Since January 2020 Elsevier has created a COVID-19 resource centre with free information in English and Mandarin on the novel coronavirus COVID-19. The COVID-19 resource centre is hosted on Elsevier Connect, the company's public news and information website.

Elsevier hereby grants permission to make all its COVID-19-related research that is available on the COVID-19 resource centre - including this research content - immediately available in PubMed Central and other publicly funded repositories, such as the WHO COVID database with rights for unrestricted research re-use and analyses in any form or by any means with acknowledgement of the original source. These permissions are granted for free by Elsevier for as long as the COVID-19 resource centre remains active.

Government Information Quarterly 38 (2021) 101572

Contents lists available at ScienceDirect

Government Information Quarterly

journal homepage: www.elsevier.com/locate/govinf

Does government social media promote users' information security behavior towards COVID-19 scams? Cultivation effects and protective motivations

Zhenya Tang [a], Andrew S. Miller [a], Zhongyun Zhou [b,*], Merrill Warkentin [a]

[a] College of Business, Mississippi State University, Mississippi State, MS 39762, United States
[b] School of Economics and Management, Tongji University, 1500 Siping Road, Shanghai, China

ARTICLE INFO

Keywords:
COVID-19
Government social media
Information security
Cybercrime
Cultivation theory
Protection motivation theory

ABSTRACT

Cybercriminals are taking advantage of the COVID-19 outbreak and offering COVID-19-related scams to unsuspecting people. Currently, there is a lack of studies that focus on protecting people from COVID-19-related cybercrimes. Drawing upon Cultivation Theory and Protection Motivation Theory, we develop a research model to examine the cultivation effect of government social media on peoples' information security behavior towards COVID-19 scams. We employ structural equation modeling to analyze 240 survey responses collected from social media followers of government accounts. Our results suggest that government social media account followers' participation influences their information security behavior through perceived severity, perceived vulnerability, self-efficacy, and response efficacy. Our study highlights the importance of government social media for information security management during crises.

1. Introduction

A major societal challenge in the early 2020s is the COVID-19 pandemic. As of 29 December 2020, more than 81 million cases of COVID-19 have been documented in over 188 countries and territories, resulting in more than 1,787,000 deaths (WHO, 2020). The COVID-19 pandemic is having a dramatic and unprecedented impact on the global economy because many countries enacted strict lockdowns that resulted in widespread business closures (Atkeson, 2020). At this same time, COVID-19-related scams emerged and rapidly propagated (Justice, 2020; Naidoo, 2020). As of April 21, 2020, the USA Federal Bureau of Investigation's (FBI) Internet Crime Complaint Center (IC3) has received more than 3500 formal complaints concerning COVID-19 scams. These FBI complaints detail scams that operate from online websites that advertise fake vaccinations and cures, fraudulent charity drives, malware, or other scams (Justice, 2020).

Online technologies (i.e. social media and websites) have become the de-facto channel for both governmental and multinational organizations like World Health Organization (WHO) and the USA Centers for Disease Control (CDC) to disseminate information and recommendations to people to avoid becoming victimized by COVID-19 scams (Beaunoyer, Dupéré, & Guitton, 2020; Chen et al., 2020; Farooq, Laato, & Islam, 2020). According to Martens et al. (2019), the best way for people to protect themselves against cybercrime is to be aware of common information security threats and then take security measures. In this way, government social media (hereafter GSM) accounts are used to help provide people with knowledge and tips about current information security threats.

Previous literature has reported that information consumption on social media during crisis or disaster events can boost individuals' offline preventative behavior such as self-isolation, washing hands, and receiving vaccinations (e.g., Farooq et al., 2020; Kim & Hawkins, 2020; Liu, 2020; Oh, Lee, & Han, 2020). However, little is known about how individuals' information consumption on social media influences their online preventative behavior. This is important because people are encouraged to work from home and cyber-attacks have subsequently increased with the rapid worldwide spread of COVID-19 (Naidoo, 2020).

In addition, the current literature on GSM has primarily focused on identifying various motivations for users to participate in GSM and devise messaging strategies during a crisis (e.g., Chen et al., 2020; Guo, Liu, Wu, & Zhang, 2020; Kaewkitipong, Chen, & Ractham, 2016; Liu & Xu, 2018). Few existing studies address how GSMs influence their

* Corresponding author.
E-mail addresses: zt192@msstate.edu (Z. Tang), asm357@msstate.edu (A.S. Miller), philzhou@tongji.edu.cn (Z. Zhou), m.warkentin@msstate.edu (M. Warkentin).

https://doi.org/10.1016/j.giq.2021.101572
Received 8 July 2020; Received in revised form 14 January 2021; Accepted 14 January 2021
Available online 23 January 2021
0740-624X/© 2021 Elsevier Inc. All rights reserved.

followers' preventative information security behavior (i.e. using anti-virus applications, not clicking email links, using secure passwords). This is important because GSM operators are unable to devise an effective strategy to attract users and generate valuable messages without a clear understanding of the potential influence of GSM on user behavior.

To address the aforementioned shortcomings, our study aims to examine the role GSM plays in motivating users' online preventive behavior such as taking security measures against COVID-19 scams. Specifically, the research question that motivates our study is "*How does GSM participation influence information security behavior regarding COVID-19 scams?*" In this study, we define information security behavior as peoples' actions they take to migrate information security threats (Boss, Galletta, Lowry, Moody, & Polak, 2015; Tu, Turel, Yuan, & Archer, 2015). We define GSM participation as GSM followers' viewing, commenting, and sharing messages created by GSM (Guo et al., 2020; Williams & Fedorowicz, 2019).

We employ both Cultivation Theory (CT) (Gerbner & Gross, 1976; Gerbner, 1978; Gerbner, Gross, Morgan, Signorielli, & Shanahan, 2002; Hermann, Eisend, & Bayón, 2020) and the Protection Motivation Theory (PMT) (Boss et al., 2015; Johnston & Warkentin, 2010; Rogers, 1975; Rogers, 1983) to study our research question. CT measures the influence of media consumption (the original subject was television viewing) on its consumers' perceptions and opinions (Gerbner & Gross, 1976; Gerbner, 1978; Gerbner et al., 2002; Hermann, Eisend, & Bayón, 2020). The cultivation effect of online media, especially social media, has also been recorded in more recent studies (e.g., Intravia, Wolff, Paez, & Gibbs, 2017; Tsay-Vogel et al., 2018; Wei, McIntyre, & Straub, 2020; Hermann, Eisend, & Bayón, 2020).

PMT posits that individual intentions in response to perceived threats (protection motivation) are affected by two processes: threat appraisal and coping appraisal (Boss et al., 2015; Johnston & Warkentin, 2010; Johnston, Warkentin, Dennis, & Mikko Siponen, 2019; Rogers, 1975; Rogers, 1983). PMT defines threat appraisal as the analysis of the perceived severity and the perceived vulnerability of a potentially harmful person, place, or thing (Rogers, 1975). Similarly, PMT defines coping appraisal as the analysis of the response efficacy and the self-efficacy of potential responses that mediate a potentially harmful person, place, or thing (Rogers, 1975). We believe that both CT and PMT are appropriate for the current study. The research model in this study is empirically assessed using data collected from a survey of followers of Chinese GSMs.

The remainder of the paper is organized as follows. We first review the literature and theoretical frameworks that guide this study and help form its hypotheses. Next, we develop our hypotheses in section 3. We then describe the data and research methods in section 4. Next, we present the results of our analysis in section 5. Finally, we conclude in section 6 with a discussion of the study's findings and propose directions for future research.

2. Theoretical background and literature review

2.1. Government social media during crises

A government social media account (GSM) is an online profile created and managed by a government agency on social media. Governmental agencies use GSMs to better provide information and services, and helps foster closer relationships with citizens (Bertot, Jaeger, & Hansen, 2012; Guo et al., 2020; Li, Yang, Chen, & Yao, 2018; Tang, Chen, Zhou, Warkentin, & Gillenson, 2019; Williams & Fedorowicz, 2019). In recent years, the use of social media platforms (e.g., Facebook, Twitter, LinkedIn, Weibo, WeChat) by government and supranational entities (e.g., UN and WHO) for crisis communications (e.g., natural disasters, weather events, and criminal/terroristic events) has increased (Chen et al., 2020; Guo et al., 2020; Kaewkitipong et al., 2016; Liu & Xu, 2018). According to Guo et al. (2020), governmental use of social media during crises may bring benefits such as improving people's crisis knowledge and understanding of the crisis, facilitating emotional relief, and controlling crisis rumors. Fig. 1 shows an example of how the FBI employs its Twitter account to remind followers to protect themselves against COVID-19 scams.

Research on GSM for crisis management is becoming increasingly prevalent. Table 1 provides a summary of the recent, relevant GSM literature. The extant literature on GSM crisis management can be divided into two related research streams. The first research stream revolves around the motivations for citizens to participate in GSM (e.g., reading, sharing, and commenting) during crises (e.g., Chen et al., 2020; Guo et al., 2020; Song, Kim, Kim, & Jung, 2015). Guo et al. (2020) study antecedents of people's GSM participation behavior during crises, and find that seeking emotional support, external political efficacy, rumor control, civic skills, and mobilization are all significant predictors of GSM participation. Similarly, Chen et al. (2020) find that the richness of media has a negative association with engagement through GSM but has a dialogic loop that facilitates their engagement. Chen et al. (2020) explain this paradox of engagement by the fact that less rich platforms like GSM facilitate a greater amount of engagement than more rich media like phone calls or face-to-face communication.

The other research stream addresses GSM's messaging strategies during crises (e.g., Kaewkitipong et al., 2016; Wukich, 2016; Chatfield and Reddick, 2018; Liu & Xu, 2018). Specifically, this research stream studies the types of messages that have been posted by GSM during disasters, and how messages are diffused through online social networks. Structuration Theory (Giddens, 1984; Orlikowski & Robey, 1991) is a commonly employed theoretical approach for this research stream. For example, Liu and Xu (2018) analyze the posts and comments in three GSM accounts across three separate disasters. In their work, Liu and Xu (2018) find that messages updated by GSMs can be grouped into four categories: official situational updates, advice for the local population, information concerning recovery processes and techniques, and responses to victims' questions and needs. Similarly, Kaewkitipong et al. (2016) find that GSM's posting activities differ across crises' three phases (pre-, during-, and post-crisis) because citizens have different information needs at these three phases.

In conclusion, while the aforementioned studies provide valuable insights, the current literature on GSM during crises is still in an early stage. Most research efforts focus on identifying citizens' motivations to participate in GSM (e.g., Chen et al., 2020; Guo et al., 2020) or GSM's messaging strategies (e.g., Kaewkitipong et al., 2016; Liu & Xu, 2018). Few studies have empirically examined the impact of GSM on citizens'

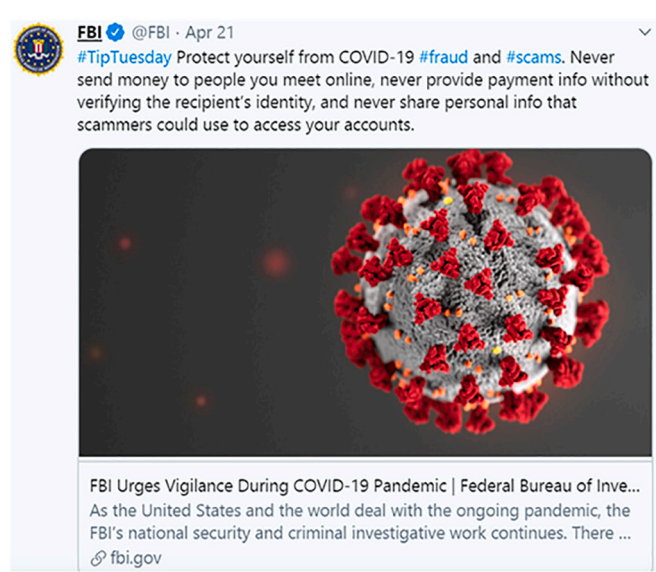

Fig. 1. Example of GSM.

Table 1
Summary of GSM research.

Articles	Research findings	Theory
Guo et al., 2020	Chinese citizens' participatory behaviors on GSM after 2015 Tianjin explosions are motivated by external political efficacy, emotional support, civic skills, mobilization, and rumor control.	Civic voluntarism model
Liu & Xu, 2018	Governmental Facebook account actions can be grouped into four categories: providing official situational updates, responding to victims' inquiries, providing advice, and providing information for recovery.	Structuration theory
Chen et al., 2020	This study examines how media richness, dialogic loop, and content type impact citizen engagement with GSM during the COVID-19 crisis.	Media richness theory, dialogic communication theory
Wukich, 2016	Governmental agencies frequently post situational awareness information and protective action messages prior to security events transpiring.	N/A
Kaewkitipong et al., 2016	GSMs post different types of information pre-, during-, and post-crisis due to evolving information needs.	Structuration theory
Chatfield and Reddick, 2018	Governments should create multiple social media accounts to create a positive network effect to diffuse disaster information.	Organization theory of information processing
Liu et al., 2014	By analyzing 67 GSMs during a three-week period, this study identifies three messaging strategies: instructing information, adjusting information, and debunking inaccurate information.	Situational crisis communication theory
Song et al., 2015	Using the 2013 Seoul Floods as an example, this study states that obtaining timely, reliable information decreases anxiety and motivates users to participate in GSM.	N/A

behavior during a crisis or disaster. We argue that without a clear understanding of the influence of GSM on user behavior, GSM operators and managers are not able to devise a fully efficient strategy to attract user participation and generated valuable messages. To fill the void, our study aims to explore the impact of citizens' GSM participation on their information security behaviors towards COVID-19 scams. In the next two sections, we discuss the literature of information security behavior, and the relevance of PMT and CT as the theoretical framework of the current study.

2.2. Information security behavior

The growth and popularity of information technology (IT) has not only significantly transformed society, but has also fostered an ever-growing wave of information security risks that impact people, businesses, and governments (Loch, Carr, & Warkentin, 1992; Straub & Welke, 1998). According to a recent report, the damage related to cybercrime is projected to reach $6 trillion annually by 2021 (Cyber-Oberver, 2020). We define information security behavior as peoples' actions taken to cope with information security risks (Boss et al., 2015; Martens, De Wolf, & De Marez, 2019; Tu et al., 2015). These actions include actions like changing passwords frequently, complying with organizational standards, thinking before clicking a link from unknown sources, backing up data, patching software, and using antivirus software (Posey et al., 2013).

Several theoretical frameworks (e.g., protection motivation theory, deterrence theory, neutralization theory, threat avoidance theory, rational choice theory) have been employed to explain ones' intentions to apply security measures to cope with information security risks (e.g., Boss et al., 2015; Johnston & Warkentin, 2010; Johnston, Warkentin, & Siponen, 2015; Liang & Xue, 2010; Martens et al., 2019; Tu et al., 2015). The theories primarily focus on the role of emotional factors (e.g., fear) and rational factors (e.g., threat severity, threat vulnerability, self-efficacy) play in determining ones' information security behavior. In addition, much of the previous research focuses on organizational contexts (e.g., Johnston et al., 2015; Johnston & Warkentin, 2010; Willison & Warkentin, 2013) or individual contexts (e.g., Liang & Xue, 2010; Martens et al., 2019; Tu et al., 2015). Little attention has been paid to individual information security behavior in the context of a crisis or disaster event.

2.3. Social media and preventive behavior

In recent years, social media services have emerged as the dominant channel for both broadcasting and seeking information about preventive behaviors (Liu, 2020; Oh et al., 2020). Researchers have generally agreed that social media use can significantly increase preventive behaviors such as self-isolation, taking a vaccination, washing hands, wearing a mask, and adherence to governmental guidance (e.g., Farooq et al., 2020; Kim & Hawkins, 2020; Liu, 2020; Oh et al., 2020). For example, by using data collected in South Korea, Oh et al. (2020) find that social media use positively relates to preventative behavior regarding infectious disease through risk perception and self-relevant emotions. Similarly, Liu (2020) finds that seeking information through social media has motivated users to practice preventive behaviors more often.

The COVID-19 pandemic has provided opportunities for cybercriminals to engage in new cybercrimes. According to Naidoo (2020), the number of cyberattacks has skyrocketed during the COVID-19 pandemic. Because of the increase in cybercrimes, individuals should practice preventive behaviors to prevent becoming a victim of a COVID-19-related scam. While the aforementioned studies (e.g., Farooq et al., 2020; Kim & Hawkins, 2020; Liu, 2020; Oh et al., 2020) provide valuable insights on the effect of social media use on offline preventative behaviors, little attention has been paid to users' online preventive behaviors such as take security measures against COVID-19 scams.

2.4. Protection motivation theory

PMT was proposed by R.W. Rogers in 1975 to explain how people process threats and select responses to protect themselves in a health context (Rogers, 1975). According to PMT, individuals respond to threats and protect themselves based on two processes: threat-appraisal and coping-appraisal (Rogers, 1975; Rogers, 1983; Johnston & Warkentin, 2010; Boss et al., 2015). The threat appraisal process assesses the threat and can be further divided into the assessment of perceived severity and perceived vulnerability (Rogers, 1975; Rogers, 1983; Witte, 1996). People assess proposed responses to threats simultaneously with their threat assessment in a process called coping appraisal. The coping appraisal process is the assessment of ones' abilities regarding the protective actions required to mitigate the threat and can be further divided into response efficacy, self-efficacy, and response costs (Rogers, 1975; Rogers, 1983; Witte, 1996; Johnston & Warkentin, 2010; Boss et al., 2015).

More recently, PMT has been used by researchers to explain individual information security behaviors in both organizational contexts (e.g., Anderson & Agarwal, 2010; Johnston et al., 2015; Johnston et al., 2019; Johnston & Warkentin, 2010) and household contexts (e.g., Liang & Xue, 2010; Martens et al., 2019; Tu et al., 2015). For example, Johnston and Warkentin (2010) investigated the influence of PMT

factors on the compliance of individual end-users with recommendations to enact specific individual computer security actions towards the mitigation of threats. Similarly, Tu et al. (2015) demonstrated that users' knowledge regarding countermeasures and experience with information security threats influence their actions towards information security risks regarding mobile device loss or theft indirectly through PMT factors. We believe PMT is directly applicable to our research question because PMT addresses both the antecedents and consequents of information security behavior. When people recognize the severity and vulnerability of threats caused by COVID-19 scams and the effectiveness of security measures, they are more willing to take action against COVID-19 scams.

2.5. Cultivation theory

Originally proposed by George Gerbner and his colleagues in the 1970s (Gerbner & Gross, 1976; Gerbner, 1978; Gerbner et al., 1994), CT is a communication theory to explain how viewers' behaviors are shaped by mass media exposure (Gerbner et al., 2002; Hermann, Eisend, & Bayón, 2020). According to CT, the more time that people spend consuming media (e.g., TV, newspaper, and magazines), the greater the likelihood that people's perceptions of the real world will align with what the media they consume depicts and conveys (Gerbner & Gross, 1976; Gerbner, 1978; Gerbner et al., 2002). The concept of cultivation was originally defined as "the independent contributions television viewing makes to viewer conceptions of social reality (Gerbner et al., 1994, p.23)." In the cultivation process, media influences people through two cognitive processes: mainstreaming and resonance. In the mainstreaming process, people with differing opinions and world viewpoints slowly evolve their views to more closely align with the mediated content they are most exposed to. Likewise, resonance occurs when media content is highly relatable and relevant to the personal lives of consumers. Strictly speaking, resonance occurs and the cultivation effect is reinforced when the view of consumers aligns with the views expressed by the media they consume (Gerbner & Gross, 1976; Gerbner, 1978; Gerbner et al., 1994; Gerbner et al., 2002; Hermann, Eisend, & Bayón, 2020).

Although cultivation studies have previously utilized TV as the media of study, CT is increasingly often applied to virtual communities and social media contexts (e.g., Intravia et al., 2017; Tsay-Vogel et al., 2018; Wei et al., 2020; Hermann, Eisend, & Bayón, 2020). Like TV, social media can cultivate perceptions and attitudes of reality, because both provide a collective symbolic environment that conveys stories and value to large groups of people (Tsay-Vogel et al., 2018; Hermann, Eisend, & Bayón, 2020). Apart from TV, the message system of social media is more fragmented, individualized, and socially closed due to the parameters of a social network (Wei et al., 2020).

The cultivation effects of social media have begun to be reported in the current literature. For instance, Hermann, Eisend, & Bayón, 2020 survey 476 German Facebook users and find that active Facebook use helps cultivate both ethnic diversity perceptions and attitudes towards ethnic diversity. Similarly, Wei et al., 2020 employ a mixed-method approach and find that exposure to tweets about a particular brand can substantially cultivate consumer attitudes towards that brand. Tsay-Vogel et al., 2018 analyze a longitudinal dataset and find support for the socializing role that Facebook plays in cultivating decreasing attitudes and behavior towards privacy. Researchers have also begun to consider GSM as a cultivation medium. By surveying followers of four U.S. police departments' Facebook and Twitter accounts, Williams and Fedorowicz (2019) find that people who often view and comment on police posts are inclined to be more satisfied with their local police department.

3. Hypotheses development

Based on protective motivation theory, we introduce perceive severity, perceived vulnerability, self-efficacy, and response efficacy into our research model. We also introduce GSM participation into our research model based on cultivation theory. We present our research model with the theorized hypotheses in Fig. 2.

Perceived severity refers to the degree of potential harm from specific threats. Prior studies have found a positive relationship between perceived severity and intention to protect (e.g., Anderson & Agarwal, 2010; Boss et al., 2015; Martens et al., 2019; Tu et al., 2015). Specifically, prior literature finds that the more harmful an individual perceives a threat to be, the more likely the individual is to enact security measures (Anderson & Agarwal, 2010; Boss et al., 2015; Martens et al., 2019; Tu et al., 2015). In contrast, if individuals do not perceive the harmfulness of a threat, they will be less likely to take mitigating actions against that threat. Therefore, we believe that people who perceive COVID-19 scams as serious are more like to engage in preventative behaviors regarding COVID-19 scams. Thus, we hypothesize the following:

H1. *Perceived severity is a positive predictor of information security behavior towards COVID-19 scams.*

Likewise, perceived vulnerability is defined as an individual's assessment of the likelihood that they will experience harm, or their perception of the vulnerability to become victimized by a certain threat (Rogers, 1975; Rogers, 1983; Witte, 1996; Johnston & Warkentin, 2010; Boss et al., 2015). The likelihood of an adaptive response is increased when perceptions of vulnerability are high. During the COVID-19 pandemic, people are encouraged to work from home and have more time to spend online (Naidoo, 2020). Because people spend more time online, people have more exposure to online COVID-19 scams (Naidoo, 2020). Therefore, we believe that people who perceive that there is a high chance of being vulnerable to COVID-19 scams are more likely to engage in preventative behaviors regarding COVID-19 scams. Thus, we hypothesize the following:

H2. *Perceived vulnerability is a positive predictor of information security behavior towards COVID-19 scams.*

People assess proposed responses to threats simultaneously with their threat assessment during a process called coping appraisal. The coping appraisal process is the assessment of ones' abilities regarding the protective actions required to mitigate the threat and can be further divided into self-efficacy, response efficacy, and response costs (Rogers, 1975; Rogers, 1983; Johnston & Warkentin, 2010; Boss et al., 2015). PMT hypothesizes that both response efficacy and self-efficacy have a positive influence on protective behaviors, whereas PMT hypothesizes that response cost has a negative influence on protective behaviors (Rogers, 1975; Rogers, 1983; Johnston & Warkentin, 2010; Boss et al., 2015).

Self-efficacy is a belief that one can successfully enact the protective behavior (Rogers, 1975; Witte, 1996). If a person is highly confident in their ability to conduct a protective action, they will be more likely to take the action. Even if individuals believe the protective action to be effective, they will still consider their own abilities to successfully enact the recommended protective action (Boss et al., 2015; Johnston & Warkentin, 2010; Tu et al., 2015). Applied to the current contexts, when users believe that they are capable of performing a coping behavior to avoid becoming victimized by COVID-19 scams, they will be more motivated to take the action. From this argument, we offer the following hypothesis:

H3. *Self-efficacy is a positive predictor of information security behavior towards COVID-19 scams.*

Response efficacy is the perceived effectiveness of the protective behavior or action in eliminating or preventing potential harm (Rogers, 1975; Witte, 1996). Previous studies have reported that response efficacy has a positive effect on enacting a protective behavior (e.g., Boss et al., 2015; Johnston & Warkentin, 2010; Tu et al., 2015). For example, Johnston and Warkentin (2010) find that response efficacy has a positive effect on end-user intentions to adopt recommended individual

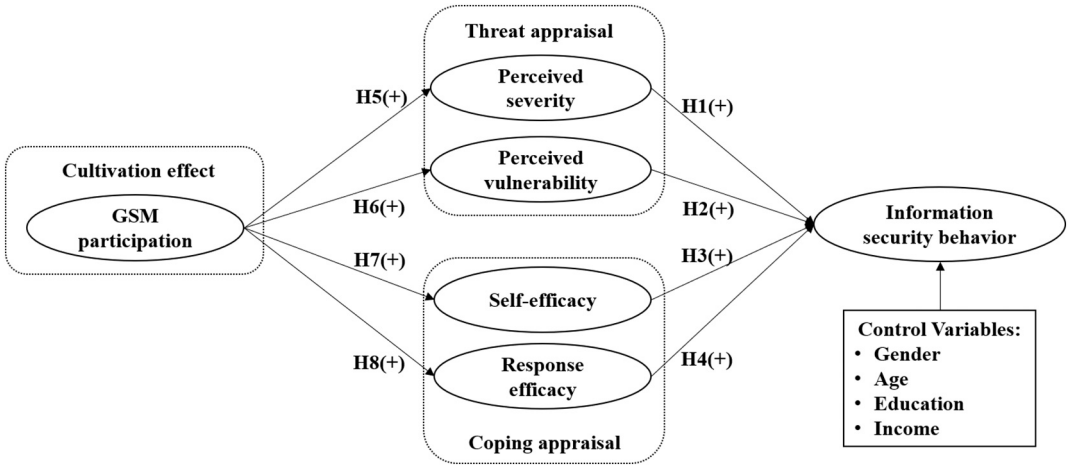

Fig. 2. Research model.

computer security actions with respect to spyware. Applied to the current context, response efficacy includes the thoughts an individual has about the effectiveness of GSM messages regarding avoidance of COVID-19 scams. It is with this background that the following hypothesis is offered:

H4. *Response efficacy is a positive predictor of information security behavior towards COVID-19 scams.*

The effects of media consumption on the threat appraisal process are well established in previous studies (e.g. Intravia et al., 2017; Kim & Hawkins, 2020; Shah, Chu, Ghani, Qaisar, & Hassan, 2020). Collectively, prior efforts illustrate that regardless of the media source (e.g., TV, newspaper, and social media), increased levels of media exposure to the disaster or crime-related information lead to increased levels of fear among citizens, because people may think what they see on media could happen to themselves, their family or others (Intravia et al., 2017; Kim & Hawkins, 2020; Shah et al., 2020). For example, Shah et al. (2020) find that exposure to disaster news in newspapers has a positive relationship with the fear of victimization among readers. Similarly, Intravia et al. (2017) demonstrate that the consumption of social media is significantly associated with the fear of crime, and that this relationship is affected by individual safety perceptions.

The cultivation effect can also be applied to GSMs and COVID-19 (Williams & Fedorowicz, 2019). GSMs are increasingly utilized to disseminate information about COVID-19 and to provide guidance for combating COVID-19 scams and misinformation. In turn, GSM follower's attitudes and perceptions towards COVID-19 scams are partially influenced by the information they receive from GSM participation. In this study, we define GSM participation as GSM followers' viewing, commenting, and sharing messages created by GSM (Guo et al., 2020; Williams & Fedorowicz, 2019). According to cultivation theory, consumers' media consumption shapes their perceptions and opinions (Gerbner & Gross, 1976; Gerbner, 1978; Gerbner et al., 2002; Hermann, Eisend, & Bayón, 2020). Since viewing, commenting, and sharing messages created by GSM can also be viewed as a type of media consumption behavior (Williams & Fedorowicz, 2019), we believe the selection of GSM participation as a factor reflects cultivation theory in the proposed model. We believe that individuals who view, comment, and share more information about COVID-19 from GSM are more likely to formulate a higher level of perceived severity and vulnerability. Therefore, the following hypotheses are proposed:

H5. *GSM participation is a positive predictor of perceived severity.*

H6. *GSM participation is a positive predictor of perceived vulnerability.*

Media not only generates fear of crime or victimization among people but also teaches people to better prepare for the disaster or crime (Farooq et al., 2020). The knowledge that people have can also serve as a foundation for which people assess the efficacy of employing protective responses (Tu et al., 2015). Such knowledge about threat assessment can be learned and obtained from media (Kim & Hawkins, 2020; Tu et al., 2015). When people have a higher level of knowledge concerning potential responses to combat threats, they will likely have greater confidence to employ such responses (Tu et al., 2015). During crises, people are going to GSMs to seek timely information and advice to avoid threats (Chen et al., 2020; Guo et al., 2020). When people obtain more timely and relevant information or advice from GSMs participation, they may exhibit more confidence with their abilities to avoid the threats. Therefore, we propose the hypotheses below.

H7. *GSM participation is a positive predictor of self-efficacy.*

H8. *GSM participation is a positive predictor of response efficacy.*

4. Research method

To examine our proposed research model and hypotheses empirically, we conduct an online survey among GSM followers in China. We select China as the country of interest because China has the largest Internet population in the world (Jin, Tang, & Zhou, 2017). According to Evans and Mathur (2005), the advantages of an online survey approach include ease of data collection, minimal costs, and access to unique populations. Because this study investigates social media users' specific behavior, online surveys are appropriate data collection methods (Li et al., 2018). We provide detailed information about the research site, measures, and data collection processes in the subsequent sections.

4.1. Research setting

In this study, we select WeChat (https://www.wechat.com/en/) users as the research subjects for data collection. Initially launched in 2011, WeChat has since become one of the world's most popular social media apps with over 1 billion daily active users (Chen, Lu, Wang, & Pan, 2019; Zheng, Qi, Dou, & Tan, 2019). WeChat subscription accounts are the WeChat equivalent of a Facebook page where organizations can interact with followers by sending notifications and replying to their comments (Chen et al., 2019; Guo, Zhang, Kang, & Hu, 2017). According to a recent report, more than 100 thousand WeChat government accounts have been launched to offer information and services (People's Daily, 2018). The rapid development of WeChat government accounts provides us a good data source.

4.2. Measurement

This study references existing literature to help design the survey instrument. In this survey, all items are measured using a seven-point Likert scale ranging from "strongly disagree" (1) to "strongly agree" (7). We adapt the items for GSM participation from Zhang et al. (2018) and Guo et al. (2020). We adapt the instrument of information security behavior, perceived severity, perceived vulnerability, self-efficacy, and response efficacy from Witte (1996), Anderson and Agarwal (2010), and Martens et al. (2019). We present the measurement scales used in this study in Table 2. To help ensure content validity, we present the adapted items to a panel of five faculty members and doctoral students who specialize in behavioral information security research. Based on the feedback from the aforementioned expert panel, we make several minor modifications to the items to improve their readability and precision.

Since the survey was conducted in China, a non-English speaking country, we follow the back-translation method suggested by Brislin (1970) to translate the original English instrument into Chinese. A translation professional and two doctoral students who are proficient in both Chinese and English were involved in the translation process. We conduct a pilot study using 24 WeChat users before we begin the full data collection to get feedback for the Chinese version of the questionnaire. We then improve the final questionnaire based on the feedback from the pilot study respondents.

The survey consists of three sections. In the first part of the survey, the main purpose of the study is detailed to participants. More specifically, this section includes the introduction of COVID-19 and a brief definition of COVID-19 scams. The second section contains the main construct items. Respondents are required to indicate the extent to which they agree or disagree on the items. The third part is devoted to demographic questions, including the respondents' gender, age, educational level, occupation, and monthly income. Respondents are also encouraged to provide any suggestions on our research at the end of the questionnaire.

4.3. Data collection

We created a link to our online survey and distributed the link using Wenjuanxing (www.wjx.com), which is an online survey service provider in China. Until Spring 2020, Wenjuanxin has more than 10 million registered users and the number of daily survey participants exceeds 5 million (Wengjuanxin, 2020). The target subjects of our study are WeChat users who have followed at least one GSM during the COVID-19 pandemic. They were recruited within two weeks through announcements sent from the authors' WeChat accounts and through posts to a university campus discussion forum. In addition, our survey is open to all freelancers in the Wenjuanxing platform. Using the snowball sampling method (Warkentin, Johnston, & Shropshire, 2011), we also asked all respondents to refer their friends and social contacts to participate in our study. Our data collection approach is consistent with previous studies using the WeChat government account followers as research participants (e.g., Li et al., 2018). To incentivize participation, we offer five RMB (approximately $0.75) to participants who complete the online survey. Following previous literature, we reject two offsets of data with the same IP address to prevent a user from participating in the investigation for more than once (Jin et al., 2017; Tang, Chen, & Gillenson, 2018). The definition and examples of GSMs in WeChat are provided at the beginning of the survey. We employ a screening question to filter out potential participants who have no experience following GSMs. We ask each respondent to provide the name of a GSM they are following. Then the respondent answers questions concerning this GSM. To further reduce response bias, we randomized the items in the survey such that each respondent receives the questions in a random order (Collier & Sherrell, 2010; Jin et al., 2017; Tang et al., 2018; Warkentin, Sharma, Gefen, Rose, & Pavlou, 2018; Zhou, Fang, Vogel, Jin, & Zhang, 2012).

In total, we collect 307 responses from GSM followers from more than 30 cities in China. We remove invalid questionnaires if either of the following criteria is true: (1) if participants provide the same answers to all questions (e.g., all 1 or all 7, 2) if participants complete the survey in an unreasonably short time (less than two minutes) (Collier & Sherrell, 2010). After removing 67 invalid samples, we obtain a usable sample of 240 valid responses for our study. Table 3 contains the demographics of

Table 2
Measures.

Constructs	Item No.	Measurement	Sources
Perceived severity	PS1	I think COVID-19 scams are a severe problem.	Partially adapted from Witte (1996) & Martens et al. (2019)
	PS2	I think COVID-19 scams are having a severe impact.	
	PS3	If I fall for a COVID-19 scam, the consequences would be severe.	
	PS4	If I fall for a COVID-19 scam, my property loss would be significant.	
	PS5	If I fall for a COVID-19 scam, I would be frustrated.	
Perceived vulnerability	PV1	If I do not pay attention, it is easy to fall for COVID-19 scams.	Anderson and Agarwal (2010); Martens et al. (2019)
	PV2	If I do not pay attention, I may become a victim of COVID-19 scams.	
	PV3	If I do not pay attention, the possibility of falling for COVID-19 scams is high.	
Self-efficacy	EFF1	Taking the necessary security measures against COVID-19 scams is easy for me.	Anderson and Agarwal (2010); Martens et al. (2019)
	EFF2	I feel comfortable taking the necessary security measures against COVID-19 scams.	
	EFF3	I can take the necessary security measures against COVID-19 scams without much effort.	
Response efficacy	RE1	Security measures against COVID-19 scams are valuable for protection.	Witte (1996)
	RE2	Security measures against COVID-19 scams work for protection.	
	RE3	Security measures against COVID-19 scams are effective for protection.	
	RE4	If I follow the security measures, my chance of falling for COVID-19 scams is reduced.	
GSM participation	PAR1	I always read the articles posted by the GSM.	Zhang et al. (2018); Guo et al. (2020)
	PAR2	I always share the articles posted by the GSM.	
	PAR3	I always recommend the articles posted by the GSM to my friends.	
Information security behavior towards COVID-19 scams	ISB1	I predict I will think before clicking the COVID-19 related links from unknown sources.	Partially adapted from Witte (1996) & Martens et al. (2019)
	ISB2	I predict I will think before donating to COVID-19 related online funds from unknown sources.	
	ISB3	I predict I will think before purchasing medical supplies from unknown online parties.	

Table 3
Demographic profile of the respondents.

Characteristic	Items	Count (N = 240)	Percent
Gender	Male	100	41.67%
	Female	140	58.33%
Age	18–20	9	3.75%
	21–25	94	39.17%
	26–30	69	28.75%
	31–40	44	18.33%
	41–65	24	10.00%
Education	High school or below	62	25.83%
	Junior college	53	22.08%
	Undergraduate	106	44.17%
	Graduate or above	19	7.92%
Occupation	Student	55	22.92%
	Non-student	185	77.08%
Monthly income	Less than ¥ 4000	85	35.42%
	4001–8000	66	27.50%
	8000–15,000	82	34.17%
	Above 15,000	7	2.92%

our sample. As shown below, approximately 60% of the respondents are female. Over 71.67% of the respondents are between 18 and 30 years old, 52.08% have a college degree or higher, 22.92% are students, and 37.08% have an income above 8000 RMB per month (approximately $1200). Our demographic information is consistent with nationwide statistics that young people and females are more likely than older people and males to use social media (CNNIC, 2018). We then compared the demographic characteristics of our research participants with research participants from previous studies that used Chinese social media users (Chen et al., 2019; Guo et al., 2017; Guo et al., 2020; Li et al., 2018). Our results show there are no statistically significant differences between our respondents and previous studies' respondents. Therefore, we do not believe that sample representativeness is a concern in our study.

To test for possible non-response bias, we conduct a *t*-test to compare the demographic characteristics between the early and last responders, as suggested in previous literature (Collier & Sherrell, 2010; Jin et al., 2017; Tang et al., 2018; Zhou et al., 2012). We do not find significant differences between the two groups of respondents, which suggests that non-response bias is not a concern in our study.

5. Data analysis and results

We perform data analysis using the Partial Least Squares Structural Equation Modeling (PLS-SEM) technique via SmartPLS 2.0 M3. We select PLS-SEM for use in this study because PLS-SEM places minimal restrictions on sample size, and because of the exploratory nature of this study (Chin, 1998; Lowry & Gaskin, 2014). Following the guidance by Anderson and Gerbing (1988), we conduct the data analysis for this study in two stages. First, we assess the reliability and validity of the constructs in the measurement model stage by employing confirmatory factor analysis. Second, we assess the relationships of our constructs in the structural model stage.

5.1. Measurement model

Reliability refers to the degree of consistency of an instrument. In this study, we assess reliability by examining the factor loadings of the measurement items. As shown in Table 4, the factor loading of each measurement item is above the suggested 0.70, which provides evidence that the items in our measurement model have ample reliability. We assess convergent validity using two criteria for each of the constructs in our study: (1) the composite reliability (CR) should be at least 0.70 (Chin, 1998, 2) the average variance extracted (AVE) should be at least 0.50 (Fornell & Larcker, 1981; Hair, Hult, Ringle, Sarstedt, & Thiele, 2017). As shown in Table 4, each of the constructs used in this study meet the recommended levels of CR and AVE, which indicates our constructs have a high level of convergent validity. To assess the constructs in a model for discriminant validity, the square root of AVE for each construct should exceed its correlations with other constructs in the measurement model. As shown below in Table 5, all diagonal elements (the square root of AVEs) of the correlation matrix exceed the off-diagonal elements in the corresponding rows and columns (the correlations between constructs), which provides support that our measurement model has ample discriminant validity.

Table 4
Psychometric table of measurement.

Constructs	Item No.	Factor loadings (CFA)	Mean	T-statistics	SD	VIF
Perceived severity (CR = 0.880, AVE = 0.595)	PS1	0.772	5.340	24.017	1.399	2.146
	PS2	0.767	5.260	20.445	1.560	2.038
	PS3	0.747	5.190	23.357	1.456	1.856
	PS4	0.759	5.030	22.729	1.559	2.140
	PS5	0.812	5.380	29.976	1.429	2.384
Perceived vulnerability (CR = 0.868, AVE = 0.688)	PV1	0.806	4.990	23.402	1.443	1.940
	PV2	0.815	4.790	26.703	1.541	1.861
	PV3	0.867	4.920	44.546	1.442	2.088
Self-efficacy (CR = 0.847, AVE = 0.649)	EFF1	0.817	4.890	28.099	1.465	1.829
	EFF2	0.794	4.940	20.473	1.390	1.719
	EFF3	0.807	4.860	25.542	1.434	1.725
Response efficacy (CR = 0.858, AVE = 0.602)	RE1	0.813	5.030	32.069	1.477	2.094
	RE2	0.798	5.110	28.207	1.445	1.937
	RE3	0.779	5.180	21.545	1.429	1.782
	RE4	0.711	5.180	12.590	1.405	1.654
GSM participation (CR = 0.807, AVE = 0.583)	PAR1	0.722	4.570	13.089	1.398	1.455
	PAR2	0.762	4.600	16.144	1.508	1.503
	PAR3	0.806	4.670	20.883	1.505	1.579
Information security behavior (CR = 0.824, AVE = 0.607)	ISB1	0.717	5.060	15.657	1.468	1.813
	ISB2	0.824	5.130	35.977	1.441	2.146
	ISB3	0.794	5.310	25.393	1.460	1.852

Multicollinearity refers to the phenomena that at least two variables in a research model are highly related in a linear fashion. To examine the multicollinearity, we follow the suggestion by Mason and Perreault Jr (1991) to calculate the value of the variance inflation factor (VIF) for each item. As shown in Table 4, the values for VIF range from 1.455 to 2.384, where are below the threshold of 3.3. Therefore, we do not believe that multicollinearity is a critical concern in our study.

Because we collect our data using a self-reported survey, common method bias (CMB) is may affect our findings. Specifically, CMB could introduce bias into the estimates of the relationships among the constructs in the study. To address CMB, we follow Podsakoff, MacKenzie, Lee, and Podsakoff (2003) and employ both procedural and statistical remedies. Procedurally, we assure anonymity to our participants and reinforce that there are no correct or incorrect answers to the items. The statistical remedies we employ include using Harman's single-factor test to assess the presence of CMB. Exploratory item analysis using principal component analysis (PCA) does not reveal a predominant factor. In addition, we perform marker variable analysis following Malhotra, Kim, and Patil (2006). In this process, we generate the adjusted correlation

Table 5
Correlation matrix and square roots of the AVEs.

	PS	PV	EFF	RE	PAR	ISB
PS	**0.772**					
PV	0.530	**0.829**				
EFF	0.473	0.372	**0.805**			
RE	0.652	0.511	0.499	**0.775**		
PAR	0.287	0.476	0.352	0.390	**0.763**	
ISB	0.667	0.553	0.553	0.597	0.382	**0.779**

matrix by selecting the second-smallest positive correlation from our constructs. Our results do not show significant differences between the path coefficients with and without the marker variables. Thus, the results of the tests indicate that CMB is not a significant problem for the current study.

5.2. Structural model

Statistical assessment of the structural model provides researchers with the overall explanatory powers, estimated path coefficients, and t-values of each path in the research model. We employ a bootstrap resampling procedure at the 95% confidence intervals using 5000 samples to assess the structural model. Fig. 3 and Table 6 both depict the results of the structural model. Overall, the model explains 57.2% of the variance of our dependent variable. Further, we find empirical support for all of our hypotheses. Perceived severity ($\beta = 0.352$, $t = 4.676$, $p < 0.001$), perceived vulnerability ($\beta = 0.202$, $t = 3.094$, $p < 0.01$), self-efficacy ($\beta = 0.251$, $t = 4.631$, $p < 0.001$), and response efficacy ($\beta = 0.150$, $t = 2.129$, $p < 0.05$) directly influence information security behavior towards COVID-19 scams, which supports H1, H2, H3, and H4. In addition, GSM participation positively influences perceived severity ($\beta = 0.288$, $t = 4.783$, $p < 0.001$), perceived vulnerability ($\beta = 0.477$, $t = 8.453$, $p < 0.001$), self-efficacy ($\beta = 0.353$, $t = 5.826$, $p < 0.001$), and response efficacy ($\beta = 0.391$, $t = 6.844$, $p < 0.001$), which supports H5, H6, H7, and H8. Moreover, we consider demographic variables including gender, age, education, and income as control variables in the structural model. The results suggest that each path between the four control variables and information security behavior are non-significant.

6. Discussion

6.1. Summary of the findings

This research generates several important findings. First, all eight of our hypotheses are supported by our findings. Our research model explains a significant proportion of the reasons why people decide to take security measures against COVID-19 scams. Therefore, our findings suggest that both CT and PMT are valuable lenses to help explain and predict GSMs' influence on people's information security behaviors during disasters like the COVID-19 pandemic. Our findings are consistent with Farooq et al. (2020) and Kim and Hawkins (2020), who argue that social media information consumption drives users to enact preventive actions through PMT factors. Exposure to GSM generated posts regarding COVID-19 scams improved individuals' protective motivations and subsequently provide positive contributions to preventive actions.

Table 6
Results of the structural model.

Hypothesis	Path coefficient	T value	S.E.	Conclusion
H1	$\beta = 0.352$***	4.676	0.074	Supported
H2	$\beta = 0.202$**	3.094	0.066	Supported
H3	$\beta = 0.251$***	4.631	0.052	Supported
H4	$\beta = 0.150$*	2.129	0.071	Supported
H5	$\beta = 0.288$***	4.783	0.063	Supported
H6	$\beta = 0.477$***	8.453	0.053	Supported
H7	$\beta = 0.353$***	5.826	0.066	Supported
H8	$\beta = 0.391$***	6.844	0.055	Supported

*$p < 0.05$; **$p < 0.01$; ***$p < 0.001$.

Second, we find that all four PMT factors are positively related to our dependent variable, which indicates that both threat and coping appraisals serve as the foundation upon which intentions to employ security measures against COVID-19 scams are formed. Perceived severity shows the greatest impact (with a path coefficient of 0.352) on behavioral intention. Self-efficacy shows the second strongest impact (with a path coefficient of 0.251) on behavioral intention. Our findings suggest that people simultaneously appraise both the severity and susceptibility of the threats from COVID-19 scams. In addition, people also develop assessments of potential mitigations against COVID-19 scams. These threat and coping appraisals form the foundation upon intention to take security measures against COVID-19 scams. Our findings align with the previous literature on PMT and information security behavior, finding that both threat and coping appraisals have positive effects on information security behavior (e.g., Johnston & Warkentin, 2010; Martens et al., 2019; Tu et al., 2015).

Third, we find that GSM participation positively affects both threat and coping appraisals. Specifically, threat and coping appraisals are partially developed through GSM participation. When GSMs broadcast messages on COVID-19 scams, it can signal to people that the threat is both serious and imminent. People who have read such a message perceive the threat of COVID-19 scams to be more server than those who did not read such a message. Noticing the serious consequences of these scams may also make them recognize themselves to be more vulnerable. Moreover, GSMs also provide followers with information regarding potential countermeasures against COVID-19 scams which grows their self- and responses-efficacy perceptions. In other words, when people are conscious of the attributes of such countermeasures, they feel more efficacious in employing them and deem that the countermeasures can decrease the harms of COVID-19 scams (Tu et al., 2015). This finding is consistent with Williams and Fedorowicz (2019), who argue that GSM follower's attitudes and perceptions are influenced by viewing,

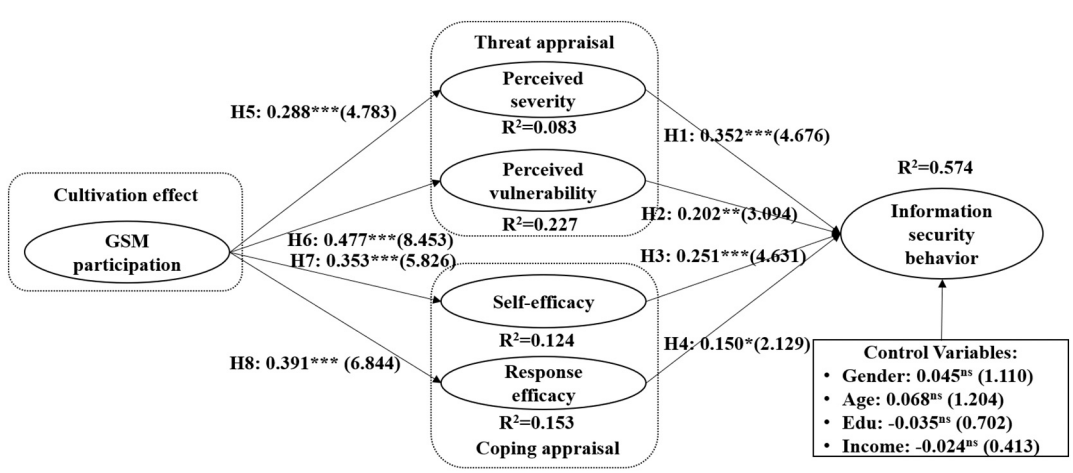

Fig. 3. Structural model results.
Note: *$p < 0.05$; **$p < 0.01$; ***$p < 0.001$.

commenting, and sharing messages created by GSM.

6.2. Theoretical contributions

The current study offers several theoretical contributions. First, research on information security behaviors during crises is still at an early stage. Despite a large number of studies that have been conducted in organizational contexts (e.g., Johnston et al., 2015; Johnston & Warkentin, 2010; Willison & Warkentin, 2013) or individual contexts (e.g., Liang & Xue, 2010; Martens et al., 2019; Tu et al., 2015), few studies examine how to best protect people from security threats during a crisis. This is important because individuals who are encouraged to work from home are at greater risk from cyber threats during a global pandemic such as COVID-19 (Naidoo, 2020). By investigating the cultivation effects of GSMs on PMT factors and users' information security behavior, this study contributes to the literature on behavioral information security during a crisis. Our findings indicate that GSM participation and PMT factors are correlated and significantly influence individuals' intentions to enact security countermeasures against COVID-19 scams. The research model we develop can also be applied to help explain people's information security behavior during other types of crises.

The second contribution is to social media emergency management literature. Currently, several existing studies seek to help identify the reasons and rationale behind people's GSM participation during a crisis time (e.g., Chen et al., 2020; Guo et al., 2020). Additionally, existing literature examines how people categorize GSM's emergency messaging strategy (e.g., Kaewkitipong et al., 2016; Liu & Xu, 2018). However, there are currently few studies that examine the impact of GSM on people's behavior during crises. By exploring the impact of GSM participation on users' intention to select security measures against COVID-19 scams, our study helps further the current understanding of GSM management during crisis time. We find that GSM participation can improve individuals' protective motivations which further influence their preventive actions regarding COVID-19 scams.

Third, while the extant literature has examined the cultivation effects of traditional mass media (e.g., TV, newspapers) on users' beliefs and attitudes, our study is among the earliest to explore cultivation effects with social media (Hermann, Eisend, & Bayón, 2020). Our study explores not only the cultivation effects of social media, but also examines the impact of GSM accounts in particular. We find that GSM exerts an indirect influence on followers' attitude and perception of COVID-19-related cyber threats through PMT factors. Since social media has emerged as a primary channel for both broadcasting and information seeking, additional research on the cultivation effect of social media is warranted.

Fourth, our study also extends the view of PMT employed by past research by incorporating the CT. Unlike previous studies that focus on highlighting the importance of threat and coping assessments in enacting security actions in organizational systems contexts (e.g., Johnston et al., 2015; Johnston et al., 2019; Johnston & Warkentin, 2010), our study focuses on the antecedents of threat and coping appraisals in the personal context. Our results show that GSMs are important information sources of threat and coping appraisals during crises. Our findings suggest that further research on such information sources would be beneficial since they have the potential to be the foundation upon which critical threat and coping estimations are formed (Tu et al., 2015).

6.3. Policy implications

This study also provides several implications for practitioners. First, the results of this study highlight the importance of cybersecurity during the COVID-19 pandemic. According to a recent survey, only 7% of Americans were working from home either full or part-time before the COVID-19 pandemic (Littmann & Moore, 2020). In the time of social distancing, most organizations are increasing their remote operations and minimizing their physical presence (Littmann & Moore, 2020). Executives are paying more attention not only to the importance of productivity of remote teams, but also to cybersecurity issues with remote teams (Castellanos, 2020). Our work provides such practitioners with insight into how social media can help provide information for mitigating cybersecurity threats from crises. Our study also highlights the importance of self-protection for personal IS users during crises. Cyber hygiene (e.g., creating complex logins and passwords, managing how your browser stores passwords), therefore, should be encouraged by practitioners to make self-protection more proactive.

Second, threat and coping appraisals are shown to be important determinants of users' intention to employ security measures against COVID-19 scams. Information security training programs that address COVID-19 scams should be designed by both government agencies and other organizations to improve people's and employees' abilities to evaluate potential threats of COVID-19 scams and employ countermeasures. They can also offer users incentives (e.g., higher pay, flexible working hours) to encourage them to undergo the required training. Information security training can help individuals improve knowledge regarding cyber threats and accordingly, their self- and response-efficacy estimations.

Third, our results also show that GSM participation can influence our dependent variable indirectly through PMT factors. This indicates that GSM as a digital cultivation medium can play an important role in influencing people's information security behavior during a crisis. Governmental agencies should continue to increase their role to share timely and relevant information on their GSM during crises. Such GSM messages can be carefully developed and selected to ensure maximum impact. Advanced data mining techniques such as deep learning, topic modeling, and natural language processing should be employed by GSMs operators to analyze comments left in the GSMs to help improve the quality of messages. In addition, GSMs can also benefit from having people with large followings share their messages.

6.4. Limitations and future directions

Despite this study's efforts to enrich the current understanding of social media management during the crisis, some limitations need to be noted. First, we only collect data from a popular social media service in one country. Our results may be biased by the design of the platform and the culture of the country. Future investigations can employ a cross-cultural or cross-platform approach to enhance the generalizability of the current study. Second, while our research model helps explain a large percentage of the variance of our dependent variable, a few other important factors such as security awareness and habit have not been considered in the model. Future explorations may add these factors to further improve our understanding of GSM management and user information security during a crisis or disaster. Third, while our online survey approach maximizes generalizability, our study does not capture the maximum amount of realism possible because we do not measure actual user behavior in this study (McGrath, 1995). Not measuring actual behavior is a limitation of studies employing cross-sectional design and is common in behavioral information security studies (e.g., Warkentin, Johnston, Shropshire, & Barnett, 2016; Zhou et al., 2012). Future studies can measure users' actual behavior towards scams by employing longitudinal or mixed-methods design (McGrath, 1995). Lastly, we do not test the moderating effects of control variables like personality, socioeconomic status, or gender. These potential moderating factors may help provide further insight into individual information security behavior. We suggest that future studies assess such moderating effects.

7. Conclusion

The COVID-19 pandemic has been exploited by cybercriminals. The objective of this research is to further the understanding of people's information security behavior during a crisis such as the COVID-19

pandemic. Specifically, we employ both CT and PMT as the theoretical frameworks to explore the role of government social media in motivating users' information security behavior towards COVID-19 scams. We empirically validate our proposed research model and hypotheses by analyzing the data that we collect from an online survey among Chinese WeChat users. We find that users' GSM participation positively impacts people's intentions to employ security measures against COVID-19 scams through perceived severity, perceived vulnerability, self-efficacy, and response efficacy. Our findings serve as a stimulus for future researchers to build a broad understanding of GSM management and information security behaviors during a crisis time and to provide insights for practitioners.

Funding

This work was supported by the National Science Foundation of China [grant numbers 71871162, 71772042], the Humanities and Social Science Fund of Ministry of Education of China [grant number 17YJC630237], and the Program for Professor of Special Appointment (Eastern Scholar) at Shanghai Institutions of Higher Learning [grant number TP2018016].

Declaration of Competing Interest

There is no conflict of interest to declare from the author team.

References

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimedia empirical examination of home computer user security behavioral intentions. *MIS Quarterly, 34*(3), 613–643.
Anderson, J. C., & Gerbing, D. W. (1988). Structural equation modeling in practice: A review and recommended two-step approach. *Psychological Bulletin, 103*(3), 411–423.
Atkeson, A. (2020). *What will be the economic impact of covid-19 in the us? Rough estimates of disease scenarios (no. w26867)*. National Bureau of Economic Research.
Beaunoyer, E., Dupéré, S., & Guitton, M. J. (2020). COVID-19 and digital inequalities: Reciprocal impacts and mitigation strategies. *Computers in Human Behavior, 111*, 106424.
Bertot, J. C., Jaeger, P. T., & Hansen, D. (2012). The impact of polices on government social media usage: Issues, challenges, and recommendations. *Government Information Quarterly, 29*(1), 30–40.
Boss, S., Galletta, D., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly, 39*(4), 837–864.
Brislin, R. W. (1970). Back-translation for cross-cultural research. *Journal of Cross-Cultural Psychology, 1*(3), 185–216.
Castellanos, S. (2020, May 18). *With remote work here to stay, IT executives reassess tech priorities* (p. A11). The Wall Street Journal. Retrieved May 18, 2020, from https://www.wsj.com/articles/with-remote-work-here-to-stay-it-executives-reassess-tech-priorities-11589825596.
Chatfield, A. T., & Reddick, C. G. (2018). All hands on deck to tweet# sandy: Networked governance of citizen coproduction in turbulent times. *Government Information Quarterly, 35*(2), 259–272.
Chen, Q., Min, C., Zhang, W., Wang, G., Ma, X., & Evans, R. (2020). Unpacking the black box: How to promote citizen engagement through government social media during the COVID-19 crisis. *Computers in Human Behavior, 110*, 106380.
Chen, Y., Lu, Y., Wang, B., & Pan, Z. (2019). How do product recommendations affect impulse buying? An empirical study on WeChat social commerce. *Information Management, 56*(2), 236–248.
Chin, W. W. (1998). Commentary: Issues and opinion on structural equation modeling. *MIS Quarterly, 22*(1), vii–xvi.
CNNIC. (2018). 41st statistical survey report on the internet development in China. Retrieved 30 December, 2020, Retrieved from http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/hlwtjbg/201803/P020180305409870339136.pdf.
Collier, J. E., & Sherrell, D. L. (2010). Examining the influence of control and convenience in a self-service setting. *Journal of the Academy of Marketing Science, 38*(4), 490–509.
Cyber-Oberver. (2020a). 29 must-know cybersecurity statistics for 2020. Retrieved September 17, 2020, from https://www.cyber-observer.com/cyber-news-29-statistics-for-2020-cyber-observer/.
Evans, J. R., & Mathur, A. (2005). The value of online surveys. *Internet Research, 15*(2), 195–219.
Farooq, A., Laato, S., & Islam, A. N. (2020). Impact of online information on self-isolation intention during the COVID-19 pandemic: A cross-sectional study. *Journal of Medical Internet Research, 22*(5), Article e19128.
Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*(1), 39–50.
Gerbner, G. (1978). Cultural indicators: Violence profile no. 9. *The Journal of Communication, 28*(3), 176–207.
Gerbner, G., & Gross, L. (1976). Living with television: The violence profile. *The Journal of Communication, 26*(2), 172–199.
Gerbner, G., Gross, L., Morgan, M., Signorielli, N., & Shanahan, J. (2002). Growing up with television: Cultivation processes. In *Media effects* (pp. 53–78). Routledge.
Giddens, A. (1984). *The constitution of society: Outline of the theory of structuration*. Univ of California Press.
Guo, J., Liu, N., Wu, Y., & Zhang, C. (2020). Why do citizens participate on government social media accounts during crises? A civic voluntarism perspective. *Information Management*, Article 103286.
Guo, L., Zhang, M., Kang, K., & Hu, M. (2017). Transforming followers into fans: A study of Chinese users of the WeChat official account. *Online Information Review, 41*(7), 1029–2045.
Hair, J. F., Hult, G. T. M., Ringle, C. M., Sarstedt, M., & Thiele, K. O. (2017). Mirror, mirror on the wall: A comparative evaluation of composite-based structural equation modeling methods. *Journal of the Academy of Marketing Science, 45*(5), 616–632.
Hermann, E., Eisend, M., & Bayón, T. (2020). Facebook and the cultivation of ethnic diversity perceptions and attitudes. *Internet Research, 30*(4), 1123–1141.
Intravia, J., Wolff, K. T., Paez, R., & Gibbs, B. R. (2017). Investigating the relationship between social media consumption and fear of crime: A partial analysis of mostly young adults. *Computers in Human Behavior, 77*, 158–168.
Jin, X. L., Tang, Z., & Zhou, Z. (2017). Influence of traits and emotions on boosting status sharing through microblogging. *Behaviour & Information Technology, 36*(5), 470–483.
Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly, 34*(3), 549–566.
Johnston, A. C., Warkentin, M., Dennis, A. D., & Mikko Siponen, M. (2019). Speak their language: Designing effective messages to improve employees' information security decision making. *Decision Sciences, 50*(2), 245–284.
Johnston, A. C., Warkentin, M., & Siponen, M. (2015). An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric. *MIS Quarterly, 39*(1), 113–134.
Justice, D. (2020b). Department of Justice Announces Disruption of Hundreds of Online COVID-19 Related Scams. Retrieved June 17, 2020, from https://www.justice.gov/opa/pr/department-justice-announces-disruption-hundreds-online-covid-19-related-scams.
Kaewkitipong, L., Chen, C. C., & Ractham, P. (2016). A community-based approach to sharing knowledge before, during, and after crisis events: A case study from Thailand. *Computers in Human Behavior, 54*, 653–666.
Kim, S. C., & Hawkins, K. H. (2020). The psychology of social media communication in influencing prevention intentions during the 2019 US measles outbreak. *Computers in Human Behavior, 106428*.
Li, Y., Yang, S., Chen, Y., & Yao, J. (2018). Effects of perceived online–offline integration and internet censorship on mobile government microblogging service continuance: A gratification perspective. *Government Information Quarterly, 35*(4), 588–598.
Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems, 11*(7), 394–413.
Littmann, M., & Moore, S. (2020). Don't abandon security during a crisis. Retrieved June 17, 2020, from https://www.cisomag.com/dont-abandon-security-during-crisis/.
Liu, F., Burton-Jones, A., & Xu, D. (2014). Rumors on Social Media in disasters: Extending Transmission to Retransmission. *In PACIS*, 49.
Liu, F., & Xu, D. (2018). Social roles and consequences in using social media in disasters: A structurational perspective. *Information Systems Frontiers, 20*(4), 693–711.
Liu, P. L. (2020). COVID-19 information seeking on digital media and preventive behaviors: The mediation role of worry. *Cyberpsychology, Behavior and Social Networking, 23*(10), 677–682.
Loch, K. D., Carr, H. H., & Warkentin, M. E. (1992). Threats to information systems: today's reality, yesterday's understanding. *MIS Quarterly, 16*(2), 173–186.
Lowry, P. B., & Gaskin, J. (2014). Partial least squares (PLS) structural equation modeling (SEM) for building and testing behavioral causal theory: When to choose it and how to use it. *IEEE Transactions on Professional Communication, 57*(2), 123–146.
Malhotra, N. K., Kim, S. S., & Patil, A. (2006). Common method variance in IS research: A comparison of alternative approaches and a reanalysis of past research. *Management Science, 52*(12), 1865–1883.
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.
Mason, C. H., & Perreault, W. D., Jr. (1991). Collinearity, power, and interpretation of multiple regression analysis. *Journal of Marketing Research, 28*(3), 268–280.
McGrath, J. E. (1995). Methodology matters: Doing research in the behavioral and social sciences. In *Readings in human–computer interaction* (pp. 152–169). Morgan Kaufmann.
Naidoo, R. (2020). A multi-level influence model of COVID-19 themed cybercrime. *European Journal of Information Systems*, 1–16. forthcoming.
Oh, S. H., Lee, S. Y., & Han, C. (2020). The effects of social media use on preventive behaviors during infectious disease outbreaks: The mediating role of self-relevant emotions and public risk perception. *Health Communication*, 1–10.
Orlikowski, W. J., & Robey, D. (1991). Information technology and the structuring of organizations. *Information Systems Research, 2*(2), 143–169.
People''s Daily. (2018). WeChat e-government. Retrieved June 17, 2020, from http://media.people.com.cn/n1/2018/0504/c419419-29965171.html.

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. *The Journal of Applied Psychology, 88*(5), 879–903.
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.
Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change1. *The Journal of Psychology, 91*(1), 93–114.
Rogers, R. W. (1983). *Cognitive and psychological processes in fear appeals and attitude change: A revised theory of protection motivation* (pp. 153–176). Social Psychophysiology: A Sourcebook.
Shah, Z., Chu, J., Ghani, U., Qaisar, S., & Hassan, Z. (2020). Media and altruistic behaviors: The mediating role of fear of victimization in cultivation theory perspective. *International Journal of Disaster Risk Reduction, 42*, Article 101336.
Song, M., Kim, J. W., Kim, Y., & Jung, K. (2015). Does the provision of emergency information on social media facilitate citizen participation during a disaster? *International Journal of Emergency Management, 11*(3), 224–239.
Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly, 22*(4), 441–469.
Tang, Z., Chen, L., & Gillenson, M. L. (2018). How to keep brand fan page followers? The lens of person-environment fit theory. *Information Technology and People, 31*(4), 927–947.
Tang, Z., Chen, L., Zhou, Z., Warkentin, M., & Gillenson, M. L. (2019). The effects of social media use on control of corruption and moderating role of cultural tightness-looseness. *Government Information Quarterly, 36*(4), 101384.
Tsay-Vogel, M., Shanahan, J., & Signorielli, N. (2018). Social media cultivating perceptions of privacy: A 5-year analysis of privacy attitudes and self-disclosure behaviors among Facebook users. *New Media & Society, 20*(1), 141–161.
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.
Warkentin, M., Johnston, A. C., & Shropshire, J. (2011). The influence of the informal social learning environment on information privacy policy compliance efficacy and intention. *European Journal of Information Systems, 20*(3), 267–284.
Warkentin, M., Johnston, A. C., Shropshire, J., & Barnett, W. D. (2016). Continuance of protective security behavior: A longitudinal study. *Decision Support Systems, 92*, 25–35.
Warkentin, M., Sharma, S., Gefen, D., Rose, G. M., & Pavlou, P. (2018). Social identity and trust in internet-based voting adoption. *Government Information Quarterly, 35*(2), 195–209.
Wei, Y., McIntyre, F. S., & Straub, D. (2020). Does micro-blogging lead to a more positive attitude toward a brand?—A perspective of cultivation theory. *Journal of Promotion Management, 26*(4), 504–523.
Wengjuanxin. (2020). Wengjuanxin milestone. Retrieved December 29, 2020, from https://www.wjx.cn/html/milestoneNew.aspx.
WHO. (2020). Coronavirus disease (COVID-19) pandemic. Retrieved June 17, 2020, from https://www.who.int/emergencies/diseases/novel-coronavirus-2019.
Williams, C., & Fedorowicz, J. (2019, January). Does social media promote the public's perception of the police: Survey results on trust cultivation. In *Proceedings of the 52nd Hawaii International Conference on System Sciences*.
Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. *MIS Quarterly, 37*(1), 1–20.
Witte, K. (1996). Predicting risk behaviors: Development and validation of a diagnostic scale. *Journal of Health Communication, 1*(4), 317–342.
Wukich, C. (2016). Government social media messages across disaster phases. *Journal of Contingencies & Crisis Management, 24*(4), 230–243.
Zhang, K. Z., Barnes, S. J., Zhao, S. J., & Zhang, H. (2018). Can consumers be persuaded on brand microblogs? An empirical study. *Information Management, 55*(1), 1–15.
Zheng, J., Qi, Z., Dou, Y., & Tan, Y. (2019). How mega is the mega? Exploring the spillover effects of WeChat using graphical model. *Information Systems Research, 30*(4), 1343–1362.
Zhou, Z., Fang, Y., Vogel, D. R., Jin, X. L., & Zhang, X. (2012). Attracted to or locked in? Predicting continuance intention in social virtual world services. *Journal of Management Information Systems, 29*(1), 273–306.

Zhenya "Robin" Tang is a doctoral student of Information Systems at the College of Business at the Mississippi State University. He holds two master degrees from the University of Memphis and Shanghai University, respectively. His research mainly focuses on the usage of social media services and their impacts in various domains (e.g., marketing, public administration, cybersecurity, sustainability, etc.). His paper appears in renowned journals such as Information & Management, Government Information Quarterly, International Journal of Information Management, Computers in Human Behavior, Behavior & Information Technology, Information Technology & People, and Resources Conservation & Recycling. He has presented his research at major conferences such as the annual Americas' Conference on Information Systems (AMCIS).

Andrew S. Miller is a PhD candidate of Information Systems in the College of Business at Mississippi State University. He has received a B.B.A. in Information Systems from the University of North Georgia. His research has been featured in the Journal of Emerging Technologies in Accounting, International Conference on Information Systems, Americas Conference on Information Systems, and the Dewald Roode Workshop on Information Systems Security Research. His current research interests involve IS economic value and business analytics.

Zhongyun (Phil) Zhou is an Associate Professor and Professor of Special Appointment in the School of Economics and Management, Tongji University, China. He holds two Ph.D. degrees from University of Science and Technology of China and City University of Hong Kong, respectively. His research interests include IT-enabled service usage, social media and commerce, knowledge management, and e-health. His papers appear in renowned journals such as Journal of Management Information Systems, European Journal of Information Systems, Information & Management, Decision Support Systems, Journal of Business Ethics, and others. He serves as a Senior Editor for Information Technology and People and an Associate Editor for Information Systems Journal and Electronic Commerce Research and Applications.

Merrill Warkentin is the James J. Rouse Endowed Professor of Information Systems and a William L. Giles Distinguished Professor at Mississippi State University. His research, primarily on the impacts of organizational, contextual, and dispositional influences on individual behaviors in the context of information security and privacy, has appeared in MISQ, Decision Sciences, JMIS, JAIS, EJIS, I&M,DSS, ISJ, CAIS, DATABASE for Advances in Information Systems, CACM, and others. He is the author or editor of seven books, and has authored or co-authored more than 300 published manuscripts, including more than 100 peer-re-viewed journal articles, with more than 18,000 citations (h-index = 41), according to Google Scholar in 2021. He holds or has held editorial roles for MISQ, ISR, JAIS, EJIS, I&M, Decision Sciences, and others. He has held leadership positions at AIS, DSI, IFIP, and ACM, and was the Program Co-Chair for AMCIS2016. His work has been funded by NATO, NSF, NSA, DoD, Homeland Security, IBM, and others. In 2018, he was named an ACM Distinguished Scientist.