5-2018

Trade-offs between Monetary Gain and Risk Taking in Cybersecurity Behavior

Xinhui Zhan
Missouri University of Science and Technology, xzxpd@mst.edu

Fiona Fui-Hoon Nah
Missouri University of Science and Technology, nahf@mst.edu

Maggie X. Cheng
New Jersey Institute of Technology, maggie.cheng@njit.edu

Trade-offs between Monetary Gain and Risk Taking in Cybersecurity Behavior

Xinhui Zhan
Missouri University of Science and Technology
xzxpd@mst.edu

Fiona Fui-Hoon Nah
Missouri University of Science and Technology
nahf@mst.edu

Maggie X. Cheng
New Jersey Institute of Technology
maggie.cheng@njit.edu

ABSTRACT

Phishers and hackers exploit users' susceptibility to deception by providing incentives. This research focuses on studying the risk-taking behavior of users in downloading software from the Internet. We proposed an experimental study to assess the degree of risks that people are willing to take for monetary gains when they download software from uncertified sources.

Keywords

Cybersecurity, human behavior, gain, risk, decision-making.

INTRODUCTION

Cyber-attack and privacy threats are very common on the Internet. Mainstream browsers like Google Chrome, Safari, and Firefox provide different types of warning systems when users are at risk of facing cyber security threats. Users are expected to assess cybersecurity risks and make rational decisions when they are conducting online transactions, accessing URLs, and downloading files from the Internet. However, as the "weakest link in the security chain" (Sasse et al., p. 122), people sometimes fail to detect threats. Previous research has explored the effectiveness of physical and structural cues and miscues (Darwish and Bataineh, 2012; Smith et al., 2016). They focused on Internet users' ability to notice and interpret cues and miscues which are embedded in webpages or emails. Researchers have also looked at the impact of human factors on users' ability to recognize fraudulent messages. They found that gender differences, human cognitive limitations, and individual differences affect our susceptibility to phishing and cyber-attacks (Dhamija et al., 2006; Downs et al., 2006). Although awareness and vigilance of cyber threats among Internet users has increased, hackers and phishers have become more sophisticated and are able better able to fabricate content. As a result, some phishing websites can easily evade filters (Dong et al., 2010). Phishers and hackers also exploit users' susceptibility to deception by providing incentives such as monetary gains or rewards. Wright et al. (2014) found that phishers framed their phishing messages as gains or benefits to induce users' vigilance. However, few studies have taken risks into consideration in examining how Internet users make trade-off decisions between the offered rewards and the risks involved. Therefore, this research is expected to fill an important gap in the literature by quantifying users' perceived risks of cyber security threats.

LITERATURE REVIEW

Assessing risks is a fundamental step in cyber security decision-making. Risk taking is often associated with specific actions and environment. Chen et al. (2015) conducted a study to assess the influence of risk information on app-installation decisions. In their study, risk information was framed as the amount of risk (negative framing) or amount of safety (positive framing). Their results indicate that summary information that is positively framed as safety has a greater effect on app-installation decisions than summary information that is negatively framed as risks. Hence, a valid risk index that is framed positively by focusing on safety can be developed to improve users' app-installation decisions.

Understanding human cognition is the key to explain users' risk-taking behavior when facing cyber security threats. Prospect Theory suggests that decision-making under risk depends on whether the potential outcome is perceived as a gain or a loss (Kahneman and Tversky, 1979). Tversky and Kahneman (1981) proposed that the choice between options can be affected by the phrasing or framing of the options. Their findings indicated that losses have a greater impact on people's decision-making than gains. Thus, Prospect Theory provides important implications for cybersecurity research.

In an experiment by Rosoff et al. (2013), they investigated whether and how human decision-making depends on gain-loss framing and the salience of a prior near-miss experience. They examined one kind of near-miss experience, resilient near-miss, which refers to the case where a user has a near-miss experience on a cyber-attack. They carried out a 2 by 2 factorial design and manipulated two levels of each of the two independent variables: frame (gain vs. loss framing) and previous near-miss experience (absence vs. presence). Their results suggest that users tend to follow a safe practice when they have prior experience with a near-miss cyber-attack. Moreover, they discovered that framing has a strong influence on cybersecurity decision-making.

Individuals tend to make decisions that are risk-adverse in a gain frame (Schroeder et al., 2006). Valecha (2016) found that the presence of both reward-based persuasion (gain frame) and risk-based persuasion (loss frame) in phishing emails increase the likelihood of response. However, the influence of framing has some limiting conditions. When subjects were required to explain their choices, the framing effect tended to be reduced (Larrick et al., 1992). Hence, framing effects could be eliminated if users are encouraged to think through the rationale underlying their choices (Takemura, 1994). Similarly, if users are experts in a particular area, the framing effect will also be reduced (Davis and Bobko, 1986).

RESEARCH METHODOLOGY

A within-subject experiment is proposed to explore the relationship between cyber security risks and their associated monetary values. A scenario-based survey approach is used to identify the users' trade-off decisions between cyber security risks and the minimum monetary value gains for users to take the associated risks. By varying the levels of cyber security risks that users face in the experiment, we are able to identify the minimum monetary value gains to entice users to take different levels of risks.

Our design has two independent variables: monetary value gain and cyber security risk. The monetary value gain is the difference between the full and offering prices of the uncertified software. Risk is operationalized as the vulnerability of the cyber risk (i.e., we display the percentage of users who reported virus/spyware/malware after downloading the software as a surrogate for operationalizing the cyber risk). In order to determine a user's threshold level of risk tolerance, we use the scenario-based approach in which subjects have to make a selection among two choices for every scenario given to them. An example of a scenario is as follows:

> *"You need to download Alpha Software that has a market price of $500 onto your primary personal computer. There are two options to download the software.*
>
> *Which option would you choose to download the software?*
>
> **Option A***: Download the software at the* **full price of $500** *with* **0% of cyber security risks***;*
>
> **Option B***: Download the software at a* **discounted price of $450** *[varying monetary value] with* **5% of cyber security risks** *[varying risk level]."*
>
> Please indicate your choice (between option A and B): _____

We then assess the user's level of risk tolerance based on the lowest amount of monetary gain that entices him or her to take a certain level of cyber risk. We propose using the linear download progression method to identify the user's threshold level for risk tolerance (i.e., where a user would not take any risk for any further discount).

In the study, option A remains unchanged throughout the experiment, whereas the risk and monetary value of option B vary. Figure 1 shows a flowchart that depicts the changes in each round of scenarios given to subjects.

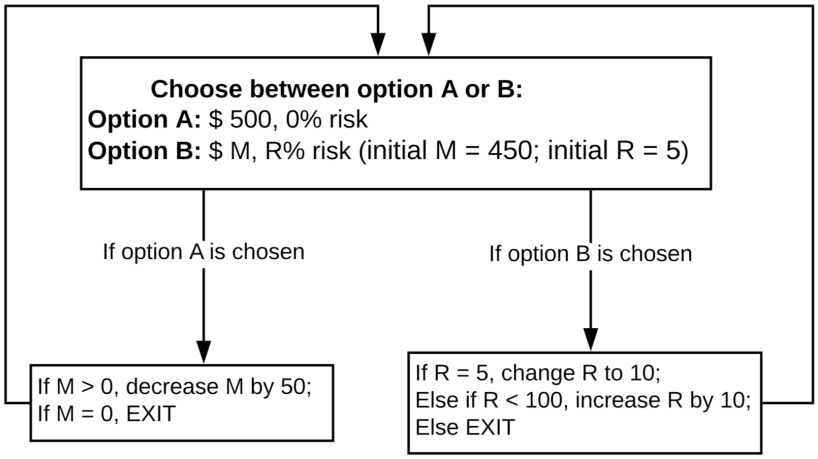

Figure 1. Flowchart of scenarios presented to subjects

EXPECTED CONTRIBUTIONS AND CONCLUSION

We are interested in quantifying the monetary values associated with different levels of risks that users are willing to take. The main contribution of this research is to offer a better understanding of the trade-off decisions that users make between monetary value gains and risks of cyber security threats. The findings of the proposed study will provide a better understanding of the distribution of users' threshold levels for risk tolerance. Additionally, the findings from this research could be useful for privacy policy design, security warning design, and user interaction design.

REFERENCES

1. Chen, J., Gates, C. S., Li, N. and Proctor, R. W. (2015) Influence of risk/safety information framing on android app-installation decisions, *Journal of Cognitive Engineering and Decision Making*, 9, 2, 149-168.
2. Darwish, A. and Bataineh, E. (2012) Eye tracking analysis of browser security indicators. *2012 International Conference on Computer Systems and Industrial Informatics (ICCSII)*, December 18-20, Sharjah, United Arab Emirates, IEEE, 1-6.
3. Davis, M. A. and Bobko, P. (1986) Contextual effects on escalation processes in public sector decision making, *Organizational Behavior and Human Decision Processes*, 37, 1, 121-138.
4. Dhamija, R., Tygar, J. D. and Hearst, M. (2006) Why phishing works. *Proceedings of the SIGCHI conference on Human Factors in Computing Systems*，ACM，581-590.
5. Dong, L., Han, Z., Petropulu, A. P. and Poor, H. V. (2010) Improving wireless physical layer security via cooperating relays, *IEEE Transactions on Signal Processing*, 58, 3, 1875-1888.
6. Downs, J. S., Holbrook, M. B. and Cranor, L. F. (2006) Decision strategies and susceptibility to phishing. *Proceedings of the Second Symposium on Usable Privacy and Security*, July 12 - 14, Pittsburgh, Pennsylvania, USA, ACM, 79-90.
7. Kahneman, D. and Tversky, A. (1979). Prospect theory: An analysis of decision under risk, *Econometrica*, 47, 2, 263-292.
8. Larrick, R. P., Smith, E. E. and Yates, J. F. (1992) Reflecting on the reflection effect: Disrupting the effects of framing through thought, *Meetings of the Society of Judgment and Decision Making*, November, St. Louis, MO.
9. Rosoff, H., Cui, J. and John, R. S. (2013) Heuristics and biases in cyber security dilemmas, *Environment Systems and Decisions*, 33, 4, 517-529.
10. Sasse, M., Brostoff, S. and Weirich, D. (2001) Transforming the 'weakest link'-a human/computer interaction approach to usable and effective security, *BT Technology Journal*, 19, 3, 122-131.
11. Schroeder, N. J., Grimaila, M. R. and Schroeder, N. (2006) Revealing prospect theory bias in information security decision making. *Emerging Trends and Challenges in Information Technology Management: 2006 Information Resources Management Association International Conference*, May 21-24, Washington, DC, USA, 176-179.

12. Smith, S. N., Nah, F. F. H. and Cheng, M. X. (2016) The impact of security cues on user perceived security in e-commerce. In *Lecture Notes in Computer Science 9750*, T. Tryfonas (editor), Springer, 164-173.
13. Takemura, K. (1994) Influence of elaboration on the framing of decision, *The Journal of Psychology*, 128, 1, 33-39.
14. Tversky, A. and Kahneman, D. (1981) The framing of decisions and the psychology of choice, *Science*, 211, 4481, 453-458.
15. Valecha, R., Chen, R., Herath, T., Vishwanath, A., Wang, J. R. and Rao, H. R. (2016) Reward-based and risk-based persuasion in phishing emails. *Proceedings of the IFIP WG8.11/WG11.13 2016 Dewald Roode Workshop on Information Systems Security Research,* October 7-8, Albuquerque, NM, USA, 1-18.
16. Wright, R. T., Jensen, M. L., Thatcher, J. B., Dinger, M. and Marett, K. (2014) Research note—influence techniques in phishing attacks: An examination of vulnerability and resistance, *Information Systems Research*, 25, 2, 385-400.