, Ehlers, W., and Smith, G., (2004), "Defense Mechanisms: Current Approaches to research and measurement," in: Defense Mechanisms: Theoretical, Research and Clinical Perspectives, U. Hentschel, G. Smith, J.G. Draguns and W. Ehlers (eds.), Elsevier, Boston, MA, pp. 3-41.

Hinde, S., (2002), "Spam, scams, chains, hoaxes and other junk mail," Computers & Security, 21(7): 592.

Hinde, S., (2003), "Spam: The evolution of a nuisance," Computers & Security, 22(6): 474.

Holmes, D.S., (1985), "Defense mechanisms," in: Encyclopedia of psychology, R.J. Corsini (ed.), Wiley, New York, pp. 341-350.

Huberman, B.A., Adar, E., and Fine, L.R., (2005), "Valuating Privacy," Workshop on Economics and Information Security2-3 June 2005, Boston, MA.

Judge, P., Alperovitch, D., and Yang, W., (2005), "Understanding and Reversing the Profit Model of Spam," WEIS05: Workshop on Economics and Information Security2-3 June 2005, Boston, MA.

Malhotra, N.K., Kim, S.S., and Agarwal, J., (2004), "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model," Information Systems Research, 15(4): 336.

Neumann, P., and Weinstein, L., (1997), "Inside Risks: Spam, Spam, Spam! ," Communications of the ACM, 40(6): 112.

Odlyzko, A., (2002), "Privacy, Economics, and Price Discrimination on the Internet " Workshop on Economics and Information Security, University of California, Berkeley, CA.

Oldham, M., and Kleiner, B.H., (1990), "Understanding the nature and use of defense mechanisms in organisational life," Journal of Managerial Psychology, 5(5): 1-15.

Ondrack, D.A., (1974), "Defense mechanisms and the Herzberg Theory: An alternate test," Academy of Management Journal (pre-1986), 17(000001): 79.

Robert E. Kraut, S.S., Rahul Telang, and James Morris., (2005), "Pricing Electronic Mail to Solve the Problem of Spam," Human-Computer Interaction, 20(1/2): 195-223.

Rosenberg, M., and Hovland, C., (1960), Attitude organization and change Yale University Press New Haven, CT.

Simon, H.A., (1982), Empirically Grounded Economic Reason MIT Press, Cambridge, MA.

Simon, H.A., and Thaler, R.H., (1986), "Rationality in Psychology and Economics/The Psychology and Economics Conference Handbook: Comments on Simon, on Einhorn and Hogarth, and on Tversky and Kahneman," The Journal of Business, 59(4): S209.

Sipior, J.C., Ward, B.T., and Bonner, P.G., (2004), "Should Spam Be on the Menu?," Association for Computing Machinery. Communications of the ACM, 47(6): 59.

Smith, H.J., Milberg, S.J., and Burke, S.J., (1996), "Information privacy: Measuring individuals' concerns about organizational practices," MIS Quarterly, 20(2): 167.

Smith, R.G.a.M.D., (2005), "Protecting Personal Information: Obstacles and Directions " WEIS05: Workshop on Economics and Information Security2-3, June, 2005, Boston, MA.

Stone, E.F., Gardner, D.G., Gueutal, H.G., and McClure, S., (1983), "A Field Experiment Comparing Information-Privacy Values, Beliefs, and Attitudes Across Several Types of Organizations," Journal of Applied Psychology, 68(3): 459.

Syverson, P., (2003), "The Paradoxical Value of Privacy," 2nd Annual Workshop on Economics and Information Security May 29-30, 2003 Robert H. Smith School of Business, University of Maryland, MD.

Vaillant, G.E., (1992), Ego mechanisms of defense: Aguide for clinicians and researchers American Psychiatric Press, Washington, DC.

Waldmann, E., (2000), "Incorporating Freud's Theory on Cognitive Processes into Business Ethics Education," Teaching Business Ethics, 4(3): 257.