7-8-2023

Exploring Users' Security-related Fact-Checking Behavior in Educational Social Media Groups: The Perspective of Health Belief Model

Zhenya Tang
University of Northern Colorado, robin.tang@unco.edu

Botong Xue
University of Wisconsin – La Crosse, bx24@msstate.edu

(Robert) Xin Luo
University of New Mexico, xinluo@unm.edu

Exploring Parents' Security-related Fact-Checking Behavior in Educational Social Media Groups: The Perspective of Health Belief Model

Short Paper

Zhenya Tang
Monfort College of Business,
University of Northern Colorado
robin.tang@unco.edu

Botong Xue
College of Business Administration
University of Wisconsin – La Crosse
bxue@uwlax.edu

Xin (Robert) Luo
Anderson School of Management
The University of New Mexico
xinluo@unm.edu

Abstract

Social media services have become increasingly prevalent among educators as a means to enhance their educational effectiveness. The group feature in these services, which allows multiple users to communicate within a shared space, has been extensively incorporated into the teaching process. Unfortunately, information security threats and risks have appeared along with the popularity of educational social media groups. In this study, we are conducting exploratory research to investigate the antecedents of users' security-related fact-checking behavior in teacher-parent social media groups based on the health belief model. A cross-sectional survey will be conducted to test our proposed research model and the data will be collected from WeChat users. We are expecting to make several contributions to the current literature on educational social media usage and behavioral information security.

Keywords: Information security behavior, educational social media usage, teacher-parents communication, health belief model

Introduction

Social media services (SMS) are changing the way the education system works nowadays (Tess, 2013, Manca & Ranieri, 2016). In the last two decades, educators are increasingly using SMSs such as *Facebook*, *WhatsApp*, *Twitter*, *Instagram*, and *WeChat* to communicate with students and parents, boost active learning, and build a community, anytime and anywhere (Prestridge, 2019). On the other hand, students also use SMSs to promote a lot of positive and useful activities, such as collaborating on international projects, sharing resource materials, and finding a summer internship. According to a recent report, 96% of American students are using at least one SMS (Wade, 2022). Similarly, 93% of UK schools are using SMS for educational and marketing purposes (Bhattacherjee, 2021).

The group is a feature available in many SMSs to facilitate interactions and discussions among people with a common background, goals, qualifications, interests, or hobbies (Park et al., 2009; Chu, 2011; Wang et al., 2012). Unlike traditional online forums and mailing lists, information can be shared between groups

without having to log into every group (Tomasi et al., 2022). The main features of SMS groups include member invitations, pinned announcements, real-time chats, and file uploads (Park et al., 2009; Chu, 2011; Tomasi et al., 2022). These groups can be created and maintained by individuals, organizations, or businesses, and can focus on a wide variety of topics. The size of SMS groups can vary from just a few members to tens of thousands. Statistics indicate that 10 million groups are existing on Facebook with 1.8 billion users using them every month (Southern, 2021).

SMS groups can be employed in educational settings to build online communities where students, teachers, parents, and other professionals can connect, collaborate, and learn from each other. Especially, teacher-parent social media groups are increasingly being created to facilitate communication between parents and teachers outside of the classroom (Wang et al., 2012; Awidi et al., 2019). Different from the class webpage that most parents might only check once in a while or when reminded, once a teacher posts a piece of information, parents in the group can be immediately notified. This means that parents and teachers can address concerns or questions as they arise, without having to wait for a scheduled meeting. Moreover, the information transmitted in the SMS groups can be in various forms such as text, voice, emoji, picture, and voice (Kaplan & Haenlein, 2010; Tang et al., 2021). This allows for more engagement between parents and teachers. Wang et al. (2012) point out that SMS groups can be employed as an effective learning management system (LMS) and can overcome multiple limitations of traditional commercial LMSs.

Every coin has two sides. Despite the SMS groups were originally designed as conduits of informative and harmonious dialogue between families and schools (Chu, 2011; Wang et al., 2012; Awidi et al., 2019), it is important to note that teachers and parents should be mindful of privacy and safety concerns when using SMS groups in educational settings. Unfortunately, SMS groups are also been weaponized by cybercriminals to spread disinformation, steal personal information, and promote scams. For example, a recent report has delineated that 49 parents in a teacher-parent group have transferred over one thousand dollars to a scammer disguised as a teacher (QQ.com, 2021). Similarly, people.com reported that Chinese scammers use teacher-parent groups more often than any other type of group to conduct online fraud (People.com, 2021). The COVID-19 pandemic has made the situation even worse as students were encouraged to study at home and cyber-attacks have subsequently increased in SMS groups (Tang et al., 2021).

According to Martens et al. (2019), being aware of common information security threats and taking relevant security measures (e.g., do not click unknown links, using antivirus applications, fact-checking, and changing passwords frequently) is the best way for social media users to protect themselves against cybercrime. It is important to explore what will influence a user's information security behavior so that effective training and awareness programs can be better designed and implemented (Ng et al., 2009; Johnston & Warkentin, 2010; Tu et al., 2015; Cram et al., 2019). Moreover, exploring what influences a user's information security behavior is critical for improving the overall security posture of an organization and reducing the likelihood of security incidents caused by human error.

In this study, we focus on fact-checking, a specific type of information security behavior (Schuetz et al., 2021), and its role in combating cyber threats in educational SMS groups. Fact-checking involves verifying the accuracy and validity of claims or information presented in SMS groups, which is critical because cybersecurity threats, such as phishing attacks, scams, malware, and social engineering attacks, often rely on false or misleading information to trick users into clicking on links, downloading malicious files, or sharing sensitive information. By fact-checking information posted in these SMS groups, users can identify and avoid these types of threats. While practitioners are urged to seek suggestions from academia to promote fact-checking and the better use of social media technologies, there has been limited research on users' security-related fact-checking behavior in educational SMS groups. Therefore, this study aims to explore the following research questions: *what are the antecedents of a user's security-related fact-checking behavior in teacher-parent social media groups?* By investigating this topic, we hope to provide insights into how to better encourage fact-checking behavior among social media users and enhance the overall security of educational social media groups.

To answer the above research question, a research model was built based on the health belief model (HBM) (Janz & Becker, 1984). HBM was initially developed by a group of social psychologists who were working in the U.S. Public Health Service in the 1950s to explain individuals' health-related behaviors (e.g., participation in health screening examinations, condom use) (Rosenstock et al., 1988; Ng et a., 2009). According to HBM, one's decision to take preventive health actions is the outcome of six groups of factors:

perceived susceptibility, perceived severity, self-efficacy, perceived benefits, perceived barriers, and cues to action (Janz & Becker, 1984; Rosenstock et al., 1988; Ng et a., 2009). Given parallels can be drawn between preventive health behavior and protective security behaviors (e.g., fact-checking), HBM has been widely employed in online contexts to explain users' security-related behaviors (Ng et al., 2009; Cram et al., 2019). Therefore, we believe HBM is a suitable theoretical perspective for the current investigation.

This study is expected to offer theoretical and practical implications in the following ways. First, the majority of current investigations focused on the positive aspects of social media usage for educational purposes (e.g., Tess, 2013; Manca & Ranieri, 2016). Despite increasing practical and theoretical concerns, studies on the dark side of social media usage in the educational setting are still limited. Our study will enrich the literature in this domain by offering a theory-driven, empirically supported framework for understanding parents' fact-checking behavior in SMS groups. Second, this study is also expected to contribute to the current literature on behavioral information security and fact-checking behavior. The proposed research model was tested in the context of teacher-parent SMS groups which differ from those typically examined in the IS literature (Tu et al., 2015; Cram et al., 2019). To the best of our knowledge, this study is the first to provide theoretical insights into the information behavior in the teacher-parent SMS groups context. Practically, the results of the current study offer practitioners rich insights into how to reduce cyber threats in educational SMS groups or other similar groups.

Literature Review

Educational social media usage

Social media services (SMS) are revolutionizing the ways how we live, how we work, and also how we learn. More and more educators are incorporating SMS into their classrooms to interact with learners and boost their educational development (Tess, 2013; Manca & Ranieri, 2016). This trend has resulted in an increase in investigations that analyze the role of SMS plays within the educational contexts. Some of these studies were dedicated to illustrating the benefits that SMS can bring to the learning process such as promoting effective communication between teachers and their students, increasing learners' engagement, and fostering collaboration (e.g., Faizi et al., 2013). Some studies, on the other hand, explore the factors that motivate users to use SMS in educational contexts (e.g., Al-Qaysi et al., 2020; Sun et al., 2020). Several frameworks such as the technology acceptance model (TAM), theory of acceptance and use of technology (UTAUT), uses and gratifications theory (U&G), and social constructivism theory were widely used in this stream of studies (Al-Qaysi et al., 2020). Other studies focused on the impact of SMS use on the educational outcomes and students'/teachers' satisfaction (e.g., Lau, 2017; Escamilla-Fajardo et al., 2021). For example, Lau (2017) found that SMS usage for academic purposes was not a significant predictor of Hong Kong undergraduate students' academic performance.

In sum, while previous investigations on educational SMS usage have explored various types of SMSs, such as Facebook and Twitter, limited research attention has been paid to the group feature that is available in many SMSs (Al-Qaysi et al., 2020). Moreover, the majority of current attempts focus on the positive aspects of educational SMS usage (Escamilla-Fajardo et al., 2021), despite increasing practical and theoretical concerns, the dark side of SMS usage in educational settings remains a relatively new research area (Zimmer, 2022). In the next subsection, the current literature on the SMS group is discussed.

Social media group

Group is a feature that is available in many popular SMSs such as Facebook, Instagram, and WeChat. Different from the regular SMS sharing to the whole public or friends list, a group offers a private space for individuals with common backgrounds, qualifications, interests, or hobbies to share information and generate discussions (Chu, 2011; Pi et al., 2013). Moreover, unlike the regular SMS in which users can control their friends list, members in SMS groups are not able to be in charge of who is accepted into, rejected, or removed from, the group (Tomasi et al., forthcoming). According to a recent report, over 1.8 billion people use Facebook groups every month, and more than half of them are in five or more groups (Southern, 2021).

Concerning the popularity, studies on SMS groups are emerging. Some studies have explored the reasons that motivate users to join SMS groups (e.g., Park et al., 2009). For example, Park et al. (2009), by surveying

1,715 college students, found that socializing, self-status seeking, information seeking, and entertainment motivate them to join Facebook groups. As the main purpose of the SMS group is to boost knowledge sharing and generate discussions, many studies have also concentrated on exploring factors that impact users' information-sharing behavior in the SMS groups (e.g., Pi et al. 2013; Ahern et al., 2016). Pi et al. (2016), for instance, suggested that attitude, subjective norms, and the sharing culture motivate users to share knowledge in SMS groups. Some studies, on the other hand, have also concentrated on analyzing the potential influence of SMS group usage on users' behavior such as political participation, academic or work performance, and mental health (e.g., Chu, 2011; Conroy et al., 2012). For example, Conroy et al. (2012) reported that users' membership in political-related SMS groups is strongly correlated with their offline political participation. Similarly, Chu (2011) found that members of SMS brand groups are more likely to form a favorable attitude toward the brand compared with non-group members.

In conclusion, although the above-mentioned studies have significantly advanced the current understanding of the SMS group phenomenon, little research attention has been paid to the dark side of these groups (Tomasi et al., forthcoming). The role of SMS group plays in our society is not always positive. For example, recent reports from trusted sources have pointed out that SMS groups have become a hotbed for COVID-19 misinformation. According to NPR News, "Facebook groups are destroying America by spreading misinformation (NPR News, 2021)." Similarly, My Hacker News also pointed out WeChat groups are becoming hotspots for scammers to exploit victims out of money (My Hacker News, 2019). The aim of this study is therefore to fill the research gap by exploring the antecedents of a user's information security behavior in teacher-parent SMS groups. The existing literature on behavioral information security is reviewed in the following subsection.

Information security behavior

Cyberattacks and data breaches are becoming a gigantic threat to individuals, organizations, and governments nowadays (Johnston & Warkentin, 2010; Crossler et al., 2013). According to a recent report from IBM and the Ponemon Institute, the global cost of cybercrime has peaked at $6 trillion annually and the average data breach cost is 4.14 million by the end of 2021 (Tunggal, 2022). As researchers estimated that human error (e.g., sharing passwords, accessing suspicious websites, oversharing information on social media) is the main cause of over half of cyber security breaches (Crossler et al., 2013; Cram et al., 2019), there is no wonder recent research attention has been paid to individuals' information security behavior which is defined as one's actions taken to deal with information security risks (Johnston & Warkentin, 2010; Posey et al., 2013; Martens et al., 2019; Tang et al., 2021). Examples of people's information security behaviors include actions like complying with organizational security policies, changing passwords regularly, using antivirus applications, and thinking before clicking an unknown source website (Posey et al., 2013). Various theoretical perspectives such as protective motivation theory (PMT), threat avoidance theory (TAH), health belief model (HBM), deterrence theory, neutralization theory, and rational choice theory (RCT) have been employed to guide current research attempts on information security behavior (Crossler et al., 2013; Posey et al., 2013; Cram et al., 2019). Most of the current attempts on this topic focus on individual contexts (e.g., Martens et al., 2019) or organizational contexts (e.g., Johnston & Warkentin, 2010; Posey et al., 2013). Despite cyberattacks increasingly threatening schools, limited research attention has been paid to the cybersecurity issue in the educational setting. To fill this gap, this study aims to explore factors that influence a user's information security behavior (e.g., fact-checking) in teacher-parent social media groups based on the health belief model.

Hypotheses Development

The proposed research model is shown in Figure 1. Based on the health belief model (HBM), perceived vulnerability, perceived severity, information exposure, responsive efficacy, self-efficacy, tie strength, and fear of missing information were introduced into the research model. Four demographic variables including education, gender, age, and income have also been included in the research model following the suggestion of Venkatesh et al. (2003).

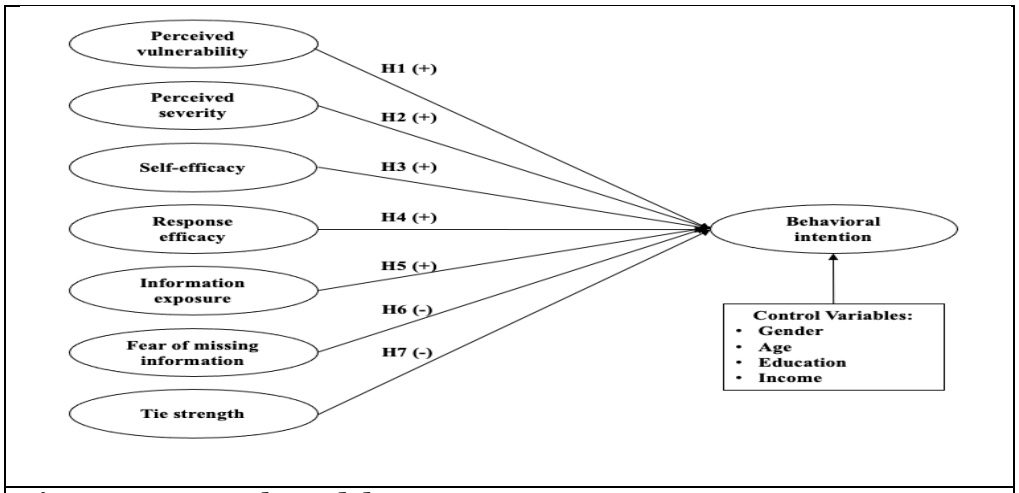

Figure 1. Research Model

Perceived vulnerability (susceptibility) is one's assessment of the likelihood he or she will experience harm (Johnston & Warkentin, 2010; Tu et al., 2015; Martens et al., 2019; Tang et al., 2021). According to HBM, people tend to engage in preventive behaviors when they perceived that they are vulnerable to a particular threat (Janz & Becker, 1984; Ng et al., 2009). In the security context, perceived vulnerability is one's perceived likelihood of a security incident will take place. It is reasonable to postulate that when an individual perceives a high chance be victimized by security incidents in a teacher-parent SMS group, he or she will be more like to engage in preventive behavior (e.g., fact-checking) in the group. Consequently, we hypothesize the following:

H1: Perceived vulnerability is positively related to teacher-parent SMS group users' fact-checking behavior

Perceived severity is one's perceived seriousness of a specific threat. A positive relationship between perceived severity and preventive behavior has been reported in previous literature (e.g., Johnston & Warkentin, 2010; Tu et al., 2015; Martens et al., 2019; Tang et al., 2021). In other words, one is more likely to engage in preventive behaviors when the perceived seriousness of the risk is high. In contrast, people tend to engage in risky or unhealthy behaviors when they believe there would be no serious consequences (Janz & Becker, 1984; Ng et a., 2009). It is reasonable to predict that when a user perceives the scams in the teacher-parent SMS group as serious, he or she will be more like to engage in preventive behavior (e.g., fact-checking) in the group. Consequently, we hypothesize the following:

H2: Perceived severity is positively related to teacher-parent SMS group users' fact-checking behavior

Self-efficacy is one's perception of his or her ability to take a certain action (Johnston & Warkentin, 2010; Tu et al., 2015; Martens et al., 2019; Tang et al., 2021). Rosenstock et al. (1988) pointed out that the role of individual differences such as self-efficacy should not be ignored in explaining people's preventive behaviors. People have to consider their competencies to successfully perform the recommender preventive action even if they believe the positive outcome of behavior change (Janz & Becker, 1984; Ng et a., 2009). It is reasonable to predict that when a user believes he or she is capable of taking certain security measures to avoid being victimized by scams in the teacher-parent SMS group, he or she will be more like to engage in preventive behavior (e.g., fact-checking) in the group. Consequently, we hypothesize the following:

H3: Self-efficacy is positively related to teacher-parent SMS group users' fact-checking behavior

Response efficacy is one's assessment of the perceived value or effectiveness of engaging in a preventive behavior or action to eliminate or decrease the potential harm (Johnston & Warkentin, 2010; Tu et al., 2015; Martens et al., 2019; Tang et al., 2021). HBM suggests that if a person believes a particular action can significantly decrease the susceptibility and severity of a threat, then he or she is likely to engage in that behavior (Janz & Becker, 1984; Ng et al., 2009). For example, people who believe that vaccines can protect against COVID-19 are more likely to get a vaccine shot. It is reasonable to predict that if a user believes taking certain security measures (e.g., thinking before clicking an unknown source link) can successfully help him or her to avoid being victimized by scams in the teacher-parent SMS group, he or she will be more

like to engage in preventive behavior (e.g., fact-checking) in the group. Consequently, we hypothesize the following:

H4: Response efficacy is positively related to teacher-parent SMS group users' fact-checking behavior

According to HBM, people are more likely to take preventive measures if they are exposed to communicated messages of a specific threat and aversion techniques (Janz & Becker, 1984; Ng et al., 2009). Previous literature has generally agreed that information exposure can affect individuals' preventive behavior by shaping their risk perceptions and also improving their skills and confidence to enact the recommended behavior (e.g., Johnston & Warkentin, 2010; Tu et al., 2015; Martens et al., 2019; Tang et al., 2021). For example, Tu et al. (2015), by employing a mixed-methods approach, found that IS users' coping and threat appraisals can be learned by being exposed to information from various sources. Similarly, Tang et al. (2021) considered government social media as an effective channel for users to learn about the threats as well as aversion techniques regarding COVID-19 scams. Following the logic, it is reasonable to predict that people who received more information about teacher-parent SMS group scams are more likely to engage in preventive behavior (e.g., fact-checking) in the group. Consequently, we hypothesize the following:

H5: Information exposure is positively related to teacher-parent SMS group users' fact-checking behavior

Perceived barriers, a person's assessment of the obstacles to enacting the preventive behavior, can reduce one's likelihood of behavior change (Janz & Becker, 1984; Rosenstock et al., 1988; Ng et al., 2009). In this study, two types of barriers are considered: fear of missing information (FOMI) and social capital. FOMI is one's fear that he or she will miss some important information in the SMS (Blackwell et al., 2017). FOMI has been linked to increased SMS use in previous literature (Blackwell et al., 2017). As one of the major purposes for users to join the teacher-parent SMS group is to interact with other parents and teachers and obtain useful information about children's education, it is reasonable to predict that users who worry about missing important information in the teacher-parent SMS group are less likely to engage in preventive behavior (e.g., fact-checking) in the group. Consequently, we hypothesize the following:

H6: Fear of missing information is negatively related to teacher-parent SMS group users' fact-checking behavior

Tie strength, the structural dimension of social capital, is the intensity or closeness of relationships between users in a social network (He et al, 2009; Hou et al., 2021; Tang et al., 2022). A stronger tie or relationship motivates people to keep interacting with other people in the same social network (He et al, 2009). Hou et al. (2021) found that tie strength can influence users' online donation behavior directly or indirectly through trust. Tang et al. (2022) indicated that people who have stronger social ties on SMSs have a higher likelihood to take part in the actions to stop rumors from spreading. Similarly, it is reasonable to predict that users who have a stronger tie in the teacher-parent SMS group are more like to trust the other users and the information they send out and less likely to engage in preventive behavior (e.g., fact-checking) in the group. Consequently, we hypothesize the following:

H7: Tie strength is negatively related to teacher-parent SMS group users' fact-checking behavior

Proposed Research Method

To test 7 hypotheses in our processed research model, we are planning to conduct a cross-sectional survey to collect data for this research. There is a number of available measurement scales for measuring the constructs in this study. All the measurement items for constructs in this research will be adopted or well-adapted from previously published research. For example, items of perceived severity, perceived vulnerability, self-efficacy, and response-efficacy are adapted from Johnston & Warkentin (2010), which are originally adapted from Witte et al. (1996), and tie strength is measured with the scale from Chu & Kim (2011). All measurement items are reflective instruments with 7 points Likert scale from 1 (strongly disagree) to 7 (strongly agree). Attention check questions will be added in the middle of the survey in order to increase the quality of the response result. In addition, following Podsakoff et al. (2003), several techniques will be used to mitigate the common method bias (CMB) before and after data is collected, including item randomization, using marker variables, and confirming anonymity.

We are sampling WeChat users in China, especially those who have experience in using teacher-parent chat groups. The survey will be developed using WenJuanXing (WJX, a Chinese online survey service). A monetary award will be provided to the participant after successful participation is confirmed. IBM SPSS and SPSS AMOS will be used to examine the reliability, validity, and conduct hypothesis test.

Conclusion

In this research, we are investigating SMS users' information security behavior under the context of in-APP group chat, especially the teacher-parent chat groups. To test our conceptual research model, we are conducting a cross-sectional survey and sampling WeChat users in China. In this research, we believe there will be several contributions. First, this study will enrich the literature in information systems and education fields by offering a theory-driven, empirically supported framework for understanding parents' information security behavior in SMS groups. Second, To the best of our knowledge, this study is the first to provide theoretical insights into the information behavior in the teacher-parent SMS groups context. Practically, the results of the current study offer practitioners rich insights into how to reduce the cyber threats in teacher-parent SMS groups or other similar groups.

Like every other research, this study also has several limitations. First, we are still capturing the user's behavioral intention instead of actual behavior. several previous studies have addressed the gap between behavioral intention and actual behavior. Therefore, we suggest that future scholars test users' actual behaviors instead of intentions. Second, we plan to collect data only from China, which is a typical oriental country. In our future step, we will consider more cultural factors to overcome such a limitation.

References

Ahern, L., Feller, J., & Nagle, T. (2016). Social media as a support for learning in universities: an empirical study of Facebook Groups. *Journal of Decision Systems*, 25(sup1), 35-49.

Al-Qaysi, N., Mohamad-Nordin, N., & Al-Emran, M. (2020). A systematic review of social media acceptance from the perspective of educational and information systems theories and models. *Journal of Educational Computing Research*, 57(8), 2085-2109.

Blackwell, D., Leaman, C., Tramposch, R., Osborne, C., & Liss, M. (2017). Extraversion, neuroticism, attachment style and fear of missing out as predictors of social media use and addiction. *Personality and Individual Differences*, 116, 69-72.

Bhattacherjee, U. (2021). 18 eye-opening social media in education statistics in 2021. Retrieved June 21, 2022, from https://markinstyle.co.uk/social-media-in-education-statistics/.

Chu, S. C. (2011). Viral advertising in social media: Participation in Facebook groups and responses among college-aged users. *Journal of Interactive Advertising*, 12(1), 30-43.

Chu, S. C., & Kim, Y. (2011). Determinants of consumer engagement in electronic word-of-mouth (eWOM) in social networking sites. *International journal of Advertising*, 30(1), 47-75.

Conroy, M., Feezell, J. T., & Guerrero, M. (2012). Facebook and political engagement: A study of online political group membership and offline political engagement. *Computers in Human Behavior*, 28(5), 1535-1546.

Cram, W. A., D'arcy, J., & Proudfoot, J. G. (2019). Seeing the forest and the trees: a meta-analysis of the antecedents to information security policy compliance. *MIS Quarterly*, 43(2), 525-554.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security*, 32, 90-101.

Escamilla-Fajardo, P., Alguacil, M., & López-Carril, S. (2021). Incorporating TikTok in higher education: Pedagogical perspectives from a corporal expression sport sciences course. *Journal of Hospitality, Leisure, Sport & Tourism Education*, 28, 100302.

Faizi, R., El Afia, A., & Chiheb, R. (2013). Exploring the potential benefits of using social media in education. *International Journal of Engineering Pedagogy*, 3(4), 50-53.

He, W., Qiao, Q., & Wei, K. K. (2009). Social relationship and its role in knowledge management systems usage. *Information & Management*, 46(3), 175-180.

Hou, T., Hou, K., Wang, X., & Luo, X. R. (2021). Why I give money to unknown people? An investigation of online donation and forwarding intention. *Electronic Commerce Research and Applications*, 47, 101055.

Janz, N. K., & Becker, M. H. (1984). The health belief model: A decade later. *Health Education Quarterly*, 11(1), 1-47.
Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, 34(3), 549-566.
Kaplan, A. M., & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of Social Media. *Business Horizons*, 53(1), 59-68.
Lau, W. W. (2017). Effects of social media usage and social media multitasking on the academic performance of university students. *Computers in Human Behavior*, 68, 286-291.
Manca, S., & Ranieri, M. (2016). Facebook and the others. Potentials and obstacles of social media for teaching in higher education. *Computers & Education*, 95, 216-230.
Martens, M., De Wolf, R., & De Marez, L. (2019). Investigating and comparing the predictors of the intention towards taking security measures against malware, scams and cybercrime in general. *Computers in Human Behavior*, 92, 139-150.
Myhackernews.com. (2019). The WeChat scams sweeping Asia. Retrieved June 21, 2022, from https://myhackernews.com/blog/the-wechat-scams-sweeping-asia/.
Ng, B. Y., Kankanhalli, A., & Xu, Y. C. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems*, 46(4), 815-825.
NPR News. (2020). Facebook groups are destroying America: Researcher on misinformation spread online. Retrieved June 21, 2022, from https://www.npr.org/2020/06/22/881826881/facebook-groups-are-destroying-america-researcher-on-misinformation-spread-onlin.
Park, N., Kee, K. F., & Valenzuela, S. (2009). Being immersed in social networking environment: Facebook groups, uses and gratifications, and social outcomes. *Cyberpsychology & behavior*, 12(6), 729-733.
People.com. (2022). Please take care of scams in educational WeChat groups during the school season. Retrieved June 21, 2022, from http://society.people.com.cn/n1/2021/0831/c1008-32213159.html.
Pi, S. M., Chou, C. H., & Liao, H. L. (2013). A study of Facebook Groups members' knowledge sharing. *Computers in Human Behavior*, 29(5), 1971-1979.
Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: a critical review of the literature and recommended remedies. *Journal of Applied Psychology*, 88(5), 879.
Posey, C., Roberts, T. L., Lowry, P. B., Bennett, R. J., & Courtney, J. F. (2013). Insiders' protection of organizational information assets: Development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors. *Mis Quarterly*, 37(4), 1189-1210.
Prestridge, S. (2019). Categorising teachers' use of social media for their professional learning: A self-generating professional learning paradigm. *Computers & Education*, 129, 143-158.
QQ.com. (2021). 49 parents were scammed in a WeChat group. Retrieved June 21, 2022, from https://new.qq.com/rain/a/20200912A0BX8N00.
Rosenstock, I. M., Strecher, V. J., & Becker, M. H. (1988). Social learning theory and the health belief model. *Health Education Quarterly*, 15(2), 175-183.
Southern, M. (2021). 1.8 billion people use Facebook groups every month. Retrieved June 21, 2022, from https://www.searchenginejournal.com/1-8-billion-people-use-facebook-groups-every-month/397109/#close.
Sun, Y., Guo, Y., & Zhao, Y. (2020). Understanding the determinants of learner engagement in MOOCs: An adaptive structuration perspective. *Computers & Education*, 157, 103963.
Schuetz, S. W., Sykes, T. A., & Venkatesh, V. (2021). Combating COVID-19 fake news on social media through fact checking: antecedents and consequences. *European Journal of Information Systems*, 30(4), 376-388.
Tang, Z., Miller, A. S., Zhou, Z., & Warkentin, M. (2021). Does government social media promote users' information security behavior towards COVID-19 scams? Cultivation effects and protective motivations. *Government Information Quarterly*, 38(2), 101572.
Tess, P. A. (2013). The role of social media in higher education classes (real and virtual)–A literature review. *Computers in Human Behavior*, 29(5), A60-A68.
Tomasi, S., Han, C., & Otto, J. (2022). Expectancy violation in a Facebook group: What is your response?. *Information Technology & People*, 35(4), 1428-1442.
Tunggal, A. (2022). What is the cost of a data breach in 2022? Retrieved June 21, 2022, from https://www.upguard.com/blog/cost-of-data-breach.
Tu, Z., Turel, O., Yuan, Y., & Archer, N. (2015). Learning to cope with information security risks regarding mobile device loss or theft: An empirical examination. *Information & Management*, 52(4), 506-517.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, 27(3), 425-478.

Wade, L. (2022). How social media is reshaping today's education system. Retrieved June 21, 2022, from https://csic.georgetown.edu/magazine/social-media-reshaping-todays-education-system/.

Wang, Q., Woo, H. L., Quek, C. L., Yang, Y., & Liu, M. (2012). Using the Facebook group as a learning management system: An exploratory study. *British Journal of Educational Technology*, 43(3), 428-438.

Zimmer, J. C. (2022). Problematic social network use: Its antecedents and impact upon classroom performance. *Computers & Education*, 177, 104368.