Do malware warnings reduce the likelihood of installing bad software?

The case of the Trojan Horse

Wahida Chowdhury

A thesis submitted to the Faculty of Graduate and Postdoctoral Affairs in partial
fulfillment of the requirements for the degree of

Master of Cognitive Science

in

Cognitive Science

Carleton University

Ottawa, Ontario

© 2013

Wahida Chowdhury

Abstract

My research focused on increasing computer security by reducing users' likelihood of installing Trojan Horses: malware hiding inside attractive software. Social cognition research suggests that reading security warnings in software reviews could reduce the likelihood of installing malware. In Study 1, 43 undergraduates viewed 30 user reviews of hypothetical games. Half the reviews were malware warnings. Ratings of the warnings' strength were used to select strong and weak warnings for Study 2. In Study 2, 45 undergraduates viewed descriptions and reviews of real computer games. I manipulated the strength and number of warnings in the reviews. Results indicated that the likelihood of installing a game was influenced by both the number and strength of malware warnings in reviews: two warnings reduced ratings of installation likelihood more than did one warning; strong warnings reduced the ratings more than did weak ones. Implications and limitations of the findings for social contributions to computer security are discussed.

Acknowledgements

“Real life isn't always going to be perfect or go our way, but the recurring acknowledgement of what is working in our lives can help us not only to survive but surmount our difficulties” – anonymous

Apart from my yearlong effort, this thesis materialized because of the continuous guidance, support, and encouragement of many people. The small space of this page is not enough to elaborate on and to do justice to their contributions, but I want to express my gratitude to each one of them. First, I would like to thank my co-supervisors, Dr. Robert Biddle and Dr. Warren Thorngate, who met with me weekly since September, 2011 to discuss my thesis. Their enthusiastic comments and feedback developed my thesis towards completion. Next, I want to thank the members of my committee, Dr. Deepthi Kamawar and Dr. John Logan, for providing their valuable comments and guidance to improve my thesis. Thanks are also due to my mother (Mrs. Momotaz Begum) for taking care of my every little need while I was busy working, and my brothers (Adel Chowdhury and Fahad Chowdhury) for listening to my ideas and providing constructive criticisms.

Last but definitely not the least, I want to thank my father, late Mr. Ruhul Chowdhury, who spent two-thirds of his life's earnings to bring me to Canada and give me the opportunity to continue my education. He watched me grow and begin my first research project (the masters thesis), but unfortunately passed away shortly before the thesis ended. I dedicate this thesis to the loving memory of my father.

Table of Contents

1. Introduction	<i>1</i>
2. Computer Security and Trojan Horses	<i>3</i>
2.1. Technical Approach against Trojan Horses	<i>4</i>
2.2. Behavioural Approach against Trojan Horses	<i>5</i>
3. Social Influence	<i>6</i>
3.1. Warning Messages when Installing Software	<i>10</i>
4. Research Hypotheses	<i>11</i>
5. Study 1	<i>14</i>
5.1. Method	<i>14</i>
5.1.1. Participants	<i>14</i>
5.1.2. Research design	<i>14</i>
5.1.3. Procedure	<i>15</i>
5.2. Results	<i>15</i>
5.3. Background Questionnaire Responses	<i>19</i>
5.4. Discussion	<i>22</i>
6. Study 2	<i>23</i>
6.1. Method	<i>23</i>
6.1.1. Participants	<i>23</i>
6.1.2. Research design	<i>23</i>
6.1.3. Game screenshots and descriptions	<i>24</i>
6.1.4. User reviews	<i>25</i>
6.1.5. Procedure	<i>27</i>

6.2. Results	28
6.3. Background Questionnaire Responses	34
6.4. Discussion	36
6.4.1. Similarities with Previous Findings	38
6.4.2. Limitations and Future Directions	39
References	41
List of Tables	vi
List of Figures	vii
List of Appendices	viii

List of Tables

- Table 1** Averages and Standard Deviations of Warnings' Strengths (5=Strong; 0=Weak) 16
- Table 2** Correlations between a Participant's Average Ratings of Four Questions 17
- Table 3** Participants' Average Ratings of Getting and Preventing Computer Problems 21
- Table 4** Average Responses of Participants in the Non-Malware and the Malware groups 30
- Table 5** Average Pre-post Rating Differences in Response to Malware and Non-Malware reviews in the same Game 31
- Table 6** Participants' Average Ratings of Getting and Preventing Computer Problems 36

List of Figures

Figure 1 Likelihood of Installing and the Four Review Types 19

Figure 2 Pre-Post Rate Change and Warning Types 33

List of Appendices

Appendix A	Reviews and Evaluation Questionnaire for Study 1	49
Appendix B	Background Questionnaire for Study 1	52
Appendix C	Informed Consent	54
Appendix D	Debriefing	57
Appendix E	Histograms of Rated Strength of Each Malware Review of Study 1	59
Appendix F	Screenshot of a Computer Game Advertisement with and without User-Reviews Used in Study 2	67
Appendix G	Computer Game Descriptions Used in Study 2	68
Appendix H	Non-Malware Reviews Used in Study 2	71
Appendix I	Malware Warnings in Reviews Used in Study 2	74
Appendix J	Screenshots of Games Used in Study 2	75
Appendix K	Background Questionnaire for Study 2	76
Appendix L	Questions with a Computer Game Advertisement Used in Study 2	79

1. Introduction

A *Trojan Horse* is an attractive-looking, malicious computer programme that can harm computer security when installed. News stories about Trojan Horses causing major security problems occur almost daily, for example, news about unauthorized computer access in commercial firms (BBC News, 2011), and about data breaches of thousands of customers of a private corporation (e.g., Chung, 2011). Trojan horses can install themselves in the click of a mouse, and the consequences of resulting security problems are often severe. Therefore, it is important to reduce the chances of Trojan Horses installations. The purpose of my thesis is to examine how ideas from social cognition might be employed to dissuade computer users from installing Trojan Horses.

Currently, there are two general approaches to protecting users from Trojan Horses. The *technical approach* attempts to develop computer hardware and software to automatically detect Trojan Horses in software, and then warn users of the danger. Such a technical approach can be effective but, as Cranor and Garfinkel (2005) argue, the technology needs to be sufficiently understood and implemented by untrained computer users to be successful. Moreover, the technology is neither foolproof nor infallible. New Trojan Horses are developed daily, and they often go undetected by security hardware and software for weeks or months required to implement new detection updates. During that time, other approaches to limiting the installation of Trojan Horses must be considered.

The *behavioural approach* usually employs cognitive principles to teach users how to detect Trojan Horses and why they should not install them. Pfleeger and Pfleeger (2011) acknowledge that, as not all car drivers are expert mechanics, not all computer

users are experts in security threats. So educating users about security threats may be helpful to induce users without technical knowledge to be secure. Education, however, is not sufficient for behavioural change. A user must also realize the need for the security information, be motivated to look for it, find it, understand it, expend time and effort to implement it.

Social cognitive theory predicts that human thought, motivation and action could be influenced by communication from others (Bandura, 1986). Classic studies by Asch (1951; see also Bond & Smith, 1996) demonstrate how the opinions and behaviour of others can influence people to conform to these opinions and behaviour. Further, decades of research in advertising show the relative ease of forming and changing attitudes through word-of-mouth communication and testimonials (e.g., Chevalier & Mayzlin, 2003; Kulviwat, Bruner, & Al-Shuridah, 2009). The surfeit of opinions and advice given and sought on the Internet in reviews of books, people, ideas, smart phones, travel destinations, etc., suggests that opinion and advice do affect knowledge, motivation, and behaviour. In the literature of social cognition it is called *social influence*.

My research examined whether or not social influence of user-reviews could reduce the likelihood of users installing on their computer seemingly desirable software, also known as Trojan Horses, which contained malware. In particular, I tried to determine how much the wording and the number of malware warnings in reviews of downloadable computer games influenced users' ratings of their likelihood of installing and running the games on their computer.

2. Computer Security and Trojan Horses

Dedicated and often professional computer experts, called *attackers* in the security literature, often attach malicious code to an otherwise desirable computer program, making the program do harmful things to a user's computer once installed. Because the program looks attractive but hides malicious code, it is named after the Greek wooden Trojan Horse that hid soldiers inside. Attackers might create their own malicious code, or use freely available programs such as those at <http://www.prorat.net/downloads.php>, or watch YouTube videos on how to make a Trojan Horse. These attackers can be anyone from teenagers to adults, from anywhere (U.S., China, Russia, Europe, etc.) and with any motive, from having fun to stealing money to initiating a cyber war. Because attackers can rarely be identified and reached, they can rarely be stopped or punished.

Once a computer is connected to the Internet, attackers can advertise their Trojan Horses worldwide. Borchgrave, Cilluffo, Cardash, and Ledgerwood (2001) report that Internet use is predicted to magnify a thousand fold every three years, "more than a million fold in a decade" (Preface, XI). The Office of the Privacy Commissioner of Canada (2011) reports that Canadians are among the world's heaviest users of the Internet, and Statistics Canada (2010) reports that over 50% of Canadian households with the Internet use more than one computer to go online. It is also not too farfetched to expect that access to computers worldwide will continue to increase because the cost of computers is rapidly decreasing while the benefits of using a computer, such as automation of various services and wider accessibility to information, are rapidly increasing.

Thus, with the ease of attaching malicious code to normal software, and with the increasing access to the Internet, a computer user can expect to encounter Trojan Horses frequently. A user who installs a Trojan Horse will unknowingly activate the malicious program hiding inside it (e.g., Lavesson, Boldt, Davidsson & Jacobsson, 2011) and compromise his/her computer security. Manufacturers strive to make computers more reliable and capable each year while service providers, software engineers, governments, private organizations, and technical experts strive to prevent and solve security and socio-economic problems arising from the installation of Trojan Horses (e.g., Government of Canada, 2010).

2.1. The Technical Approach against Trojan Horses

Turing's (1938) proof of the halting problem suggests it is impossible to detect if a program is or is not malicious while it is running. This implies we have to stop the operation of a Trojan Horse before we install it. Technical approaches to prevent users from installing Trojan Horses have led to improvements in antivirus software to detect a Trojan Horse (e.g., Gribble, Levy, Moshchuk, & Bragin, 2012).

Technical approaches reduce a user's responsibility for his/her computer security, but the approaches are often expensive to implement and slow to disperse. It is also worth noting that antivirus software might fail to detect a Trojan Horse. This is because a version of antivirus software matches its constantly updated list of malicious code-sequences with the code-sequence of any new piece of software a user installs (Kephart & Arnold, 1994). However, attackers are constantly varying codes to produce new versions of malware that temporarily escape detection. In the 1-12 months it takes for a

version of antivirus software to add new sequences of code to its malware dictionary, much damage can be done.

2.2. The Behavioural Approach against Trojan Horses

Behavioural approaches to prevent users from installing Trojan Horses include user education. Websites such as <http://isc.sans.org>, <http://www.iss.net>, and <http://www.insecure.org> (Dubin, 2008) offer extensive educational materials about how to detect Trojan Horses; www.getcybersafe.gc.ca, a Canadian federal government initiative, offers several webpages describing risks of installing Trojan Horses from email attachments, social network, file sharing, etc., and provide users with tips on how to avoid these risks. Experts in computer security also have published many books and articles giving advice on how to detect and avoid installing Trojan Horses. For example, Cranor and Garfinkel (2005), Pfleeger and Pfleeger (2011), and Rothke (2005) write that a computer user can avoid installing malware by following many rules, such as by avoiding phishing emails, and by opening email attachments cautiously.

However, just as teaching people that smoking causes cancer might not induce them to stop smoking, educating people that Trojan Horses cause security problems might not induce them to be careful when installing new software. Adams and Sasse (1999) argue, “It is important to challenge the view that users are never motivated to behave in a secure manner” (p.45). Still, it is safe to assume that users are not always motivated to behave securely (e.g., Stanton, Caldera, Isaac, Stam &, Marcinkowski, 2003).

Forcing users to comply with security guidelines or threatening users with punishment for non-compliance might seem to solve the problem of users’ motivation,

and many attempts have been made to influence secure behaviour through rules and regulations tied to rewards or punishments. For example, many work organizations set rules on what can be installed from which websites. However, surveys suggest compliance with security standards is low (Barlette & Fomin, 2009), and most users ignore standards, such as End User License Agreements, that describe before installation what a piece of software does (Chia, Heiner & Asokan, 2012; Thorngate & Tavakoli, 2007). Furthermore, we know from psychology and human-computer interaction that forcing secure behaviour is unsuccessful when the behaviour doesn't correspond to users' habits (e.g., Adams & Sasse, 1999) or to their mental models of security (e.g., Boss, 2007). This leaves users still vulnerable to installing Trojan Horses.

3. Social Influence

Ideally, to increase computer security we should influence the behaviour of attackers, convincing them to stop their wicked ways. Rianti and Gonzalez (2009) suggest this might be done by creating distrust among attackers, but the suggestion seems impractical; attackers are difficult to find and even more difficult to prosecute. So I have focused on influencing users behave more securely.

Social cognitive theory assumes that a person's behaviour is influenced by his/her cognition and social environment (e.g., Bandura, 1986; Wallace, Buckworth, Kirby & Sherman, 2000). Asch (1951) demonstrated the assumption in his classic study on social influence; he induced people to conform to a social norm of estimating line length by manipulating in a group perception experiment what others said about the lengths of lines. His experiment showed the power of social influence in changing people's behaviour and ignited more research on the phenomenon.

Bandura, Grusec, and Menlove (1967) demonstrated that children changed their attitude towards dogs, from fearful to playful, simply by watching video clips of other children playing with dogs. O'Connor (1972) conducted a similar experiment and showed that, after watching video clips of children taking part in social activities, withdrawn children started taking part in school activities the way typically developing children do, while those who did not watch the video clips remained withdrawn. Milgram, Bickman, and Berkowitz (1969) demonstrated adults were also susceptible to such social influence. When a lone experimenter stared up at a blank spot on a storefront wall from a busy sidewalk, no one stopped to look at the same spot, but a crowd formed to look at the spot when the experimenter was accompanied by other experimenters doing the same thing.

Koval, Pederson, and Mills (2000) studied correlations between several factors, including social influence, and initiation of smoking among school students. They found stressful life events alone were not sufficient to initiate smoking; the events had to be coupled with social influence from peers to initiate smoking. Utilizing the powerful effect of social influence, donation collectors often leave dollar notes in see-through baskets to give the impression that others made donations (Cialdini, 2009) and advertisers often use comments such as “four out of five physicians recommend it!”

Do messages from fellow consumers also induce social influence? Early studies suggest that face-to-face, word-of-mouth messages were often influential among consumers seeking information about new products (Coleman, Katz, & Menzel, 1957; Howard & Sheth, 1969; Katona & Mueller, 1954), and could induce customers to accept or reject new products (Beal & Rogers, 1957; Bell, 1967; Sheth, 1968). Lilien and Reo (1978) developed a mathematical model incorporating word-of-mouth as the mediator

between current and future customers and predicting sales of a product. The authors concluded that new products benefit most from word-of-mouth messages at the onset of product sales.

More recently, Kulviwat, Bruner, and Al-Shuridah (2009) showed that the acceptance of a new technological product depends, in part, on what others say about the product – a form of social influence. Although collective cultures were found to be more susceptible to face-to-face social influence than were individualistic cultures (e.g., Bond & Smith, 1996), social influence was universal in computer-mediated communication when people didn't see each other (Cinnirella & Green, 2007) or didn't know each other's names (Spears, Sakhel, & Groot, 2001).

Are online user-reviews also influential? Chevalier and Mayzlin (2003) studied the effect of online book reviews on the sales of amazon.com and barnesandnoble.com. They found that the greater the number and length of book reviews, the greater the sales, suggesting that social influences were occurring. Duan, Gu, and Whinston (2008) analyzed the effect of online user reviews on movie sales. The authors found online users' *ratings* of movies did not have a significant effect but users' written reviews significantly influenced movie ticket sales. The authors concluded that both online user reviews and face-to-face word-of-mouth messages induce customers to buy products.

Furthermore, Chintagunta, Gopinath, and Venkataraman (2010) found that the quality of reviews made greater impact than the number. Research on how messages of different qualities affect attitude change has been voluminous since the early work of Hovland (1948; see also Hovland, Lumsdaine & Sheffield, 1949). All of the research reinforces the idea that the language of messages has powerful effects on attitude

formation and that changing cognition via a message depends a great deal on the characteristics of and the relationship between the audience and the speaker of the message, the kind of behaviour that the speaker wants to change, etc. (Chaiken, 1979, 1980; Guerini, Stock, & Zancanaro, 2007; Tykocinski, Higgins, & Chaiken, 1994). My research tried to induce people not to do something, namely not to install games purported to be Trojan Horses.

How do warning messages influence people? Messages warning people not to perform a task might produce fear or other negative emotions. Eagly (1974) found that messages producing negative emotions often interfered with the comprehension of the message. However, a meta-analysis of studies on messages that associated strong fear with health-related responses found that such messages had strong persuasive power (Witte & Allen, 2000). Prentice-Dunn, Floyd and Flourney (2000) found that the order in which information was presented in a warning message influenced compliance with the message. The authors, for example, found that presenting information first about a health threat and then about coping with the threat, rather than vice versa, induced more people to comply with the coping message. Other studies found that the layout and style of message influenced attitude change. Hammond (2011), for example, found that health warning messages with larger fonts and pictures were more effective than smaller and picture-less warning messages.

How do warning messages read on computer screens affect conformity? Floyd, Whelan, and Meyers (2006) studied the effectiveness of viewing warning messages on computer screens about online gambling. Floyd et al. found that participants who received the warning messages engaged in less gambling behaviour than the participants

who did not receive such messages. Monaghan and Blaszczyński (2009) report that these warning messages were most effective when the experimenters asked readers to reflect on the messages.

3.1. Warning Messages when Installing Software

Many desktop and mobile platforms show a warning message on their computer screen when users click to install software uncertified by a trusted vendor. However, the warning messages are often ambiguous. For example, a warning message might warn users that the software maybe harmful, without stating clearly why or how the software may be harmful. In addition, such messages often give false alarms (warning users against non-malicious software). If the first time a user ignores a warning and nothing harmful happens after installation, the user is likely to ignore an alarm next time he/she tries to install a piece of software with a similar warning. If nothing harmful happens after second-time installation as well, the user might become even more likely to ignore next alarm. Eventually, the user might ignore all warning messages associated with software installation (Chia et al., 2012).

Some websites, such as www.phishtank.com and www.mywot.com collect public opinions on trustworthiness and reliability of websites. However, anecdotal evidence suggests that relatively few computer users are aware of such sites, and studies by Krug (2006) and Redish (2007) of what users do on websites report that users rarely do more than scan a webpage for desired information, ignoring most of what a site offers. The findings suggest that online community sites on security might not be effective unless a user knows of their existence and knows what he or she is looking for.

Chia et al. (2012), in one of their studies, showed participants four different, little-known pieces of software and compared installation decisions of the software with and without warnings from other users. Researchers found the number of decisions to install the software with no warnings in reviews were higher than the software with warnings. However, the researchers did not report tests of significance for installation decisions with warnings versus decisions without warnings and, because the same piece of software was always associated with the same review in the same order, there were confounds in the research design. Perhaps, for example, participants did not want to install the software even before seeing reviews. My thesis controlled for confounds by randomly pairing a computer game with reviews from other users; so a game was paired with non-malware reviews for some participants and with malware warnings for others. I also randomized the order of reviews, so each participant saw malware or non-malware reviews associated with a game in a re-randomly shuffled order.

4. Research Hypotheses

The guiding assumption of my thesis, supported by the research above, is that people can be influenced by what others do and what others say they should do. If true, then computer users should be influenced by reading reviews of software written by other users. In particular, if some users suggest in their reviews that a computer program contains or might contain malware, then other users reading the reviews should decrease their likelihood of installing the software. My research manipulated: (a) the *strength* (explicitness), and (b) the *number* of malware-related user warnings in reviews of computer games to determine if these variables influenced likelihood of installing the reviewed game.

I performed two studies to investigate these possible influences. I conducted Study 1 as a manipulation check to determine which malware warnings I wrote would be rated by users as highest and lowest in strength. To do so, I showed on a computer screen, one at a time, security warnings suggesting a game might contain malware and asked participants to rate each warning's strength.

I then performed Study 2 as a test of the effects of one-versus-two, strong-versus-weak malware warning messages in a more realistic simulation of online game reviews. I showed on a computer screen, one at a time, advertisements (screenshots plus developers' one-paragraph description) of ten computer games. As soon as a participant rated his/her likelihood of installing the advertised game on his/her computer, I showed three user reviews below the advertisement. I then asked each participant to read the reviews, indicate which review they thought was the most important, then re-rate his/her likelihood of installing the reviewed game.

Four of the ten advertisements employed in study 2 included malware warnings in their three-review sets – warnings selected as either weak or strong from those rated in study 1. One of these four advertisements had one weak malware warning and two regular reviews; another of the four advertisements had one strong malware warning and two regular reviews. A third advertisement had two weak warnings and one regular review; and the fourth advertisement had two strong warnings and one regular review. The remaining six three-review sets contained only comments about other aspects of the games. I shuffled the order of three reviews in each advertisement and shuffled the order of advertisements for each participant so that the position of reviews or advertisements did not confound my results. The pre-post differences in average ratings of the four

games containing at least one malware review versus the six games with no malware reviews allowed me to test my first hypothesis.

- Hypothesis 1: *Malware warnings in reviews will decrease participants' rated likelihood of installing a game on their computer more than will (positive or negative) non-malware reviews.*

Previous studies show the wording of review influences conformity to the review (e.g., Chintagunta et al., 2010). Comparing pre-post differences in ratings of the games with weak versus strong warning in reviews allowed me to determine how the wordings of malware warnings influenced changes in participants' likelihood of installing the reviewed games and to test my second hypothesis.

- Hypothesis 2: *Strong malware warnings in reviews will decrease participants' rated likelihood of installing a game on their computer more than will weak malware warnings in reviews.*

Previous studies also show that the greater the number of people expressing the same opinion, the greater the influence (e.g., Asch, 1951; Milgram et al., 1969). My research design allowed me to determine how the number of malware warnings influenced changes in participants' likelihood of installing the reviewed games and to test my third hypothesis:

- Hypothesis 3: *Two malware warnings in reviews will decrease participants' rated likelihood of installing a game on their computer more than will one malware warning in reviews.*

5. Study 1

5.1. Method

5.1.1. Participants. Forty-three students (30 females, 10 males, and 3 of unstated gender) ranging in age from 17 to 25 years participated in the study. The participants were recruited from Introduction to Psychology and Research Methods in Psychology courses via Carleton University's online participant recruiting system. The recruitment requested undergraduate students who were interested in computer games but not majoring in computer science. Participants received course credits for their participation per the Psychology Department's regulations.

5.1.2. Research design. My independent variable was the wording of user reviews. I created 15 different user reviews suggesting that a hypothetical computer game contained malware; the reviews varied in what I believed to be the strength of their wording (for example, "My anti-virus software detected a virus in the game. Don't download it!" versus "The software is good, but after I paid for it, my credit card was charged for it 3 times.", etc.). In addition, I created 15 non-malware reviews that mentioned other game features (for example, "Nice, low-key entertainment.", "Love it!! Didn't like the music but the game is challenging without too much exertion."). To control for order effects, I reshuffled the order of the 30 reviews for each participant.

My dependent variables were responses on four, 6-point (0= not at all; 5 = very much) rating scales. All 30 reviews were rated on two of these four scales: (a) How likely are you to install and run a free copy of this game on your computer? (b) How much do you want to play this game? The 15 malware reviews were rated on two additional scales: (c) How likely do you think the game contains malware? (d) How strong do you think the

malware warning is? Appendix A lists the 15 malware warnings, the 15 non-malware reviews, and the rating scale questions.

All participants also completed a brief background questionnaire concerning their age, sex, computer use, use of reviews before installing software, knowledge of computer security, experience with security problems, etc. The questionnaire allowed me to explore how my dependent variables were correlated with answers to the background questionnaire. The background questionnaire is shown in Appendix B.

5.1.3. Procedure. Participants completed the tasks of Study 1 online by signing into a Fluid Surveys survey research account I created for the project. As soon as they reached the study's website, they were shown a page containing the mandatory Informed Consent form (Appendix C). After clicking the "I agree to participate" button on the form, they were shown a fresh shuffling of the thirty reviews, one review per web page, with the 2 or 4 rating questions under each review (Appendix A). After participants rated the last review, they were shown the background questionnaire and were asked to complete it (Appendix B). Finally, they saw a debriefing page (Appendix D) that provided a rationale for the study, gave them links to university authorities they could contact with any concerns, and thanked them for their participation.

5.2. Results

For Study 2, I required three strong and three weak warnings. In order to determine the strength of each of 15 malware warnings, I examined histograms of each warning's rated strength (response to the question: How strong do you think the malware warning is) by each participant. The resulting histograms were more-or-less unimodal (see Appendix E), and so I decided a warning's rated strength was adequately represented

by its average and standard deviation. Table 1 shows the average rating of each warning in descending order along with its standard deviation.

Table 1

Averages and Standard Deviations of Warnings' Strengths (5=Strong; 0=Weak).

Malware warning	Strength rating	Standard Deviation
I think the game stole my credit card information because after I installed the game my credit card started receiving charges I didn't make.	4.19	1.07
Dang! It sure is malware. When I registered and downloaded the game, it stole my credit card information!	4.00	1.52
This is scary. After I installed the game, my email contacts kept receiving weird messages from me! I ended up uninstalling the game.	3.98	0.99
I lost some of my word file documents after I downloaded this game. The developer of this game seems to be a hacker. Gamers beware!	3.86	1.51
The game crashed my computer! I could not do anything at all!! I ended up buying a new hard disk and lost all my files.	3.84	1.40
This game changes my email password!	3.79	1.32
My anti-virus software detected a virus in the game. Don't download it!	3.72	1.30
What's with a constant warning that I got a virus? I think I should uninstall the game.	3.65	1.09
The software is good, but after I paid for it, my credit card was charged for it 3 times.	3.19	1.57
Sounded good but my computer stopped working every time I tried the game.	3.19	1.33
Wel, I couldn't get this software to run. It kept crashing. And now my computer runs much slower than it did.	3.00	1.40
The game is nice but after I installed the game my contact list disappeared. I am not sure but maybe it's because of the game.	2.74	1.35
The game is attractive but keeps asking me for my Facebook password.	2.53	1.52
The game has some cool graphics but my computer malfunctions when I run it.	2.44	1.45
The game makes my computer as slow as a snail's pace!	2.09	1.59

In order to ensure that warnings used in Study 2 differed significantly in strength ratings, I performed a 1x6 within-subject ANOVA with the three highest-ranked and the three lowest-ranked warnings of Study 1. The test indicates that average strength ratings for the three highest-ranked and the three lowest-ranked warnings were significantly different, $F(5, 165) = 19.01, p < .05, eta\ square = .37$. Bonferroni tests show that each of the three highest ratings was significantly different from each of the three lowest ratings, $p < .001$. However, there was no significant difference among the three highest average ratings, and among the three lowest average ratings.

In order to explore how the strength of the 15 malware warnings influenced answers to the four rating questions, I correlated the 15 malware warnings with the average ratings for the four rating questions (see Table 2).

Table 2

Correlations between a Participant's Average Ratings of Four Questions.

	How strong do you think the malware warning is?	What is the likelihood that the game contains malware?	How likely are you to install and run a free copy of the game on your computer?	How much do you want to play the game?
How strong do you think the malware warning is?	-	.97**	-.93**	-.83**
What is the likelihood that the game contains malware?	-	-	-.96**	-.87**
How likely are you to install and run a free copy of the game on your computer?	-	-	-	.95**

Note. ** All correlations are significant at the .001 level

The positive correlations of Table 2 indicate that, on average, the stronger participants thought a malware warning was, the more likely they were to think the reviewed hypothetical game contained malware. Also, the more participants wanted to play a game, the more likely they were to run the game on their computer. The negative correlations of Table 2 indicate that, on average, the higher the rating for warning strength and the more likely participants thought a game contained malware, the less the participants wanted the game, and the lower was the participants' likelihood of installing the game.

In order to determine if participants' rated likelihoods of installing hypothetical games after viewing malware warnings were different from their rated likelihoods after viewing non-malware reviews, I averaged the likelihoods of installing after each malware and non-malware reviews. On average, participants likelihood of installing games was significantly lower after viewing malware warnings ($M = .41$, $SD = 0.21$) than after viewing non-malware reviews ($M = 2.68$, $SD = 0.89$), $t(14) = -9.31$, $p < .001$. The finding suggests malware warnings in game reviews reduce people's intention to install the games more than do non-malware reviews.

A 1x4 within-subject ANOVA indicates that, on average, participants' likelihood of installing after viewing the 4 types of game reviews (malware warnings, negative non-malware reviews, mixed non-malware reviews, and positive non-malware reviews) were significantly different from each other, $F(1.15, 24.93) = 58.19$, $p < .001$, *eta square* = .95. Figure 1 shows the average likelihood of installing in response to the four types of reviews.

Figure 1. Likelihood of Installing and the Four Review Types.

Visual inspection of Figure 1 suggests malware warnings resulted in lower likelihood of installing a hypothetical game than did positive, negative or mixed non-malware reviews. Bonferroni tests show that, on average, participants' likelihood of downloading games with malware warnings was significantly lower than the likelihood of downloading games with positive and mixed non-malware reviews. However, the average likelihood of installing games with malware warnings was not significantly different from the likelihood of installing games with negative non-malware reviews.

5.3. Background Questionnaire Responses

All participants reported owning a computer (31% owned a Mac and 69% owned a Windows computer). Participants reported downloading a median of 150.0 computer files (*range* = 3 to 2100, *SD* = 462.4), and posting a median of 0.0 software reviews (*range* = 0 to 75, *SD* = 12.7) in the past 12-months. In response to how often they read user reviews, participants rated, on average, 3.0 on a 6-point scale (0 = never and 5 = always).

Furthermore, participants reported playing computer games for a median of 4.5 hours per week ($range = 0-20$, $SD = 4.6$). Three participants reported not playing any games and one participant did not report anything. There were several possible reasons for the anomaly; for example, the participants might have come to the study without meeting the game experience requirement, or they might have once played computer games but stopped long ago. I had to decide whether to exclude these participants in my analyses or to consider them a separate group, or include them with all other participants. To make my choice I compared these four participants' responses to my dependent variables with the responses given by the remaining 39 participants. There were no reliable differences. I therefore decided to include them in my analyses.

The assessment of participants' experience with security problems revealed that, in the past year, participants knew a median of 3.0 ($range = 0$ to 15 , $SD = 3.3$) people whose computer had been infected with a virus or other malware. They also reported a median of 1.0 ($range = 0$ to 100 , $SD = 15.8$) instances of their own computer being infected by a virus or other malicious software, a median of 1.0 ($range = 0$ to 50 , $SD = 9.1$) instances of their computer not working, a median of 0.0 ($range = 0$ to 2 , $SD = 0.3$) instances of losing personal computer files, and a median of 0.0 ($range = 0$ to 10 , $SD = 1.9$) instances of someone accessing their online accounts without their permission.

In response to the background questions on security behaviour, 30% of participants reported they did not update their operating system each time an update was available, 26% reported they did not have anti-virus software, and 47% reported they did not have any other protective software. Also, participants' average ratings of getting and

preventing a computer problem in the next 12-months suggested they did not think they were highly vulnerable to security problems (see Table 3).

Table 3

Participants' Average Ratings of Getting and Preventing Computer Problems.

Getting a Computer Problem in the Next 12 Months	Average Rating (0%= never , 100% = always)
Your computer will stop working (e.g. will freeze or crash)	16%
You will lose personal files on your computer	5%
Someone will access your online accounts without your permission	7%
You will have a virus or other malicious program on your computer	13%
Preventing a Computer Problem in the Next 12 Months	Average Rating (0 = no control, 5 = full control)
Preventing crashes of your computer	3.0
Preventing loss of personal files on your computer	3.0
Preventing others accessing your online accounts without your permission	4.0
Preventing a virus or other malicious program on your computer	3.0

I predicted two personality traits (impulsiveness and willingness to take risks) would affect aversion to malware because I thought these traits could make people ignore warnings in reviews. Analyses of participants' self-assessments of personality revealed that, on average their impulsiveness rated 3.0 on a 6-point scale (where 0 = I don't stop to think before doing anything, and 5 = I always think before doing anything) and love for taking risks rated 2.0 (where 0 = I hate to take risks, and 5 = I love to take risks). I conducted several correlational analyses to determine if there were significant relationships between likelihood of installing games after viewing malware warnings and answers on the background questionnaire (i.e., age, gender, experience with user reviews,

experience with security problems, security behaviour, impulsiveness, and love for taking risks). None of the correlations were significant.

5.4. Discussion

Recall that the primary purpose of Study 1 was to perform a manipulation check for the strength of malware warnings used in Study 2. This was addressed by showing participants, in an online survey, 15 randomly shuffled malware warnings as reviews of hypothetical games, then asking participants to rate the strength of each warning. The results demonstrated that the three highest-ranked warnings had significantly higher strength ratings than did the three lowest-ranked warnings. These six were therefore utilized in Study 2 to form strong and weak levels of the warning strength variable.

Further analysis showed that, regardless of a participant's age, gender, experience with computer problems, etc., average likelihood ratings of installing a hypothetical game after reading malware warnings were lower than were the likelihood ratings after reading non-malware reviews. Similar to social cognitive theory (Bandura, 1986), the findings suggested that human thought, motivation and intention could be influenced by communication from others. The findings also supported my first hypothesis that malware warnings in reviews will decrease participants' rated likelihood of installing a game on their computer more than will non-malware reviews.

However, contrary to my first hypothesis, negative, non-malware reviews did not have a significantly greater effect on the rated likelihood of installing than did the malware warnings. Perhaps people's cognition is similarly influenced by negative, non-malware reviews and malware warnings, or perhaps my sample size of negative, non-malware reviews ($n=4$) was too small to detect the difference.

Study 1 demonstrated that I could construct malware reviews that, when presented alone, would reduce the likelihood of downloading software. In the real world, few people evaluate software based on a single review with no accompanying software screenshot, description or additional reviews. Would malware warnings presented in the context of a screenshot, description, and other reviews be equally effective in altering the likelihood of installing software? Study 2 addressed this question.

6. Study 2

6.1. Method

6.1.1. Participants. A different sample of 45 undergraduate students (34 males and 11 females) ranging in age from 18 to 28 years participated in Study 2. Similar to Study 1, I recruited participants for Study 2 via the Psychology Department's online participant volunteer recruiting system. Computer science majors were requested not to participate because their presumed knowledge of computer security might skew my results. I also verbally confirmed that a participant's major was not computer science before I began a participant session. I made a 45-minutes appointment with each participant to complete the study at a lab in the Human Computer Interaction Building at Carleton University. The participants received course credits for their participation per the Psychology Department's regulations.

6.1.2. Research design. I tested my hypotheses that malware warnings and their strength and number influenced people's likelihood of installing a computer game using a 2x2, within-subject, factorial design. The four games used in the research design were imbedded inside a larger task requiring participants to rate ten computer games before and after viewing three reviews of each. My dependent variable was the pre-post

difference in participants' ratings of the likelihood that they would install a free copy of each game on their own computer.

My two independent variables were (a) the strength of the malware warnings (strong versus weak malware warnings embedded in a game's three user reviews), and (b) the number of malware warnings (one versus two malware warnings embedded in a game's three user reviews). The independent variables were manipulated in four of the 10 games shown. In order to control for game-review confounds, the four games were randomly re-sampled from the pool of ten games shown to each participant, so different games were paired with the 2x2 design for each participant.

The remaining six games served as control to reduce the chances that participants would second-guess the purpose of my study. Each of these six control games had three, real, non-malware reviews written by other users and copied from their game websites. A computer program I wrote in LiveCode controlled the random sampling and presentation order of all 10 game advertisements.

Each participant was asked to complete a brief background questionnaire (see Appendix K). Their responses on the questionnaire allowed me to explore possible covariates on pre-post rating differences. One of the covariates was whether or not participants previously played the games. Others included participants' answers to computer security knowledge and behaviour questions.

6.1.3. Game screenshots and descriptions. Each participant examined on a computer monitor, one at a time, advertisements for 10, real computer games available to download from the Internet at www.myplaycity.com. Each game advertisement contained: (a) a screenshot of the advertised game at the right of the screen (see

Appendix J for examples), (b) a brief, written description of the game, three to five sentences long at the left of the screen (see Appendix G for all 10 game descriptions), and (c) two questions under the description: (1) whether they had played the advertised game before, and (2) how likely they were to run the game on their computer (rated on a 7-point scale: Not at all likely = 1 to 7 = Very likely). As soon as participants saw a game advertisement and answered the two questions, three brief user reviews were added to the screen under the game description. Participants were instructed to read these reviews, to indicate which review was most important, then to re-rate how likely they were to install the game on their computer. See Appendix L for all the questions presented with a game advertisement, and Appendix F for a game advertisement screenshot with and without user reviews.

6.1.4. User reviews. As mentioned earlier, each advertisement showed three reviews ostensibly written by other users who had previously downloaded and played the computer game. Each of the three reviews of a game began with a “star” rating showing from one (* = poor) to five (***** = excellent) stars. The star ratings were then followed by a sentence giving a brief review.

Three reviews of the six randomly-selected control games were non-malware reviews, that is, they mentioned nothing about malware or computer problems, and each were preceded by one to five star ratings. Appendix H lists 30 non-malware reviews (3 for each of the 10 game advertisements).

The remaining four, randomly-selected game advertisements constituted my 2x2 research design. Each of the four contained a mix of real reviews and those I selected from Study 1 to represent the two kinds of malware warnings (S = strong versus W =

weak), and the number of malware warnings (1 versus 2). I needed three strong reviews and three weak reviews to insert into the review sets. These six, filler reviews were the three strongest and the three weakest malware warnings taken from Table 1 of Study 1 (see Appendix I). To control for possible confounds, they were randomly assigned to their appropriate slots so that no two participants saw the same combinations of malware and non-malware reviews.

A “one-star” rating preceded each malware warning. Examples of the four experimental game advertisements (S1, S2, W1, W2) are shown below.

- Advertisement S1 contained two real reviews and one strong malware warning such as “* I think the game stole my credit card information because after I installed the game my credit card started receiving charges I didn’t make.”.
- Advertisement S2 contained one real review and two strong malware warnings such as “* This is scary. After I installed the game, my email contacts kept receiving weird messages from me! I ended up uninstalling the game.” and “* Dang! It sure is malware. When I registered and downloaded the game, it stole my credit card information!”.
- Advertisement W1 contained two real reviews and one weak malware warning such as “* The game makes my computer as slow as a snail’s pace!”.
- Advertisement W2 contained one real review and two weak malware warnings such as “* The game has some cool graphics but my computer malfunctions when I run it.” and “* The game is attractive but keeps asking me for my Facebook password.”.

In order to minimize the confounds that might occur if the manipulated variables (strength and number) were always associated with the same four game advertisements in the same order, each participant had S1, S2, W1 and W2 associated with a different shuffling of the ten advertisements. For example, Participant 1 might see S1, S2, W1 and W2 associated with advertisements 6, 2, 9, and 4; Participant 2 might see S1, S2, W1 and W2 associated with advertisements 5, 1, 10, and 7, etc. I also re-randomized order of a game's three reviews for each participant to avoid the order of information effects found in previous studies (see for example, Prentice-Dunn et al., 2000).

6.1.5. Procedure. When participants came to the lab in the Human Computer Interaction Building, I welcomed them and engaged them in a brief conversation about their major and courses. Next, I explained the informed consent and the instructions for completing the study, and asked for their verbal commitment that they would read reviews and answer all questions honestly. Then the experiment proceeded through the following steps:

1. Participants were shown on an MS Window's computer screen a page containing the mandatory Informed Consent form (Appendix C).
2. After clicking the "I agree to participate" button on the form, they were shown, one at a time, a fresh shuffling of the ten advertisements of computer games with questions.
3. As soon as participants answered the questions for a game, its three user reviews appeared. To increase the chances that participants would read the reviews, they were asked to indicate on the screen which review they thought was the most important.

4. Then participants were asked to re-rate their likelihood of installing the reviewed game (Appendix L).
5. After participants rated all 10 advertisements, they were shown the background questionnaire regarding their age, gender, personality, use of computer, security behaviour, etc. (Appendix K).
6. Finally, they saw a debriefing page (Appendix D), were thanked and excused.

6.2. Results

Recall Hypothesis 1 states that malware warnings in reviews will decrease participants' rated likelihood of installing a computer game more than will non-malware reviews. This implies that ratings of the likelihood of downloading a game before viewing its malware warnings (pre-rating) would be higher than the likelihood rating after viewing its malware warnings (post-rating); subtracting the post rating from the pre rating (pre-post rating difference) would therefore be higher for the four games with malware warnings in reviews than it will be for the six control games with non-malware reviews.

In order to test this hypothesis, I first examined whether participants were responding similarly to the four malware versus the six control games before reading any reviews. Within-subject t-tests show that there was no significant before-reviews difference in participants' average rated likelihood of downloading the four experimental games ($M = 3.57$, $SD = 1.11$) and six comparison games ($M = 3.78$, $SD = 1.35$), $t(44) = 1.45$, $p > 0.05$.

I next calculated each participant's pre-post differences in their rated likelihood of installing each of the 10 computer games, and averaged a participant's four pre-post

differences in the games with malware warnings in reviews and the six pre-post differences in the games with no malware warnings in their reviews. A within-subject t-test shows, on average, participants' pre-post rating difference in the four games with malware warnings was significantly greater ($M = 1.15$, $SD = 1.05$) than the pre-post rating difference in the six games with non-malware reviews ($M = -.20$, $SD = .42$), $t(44) = -9.39$, $p < .001$. This indicates malware warning(s) in game reviews resulted in a greater drop in likelihood to install games.

In order to gain more evidence concerning my first hypothesis, I compared the responses of participants who saw malware warnings in a game's reviews (malware group) with the responses of participants who saw no malware warnings in the same game's reviews (no-malware group). For both the groups I averaged (a) responses to whether participants played a game before, and (b) rated likelihood of installing a game before and after viewing reviews. Table 4 reports the average likelihood of each group downloading a game before and after viewing reviews.

Table 4

Average Responses of Participants in the Non-Malware and the Malware groups.

Game	Malware group		Non-malware group	
	Likelihood of installing a game before viewing malware reviews	Likelihood of installing a game after viewing malware reviews	Likelihood of installing a game before viewing non-malware reviews	Likelihood of installing a game after viewing non-malware reviews
Farm frenzy	2.54	1.92	3.50	3.81
Jigsaw puzzle	2.87	1.27	2.97	3.13
Delicious deluxe	3.94	2.06	3.66	3.72
Royal envoy	3.59	2.71	4.39	5.25
Wild west story	3.85	2.58	2.47	2.95
Cute monsters	2.75	1.58	3.85	3.48
Mad battle	4.27	3.19	5.47	5.53
Super motocross	4.53	2.60	4.50	4.87
Nanny mania	2.75	1.88	3.81	3.43
Rainforest adventure	3.94	3.38	3.38	4.00

Between-subject t-tests show on average, there was no significant difference among the 20 cases of rated install-likelihood before viewing reviews, $t(18) = -.85$, $\rho > 0.05$. However, the test also shows average install-likelihood rating after viewing malware warnings was significantly lower ($M = 2.32$, $SD = .69$) than the install-likelihood rating after viewing non-malware reviews ($M = 4.01$, $SD = .90$), $t(18) = -4.74$, $\rho < .001$.

Next, to confirm whether the likelihood of installing and running a game dropped more from pre-rated likelihood of installing in the malware group than it did in the non-malware group, I subtracted each participant's post-rated likelihood of installing from the pre-rated likelihood of installing, and averaged the pre-post rating difference for each game in both the malware and non-malware groups (see Table 5).

Table 5

Average Pre-post Rating Differences in Response to Malware and Non-Malware reviews in the same Game.

Game	Pre-post differences in response to malware reviews	Pre-post differences in response to non-malware reviews
Farm frenzy	0.62	-0.31
Jigsaw puzzle	1.6	-0.16
Delicious deluxe	1.88	-0.06
Royal envoy	0.88	-0.86
Wild west story	1.27	-0.48
Cute monsters	1.17	0.37
Mad battle	1.08	-0.06
Super motocross	1.93	-0.37
Nanny mania	0.87	0.38
Rainforest adventure	0.56	-0.56

A between-subjects t-test on the two columns of numbers in Table 5 shows average pre-post drop in installation likelihood among participants shown malware warning(s) ($M = 1.19$, $SD = .49$) was significantly greater than the pre-post drop among participants not shown malware warnings ($M = -.21$, $SD = .39$), $t(18) = 7.07$, $p < .001$.

Next, I investigated the effects of one-star non-malware (negative) reviews versus one-star malware warnings on likelihood of installing games. I averaged pre-post rating differences of participants who saw one-star non-malware reviews in Jigsaw Puzzle game's reviews ($n=28$) and of the same or different participants who saw one-star non-

malware reviews in Nanny Mania games' reviews ($n=21$). I also averaged pre-post rating differences of participants who saw one-star malware warnings in Jigsaw Puzzle game's reviews ($n=8$) and of the same or different participants who saw one-star malware warnings in Nanny Mania games' reviews ($n=5$).

A between-subject t-test with participants who saw one-star non-malware reviews in Jigsaw Puzzle or nanny mania games' reviews ($n = 28 + 21 = 49$), and participants who saw one-star malware warnings in Jigsaw Puzzle or Nanny mania games' reviews ($n = 8 + 5 = 13$) shows, the average likelihood rating of downloading the games was not significantly different before viewing the reviews, $t(60) = .15$, $p > .05$. However, the average pre-post rating drop in response to malware warnings in the games' reviews was significantly larger ($M = 1.46$, $SD = 1.76$) than the average pre-post drop in response to the games' one-star non-malware reviews ($M = .06$, $SD = .69$), $t(13) = 2.81$, $p < .05$.

My next analyses employed 2x2 factorial, within-subject analysis of variance on the four games with malware warnings. Strong malware warnings produced a significantly greater reduction in the rated likelihood of installing a game than did weak malware warnings, $F(1,44) = 14.3$, $p < 0.01$, *eta square* = 0.25. Two malware warnings produced a significantly greater reduction in the rated likelihood of installing a game than did one malware warning, $F(1,44) = 17.3$, $p < 0.01$, *eta square* = 0.28. There was no significant strength-by-number interaction, $F(1,44) = 0.20$, $p > 0.10$, *eta square* = 0.01.

The results indicate a significant main effect of malware warning strength, a significant main effect of malware warning number, but no significant interaction in the likelihood of downloading and running games. The results were consistent with two of my hypotheses (Hypothesis 2 and Hypothesis 3):

- Strong malware warnings in reviews decreased participants' rated likelihood of installing a computer game more than did weak malware warnings in reviews;
- Two malware warnings in reviews decreased participants' rated likelihood of installing a computer game more than did one malware warning in reviews.

A 1x4 within-subject ANOVA indicated, on average, participants' pre-post difference in response to the four strength + number combinations of warnings in game reviews (two strong warnings, two weak warnings, one strong warning, and one weak warning) were significantly different from each other, $F(2.50, 109.88) = 8.83, p < .001$, $\eta^2 = 0.17$. Bonferroni tests show that, on average, participants' pre-post difference with two strong warnings was significantly different from the pre-post difference with one weak warning. Pre-post rating was not, however, significantly different between any other pair of warning types. Figure 2 shows average pre-post differences in rated likelihood of installing in response to the four types of malware warnings in reviews.

Figure 2. Pre-Post Rate Change and Warning Types.

6.3. Background Questionnaire Responses

All participants reported owning a computer; 36% owned a Mac and 64% owned a Windows computer. Participants reported downloading a median of 100.0 (*range* = 2 – 5000, *SD* = 824.5) computer files, and posting a median of 0.0 (*range* = 0 – 50, *SD* = 8.4) software reviews in the past 12-months. In response to how often they read user reviews, participants rated on average 6 on a 7-point scale, in which 1 denoted never and 7 denoted always.

Furthermore, participants reported playing computer games for a median of 5.0 hours per week (*range* = 0 – 60, *SD* = 9.9). There were two participants who reported playing computer games 0 hours per week, even though I had required participants to have some experiences playing games. As in study 1, I compared these 2 participants' responses to my dependent variables with the responses given by the remaining 43 participants. There were no reliable differences. I therefore decided to include them in my analyses.

Seventy-three percent of participants reported reading all of the reviews presented in this study; the remaining 27% of participants reported reading, on average, 72% of the study's reviews. Exploratory analyses of ratings of the likelihood that participants will install a game on their computer revealed no reliable differences between participants who reported reading all reviews versus participants who reported reading fewer than 100% reviews. Even the two participants who reported reading fewer than 50% of the reviews appeared to be influenced as much by the warnings as the remaining participants. Perhaps their reading estimates were inaccurate, or perhaps they read only malware warnings.

The assessment of participants' indirect and direct experience with security problems revealed the following. In the past year, participants knew a median of 2.0 (*range* = 0 – 20, *SD* = 4.1) people whose computer had been infected with a virus or other malware. They also reported a median of 1.0 (*range* = 0 to 100, *SD* = 15.4) instances of their own computer being infected by a virus or other malicious software, a median of 2.0 (*range* = 0 – 60, *SD* = 13.6) instances of their computer not working, a median of 0.0 (*range* = 0 – 100, *SD* = 16.5) instances of someone accessing their online accounts without their permission, and a median of 0.0 (*range* = 0 – 30, *SD* = 4.7) instances of losing their computer files.

In reply to the background questions about their own security behaviour, 38% of participants reported they did not update their operating system each time a new version was available, 71% reported they had anti-virus software but only 33% reported checking for updates to their anti-virus software. In addition, 49% reported they had other protective software but only 29% of those who had protective software reported they updated their software when an update was available. Table 6 shows participants' average ratings of getting and preventing a computer problem in the next 12-months. The results suggest they do not believe they are highly vulnerable to security problems.

Table 6

Participants' Average Ratings of Getting and Preventing Computer Problems.

Getting and Preventing a Computer Problem in the Next 12 Months	Average rating (0%= never and 100% = always)
Your computer will stop working (e.g. will freeze or crash)	24%
You will lose personal files on your computer	6%
Someone will access your online accounts without your permission	11%
You will have a virus or other malicious program on your computer	19%
Preventing crashes of your computer	42%
Preventing loss of personal files on your computer	70%
Preventing others accessing your online accounts without your permission	74%
Preventing a virus or other malicious program on your computer	60%

As in study 1, I predicted two personality traits (impulsiveness and willingness to take risks) would affect aversion to malware. The self-assessments of participants' personality traits revealed, on average, their impulsiveness rated 5.1 on a 7-point scale (1 = I don't stop to think before doing anything, to 7 = I always think before doing anything) and risk-taking rated 4.3 (1 = I hate to take risks, to 7 = I love to take risks).

Pearson correlations suggest the likelihood of installing games after viewing malware warnings was significantly correlated with previous experiences with computer stopping to work ($r = 0.41, p < .005$), and with computer files disappearing ($r = 0.37, p < .01$). However, other answers to the background questions (for example, age, gender, computer use, personality, etc.) were not significantly correlated.

6.4. Discussion

Recall the purpose of the second study was to test my three hypotheses: (a) malware warnings in reviews will reduce participants' rated likelihood of installing games more than will (positive or negative) non-malware reviews; (b) strong malware

warnings in reviews will decrease participants' rated likelihood of installing a computer game more than will weak malware warnings in reviews; and (c) Two malware warnings in reviews will decrease participants' rated likelihood of installing a computer game more than will one malware warning in reviews. To test the hypotheses, I asked participants to rate the likelihood of installing ten randomly-shuffled computer game advertisements before viewing the games' reviews from other users, and again after viewing reviews. Four games were randomly selected for each participant to show one or two, strong or weak malware warnings. Analysing the pre-post difference in rated likelihood of installing the games allowed me to test my hypotheses.

Results demonstrated that even though participants rated the computer games similarly before viewing game reviews, their ratings changed after they viewed the reviews; the average post-rated likelihood of installing a game after viewing malware warnings was significantly lower than the average post-rated likelihood of installing the game after viewing non-malware reviews. Also, the non-significant difference found between malware warnings and negative non-malware reviews in Study 1 became significant in Study 2. Furthermore, the results demonstrated that the cognitive rule integrating information about strength and number of malware reviews was additive. The number and the strength of malware warnings independently influenced the drop in rated likelihood of downloading.

In addition, the findings were not significantly correlated with participants' age, gender, and self-assessments of computer use, download behaviour, risk taking behaviour, and impulsiveness. Two experiences with computer-problems (computer not working and losing computer files) were found to significantly affect post-rated

likelihood of installing a game after viewing malware warnings in a game's reviews. However, this finding could not be generalized to other direct experiences with computer problems (getting hacked and getting a malicious software on computer), or to an indirect experience with computer problem (number of people heard of getting infected by a malicious computer program). The results suggest that there are individual differences in the kind of experiences with computer problems that might affect people's aversion to malware. Future studies should assess in more detail individual differences in sensitivity to malware warnings from other users.

6.4.1. Similarities with Previous Findings. A number of previous studies in social cognition demonstrated that a person's thought, motivation, and action are influenced by communication from others (e.g., Asch, 1951; Bandura et al., 1967; Koval et al., 2000; Kulviwat, 2009). My study extended this work by demonstrating that participants' rated likelihood of installing computer games was influenced by communication from other game users. Malware warnings from users in games' reviews significantly lowered people's intention to install the games. Similar to the findings of Chia et al. (2012), my findings suggest malware warnings from users might be a form of *crowd sourcing*, making use of communications from members of the user community to warn others of malware quickly and efficiently. Such malware reviews therefore have the potential to complement technical solutions to malware problems.

My findings demonstrated three more things. First, similar to Duan et al. (2008), I demonstrated that written reviews from users were more influential than their star-ratings; one-star malware warnings lowered people's rated likelihood of installing than did one-star non-malware reviews. Second, similar to Chintagunta et al. (2010), I

demonstrated that wording of a review affected its influence; strong reviews were more influential than weak reviews. Perhaps the quality of writing would influence the effectiveness of malware warnings as well. Third, similar to the finding of Asch (1951) and Milgram et al. (1969) that the higher the number of people expressing the same opinion the higher the conformity rate, I found that two malware warnings in reviews were more influential than was one malware warning.

6.4.2. Limitations and Future Directions. Like all studies, mine were not without limitations. First, my studies asked participants to rate the likelihood they would install a game, but did not investigate whether their ratings were correlated with installation behaviour. I did this to avoid ethical issues, such as asking participants to install on their own computer a malicious program that they were told was harmful. Nevertheless the question of intention-behaviour links in the area of malware remains. Future studies would benefit from investigating the relation between the rated likelihood to behave securely and secure behaviour.

A second limitation of my studies is that they consider only computer games. It could be claimed that people read, and are affected by, reviews before installing a computer game, but not before installing other software such as apps for productivity or for gathering online information. Future studies should test the generalizability of malware warnings beyond game reviews.

A third limitation of my studies is that they assume, at least implicitly, that members of the user community who write reviews are all honest and community-minded. No doubt many are; no doubt some are not. Warnings of malware could be fabricated to mislead users with false alarms, possibly creating a “Wolf! Wolf!” effect

(e.g. BBC News, 2013), or reviews with malware warnings could be countered with claims of safety or personal attacks on those who produce the malware warnings. The participants in my studies reported reading more reviews than posting them – a finding consistent with Chia et al.'s (2012) speculation that a few active users might influence a large number of people by negatively reviewing a good piece of software or by positively reviewing a bad piece.

The possible proliferation of false reviews remains a concern for the future effectiveness of malware warnings as a security measure. Still, my research demonstrates that malware warnings have the potential to reduce security problems, and thus to complement other tactics designed to make computing more secure.

References

- Adams, A., & Sasse, M. A. (1999). Users are not the enemy: Why users compromise computer security mechanisms and how to take remedial measures. *Communications of The ACM*, vol. 42 (12), 41-46.
- Asch, S. E. (1951). Effects of group pressure upon the modification and distortion of judgment. In H. Guetzkow (Ed.). *Groups, leadership and men*. Pittsburgh, PA: Carnegie Press.
- Bandura, A. (1986). Social foundations of thought and action: A social cognitive theory. Prentice-Hall, Inc.
- Bandura, A., Grusec, J. E., & Menlove, F. L. (1967). Vicarious extinction of avoidance behaviour. *Journal of Personality and Social Psychology*, vol. 5, 16-23.
- Barlette, Y., & Fomin, V. V. (2009). Chapter VI: The adoption of information security management standards—A Literature Review. In Knapp, K. J. (Ed.). *Cyber security and global information assurance: threat analysis and response solutions*. Hershey, PA : Information Science Reference.
- BBC News. (2013). Samsung probed in Taiwan over 'fake web reviews'. *BBC News*. Retrieved online on 24 April, 2013 from <http://www.bbc.co.uk/news/technology-22166606>.
- BBC News. (2011). Chemicals and defence firms targeted by hacking attack. *BBC News*. Retrieved online on 2 December, 2011 from <http://www.bbc.co.uk/news/technology-15529930>.
- Beal, G. M., & Rogers, E. M. (1957). Informational sources in the adoption of new fabrics. *Journal of Home Economics*, vol. 49, 166-168.

- Bell, G. D. (1967). Self confidence and persuasion in car buying. *Journal of Marketing Research*, vol. 4, 46-52.
- Bond, R., & Smith, P. B. (1996). Culture and conformity: A meta-analysis of studies using Asch's (1952b, 1956) line judgment task. *Psychological Bulletin*, vol. 119(1), 111-137.
- Boss, S. R. (2007). Control, perceived risk, and information security precautions: external and internal motivations for security behaviour (Doctoral Dissertation, University of Pittsburgh).
- Chaiken, S. (1979). Communicator physical attractiveness and persuasion. *Journal of Personality and Social Psychology*, vol. 37(8), 1387-1397.
- Chaiken, S. (1980). Heuristic versus systematic information processing and the use of source versus message cues in persuasion. *Journal of Personality and Social Psychology*, vol. 39(5), 752-766.
- Chevalier, J. A., & Mayzlin, D. (2003). The effect of word of mouth on sales: Online book reviews. *Journal of Marketing Research*, NBER Working Paper No. 10148.
- Chia, P. H., Heiner, A. P., & Asokan, N. (2012). Use of ratings from personalized communities for trustworthy application installation. *Lecture Notes in Computer Science*, vol. 7127, 71-88.
- Chintagunta, P. K., Gopinath, S., & Venkataraman, S. (2010). The effects of online user reviews on movie box office performance: Accounting for sequential rollout and aggregation across local markets. *Journal of Marketing Science*, vol. 29(5).
- Chung, E. (2011). Sony data breach update reveals 'bad practices'. *CBC News*. Retrieved online on 30 November, 2011 from

<http://www.cbc.ca/news/technology/story/2011/05/03/sony-data-breach-playstation.html>.

Cialdini, R. B. (2009), chapter 4: social proof: truths are us. In Cialdini, R. B. *influence: science and practice* (pp.97-138). USA: Pearson Education, Inc.

Cinnirella, M., & Green, B. (2007). Does ‘cyber-conformity’ vary cross-culturally? Exploring the effect of culture and communication medium on social conformity. *Computers in Human Behaviour*, vol. 23(4), 2011-2021.

Coleman, J, Katz, E., & Menzel, H. (1957). The diffusion of an innovation among physicians. *Sociometry*, vol. 20, 253-270.

Cranor, L., & Garfinkel, S. Eds. (2005). *Security and usability*. Canada: O’Reilly Media, Inc.

De Borchgrave, A., Cilluffo, F. J., Cardash, S. L., & Ledgerwood, M. M. (2001). *Cyber threats and information security: meeting the 21st century challenge*. Washington: The CSIS Press.

Duan, W., Gu, B., & Whinston, A. B. (2008). Do online reviews matter? — An empirical investigation of panel data. *Decision Support Systems*, vol. 45(4), 1007-1016.

Dubin, J. (2008). *The little black book of computer security, second edition*. Loveland, CO : 29th Street Press.

Eagly, A. A. (1974). Comprehensibility of persuasive arguments as a determinant of opinion change. *Journal of Personality and Social Psychology*, vol. 29(6), 758-773.

- Floyd, K., Whelan, J. P., & Meyers, A. W. (2006). Use of warning messages to modify gambling beliefs and behaviour in a laboratory investigation. *Psychology of Addictive Behaviours*, vol. 20(1), 69-74.
- Gribble, S., Levy, H., Moshchuk, A., & Bragin, T. (2012). U.S. Patent No. 8,196,205. Washington, DC: U.S. Patent and Trademark Office.
- Government of Canada. (2010). *Canada's cyber security strategy: for a stronger and more prosperous Canada*. Retrieved from http://www.publicsafety.gc.ca/prg/ns/cbr/_fl/ccss-scc-eng.pdf
- Guerini, M., Stock, O., & Zancanaro, M. (2007). A taxonomy for strategies for multimodal persuasive message generation. *Applied Artificial Intelligence*, vol. 21(2), 99-136.
- Hammond, D. (2011). Health warning messages on tobacco products: a review. *Tobacco Control*, vol. 20(5), 327-337.
- Hovland, C. I. (1948). Psychology of the communicative process. In Schramm, W. (Ed.). *Communications in modern society*, 59-611. Urbana: University of Illinois Press.
- Hovland, C. I., Lumsdaine, A. A., & Sheffield, F. D. (1949). *Experiments on mass communication*. Princeton: Princeton University Press.
- Howard, J., & Sheth, J. N. (1969). *The theory of buyer behaviour*. New York: John Wiley and Sons, Inc.
- Katona, G., & E. Mueller. (1954). A study of purchase decisions. In Clark, L. M. (Ed.). *Consumer Behaviour: The Dynamics of Consumer Reaction* (pp. 34-87). New York: New York University Press.

- Kephart, J. O., & Arnold, W. C. (1994). Automatic extraction of computer virus signatures. In R. Ford (ed.), *Proceedings of the 4th virus bulletin international conference* (pp. 178-184). Abingdon, England: Virus Bulletin Ltd.
- Koval, J. J., Pederson, L. L., & Mills, C. A. (2000). Models of the relationship of stress, depression, and other psychosocial factors to smoking behaviour: A comparison of a cohort of students in grades 6 and 8. *Preventive Medicine*, vol. 30, 463–477.
- Krug, S. (2006). *Don't make me think! A common sense approach to web usability*. USA: New Riders.
- Kulviwat, S., Bruner, G. C., & Al-Shuridah, O. (2009). The role of social influence on adoption of high tech innovations: The moderating effect of public/private consumption. *Journal of Business Research*, vol. 62(7), 706-712.
- Lavesson, N., Boldt, M., Davidsson, P., & Jacobsson, A. (2011). Learning to detect spyware using end user license agreements. *Knowledge and Information Systems*, 26(2), 285-307.
- Lilien, G. L., & Reo, A. G. (1978). A marketing promotion model with word of mouth effects. *MIT Working paper, Alfred P. Sloan School of Management*.
- Milgram, S., Bickman, L., & Berkowitz, O. (1969). Note on the drawing power of crowds of different size. *Journal of Personality and Social Psychology*, vol. 13, 79-82.
- Monaghan, S., & Blaszczynski, A. (2009). Electronic gaming machine warning messages: Information versus self-evaluation. *The Journal of Psychology*, vol. 144(1), 83-96.

- O'Connor, R. D. (1972). Relative efficiency of modeling, shaping and the combined procedures for modification of social withdrawal. *Journal of Abnormal Psychology, 79*, 327-334.
- Office of the privacy commissioner of Canada. (2011). *Protecting your privacy online*. Retrieved online on 7 December, 2011 from http://www.priv.gc.ca/fs-fi/02_05_d_13_rev_e.cfm.
- Pfleeger, C. P., & Pfleeger, S. L. (2011). *Analyzing computer security: a threat/vulnerability/countermeasure approach*. Upper Saddle River, NJ: Prentice Hall.
- Prentice-Dunn, S., Floyd, D. L., & Flournoy, J. M. (2000). Effects of persuasive message order on coping with breast cancer information. *Health Education Research, vol. 16(1)*, 81-84.
- Radianti, J., & Gonzalez, J. J. (2009). Chapter I: Dynamic modeling of the cyber security threat problem—The black market for vulnerabilities. In Knapp, K. J. (Ed.). *Cyber security and global information assurance: threat analysis and response solutions*. Hershey, PA : Information Science Reference.
- Redish, J. (2007). *Letting go of the words: writing Web content that works*. Amsterdam, Boston : Elsevier/Morgan Kaufmann Publishers.
- Rothke, B. (2005). *Computer security: 20 things every employee should know, second edition*. New York: McGraw-Hill.
- Sheth, J. N. (1968). Perceived risk and diffusion of innovation, insights into consumer behaviour. In J. Arndt (Ed.). Boston: Allyn and Bacon.

- Spears, R., Sakhel, K., & De Groot, D. (2001). Social influence in computer-mediated communication: The effects of anonymity on group behaviour. *Personality and Social Psychology Bulletin*, vol. 27(10), 1243-1254.
- Stanton, J. M., Caldera, C., Isaac, A., Stam, K. R., & Marcinkowski, S. J. (2003, April). Behavioural information security: defining the criterion space. In P. M. Mastrangelo & W. J. Everton (Eds). *The Internet at work or not: preventing computer deviance*. Symposium presentation at the meeting of the Society for Industrial and Organizational Psychology, Orlando, FL, USA.
- Statistics Canada. (2010). Canadian Internet use survey. *The Daily*. Retrieved online on 1 December, 2011 from <http://www.statcan.gc.ca/daily-quotidien/110525/dq110525b-eng.htm>.
- Thorngate, W., & Tavakoli, M. (2007). *EULAs: Who reads them? Report for the Canadian Internet Policy and Public Interest Clinic*. Unpublished manuscript, University of Ottawa, Ottawa, Canada.
- Turing, A. M. (1938). On computable numbers, with an application to the Entscheidungsproblem. A correction. In *Proceedings of the London Mathematical Society*, vol. s2-43 (1), 544-546. doi: 10.1112/plms/s2-43.6.544
- Tykocinski, O., Higgins, E. T. & Chaiken, S. (1994). Message framing, self-discrepancies, and yielding to persuasive messages: The motivational significance of psychological situations. *Personality and Social Psychology Bulletin*, vol. 20(1), 107-1111.

- Wallace, L. S., Buckworth, J., Kirby, T. E., & Sherman, W. M. (2000). Characteristics of exercise behaviour among college students: Application of social cognitive theory to predicting stage of change. *Preventive Medicine*, vol. 31(5), 494-5011.
- Witte, K. W., & Allen, M. (2000). A meta-analysis of fear appeals: Implications for Effective Public Health Campaigns. *Health Education Behaviour*, vol. 27(5), 591-6111.

Appendix A. Reviews and Evaluation Questionnaire for Study 1

Review 1. I lost some of my word file documents after I downloaded this game. The developer of this game seems to be a hacker. Gamers beware!

Review 2. Dang! It sure is malware. When I registered and downloaded the game, it stole my credit card information!

Review 3. My anti-virus software detected a virus in the game. Don't download it!

Review 4. Well, I couldn't get this software to run. It kept crashing. And now my computer runs much slower than it did.

Review 5. The software is good, but after I paid for it, my credit card was charged for it 3 times.

Review 6. Sounded good but my computer stopped working every time I tried the game.

Review 7. What's with a constant warning that I got a virus? I think I should uninstall the game.

Review 8. The game has some cool graphics but my computer malfunctions when I run it.

Review 9. The game is nice but after I installed the game my contact list disappeared. I am not sure but maybe it's because of the game.

Review 10. The game is attractive but keeps asking me for my Facebook password.

Review 11. The game crashed my computer! I could not do anything at all!! I ended up buying a new hard disk and lost all my files.

Review 12. The game makes my computer as slow as a snail's pace!

Review 13. I think the game stole my credit card information because after I installed the game my credit card started receiving charges I didn't make.

Review 14. This game changes my email password!!

Review 15. This is scary. After I installed the game, my email contacts kept receiving weird messages from me! I ended up uninstalling the game.

Questions after reviews 1-15

- a. What is the likelihood that the game contains malware (software that harms your computer or that compromises your privacy or security)? not at all likely 1 2 3 4 very likely
- b. How strong do you think the malware warning is? not at all strong 1 2 3 4 very strong
- c. How likely are you to install and run a free copy of the game on your computer? not at all likely 1 2 3 4 very likely
- d. How much do you want to play the game? not at all 1 2 3 4 very much

Review 16. I thought it's kinda boring game when I played first time but this is really attractive! I love this game now and cannot stop playing it!!

Review 17. Nice, low-key entertainment.

Review 18. Love it!! Didn't like the music but the game is challenging without too much exertion.

Review 19. I thought it was pretty good, the controls were a little off but the rest was good.

Review 20. Reviews on the Run gave it 1/10 for annoying controls. I agree.

Review 21. This game the best but needs more levels.

Review 22. The game is ton of fun but I was shocked at how quickly I completed it.

Review 23. Gosh, it wants me to pay for more levels!

Review 24. Good graphics, good story. Very enjoyable.

Review 25. Stars are hard to win with the time given.

Review 26. Very good, really easy to start but gets challenging real fast!

Review 27. Awesome game for computer. More levels would make it 5 stars.

Review 28. Love the tournaments! Not keen on the boosts in the regular game. But still a great game.

Review 29. It's a fun game to play but the food doesn't seem to earn as much money as it should.

Review 30. It didn't have a good selection of pictures.

Questions after reviews 16-30

- a. How likely are you to install and run a free copy of the game on your computer? not at all likely 0 0 0 0 very likely
- b. How much do you want to play the game? not at all 0 0 0 0 very much

Appendix B. Background Questionnaire for Study 1

1. Age (in years) ____

2. Sex ____

3. How many hours per week do you play computer games? ____

4. In the past year, how many people you know have told you about getting a computer virus or other malicious software on their computer? ____

11. Do you own a computer? ____ If yes,

11.1 What operating system are you using? Windows __, Mac __, Other __

11.2 During the past year, about how many hours per day have you used your computer?

11.3 In the past year, about how many computer files (videos, audios, photos, and other computer programs) have you downloaded from the Internet to your computer? ____

11.4 Do you install updates to your operating system each time they are available? ____
yes, ____ no

11.5 Do you have anti-virus software in your computer? ____

11.11.1 If yes, do you check for updates to your anti-virus software at least once a month? ____ yes, ____ no

11.6 Do you have any other software to protect your computer from security threats?

11.6.1 If yes, do you check for updates at least once a month? ____ yes, ____ no

11.7 In the past 12 months, how many times have you encountered the following computer problems? Answer on a scale from 0 to 100+ times.

a) Your computer stopped working (e.g., froze or crashed): ____

b) You lost personal files on your computer (e.g., files disappeared) _____

c) Someone accessed your online accounts without your permission _____

d) You detected a virus or other malicious program on your computer _____

11.8 In the next 12 months, what do you think are the chances that your computer will have the following problems? Answer on a scale from 0 to 100 % chance.

a) Your computer will stop working (e.g. will freeze or crash) _____

b) You will lose personal files on your computer _____

c) Someone will access your online accounts without your permission _____

d) You will have a virus or other malicious program on your computer _____

11.9 How much personal control do you believe you have in preventing the following problems? Answer on a scale from 0 = no control at all to 5 = complete control.

a) Preventing crashes of your computer _____

b) Preventing loss of personal files on your computer _____

c) Preventing others accessing your online accounts without your permission _____

d) Preventing a virus or other malicious program attacking your computer _____

6. How often do you read user reviews before downloading software? never 0 0 0 0
always

7. How many software reviews have you posted in the past year (0 to 100+)? _____

8. In general how impulsive do you think you are? [I don't stop to think before doing anything 1 2 3 4 I always think before doing anything]

9. How much do you like to take risks? I hate to take risks 1 2 3 4 I love to take risks

Appendix C. Informed Consent

The purpose of an informed consent is to ensure that you understand the purpose of the study and the nature of your involvement. The informed consent must provide sufficient information such that you have the opportunity to determine whether you wish to participate in the study. For clarification, please ask the researcher.

Title: Evaluating user reviews of computer games

Principal Researcher: Ms Wahida Chowdhury (Wahida_chowdhury@carleton.ca, or call (613) 520-2600 ext. 6317)

Co-supervisors: Dr. Robert Biddle (613 520-2600 ext. 6317) & Dr. Warren Thorngate (613-520-2600 ext. 1097)

Concerns: With regards to ethical concerns about this study, please contact Dr. Avi Parush, Chair of Carleton University Ethics Committee for Psychological Research, at 613 520-2600 ext. 6026 or send an email to: avi_parush@carleton.ca. For any other concerns pertaining to this study, please contact Dr. Joanne LeFevre, Director of the Institute of Cognitive Science, at 613-520-2600 ext. 2693 or send an email to: Joanne_LeFevre@carleton.ca.

Purpose: In this study I am interested in learning how the wording of user reviews of computer games affects the attitudes of other users towards the games.

Task Requirements: This study asks undergraduate participants to read 30 brief user reviews of computer games. After reading each review, participants will be asked to make a few ratings of the reviewed game: 1. the likelihood that the game contains malware (software that harms your computer or that compromises your privacy or security), 2. How strong participants think a malware warning is, 3. the likelihood that

participants would install and run a free copy of the game on their computer, and 4. how much participants would want to play the game. In addition, participants will be asked to complete a background questionnaire.

Locale, Duration and Compensation: The study will take place from any computer with an Internet connection for about 30 minutes. You will receive course credits for your participation.

Benefits/compensation: You will receive a 0.25% increase in your final grade in PSYC 1001, 1002, 2001, 2002 or NEUR 2001, 2002 for participating in this study.

Potential Risk and Discomfort: This study is not associated with any potential for harm. You may decline to answer questions that you do not feel comfortable answering and you may decide to withdraw your data from the study at any time.

Anonymity/Confidentiality: The data collected in this study are strictly confidential. All data are coded such that your name is not associated with the responses you provide. Any identifying information associated with your code will be confined to a single page that will be separated from your questionnaire, and kept in a separate, secured file by the research investigators, who will keep this information confidential. The informed consent and all other identifying information will be destroyed after three years. The anonymously coded data will be kept and will be used for research and teaching purposes.

Right to withdraw: Your participation in this study is entirely voluntary. At any point during the study, you have the right to not complete certain questions, or to withdraw without penalty. If you withdraw, you have the right to request that your data be deleted.

Researcher's signature: Ms Wahida Chowdhury

Consent

I have read the above consent form and description of the study. I understand that the data collected will be used for research as well as publishing and teaching purposes. By checking the "I consent" checkbox below, I agree to participate in the study, and this in no way constitutes a waiver of my rights.

This study has received clearance by the Carleton University Psychology Research Ethics Board (Reference #12-133)

(checkbox) I consent

(checkbox) I do not consent

Appendix D. Debriefing

Thank you for participating in my experiment.

What am I trying to learn in this research?

As previously stated, my experiment examines how effective user reviews are in changing the attitudes of other users.

What are the research questions?

I am varying some of the kinds of reviews to see how these variations might influence reactions of users like yourself. For example, some of the reviews you saw had warnings about viruses and other malware. This allows us to compare how malware-related versus non-malware-related reviews affect your responses.

Why is this important to scientists or the general public?

As user reviews increase in popularity, it is important to know their effects on users who read them. Answers to my research questions will help presentation of online software to you and others.

Where can I learn more?

If you wish to learn how online user reviews are widely used elsewhere, see Masum, H. & Tovey, M. (Eds.). (2011). *The Reputation Society: How Online Opinions Are Reshaping the Offline World*. Cambridge, Massachusetts; London, England: The MIT Press.

What if I have questions later?

For any questions or concerns regarding the research, please contact the researcher Wahida Chowdhury either by email Wahida_chowdhury@carleton.ca or call (613) 520-2600 ext. 6317. For ethical concerns, please contact Dr. Avi Parush, Chair of the Carleton

University Ethics Committee for Psychology Research, at (613) 520-2600 ext. 6026 or send an email to: avi_parush@carleton.ca. For any other concerns pertaining to this study, please contact Dr. Joanne LeFevre, Director of the Institute of Cognitive Science, at (613) 520-2600 ext. 2693 or send an email to: Jo-anne_LeFevre@carleton.ca.

This study has received clearance by the Carleton University Psychology Research Ethics Board (Reference #12-133).

Appendix E. Histograms of Rated Strength of Each Malware Review of Study 1

Review 1. I lost some of my word file documents after I downloaded this game. The developer of this game seems to be a hacker. Gamers beware!

Review 2. Dang! It sure is malware. When I registered and downloaded the game, it stole my credit card information!

Review 3. My anti-virus software detected a virus in the game. Don't download it!

Review 4. Well, I couldn't get this software to run. It kept crashing. And now my computer runs much slower than it did.

Review 5. The software is good, but after I paid for it, my credit card was charged for it 3 times.

Review 6. Sounded good but my computer stopped working every time I tried the game.

Review 7. What's with a constant warning that I got a virus? I think I should uninstall the game.

Review 8. The game has some cool graphics but my computer malfunctions when I run it.

Review 9. The game is nice but after I installed the game my contact list disappeared. I am not sure but maybe it's because of the game.

Review 10. The game is attractive but keeps asking me for my Facebook password.

Review 11. The game crashed my computer! I could not do anything at all!! I ended up buying a new hard disk and lost all my files.

Review 12. The game makes my computer as slow as a snail's pace!

Review 13. I think the game stole my credit card information because after I installed the game my credit card started receiving charges I didn't make.

Review 14. This game changes my email password!!

Review 15. This is scary. After I installed the game, my email contacts kept receiving weird messages from me! I ended up uninstalling the game.

Appendix F. Screenshot of a Computer Game Advertisement with and without User

Reviews Used in Study 2

Download **wild west game** and help rebuild home town in this exciting wild west game! Use your match making abilities, awesome power-ups and sharp eyesight to repair all the buildings and get people to move into your town. Have days of fun with this great Match 3 and Hidden Object mix.

Step1. Have you ever played this game? ☐ Yes ☒ No

Step2. Rate the game

How likely are you to install and run a free copy of this game on your computer?

Not at all likely Very likely

OK

Withdraw

Screenshot 1: An advertisement without reviews

Download **wild west game** and help rebuild home town in this exciting wild west game! Use your match making abilities, awesome power-ups and sharp eyesight to repair all the buildings and get people to move into your town. Have days of fun with this great Match 3 and Hidden Object mix.

User reviews

*** Awesome game for computer. More levels would make it 5 stars.

** I have seen better.

***** Very good, really easy to start but get challenging real fast!

Step3. Which review was the most important to you?

☐ Top review ☐ Middle review ☒ Bottom review

Step4. Re-rate the game

How likely are you to install and run a free copy of this game on your computer?

Not at all likely Very likely

Go to next game

Withdraw

Screenshot 2: An advertisement with reviews

Appendix G. Computer Game Descriptions Used in Study 2

1. Farm frenzy

Download **Farm Frenzy 2** and start your country business! You are the owner of a bakery, a confectionary, a cheese factory and 9 other buildings that comprise your farm business. The only annoying feature that can spoil your thoroughly designed business plans are the bears. This time you have to face the risk of being looted by four different types of bears that haunt your farm and turn your plans upside down.

2. Rainforest adventure

Download **Rainforest Adventure** and follow a path of puzzling fun through a vibrant rainforest in this colorful new and challenging rainforest game! Swap tropical game pieces to make matching groups of three or more and turn the board to gold in more than 120 brain-bending levels.

3. Cute monsters

Download **cute monster** games and enjoy having battles with monsters. Every year the Lord of Hell gathers all of his henchmen to take part in amusing fights for the title of the best team in Hell. As they can't die because they are already in Hell, the fights turn into a funny party and a rapid self-expression!

4. Royal envoy

Download **Royal Envoy** and save the wonderful land of countless islands from the merciless forces of nature. Construct and upgrade homes and buildings for the island citizens and become the chief city planner of marvelous Islandshire. Think your way to triumph in this challenging and mesmerizing rebuilding game with pirates, treasures and hot-air balloon adventures!

11. Wild west story

Download **wild west game** and help rebuild home town in this exciting wild west game! Use your match making abilities, awesome power-ups and sharp eyesight to repair all the buildings and get people to move into your town. Have days of fun with this great Match 3 and Hidden Object mix.

6. Super motocross

Download the game **Super Motocross** and take part in the coolest motorcycles! Winds and roads are your elements! Pass all the challenges in the topics and become a real freestyle motocross champion! Twisting roads, mind-blowing jumps and hazardous barriers are waiting for you right now!

7. Mad battle

Download the battle game “**Mad Medley Battle**”, and get off whole-hog! Decision makers ordered you to collect elements of a powerful weapon. They are scattered in tropics of South America where hostile soldiers are concentrated. You are moving across the area on an armor-clad vehicle, defending from the enemies, and collecting trunks. The battle game will make you play for hours!

8. Nanny Mania

Think you can manage a household? Think being a stay at home mom is easy? Well let's give it a try! **Nanny Mania** puts you in the heart of what it takes to take care of a regular house. We start you off easy with only one child, and Mom and Dad to take care of in a small house, but you slowly get better but the job does not get easier. Try cleaning, cooking, laundry, and taking care of the parents, 4 kids and a whole heap of trouble.

9. Delicious deluxe

Download **restaurant cooking game** and take a bite out of Delicious today! Success in this restaurant cooking game means more tables, bigger restaurant, and a menu full of uniquely delectable items. Tasty treats may keep your customers happy, but it's going to take quick clicks and careful timing to get your ambitions off the ground.

10. Jigsaw battle

Download **jigsaw** game right now and put together challenging puzzles as quickly as you can! Open up this virtual box of jigsaw matches and piece together tons of different images. Change the number of pieces per puzzle, turn on rotating pieces, and choose from different categories in this incredible jigsaw game.

Appendix H. Non-Malware Reviews Used in Study 2

1. Farmfrezy

**** I thought its kinda boring game when I played first time but this is really attractive! I love this game now and cannot stop playing it!!

***** This game is the best game ever.

*** Farm Frenzy doesn't produce wool, eggs, or milk, but it does offer some low-key farming strategy.

2. Rainforest adventure

**** Nice, low-key entertainment

***** Music is soothing and game is challenging not goofy at all.

*** Love it!! Didn't like the music but the game is challenging without too much exertion.

3. Cute monsters

*** I thought it was pretty good, the controls were a little off but the rest was good.

***** A solid game with good controls.

** Reviews on the Run gave it 1/10 annoying controls

4. Royal envoy

***** Good graphics, good story. Very enjoyable.

**** Stars are hard to get with the time given.

***** It's challenging and unique. I can't stop playing it.

5. Wild west story

- ***** Very good, really easy to start but get challenging real fast!
- *** Awesome game for computer. More levels would make it 5 stars.
- ** I have seen better.

6. Super motocross

- ***** Love the tournaments! Not keen on the boosts in the regular game. But still great game.
- ***** Addicted to it like crazzzzzzy!!!
- ***** Excellent, just enough of a challenge to be fun and addictive!

7. Mad battle

- ***** Good game, a lot of fun, good graphics.
- **** Great for killing time, slightly addictive in my own personal opinion.
- ** Not many techniques available.

8 Nanny mania

- ***** This game the best but needs more level.
- *** The game is ton of fun but I was shocked at how quickly I completed it.
- * Gosh, it wants me to pay for more levels!

9. Delicious deluxe

- ***** Can't complain.....tons of fun and totally addictive!

** It's a fun game to play but the food doesn't seem to earn as much money as it should.

*** Wish the dishes were more expensive.....regardless it's a fun game!

10. Jigsaw battle

*** If you enjoy jigsaws you'll enjoy this. More variety of picture categories would be nice though, like a nice folk art winter scene.

***** This is the best puzzle game for computer.

* It didn't have a good selection of pictures

Appendix I. Malware Warnings in Reviews Used in Study 2

Strong malware warnings:

1. I lost some of my word file documents after I downloaded this game. The developer of this game seems to be a hacker. Gamers beware!
2. Dang! It sure is malware. When I registered and downloaded the game, it stole my credit card information!
3. My anti-virus software detected a virus in the game. Don't download it!

Weak malware warnings:

1. Well, I couldn't get this software to run. It kept crashing. And now my computer runs much slower than it did.
2. The software is good, but after I paid for it, my credit card was charged 10 times more than the cost.
3. Sounded good but I could not run it, my computer stops working every time I tried.

Appendix J. Screenshots of Games Used in Study 2

Appendix K. Background Questionnaire for Study 2

1. Age (in years) ____
2. Sex ____
3. How many hours per week do you play computer games? ____
11. In the past year, how many people you know have told you about getting a computer virus or other malicious software on their computer? _____
6. In general how impulsive do you think you are? [I don't stop to think before doing anything 2 3 4 5 6 I always think before doing anything]
7. How much do you like to take risks? I hate to take risks 2 3 4 5 6 I love to take risks
8. What percentage of this experiment's reviews did you read?
9. How often do you read user reviews before downloading software? never 2 3 4 5 6 always
10. How many software reviews have you posted in the past year (0 to 100+)?
11. Do you own a computer? _____ If yes,
 - 11.1 What operating system are you using? Windows __, Mac __, Other __
 - 11.2 During the past year, about how many hours per day have you used your computer?
 - 11.3 In the past year, about how many computer files (videos, audios, photos, and other computer programs) have you downloaded from the Internet to your computer?
 - 11.4 Do you install updates to your operating system each time they are available?
____ yes, ____ no
 - 11.5 Do you have anti-virus software in your computer? _____

11.5.1 If yes, do you check for updates to your anti-virus software at least once a month? ____ yes, ____ no

11.6 Do you have any other software to protect your computer from security threats? ____

11.6.1 If yes, do you check for updates at least once a month? ____ yes, ____ no

11.7 In the past 12 months, how many times have you encountered the following computer problems? Answer on a scale from 0 to 100+ times.

- a) Your computer stopped working (e.g., froze or crashed): ____
- b) You lost personal files on your computer (e.g., files disappeared) ____
- c) Someone accessed your online accounts without your permission ____
- d) You detected a virus or other malicious program on your computer ____

11.8 In the next 12 months, what do you think are the chances that your computer will have the following problems? Answer on a scale from 0 to 100 % chance.

- a) Your computer will stop working (e.g. will freeze or crash) ____
- b) You will lose personal files on your computer ____
- c) Someone will access your online accounts without your permission ____
- d) You will have a virus or other malicious program on your computer ____

11.9 How much personal control do you believe you have in preventing the following problems? Answer on a scale from 0 to 100 % control.

- a) Preventing crashes of your computer ____
- b) Preventing loss of personal files on your computer ____
- c) Preventing others accessing your online accounts without your permission ____

d) Preventing a virus or other malicious program attacking your computer _____

Appendix L: Questions with a Computer Game Advertisement Used in Study 2

Before viewing reviews:

Have you ever played this game before? __ yes, __ no

How likely are you to install and run a free copy of this game on your computer? Answer
from Not at all likely 1-----4-----7 Very likely

After viewing reviews:

Which review is the most important to you? _ Top review, _ Middle review, _ Bottom
review

How likely are you to install and run a free copy of this game on your computer? Answer
from Not at all likely 1-----4-----7 Very likely