PROCEEDINGS OF THE INTERNATIONAL
CRISIS AND RISK COMMUNICATION CONFERENCE
MARCH 10-12, 2025. CLEMSON SC, USA

Can young people be persuaded to adopt secure behavior in cyberspace? An experimental study based on Protection Motivation Theory

Florian Meissner

Macromedia
University of Applied
Sciences, Cologne Germany

Alexander Johannes Wilke

Macromedia
University of Applied
Sciences, Cologne Germany

Miglė Puikytė

Macromedia
University of Applied
Sciences, Cologne Germany

Abstract: In an increasingly digital world, understanding cyber risks and threats as well as effective countermeasures is key. Young people, although they are a risk group due to their extensive use of digital media, have a low risk perception. Thus, effective communication is needed to encourage secure behavior in the digital space. Little is known, however, about how to communicate with young people about cybersecurity. In a 2x6 experiment based on Protection Motivation Theory, we tested the effect of risk messages with 14- to 21-year-olds (n = 1193) using Instagram video and text formats as stimuli. The results show that the format has no significant influence on the protection motivation. However, the results indicate that perceptions of response efficacy, self-efficacy, and response costs were significant predictors of behavioral intention.

Keywords — Cybersecurity communication, Experimental design, Protection Motivation Theory, Risk Communication

---

SUGGESTED CITATION: Meissner, F., Wilke, A. J., & Puikytė, M. (2025). Can young people be persuaded to adopt secure behavior in cyberspace? An experimental study based on Protection Motivation Theory. *Proceedings of the 2025 International Crisis and Risk Communication Conference*, 13(1). https://www.doi.org/10.69931/011c144515

INTRODUCTION

Young people—although often called *digital natives*—do not necessarily display secure behavior online. Despite their high digital engagement, particularly on social media, young users often lack basic cybersecurity knowledge and underestimate risks [1]. Consequently, they are one of the most vulnerable groups when it comes to cybercrime [1].

A critical challenge lies in the lack of protective behavior. Many perceive cybersecurity guidelines as overly complex, resulting in "security fatigue" [2]. This fosters resignation and reduces proactive behavior, especially among teenagers and young adults [3]. Therefore, strengthening cybersecurity awareness and promoting secure online behavior among young users is imperative. Communication strategies must be actionable, relatable, and tailored to the audience's needs.

ISSN: 3068-6539

https://doi.org/10.69931/001c.144515

Against this backdrop, we conducted an experimental study based on Protection Motivation Theory to understand how risk communication should be designed to promote secure online behavior among teenagers and young adults.

THEORETICAL FOUNDATION

Protection Motivation Theory (PMT) explains how fear appeals, efficacy, and attitude changes influence protective motivation, which can be considered as antecedent to protective behavior [4]. PMT posits that threat appraisal (perceived severity, vulnerability) and coping appraisal (response efficacy, self-efficacy, response costs) are key antecedents of protective actions.

PMT has been widely applied in cybersecurity research. Haag et al. [5] systematically reviewed 67 studies—55.2% in non-occupational settings, 41.8% in workplaces, and 3% in both. The findings indicate that key elements of the theory have been empirically supported across different domains, with 21.3% of studies fully and 55.8% partially confirming its core assumptions—highlighting its applicability in both professional and everyday cybersecurity contexts [5]. Complementing this, Mou et al. [6] conducted a meta-analysis combined with structural equation modeling based on 92 datasets. Their analysis identified perceived severity, response efficacy, and self-efficacy as the most consistent predictors of individuals' motivation to adopt protective behaviors. Therefore, we pose the following hypotheses:

- H1: Messages that are designed according to the principles of PMT are more effective than generic communication (neutral messages) in motivating users to adopt cyber security measures.
- H2: Messages that highlight response efficacy and self-efficacy are more effective in motivating users to adopt cyber security measures than messages that only stress severity and vulnerability.

LITERATURE REVIEW

The literature about cybersecurity communications is scarce; with regard to teenagers and young adults, the field remains largely unexplored. Yet there are some experimental studies, which have explored approaches to improving cybersecurity awareness among adolescents. Lastdrager et al. [7] found that phishing training improved Dutch elementary students' scores by 14%, primarily in recognizing phishing attempts. Bioglio et al. [8] used gamification to teach 9- to 11-year-olds about social network privacy risks. The results among the 450 students surveyed show increased engagement and awareness.

Among relevant information sources social media platforms play an increasingly important role on the topic of cybersecurity [1]. However, there remains a significant research gap concerning the broader representation of cybersecurity on social media. For instance, little is known about how message design and media format interact regarding risk communication on cybersecurity. Since the format is also a key factor in increasing the user's trust in a displayed security risk message [9] and many young people are accustomed to video formats through social media [10], this study assumes that:

- **H3:** There are interaction effects between the message format and the content of respective messages.

METHODS OR PROCEDURES

This study employs an experimental design with a sample of German teenagers aged 14 to 21 (n = 1193, M =17.29) to evaluate the effectiveness of messages incorporating elements of PMT in influencing adolescents' cybersecurity protection motivation. The stimuli were designed in two different formats—text and video—and addressed two core components of PMT: threat appraisal, focusing on identity theft via social media, and coping appraisal, emphasizing the use of a password manager as a protective measure. All stimuli were pre-tested and optimized before the main survey. Participants were randomly assigned to one of twelve conditions, which either emphasized threat appraisal alone, threat appraisal combined with individual coping elements, or the full coping appraisal approach. A control group was exposed to neutral messages related to digitalization without any cybersecurity content. To assess communication effectiveness, the study measured behavioral intention, reflected in participants' self-reported intention to adopt security measures, and actual behavior, indicated by whether they clicked on a link offering a free password manager.

Additionally, the study collected data on perception of each of the PMT variables as well as various covariates, including sociodemographic factors, Instagram usage and trust, willingness to take risks, knowledge of identity theft, and prior experiences with cyber threats. In each case, participants were asked to indicate their (dis)agreement with respective statements on a seven-point Likert scale (1-fully disagree, 7-fully agree). Furthermore, we included two treatment check questions to see if the participants understood the information provided in stimuli.

Since Instagram is a familiar platform for young people, embedding the stimuli within a social media format helped enhance the external validity of the experiment. The video formats were created using Lumen5 software based on the text for the text format. The visual and textual elements of the threat appraisal were kept constant across the different formats.

RESULTS

Participants showed a high overall behavioral intention to protect themselves online (M=5.63, SD=1.05). A two-way ANOVA showed no significant differences in behavioral intention between the treatment groups; the behavioral intention

was similarly high in all the groups. A Tukey HSE-test of pairwise-comparison of six stimuli groups showed no significant results. Thus, H1 and H2 were rejected, as neither the comparison of PMT-based stimuli and neutral message, nor that of stimuli stressing coping appraisal revealed any significant differences in the effectiveness of these stimuli.

To test the interaction effect between the message format and content, we conducted a two-way ANOVA with interaction effects. Again, no significant effects were found. Tukey HSE-test of pairwise-comparisons also showed no significant differences. H3 was thus also rejected.

Only very few (n=60, 5%) participants showed actual protective behavior. The independent samples Chi-Squared test thus showed no significant behavioral differences between the treatment groups ($\chi^2 = 4.582$; $p = .469$, Cramer's $V = 0.062$, $p = .469$). As only a small fraction of participants showed actual behavior, we did not conduct further analyses to test the influence of interaction of stimuli characteristics on behavior.

EXPLORATORY ANALYSIS

Furthermore, we conducted exploratory analyses to better understand if the stimuli characteristics interacted with the perception of PMT elements and if this interaction had an influence on behavioral intention. We conducted a logistic regression analysis, as the assumption of normality, linearity, and homoscedasticity, essential for a linear regression, were violated and the criterion variable was strongly skewed (the behavior intention was excessively high, M= 5.63; W=0.942, p<.001). We binarized the criterion by dividing the participants into a group with high behavioral intention (mean ≥ 6) and a group with low behavioral intention (mean < 6), which resulted in two approximately equal-sized groups.

To explore the influence of content, we ran six logistic regression models for each PMT dimension plus the neutral one. We modelled the exposure to a specific stimulus as a Dummy-variable, which we included in respective models. All models included mean scores of perceptions of separate PMT elements (perceived severity, perceived vulnerability, maladaptive rewards, response costs, response efficacy, and self-efficacy). To explore the interaction between stimulus content and perceptions of PMT elements, in each of the models we included interaction terms between stimulus content and respective PMT elements. Furthermore, following the theoretical framework, we modelled both direct effects of perceived vulnerability, perceived severity, and fear, as well as interaction terms between perceived vulnerability and fear, and perceived severity and fear. To account for multiple testing, we adjusted the alpha level by dividing the common .05 threshold by 7, which resulted in a corrected alpha level of .007.

Our results showed that perceptions of response efficacy, self-efficacy, and response costs, as well as the interaction of fear with perceived severity were significant predictors of behavioral intention at the adjusted significance level of .007 across all models (Table 1). Odds ratios below one indicate a decrease of probability in showing high behavioral intention whereas values above one indicate an increase.

Table 1. ***Odds Ratios (OR) of variables associated with behavioral intention***

Perception of																	
Fear		**Severity**		**Maladapt. Rewards**		**Response Costs**		**Response Efficacy**		**Self-Efficacy**		**Fear* Severity**		**Stimulus exposure**		**Stimulus* Severity**	
OR	*p*	OR	*p*	OR	*p*	OR	*p*	OR	*p*	OR	*p*	OR	*p*	OR	*p*	OR	*p*
0.78	0.142	0.71	0.359	1.13	0.083	0.60	< .001	1.65	< .001	1.60	< .001	1.11	0.002	0.23	0.064	1.42	0.021

Note: Only Odds Ratios of variables included in the logistic regression models after the stepwise procedure are reported.

Of all the stimuli tested, only exposure to the threat appraisal stimulus showed a marginal association with behavioral intention ($p = .06$); however, this effect did not reach statistical significance after correction for multiple comparisons. Similarly, the interaction between this stimulus and perceived severity was non-significant. The interaction between this stimulus and perceived severity was also non-significant. Nevertheless, this model showed the best fit among those tested (AIC_{TA}=1237.7), with all the other models yielding higher AIC values (AIC=1241.7), indicating a lower fit. Each of the models explained approximately 25% of variance in behavioral intention, as indicated by McFadden's adjusted R2 (range = 0.247-0.249).

When it comes to formats, exposure to video format was found to significantly reduce the behavior intention as compared to exposure to text stimuli at the significance level of .05 (OR=0.21, p=.024), yet this association did not survive the alpha level correction for multiple testing. Similarly to previous results, perceptions of response efficacy (OR=1.45, $p < .001$), self-efficacy (OR=1.62, $p < .001$), and response costs (OR=0.60), $p < .001$), as well as the interaction of fear with perceived severity (OR=1.12, $p < .001$) significantly predicted the behavioral intention at the adjusted significance level of .007. This model showed a similar fit as the model with Threat appraisal stimulus (AIC=1237.2) and explained 25% of variance in behavioral intention (McFadden's adjusted R2=0.249).

DISCUSSION

Compared to previous studies, risk awareness and knowledge appear to be more pronounced among teenagers and young adults [1]. This is particularly evident in the high behavioral intention values across all groups. However, it can be seen that despite high behavioral intentions, the actual behavior is rarely implemented. These results are supported by previous studies [3].

The results of the present study with regard to PMT are also consistent with previous studies [5; 6]. Our study confirms that the coping appraisal variables in particular, such as response efficacy, self-efficacy and response costs, are relevant predictors of behavioral intention within the young target group. However, this observation was independent of

the stimuli used for the experiment although these had been optimized after a pre-test, showed how challenging it is to effectively address this age group in an online experiment. A possible explanation is that the stimuli did not fully correspond to the viewing/usage habits of the test subjects. The focus was more on educational rather than entertaining content.

No significant differences were found with regard to the format. These findings deviate from previous studies [9], suggesting that the format is influencing the perception of the messages.

However, the present study also has some limitations. Firstly, only a single exposure was used for the study which was neither sufficient to influence behavioral intention nor actual behavior. Future research should therefore carry out multi-wave surveys and, if possible, also conduct observations to track protective behavior. The survey as a methodology has only limited potential with regard to observing actual behavior.

CONCLUSION

To conclude, this study has shown how challenging it is to use risk communication to encourage young people to engage more with the topic of cybersecurity, at least using a one-off exposure. Approaches must therefore be more long-term in order to bring about an actual and potentially lasting change in behavior. This seems particularly relevant since new cyber threats keep emerging, partially due to the rise of artificial intelligence. Thus, more research needs to be conducted to explore ways to sensitize young people to such threats at an early stage and to inform them about effective countermeasures.

Author Biography

Dr. Florian Meissner is Professor for Media Management and Journalism at Macromedia University of Applied Sciences in Cologne (Germany). fl.meissner@macromedia.de

Alexander Wilke M.A. is Project Researcher at Macromedia University of Applied Sciences in Cologne (Germany). al.wilke@macromedia.de

Migle Puikytė B.A. is a Research Assistant at the Macromedia University of Applied Sciences in Cologne (Germany). m.puikyte@macromedia.de

REFERENCES

[1] Herbert, F., Becker, S., Buckmann, A., Kowalewski, M., Hielscher, J., Acar, Y., Durmuth, M., Zou, Y., & Sasse, M. A. (2024, May). Digital Security—A Question of Perspective A Large-Scale Telephone Survey with Four At-Risk User Groups. 2024 IEEE Symposium on Security and Privacy (SP). EEE Symposium on Security and Privacy (SP), Los Alamitos, CA, USA. https://doi.org/10.1109/SP54263.2024.00027

[2] Stanton, B., Theofanos, M. F., Prettyman, S. S., & Furman, S. (2016). Security Fatigue. IT Professional, 18(5), 26–32. https://doi.org/10.1109/MITP.2016.84

[3] Xie, W., Fowler-Dawson, A., & Tvauri, A. (2019). Revealing the relationship between rational fatalism and the online privacy paradox. Behaviour & Information Technology, 38(7), 742–759. https://doi.org/10.1080/0144929X.2018.1552717

[4] Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. Journal of Applied Social Psychology, 30(2), 407–429. https://doi.org/10.1111/j.1559-1816.2000.tb02323.x

[5] Haag, S., Siponen, M., & Liu, F. (2021). Protection motivation theory in information systems security research: A review of the past and a road map for the future. ACM SIGMIS Database: The DATABASE for Advances in Information Systems, 52(2), 25–67. https://doi.org/10.1145/3462766.3462770

[6] Mou et al. (2022). A Test of Protection Motivation Theory in the Information Security Literature: A Meta-Analytic Structural Equation Modeling Approach. Journal of the Association for Information Systems. https://doi.org/DOI: 10.17705/1jais.00723

[7] Lastdrager, E., Gallardo, I. C., Hartel, P., & Junger, M. (2017). How Effective is Anti-Phishing Training for Children? In USENIX Association (Ed.), Proceedings of SOUPS 2017, Thirteenth Symposium on Usable Privacy and Security: July 12-14, 2017, Santa Clara, CA, USA (pp. 228–239). Symposium on Usable Privacy and Security, Berkeley, CA. USENIX Association.

[8] Bioglio, L., Capecchi, S., Peiretti, F., Sayed, D., Torasso, A., & Pensa, R. G. (2019). A Social Network Simulation Game to Raise Awareness of Privacy Among School Children. IEEE Transactions on Learning Technologies, 12(4), 456–469. https://doi.org/10.1109/TLT.2018.2881193

[9] Nurse, J. R. C., Creese, S., Goldsmith, M., & Lamberts, K. (2011). Trustworthy and effective communication of cybersecurity risks: A review. In G. Bella & G. Lenzini (Eds.), 2011 1st Workshop on Socio-Technical Aspects in Security and Trust (STAST) (pp. 60–68). IEEE. https://doi.org/10.1109/STAST.2011.6059257

[10] Von Oehsen, D. (2024). Ergebnisse der ARD/ZDF-Medienstudie 2024: Negativtrend der linearen Mediennutzung setzt sich fort. Media Perspektiven, 24, 1–9.