JMLE
JOURNAL OF MEDIA LITERACY EDUCATION

Journal of Media Literacy Education, 13(1), 67-78, 2021
https://doi.org/10.23860/JMLE-2021-13-1-6
ISSN: 2167-8715

Effectiveness of protection motivation theory based: Password hygiene training programme for youth media literacy education

Hee Jhee Jiow

Singapore Institute of Technology, Singapore

Florence Mwagwabi

Murdoch University, Singapore

Anita Low-Lim

TOUCH Community Services, Singapore

OPEN ACCESS

Peer-reviewed article

Citation: Jiow, H. J., Mwagwabi, F., & Low-Lim, A. (2021). Effectiveness of protection motivation theory based: Password hygiene training programme for youth media literacy education. *Journal of Media Literacy Education, 13*(1), 67-78. https://doi.org/10.23860/JMLE-2021-13-1-6

Corresponding Author:
Hee Jhee Jiow
jhee.jiow@singaporetech.edu.sg

Copyright: © 2021 Author(s). This is an open access, peer-reviewed article published by Bepress and distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited. JMLE is the official journal of NAMLE.

Received: May 27, 2020
Accepted: August 15, 2020
Published: May 24, 2021

Data Availability Statement: All relevant data are within the paper and its Supporting Information files.

Competing Interests: The Author(s) declare(s) no conflict of interest.

Editorial Board

ABSTRACT

This study adopts an experimental design to investigate the effectiveness of a password hygiene training programme. The password hygiene training programme adopted the Protection Motivation Theory's framework in its development, and was delivered online to 84 students aged 13 to 16. Strength of password measures, such as time taken, and number of tries required, to crack the password, were administered pre and post intervention. The findings revealed that the password hygiene training programme was effective in changing actual password setting behaviour. This study also provided hints on which perceptual changes, based on the theory's framework, was most influential in the exercise.

Keywords: *password setting, effective, youth programme, protection motivation theory*.

INTRODUCTION

As Singapore gravitates towards building a Smart Nation, it is essential that citizens of all ages harden their defences against cyber and information security threats. Individuals can equip themselves with prior cybersecurity knowledge and a good set of skills to steer clear of such dangers, adopting a protectionist media literate posture (Magolis & Briggs, 2016; Siu, 2016; Turin & Friesem, 2020). Studies have shown that increased usage of technology and social media simultaneously presents adolescents with opportunities to engage in risky online behaviour (Ciccone, 2019; Marron, 2015; Whitty et al., 2015). Furthermore, this exposes them to cyber-related threats such as hacking and cyberbullying (Barbovschi, 2014; Ciccone, 2019; Meter & Bauman, 2015; Mishna et al., 2012; Vanderhoven et al., 2013).

Many global studies found that adolescents often possess poor and lax password-related habits at the expense of potentially risking their personal security (Barbovschi, 2014; Mishna et al., 2012; Van Ouytsel et al., 2016; Vanderhoven et al., 2013). Moreover, passwords are the most widely used method of user authentication on the Internet that protects personal and confidential information. It is also apparent that such worrying habits are prevalent amongst Singaporeans. A Public Awareness Survey found that in 2017, 24 percent of Singaporean respondents shared their passwords with their family and peers while 30 percent still utilised the same passwords for work and personal accounts (Cyber Security Agency of Singapore, 2020).

For these reasons, this paper registers a sense of urgency to develop a password awareness programme in order to inculcate healthier password-related practices amongst the vulnerable youths in Singapore. Adopting Roger's (1975) Protection Motivation Theory (PMT) as our theoretical model, this paper seeks to develop a contextualised password hygiene training programme based on the PMT principles, and investigate its effectiveness in improving password-related practices of youths. Doing so, this paper hopes to further inform and improve media literacy education efforts.

Existing password-related training programmes and its effectiveness

There is a range of password-related training programmes conducted globally that are designed to improve password security practices in the face of cyber- and information system-related threats. Such programmes are often conducted through face-to-face lectures with a few exceptions employing interactive online teaching and e-learning materials (Charoen et al., 2007; Mwagwabi et al., 2014) or circulating password safety information (Horcher & Tejay, 2009).

Although most of such programmes are generally structured to provide information on good password practices and heighten awareness of the rise of password-related threats, there are contrasting findings on the effectiveness of such programmes. Hart (2008) found that lessons targeted at improving students' password practices were ineffective in changing password habits while Horcher and Tejay (2009) found that the company's weekly articles aimed at circulating good password-related advice were only voluntarily read by less than 10 percent of its employees. Contrary to these findings, Eminağaoğlu et al.'s (2009) study on workplace information security awareness found that there was a decrease in weak password usage amongst employees who underwent the informative training course provided. In support of the effectiveness of password-related training programmes, Lorenz et al.'s (2013) study on password security and training also found similar positive effects on its participants' password habits.

However, some studies found interesting results where the effectiveness of password-related training programmes was seemingly dependent on factors such as content specificity and the academic background of student participants. For example, McCrohan et al.'s (2010) experimental study on the effectiveness of password lectures on undergraduates found that high-information lectures, which comprised detail specific information on password-related threats relating to e-commerce and information systems were effective in improving undergraduates' password behaviours. However, low-information lectures, which consist of general background information on passwords and computers security, were deemed ineffective (McCrohan et al., 2010). Taneski et al. (2015) found that lectures on good password habits yielded polarizing results, where improvement in characteristics of set passwords and higher frequency of password change were found amongst students from the faculty of tourism but not from the faculty of electrical engineering and computer science. This alludes to the possibility that the receptivity and effectiveness of password security training are influenced by ones' discipline or area of study. The possible underestimation of cybersecurity risks calls for a need for greater education on online threats (Taneski et al., 2015). However, Helkala (2011)

found that informative lessons on password security were effective in improving students' password strength to some extent. The positive effect amongst the students seemed to have diminished after six months without reminders. Helkala's (2011) findings suggests that the provision of information on proper password hygiene practices alone is ineffective in altering participants' habits in the long run. Thus, performance reviews and improvements on password security programmes must be considered for a long-lasting effect on users.

Additionally, there were programmes that supplement information on password security with specialised education and hands-on training. Such programmes are specifically designed to improve the self-efficacy and proficiency of users' password practices and were found to be more effective in improving participants' password behaviours. For instance, studies involving education and training of users' proficiency in using password management applications found that participants were more likely to employ these applications after attending the proficiency training provided (Ciampa et al., 2011). Ciampa et al. (2011) argued that being proficient enables participants to see the benefits of utilizing these applications, thus resulting in positive changes in their password-setting behaviours. Similarly, Charoen et al. (2007) created a password-related programme that aims to improve participants' proficiency and self-efficacy by exposing them to methods to remember lengthy passwords. Such methods include utilizing memorable phrases that are reminiscent of personal experiences. After the training, participants were able to remember strong passwords with 15 characters comprised of at least two numbers and one symbol (Charoen et al., 2007). There is a possibility that such skills could influence users to apply good password practices in their lives.

While there is no "one-size-fits-all" (Rasi et al., 2019, p. 2) media literacy programme, noticeably, existing password-setting workshops are generally designed and conducted for workplace employees (Eminağaoğlu et al., 2009; Horcher & Tejay, 2009) and university students (Ciampa et al., 2011; Hart, 2008; Helkala, 2011; McCrohan et al., 2010; Taneski et al., 2015). Hence, it is important to address the lack of password-related training available for young adolescents (Magolis & Briggs, 2016; Vanderhoven et al., 2013). With many global studies finding evidence of adolescents possessing poor and lax password practices that makes them more vulnerable to threats such as hacking (Barbovschi, 2014; Mishna et al., 2012; Van Ouytsel et al., 2016), there is a need to develop a contextualised password hygiene training programme that caters specifically to this age group, with high media literacy educational needs (Rasi et al., 2019; Vanderhoven et al., 2013). Upon consideration of the lack of targeted password setting and management programmes catering to adolescents in Singapore, this paper argues that such a development is crucial. This position will be further discussed in the next section.

In order to differentiate itself from existing password-related training programmes found globally (e.g. password security, password protection and password awareness training), this paper will adopt the term 'Password Hygiene Training Programme' or 'PHTP,' to refer to programmes targeted at helping participants manage and set strong, robust and high-quality passwords.

Password Hygiene Training Programme (PHTP) in Singapore

In comparison to other countries, it must be noted that there is a general shortage of PTHP in Singapore, where information and/or training on healthy password hygiene often appear in small segments in information security awareness training and cyber-wellness programmes available, such as Information Security Awareness Program by PDA Professional Development Associates (n.d.), Security Essentials Bootcamp Style by SANS Secure (n.d.), and media literacy workshops, termed as "Cyberwellness," by ACP Computer (n.d.). Furthermore, such programmes seldom narrow in on the effectiveness of improving password behaviours, which is key goal of media literacy education, of its participants (Magolis & Briggs, 2016; Turin & Friesem, 2020; Vanderhoven et al., 2013). This is a cause of concern as many Singaporeans are reported to have poor password hygiene, making them more susceptible to cyber and information system-related threats (Cybersecurity Agency of Singapore, 2020).

In Singapore schools, media literacy programmes have gained traction to equip students from primary school to tertiary level, with life-long social-emotional competencies and sound values to ensure respectful, responsible and safe information and communication technology usage (Ministry of Education, n.d.). Media literacy educational agencies, such as TOUCH Cyber Wellness (TCW), are often employed to carry out such outreach programmes in forms of school-wide assemblies, workshops and seminars. These media literacy programmes serve to educate parents, students

and teachers on a range of media literacy issues, such as cybersecurity, pertaining to this age group. It is apparent that most media literacy education programmes in schools predominantly focus on cyberbullying, gaming addiction, screen time usage, and social media use, with only a small password-related segment that provides the bare minimal information on password setting. We have chosen to work together with TCW (n.d.) to develop a PHTP that aims to effectively improve the password behaviours of adolescents in Singapore and test its effectiveness.

Protection Motivation Theory (PMT)

To inform the development of our PHTP, PMT was employed as the theoretical model to motivate participants to improve poor password behaviours. This choice is also consistent with the protectionist posture of medial literacy education (Turin & Friesem, 2020). PMT was first developed by Roger (1975) to understand the factors that motivate individuals' intentions and behaviours in relation to managing the risk of a medical disease or protecting themselves from health problems.

According to Roger (1975, 1983), motivation is derived from an individual's threat appraisal and coping appraisal of a risky situation. The threat-appraisal process comprises ones' (1) Perceived Severity, the degree of harm perceived from a threat, as well as ones' (2) Perceived Vulnerability, the susceptibility of experiencing the harm (Roger, 1975, 1983). The coping-appraisal process consists of ones' (3) Perceived Effectiveness – the effectiveness of the recommended measures to reduce or prevent possible harm, ones' (4) Perceived Self-Efficacy – the degree of confidence in carrying out the recommended measures as well as ones' response cost – the (5) Perceived Costs in terms of monetary, time and effort of undertaking and adopting the recommended measures (Roger, 1975, 1983). Functioning as a model, Roger (1975, 1983) posits that an individual is more likely to pursue protective actions and behaviours if they have higher perceived vulnerability to, and higher perceived severity of, the threat, and, higher perceived effectiveness, higher perceived self-efficacy and lower response cost of performing the recommended protective measures.

Engaging these elements may ultimately influence a person's decision – either to start, continue or discontinue a specific behaviour that is considered risky (Zhang & McDowell, 2009). While the adoption of this model's factors bears resemblance to Vanderhoven et al.'s (2013) work, in researching the attitudes of adolescents in effecting safe behaviour practices, this study goes further to measure actual behaviour instead of reported behaviour. Following this line of logic, we set out to develop an effective PHTP based on the PMT principles – which will be further elaborated in the next section.

Integration of PMT factors in the development of the PHTP

Singapore Institute of Technology (SIT) in collaboration with Murdoch University (MU) and TCW developed a PMT-based PHTP to train and educate adolescents/students aged 13 to 16. The programme incorporated each of the five PMT factors into the crafting of e-module materials that aims to motivate students' intentions and behaviours towards protecting themselves from the dangers of password-related threats, through the management and setting of strong and high-quality passwords.

The section on perceived vulnerability comprises two parts that aim to highlight adolescents' susceptibility when encountering password-related threats. The first part consists of global and local statistics on hacking cases amongst adolescents along with a few case studies on how and why such accounts were breached. The second part comes in the form of dynamic password feedback, where interactive prompts on password strength and vulnerability to hacking appear while participants create passwords for an account tasked after going through the PHTP. Perceived severity then addresses the consequences of being hacked, starting with general consequences of having poor or lax password security practices followed with the presentation of actual case studies to demonstrate severity. The next component relating to perceived protection effectiveness demonstrates the effectiveness of past PHTPs in efforts to convince students that password-related intervention would be effective in the removal or prevention of harms. Additionally, it is proposed that changes must be in accordance with social media password requirements in order to stay up to date with such technologies. Perceived protection self-efficacy then addresses how easily adolescents can protect themselves from password-related threats, where case studies and public incidences were shown to heighten the belief that individuals can successfully enact the recommended behaviour to ensure cybersecurity and privacy. Response cost - also known as perceived cost - was integrated in each of the PHTP's recommended password security measures, which were

kept short, simple and easy to remember, making it easier for adolescents to adopt such practices into their lives.

The information, statistics and case studies utilised for the PHTP were taken from credible sources online. Upon consultation with TCW, a final prototype of the programme was developed to ensure that the messages conveyed were suitable for youth.

Testing the effectiveness of the PHTP

After developing the PMT-based PHTP, this paper sought to investigate the programme's effectiveness. Previous studies have measured the effectiveness of PMT-based programmes based on participants' intentions to comply with the recommended protective measures. An example is Mwagwabi et al.'s (2014) password-related experimental study which surveyed participants on their intentions to comply with password guidelines. The treatment group in this study received password security information and an exercise to test on their proficiency in setting strong passwords (based on PMT variables) while the control group did not. Here, Mwagwabi et al. (2014) found that perceived severity, perceived password effectiveness, and password self-efficacy had influenced users' intentions to satisfy the abovementioned password guidelines. Similarly, Zhang and McDowell's (2009) study investigated the effect of a PMT-based model on users' intentions to use strong passwords, where they found that fear, response cost, and response efficacy were significantly associated with such intentions.

Although numerous behavioural studies suggest that individuals' intentions to perform a task influence the actual behaviours (Egelman et al., 2016; Johnston & Warkentin, 2010; Shropshire et al., 2015), there is little research examining the link between intentions and actual behaviours in relation to password setting. Hence, our study seeks to evaluate the programme's effectiveness by measuring actual password behaviours instead, in terms of the strength and quality of participants' set passwords captured before and after the implementation of PHTP. The effectiveness of the programme is thus assessed in two ways – by measuring the total time taken, and the number of tries taken, to crack these passwords. A longer duration and a greater number of tries needed to crack participants' set passwords after the programme would indicate that PHTP is effective in improving participants' actual password setting behaviours.

In addition, the study intends to measure the changes in participants' perception in each of the PMT factors to improve the explanatory strength of the findings based on the theoretical model integrated into the PHTP that was developed. This study hypothesizes that participants will have higher perceived vulnerability, higher perceived severity, higher perceived effectiveness, higher perceived self-efficacy and lower response cost after experiencing the PHTP. This is indicative of participants' increased motivation to alter their password behaviours.

As such, the research questions are:

RQ1: How effective is the PHTP in influencing behaviour change?

RQ2: Which perception(s)/factor(s) better explain the behaviour change?

METHODS

This study adopted an experimental design, with pre and post measures of behaviour and perceptions.

Participants and procedure

Approval for the study was sought and obtained from the SIT's Institutional Review Board, and consent was obtained from the respective principals and administrators of selected schools, for recruitment of students as participants for the programme as well as the administration of the survey. This study was supported by the SIT Ignition Grant (Project Ref: R-MNR-E103-C003). The final usable sample consists of 84 students aged between 13 and 16 who were selected by TCW trainers during their media literacy education programme across 13 Singapore secondary schools from November 2017 to May 2018. The inclusion criteria for participants in this study were basic utilization of online services such as emails, social media and blogging as well as general understanding of the English language.

As participants were minors, both participants' assent and their parents' consent were sought. Following the provision of a participant information sheet that details the programme and research purposes, measures that will be taken to ensure anonymity, confidentiality and privacy of data collected as well as important contact details for further clarification. Using an index number to maintain anonymity, participants were then instructed to create an account with a password on a journal website where students will be documenting their personal learning and feedback after every lesson. This website was specifically designed by MU, and

managed by TCW during the conduct of lessons. Participants were then given a link to complete a pre-programme survey, before being given online access to the programme's e-module materials, which were to be reviewed by participants at their own time and leisure. After reviewing the lesson materials online, participants were instructed to reset their passwords on the same journal website that was given to them at the start, in order for them to document their learning and feedback on the lesson. Dynamic password feedback in the form of interactive prompts on password strength and vulnerability to hacking was featured in the password resetting process, as a way to increase participants' perceived vulnerability. Upon completion, participants were then prompted a link directing them to a post-programme survey. Only fully completed pre and post-surveys, relevant for RQ2, as well as set passwords captured before and after the programme, relevant for RQ1, were used, resulting in a usable sample of 84 data points.

Measures

Since there were no relevant instruments designed to assess the strength and quality of participants' set passwords, measures for actual password behaviour were created, by MU, specifically for this study to test the effectiveness of our PTHP programme, and answer RQ1. Both the pre- and post-programme surveys consist of standardized items, which were mostly adapted from other PMT studies. These items measured participants' general perceptions (see sample items in the individual PMT factors highlighted below) of the five PMT factors related to password behaviour, but not specifics such as statistics and/or case studies recounted during the online lesson.

Actual Password Behaviour (Password Strength and Quality)

In response to RQ1, we measured the password strength and quality by analysing the total time it takes to crack the passwords using an algorithm that adopted Shannon's (2001) mathematical formula for calculating password entropy (PE) ─ a measure of password unpredictability using character variation analysis. This algorithm was developed by MU as part of their students' course requirement. The scores in the two measures would equate to the time taken to crack and number of tries to crack, where long time taken and greater number of tries to crack would signify the programme's effectiveness in improving participants' actual password behaviours in setting stronger and higher quality passwords.

Protection Motivation Theory

In response to RQ2, items measuring the five PMT factors were adapted from other studies employing PMT, such as Milne et al. (2002), Workman et al. (2008), Zhang and McDowell (2009), Johnston and Warkentin (2010), Liang and Xue (2010) and Posey et al. (2015).

Perceived Vulnerability. Perceived vulnerability is defined as the extent to which participants feel they are susceptible to password-related threats. To measure perceived vulnerability, a combination of six items were adapted. Each item consists of a short statement asking participants of their perceived vulnerability towards password-related threats (e.g. "It is likely that someone could successfully guess my social media passwords"), which is to be rated using a 7-point Likert scale from (1) "Strongly Agree" to (7) "Strongly Disagree." Hence, higher scores on such items are indicative of individuals having lower perceived vulnerability, where participants would feel that they are less susceptible to password-related threats.

Perceived Severity. Perceived severity is defined as the degree of which participants perceive harm can be inflicted from password-related threats. To measure perceived severity, six items were adapted. Each item consists of a short half-statement asking participants of their perceived severity of password-related threats (e.g. "An attack on my social media account would be…") rated using a 7-point Likert scale from (1) "Not at All Severe" to (7) "Very Severe." Hence, higher scores on such items would mean that individuals have higher perceived vulnerability.

Perceived Effectiveness. Perceived effectiveness is defined as the extent to which participants believe that the recommended password security measure will successfully prevent the password-related threats. To measure perceived effectiveness, six items were adapted. These items are in line with the password guidelines described in the National Institute of Standards and Technology Special Publication 800-118 (Scarfone & Souppaya, 2009) and the United States Computer Emergency Readiness Team (McDowell & Morda, 2020). Each item consists of short statements (e.g. "I can protect my social media accounts better if I use strong passwords") rated on a 7-point Likert scale (1 = "Strongly Disagree" and 7 = "Strongly Agree").

Higher scores on such items are indicative of individuals having higher perceived effectiveness, where participants strongly believe that the recommended password security measures will successfully prevent the password-related threats.

Perceived Self-efficacy. Perceived self-efficacy is defined as the degree of which participants believe that they are personally capable of implementing the recommended password-related measures. To measure perceived self-efficacy, six items were adapted. Each item consists of a short or half-statement asking participants of their perceived self-efficacy of healthy password practices (e.g. as "I would be able to use strong passwords, if I had a lot of time").

All items are to be rated using a 7-point Likert scale on a range from (1) "Strongly Disagree" to (7) "Strongly Agree", except for an item "For me, creating strong passwords is…" which is rated from (1) "Hard" to (7) "Easy." Altogether, higher scores on such items would signify that individuals have higher perceived self-efficacy, where participants strongly believe that they are capable of adopting the recommended password hygiene practices.

Perceived Cost. Perceived cost is defined as the extent to which participants perceive the recommended measures as difficult or inconvenient. To measure perceived cost, five items were adapted. Factors such as time costs of memorising passwords and ease of typing contributing to poor password quality (Grawemeyer & Johnson, 2010; Tam et al., 2009) were included in the measurement, rated on a 7-point Likert scale (1 = "Strongly Disagree" to 7 = "Strongly Agree"). An example of an item is "Strong passwords are difficult to remember." Higher scores on such items are indicative that individuals have higher perceived cost, where participants perceived that the recommended measures are difficult and inconvenient to adopt.

Statistical analyses

Paired samples t-tests were conducted. Means of time taken to crack set passwords, number of tries to crack set passwords, as well as the means of each of the five PMT factors, were compared between two time points - before and after the PHTP.

FINDINGS

Table 1 shows that the results from the paired samples t-tests conducted on time taken and number of tries to crack participants' set passwords as well as on each of the five PMT factors - taken pre- and post-programme, along with the compiled descriptive statistics of all data.

Actual password behaviour

As displayed in Table 1, there are statistically significant differences in the pre- to post-programme for actual password behaviour in terms of time taken to crack and number of tries required to crack participants' set passwords.

Results showed a greater number of tries were required to crack participants' set password after going through the PTHP (M = 5.50E+97, SD = 1.99E+98) than before the programme was conducted (M = 2.64E+88, SD = 1.02E+89). Similarly, more time was required to crack participants' password after going through the PTHP (M = 4.94E+84, SD = 1.79E+85) than before the programme was conducted (M = 2.38E+75, SD = 9.16E+75).

Amounting to an estimated 200 billion percent increase in each of the variables, these results suggest that the programme has strongly influenced participants to set stronger and higher quality passwords that takes a longer time and greater number of tries to crack - towards its intended effect of improving participants' actual password behaviours.

PMT Factors

As shown in Table 1, the paired samples t-tests conducted reported a mixture of favourable and unfavourable results pertaining to each of the five PMT factors. The differences between the pre and post-programme results, however, were all not statistically significant. As such, the following discussions on these results will be confined to making claims on the sample.

Perceived Vulnerability. With higher scores indicative of lower perceived vulnerability, the results showed participants reporting higher levels of perceived vulnerability after (M = 4.76, SD = 1.39) than before the programme (M = 4.80, SD = 1.32). These results were favourable, and suggests that PHTP may slightly increase ones' perceived susceptibility to password-related threats.

Table 1. *Descriptive Statistics and t-test results for the time taken and number of tries to crack set passwords and each variable of the PMT model – pre and post-programme*

	Pre-Programme		Post-Programme		95%CI for Mean Difference				
	M	***SD***	***M***	***SD***		***t***	***df***	***Sig***	***Favour -able?***
Number of Tries to Crack	2.64E+88	1.02E+89	5.50E+97	1.99E+98	-8.09E+84, -1.79E+84	-3.10	125	.002*	Yes
Time Taken to Crack	2.38E+75	9.16E+75	4.94E+84	1.79E+85	-9.00E+97, -1.99E+97	-3.10	125	.002*	Yes
Perceived Vulnerability	4.80	1.32	4.76	1.39	-.303, .374	.210	83	.834	Yes
Perceived Severity	4.79	1.62	4.53	1.60	-.0207, .545	1.84	83	.069	No
Perceived Effectiveness	1.85	.858	1.86	.909	-.233, .206	-.126	83	.900	Yes
Perceived Self-Efficacy	2.65	1.07	2.48`	.891	-.0227, .376	1.76	83	.082	No
Perceived Cost	3.63	1.57	3.61	1.44	-.265, .307	.149	83	.882	Yes

Note: * p < .05; E = "times 10 to the power of" (e.g. 1E+75 = 1 x 1075)

Perceived Severity. Participants have higher perceived severity before (M = 4.79, SD = 1.62) than after the programme (M = 4.53, SD = 1.60). With participants' average perceived severity decreasing after the programme, our results suggest that the programme may have influenced participants to perceive a lesser degree of harm deriving from password-related threats – reporting the programme unfavourably against the intended effect.

Perceived Effectiveness. Participants reported higher perceived effectiveness after (M = 1.86, SD = .909) than before the programme (M = 1.85, SD = .858). With participants' average perceived effectiveness increasing after the programme, these results may indicate that the programme slightly influenced participants to believe that the recommended password security measures will successfully prevent password-related threats.

Perceived Self-Efficacy. The results showed that participants rated higher perceived self-efficacy before (M = 2.65, SD = 1.07) than after the programme (M = 2.48, SD = .891). With the participants' average perceived self-efficacy decreasing after the programme, the findings suggest that the programme may influence participants to believe that they are less capable of setting strong password – appraising PHTP unfavourably against the intended effect.

Perceived Cost. Participants reported lower perceived cost after (M = 3.61, SD = 1.44) than before the programme (M = 3.63, SD = 1.57). With participants' average perceived cost decreasing after the programme, this suggests that the programme may have influenced participants to perceive lesser inconvenience and costs in setting strong passwords and adopting other healthy password-related practices – appraising PHTP favourably towards its intended effect.

DISCUSSION

Overall, the results found that our designed PHTP was strongly effective in improving participants' actual password behaviours, specifically in setting a stronger and higher quality password that takes a significantly longer time and greater number of tries to crack. The effectiveness of our information-based programme bears similarity to Helkaka's (2011) findings, where provision of information on password hygiene was found to be strongly effective in altering students' password behaviours – although further research may be required to investigate the programme's long-term effects on participants. Furthermore, the efficiency of the programme comes without face-to-face interaction, suggesting the utility of efficiently employing online teaching materials and interactive e-modules to specifically train adolescents/students in managing and setting robust passwords – similar to media literacy

education programmes in studies by Charoen et al. (2007) and Mwagwabi et al. (2014).

We were also hoping to use the PMT factors to determine which factor(s) played a role in influencing the changes in participants' password behaviours upon conducting the PHTP. However, the results were not statistically significant. Relating back to Taneski et al.'s (2015) study, the insignificant results could be due to the different receptivity of our PTHP across different academic background and disciplines. As such, results were mixed and ambivalent. This is an area that future research should review when replicating this study, further entrenching Rasi et al's (2019) claim that a "one-size-fits-all program(me) will not work" (p. 2). Nevertheless, we proceeded with the analysis, where the PMT factors helped identify which perception changed favourably or unfavourably as a result of the PHTP and perhaps, relating these changes to the programme's effectiveness in improving participants' password behaviours.

In particular, our PHTP had succeeded to effect favourable changes in three of the PMT factors, finding participants having higher perceived vulnerability, higher perceived effectiveness and lower perceived cost after the e-module programme. Upon consideration of the significant increase in time taken and number of tries to crack participants' set passwords collated post-programme, it is reasonable to opine that adolescents are more likely to practice better password hygiene if they perceive themselves more susceptible to password-related threats and believe that the recommended password measures are easy to adopt and effective in preventing such threats.

Such associations are aligned with past studies such as Workman et al. (2008), Herath and Rao (2009), and Boss et al. (2015), who found evidence that perceived vulnerability, perceived effectiveness and perceived cost affect ones' compliance in a range of protective measures – from the installation of anti-malware programmes to the adoption of recommended workplace security practices.

Relating back to McCrohan et al.'s (2010) experimental study, the effectiveness of our PHTP could be linked to its content design and specificity that also demonstrates the successful integration of the abovementioned PMT factors into the e-module materials. The incorporation of specific information (i.e. statistics and case studies of hacking cases amongst adolescents, changes in social media password requirements, effectiveness of past PHTPs and recommended password security measures that are made easier for adolescents to adopt) have influenced favourable changes in youths' perceptions – specifically in increasing their susceptibility of encountering password-related threats, increasing the perceived effectiveness and convenience of adopting the recommended password security measures. In alignment with Charoen et al.'s (2007) findings, the dynamic password feedback also assisted in improving the proficiency of participants in setting stronger and higher quality passwords, making adolescents aware of their password strength as well as their susceptibility to hacking. Overall, this design provides insights for the development of evidence-based intervention media literacy programme that could effectively improve the capabilities of vulnerable youths in practising better password hygiene. Future research could also expand further and test the effectiveness and applicability across other media literacy contexts.

Nonetheless, participants' perceived severity and perceived self-efficacy did not appear to be favourably changed upon facilitation of the PHTP. In order to explain the decrease in perceived severity, we opine that as the PHTP used case studies which depict very severe consequences, the participants may have concluded that their predicament may be less severe, and therefore did not strongly identify with it.

For example, our case study features a hacker gaining access into a social media account, with the following consequences: loss of private information, financial losses, spread of viruses, decreased privacy, identity theft or damaged reputation. Yet, as social media platforms are popularly used as leisure activities amongst adolescents (Lenhart, 2015; Lenhart et al., 2010; Wilson et al., 2010), adolescents are unlikely to be concerned with financial losses and decreased privacy. As such, participants may have perceived the consequences to be less severe than those depicted in the case studies mentioned in the PHTP. Moreover, we also suspect that participants' confidence in the efficiency of website mediators in rectifying password-related threats contributes to adolescents' rating of low perceived severity.

There were difficulties in locating case studies in the public domain that demonstrated how easy it was to adopt healthy password hygiene measures to protect themselves from hacking and other password-related threats. As such, we incorporated that PMT component into all the other PMT segments of PHTP. A dedicated segment on this issue could have favourably influenced the participants' perceived self-efficacy.

CONCLUSION

This study sought to develop and test the effectiveness of a PMT based PHTP in order to inform and improve media literacy education. While the study was not able to obtain statistically significant measures for the perceptual changes, it was successful in confirming the effectiveness of the PHTP by measuring the actual change in password setting behaviour. This study has identified potential PHTP development gaps for the purposes of effecting perceptual changes in the various PMT factors, which will aid in charting future developments and studies in the media literacy education space. Hence, we seek to further refine the PHTP in these aspects.

ACKNOWLEDGEMENTS

This work was supported by the Singapore Institute of Technology Ignition Grant (Project Ref: R-MOE-E103-C003).

REFERENCES

ACP Computer. (n.d.). *Cyberwellness*. https://www.acpcomputer.edu.sg/index.php/cyberwellness/

Barbovschi, M. (2014). Dealing with Misuse of Personal Information Online - Coping Measures of Children in the EU Kids Online III Project. *Communications: The European Journal of Communication Research, 39*(3), 305-326. http://dx.doi.org/10.1515/commun-2014-0114

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What Do Users Have to Fear? Using Fear Appeals to Engender Threats and Fear That Motivate Protective Security Behaviors. *MIS Quarterly, 39*(4), 837-864.

Charoen, D., Raman, M., & Olfman, L. (2007). Improving End User Behaviour in Password Utilization: An Action Research Initiative. *Systemic Practice and Action Research, 21*(1), 55-72. https://doi.org/10.1007/s11213-007-9082-4

Ciampa, M., Revels, M., & Enamait, J. (2011). Online Versus Local Password Management Applications: An Analysis of User Training and Reactions. *Journal of Applied Security Research, 6*(4), 449-466. https://doi.org/10.1080/19361610.2011.604070

Ciccone, M. (2019). Teaching Adolescents to Communicate (Better) Online: Best Practices from a Middle School Classroom. *Journal of Media Literacy Education, 11*(2), 167-178.

Cyber Security Agency of Singapore. (2020, August 1). *Singapore Cyber Landscape 2017*. https://www.csa.gov.sg/~/media/csa/documents/publications/singaporecyberlandscape2017.pdf

Egelman, S., Harbach, M., & Peer, E. (2016). *Behavior Ever Follows Intention? A Validation of the Security Behavior Intentions Scale (SeBIS).* Paper presented at the Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems, San Jose, California, USA.

Eminağaoğlu, M., Uçar, E., & Eren, Ş. (2009). The Positive Outcomes of Information Security Awareness Training in Companies – A Case Study. *Information Security Technical Report, 14*(4), 223-229. https://doi.org/10.1016/j.istr.2010.05.002

Grawemeyer, B., & Johnson, H. (2010). Using and managing multiple passwords: A week to a view. *Interacting with Computers, 23*(3), 256-566.

Hart, D. (2008). Attitudes and practices of students towards password security. *Journal of Computing Sciences in Colleges, 23*(5), 169-174.

Helkala, K. (2011). Password Education Based on Guidelines Tailored to Different Password Categories. *Journal of Computers, 6*(5). http://dx.doi.org/10.4304/jcp.6.5.969-975

Horcher, A. M., & Tejay, G. P. (2009, June 8-11). *Building A Better Password: The Role of Cognitive Load in Information Security Training* [Paper Presentation]. IEEE International Conference, Dallas, TX, USA.

Johnston, A. C., & Warkentin, M. (2010). Fear Appeals and Information Security Behaviors: An Empirical Study. *MIS Quarterly, 34*(3), 549-566.

Lenhart, A. (2015, April 9). *Teens, Social Media & Technology Overview 2015*. https://www.pewresearch.org/internet/2015/04/09/teens-social-media-technology-2015/

Lenhart, A., Purcell, K., Smith, A., & Zickuhr, K. (2010, February 3). *Social Media & Mobile Internet Use among Teens and Young Adults. Millennials*. http://files.eric.ed.gov/fulltext/ED525056.pdf

Liang, H., & Xue, Y. (2010). Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective. *Journal of the Association for Information Science and Technology, 11*(7), 394-413.

Lorenz, B., Kikkas, K., & Klooster, A. (2013, July 21-26). *The Four Most-Used Passwords Are Love, Sex,*

Secret, and God": Password Security and Training in Different User Groups [Paper Presentation]. International Conference on Human Aspects of Information Security, Privacy, and Trust, Las Vegas, NV, United States.

Magolis, D., & Briggs, A. (2016). A Phenomenological Investigation of Social Networking Privacy Awareness through a Media Literacy Lens. *Journal of Media Literacy Education*, *8*(2), 22-34.

Marron, M. (2015). New Generations Require Changes Beyond the Digital'. *Journalism and Mass Communication Educator, 70*(2), 123-124.

McCrohan, K. F., Engel, K., & Harvey, J. W. (2010). Influence of Awareness and Training on Cyber Security. *Journal of Internet Commerce, 9*(1), 23-41. https://doi.org/10.1080/15332861.2010.487415

McDowell, M., & Morda, D. (2020, August 1). *Socializing securely: Using Social Networking Services:United States Computer Emergency Readiness Team (US-CERT)*. https://www.us-cert.gov/sites/default/files/publications/safe_social_networking.pdf

Meter, D., & Bauman, S. (2015). When Sharing Is a Bad Idea: The Effects of Online Social Network Engagement and Sharing Passwords with Friends on Cyberbullying Involvement. *Cyberpsychology, Behavior, and Social Networking*, *18*(8), 437-442.

Milne, S., Orbell, S., & Sheeran, P. (2002). Combining motivational and volitional interventions to promote exercise participation: Protection motivation theory and implementation intentions. *British Journal of Health Psychology, 7*(2), 163-184.

Ministry of Education. (n.d.). *Cyber Wellness.* https://beta.moe.gov.sg/programmes/cyber-wellness/

Mishna, F., Khoury-Kassabri, M., Gadalla, T., & Daciuk, J. (2012). Risk Factors for Involvement in Cyber Bullying: Victims, Bullies and Bully-Victims. *Children and Youth Services Review, 34*(1), 63-70.

Mwagwabi, F., McGill, T., & Dixon, M. (2014, January 6-9). *Improving Compliance with Password Guidelines: How User Perceptions of Passwords and Security Threats Affect Compliance with Guidelines* [Paper Presentation]. 47th Hawaii International Conference on System Sciences, Waikoloa, HI, United States.

PDA Professional Development Associates. (n.d.). *Information Security Awareness Program*. https://www.pdatrain.com.sg/course/information-security-awareness-programme/

Posey, C., Roberts, T., & Lowry, P. B. (2015). The impact of organisational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems, 32*(4), 179-214.

Rasi, P., Vuojärvi, H., & Ruokamo, H. (2019). Media Literacy Education for All Ages. *Journal of Media Literacy Education, 11*(2), 1-19. https://doi.org/10.23860/JMLE-2019-11-2-1

Roger, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change. *The Journal of Psychology, 91*(1), 93-114.

Roger, R. W. (1983). Cognitive and Physiological Processes in Fear Appeals and Attitude Change: A Revised Theory of Protection Motivation. In J. T. Cacioppo & R. E. Petty (Eds.), *Social Psychophysiology: A Sourcebook* (pp. 153-176). Guilford Press.

SANS Security. (n.d.). *SEC401: Security Essentials Bootcamp Style*. https://www.sans.org/course/security-essentials-bootcamp-style

Scarfone, K., & Souppaya, M. (2009, April 21). *Guide to enterprise password management (draft): recommendations of the National Institute of Standards and Technology*. https://csrc.nist.gov/csrc/media/publications/sp/800-118/archive/2009-04-21/documents/draft-sp800-118.pdf

Shannon, C. E. (2001). A mathematical theory of communication. *SIGMOBILE Mobile Computing and Communications Review, 5*(1), 3-55.

Shropshire, J., Warkentin, M., & Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers & Security, 49*, 177-191.

Siu, L. H. (2016). Defining a smart nation: The case of Singapore. *Journal of Information, Communication and Ethics in Society, 14*(4), 323-333.

Tam, L., Glassmana, M., & Vandenwauverb, M. (2009). The psychology of password management: A tradeoff between security and convenience. *Behaviour & Information Technology, 29*(3), 233-244.

Taneski, V., Hericko, M., & Brumen, B. (2015, May 25-29). *Impact of Security Education on Password Change* [Paper Presentation]. 38th International ICT Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia.

TOUCH Cyber Wellness. (n.d.). http://touchcyberwellness.org/

Turin, O., & Friesem, Y. (2020). Is that media literacy?: Israeli and US media scholars' perceptions of the field. *Journal of Media Literacy Educatio*n, *12*(1), 132-144. https://doi.org/10.23860/JMLE-2020-12-1-10

Van Ouytsel, J., Van Gool, E., Walgrave, M., Ponnet, K., & Peeters, E. (2016). Exploring the Role of Social Networking Sites within Adolescent Romantic Relationships and Dating Experiences. *Computers in Human Behavior, 55*(Part A), 76-86.

Vanderhoven, E., Schellens, T., & Valcke, M. (2013). Exploring the Usefulness of School Education about Risks on Social Networking Sites: A Survey Study. *Journal of Media Literacy Education, 5*(1), 285-294.

Whitty, M., Doodson, J., Creese, S., & Hodges, D. (2015). Individual Differences in Cyber Security Behaviors: An Examination of Who is Sharing Passwords. *Cyberpsychology, Behavior, and Social Networking, 18*(1), 3-7.

Wilson, K., Fornasier, S., & White, K. M. (2010). Psychological Predictors of Young Adults' Use of Social Networking Sites. *Cyberpsychology, Behavior, and Social Networking, 13*(2), 173-177.

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior, 24*(6), 2799-2816. https://doi.org/10.1016/j.chb.2008.04.005

Zhang, L., & McDowell, W. C. (2009). Am I Really at Risk? Determinants of Online Users' Intentions to Use Strong Passwords. *Journal of Internet Commerce, 8*(3-4), 180-197. https://doi.org/10.1080/15332860903467508