IADIS International Journal on WWW/Internet
Vol. 15, No. 1, pp. 31- 46
ISSN: 1645-7641

# DEVELOPING AND IMPLEMENTING TTAT-MIP FOR THE AVOIDANCE OF MALWARE THREATS THROUGH ONLINE SOCIAL NETWORKS

Ehinome Ikhalia[1], Dr Alan Serrano[1], Dr David Bell[1] and Johannes Arreymbi[2]
[1]*Department of Computer Science, Brunel University, London,Uxbridge, UK*
[2]*Ehino Solutions, London, UK*

**ABSTRACT**

Online social networks (OSNs) have transformed the manner social relationships are formed; as it includes digital functionalities to assist users to connect with friends and family as well as conduct their businesses. There has also been a rapid increase in the success of malware attacks targeting users of OSNs. Through social engineering, attackers continue to exploit the trust factor inherent amongst users to lure them into downloading malware on their computer device. In this paper, we examine the Technology Threat Avoidance Theory (TTAT) for the avoidance of malware threats. Potential drawbacks of TTAT were identified and discussed. We present evidence based on the literature for extending the Technology Threat Avoidance Theory to include a new construct – Mass Interpersonal Persuasion (MIP) - (TTAT-MIP) for users of online social networks. A novel Facebook animation video APP is also proposed as a tool to make social network users aware about the nature and dynamics of malware threats. Our work attempts to make a contribution to theory and practice by describing the relationship between the extended version of TTAT (TTAT-MIP) and the architecture of the proposed Facebook animation video App.

**KEYWORDS**

Social networks, malware attacks, mass interpersonal persuasion, threat avoidance, social engineering, human vulnerability

## 1. INTRODUCTION

The biggest security challenge associated with the use of online social networks is malware distribution through social engineering (Faghani *et al*, 2012; Fire *et al*, 2013). Social engineering is a persuasive technique malware attackers often utilize because it depends on mainly on human vulnerability. Basically, social engineering often involves tricking users into executing tasks that they normally would not (e.g. downloading malware on their computer

systems unknowingly) (Algarni *et al*, 2013). On social networks, social engineering has become very pervasive and prevalent and has been used continuously to propagate malware attacks (Ikhalia & Arreymbi 2014).

Within online social network settings, a common social engineering technique employed is; persuading users to click on malicious video links which often redirects them into a replica of a legitimate website with a prompt to update a 'software' needed to watch the video (Thomas & Nicol 2010). The 'software' is essentially a malware which enables the attacker to remotely control the victim's computing system. When the malware is installed, it posts the malicious link to the victim's personal social network space (for example Facebook timeline), and tags his/her social connections (often called, friends/followers), thereby infecting every user that clicks it. The malware is also able to send private messages to victims' connections, spreading the infection even further (Baltazar et al, 2009; Gao et al., 2011; Palmer, 2013).

Attackers always find new methods to exploit the ignorance, curiosities, and trust of users' to lure them to download and install malware on their computer devices (Faghani et al. 2012). Efforts by security practitioners to combat these adverse trends have not been effective enough to handle the biggest social network security challenge – human vulnerability (Braun & Esswein, 2013, Ikhalia & Arreymbi, 2014). Although social engineering poses an ominous persistent threat to many organizations, OSNs seem to be an easy platform for exploiting users' vulnerability to propagate malware (Ikhalia & Arreymbi, 2014). The interactive structure of OSNs, as well as users' inability to detect malicious tricks that lure them to install malware on their computer devices may have contributed to the speed at which malware attacks are being propagated (Gulati, 2003). This work will attempt to address some of the issues by proposing a malware threat avoidance theory (TTAT-MIP) that would help to motivate users to avoid social-engineering-based malware attacks carried out through OSNs.

TTAT-MIP has been derived from the Technology Threat Avoidance Theory (TTAT; Liang and Xue, 2009) which explains the motivation for technology threat avoidance by users of online social networks. The essential principle of TTAT-MIP is that when online social network (OSN) users perceive a malware threat they are motivated to use a safeguarding measure to avoid the threat if they perceive that it would be effective for threat avoidance. In the process of avoiding malware threats by online social network users a set of key factors that demonstrates the perceptions, motivations, and behavior of users. OSN users' malware threat perceptions are affected by the perceived likelihood of the threat's occurrence as well as the perceived severity of its negative consequences. By drawing from previous studies on health protective behaviour (Janz and Becker, 1984; Rosenstock, 1974), we theorize that there are four key factors considered by OSN users when evaluating the degree of avoidance of a malware threat – the effectiveness of the safeguard, the self-confidence in applying the safeguard, the cost of applying the safeguard and the mass interpersonal persuasiveness (MIP) of the safeguard.

Mass interpersonal persuasion (MIP) can be defined by six key components; persuasive experience, automated structure, social distribution, rapid cycle, huge social graph and measured impact (Fogg, 2009). MIP is an experience designed to change human behaviours and make a lasting impact on their lives. For example, an IT security company could design an experience to improve the attitude of social network users about IT security by asking them to watch a malware threat awareness video on social media such as Facebook, rank their awareness levels and share their scores with their friends on their timeline.

Based on the theoretical constructs of TTAT-MIP, we also propose a new Facebook animation video App for creating security awareness for OSN users. We describe the architecture of the App and analyse its relationship with TTAT-MIP. Our work has a major implication for Information Systems (IS) researchers and software practitioners seeking to develop digital systems that have sufficient theory-base.

## 1.1 Related Work

Previous works have been conducted towards the development of effective end-user security awareness systems to mitigate the impact of malicious attacks. Abrams et al., 2013; Aggarwal, 2012; Doostari et al, 2013, focused on developing software to detect malicious attacks. However, their proposed system is mainly reactive in nature; implying that, the implications of attacks may occur before remediation measures are applied. There is evidence in literature (Tidwell 2011) which suggests that more research work needs to focus on proactive security awareness systems tailored to address the threats faced by users in the technological setting through which malware attacks are being executed.

Wilson et al, (2003) suggests that numerous security awareness frameworks exist which prescribes the required steps to design and implement an efficient and effective security awareness system. A thorough understanding of the steps is compulsory to develop and tailor such an awareness program for a specific technological setting. Some of the methods that have been used include professional training, newsletters, and websites to deliver security awareness information to users. Unfortunately, the nature of these methods could be relatively daunting, costly and strenuous to the end-users who have no technical background in information technology.

In the context of online social networks, an effective and proactive security awareness system that could be useful in avoiding malware attacks must adopt some of the features and characteristics that define users' engagement on the platform. Features such as; video embedding capabilities, social interaction, and active user participation. Ikhalia & Serrano (2015) proposed a novel framework for the development of security awareness systems for OSN users; five components were deduced and proposed; ***Timeboxing, End-User Engagement, Platform Integration, Activity Specific and Knowledge Testing.*** In addition to these factors, this paper supports the theory that motivation is also a key theoretical component for OSN users to avoid malware attacks based on the research conducted by Liang & Xue (2009). Hence, we explore the technology threat avoidance theory (TTAT) through avoidance motivation. We have also included a new construct – mass interpersonal persuasion (MIP) to the TTAT model to motivate OSN users to avoid malware attacks. A security awareness system driven by MIP involves creating persuasive experiences deployed using automated software tools within a small amount of time in a highly socially distributed technological platform embedded with capabilities to measure its impact (Fogg & Hall, 2008). MIP focuses on changing users' thoughts and behaviors and not just informing them. This factor could be extremely useful for deploying security awareness in a setting were security compliance is non-mandatory. The next section describes the TTAT model and a few limitations on its practical application within OSNs.

This work will attempt to improve upon existing research efforts towards security awareness by proposing a malware threat avoidance theory (MTAT) that will help to persuade users to avoid social-engineering-based malware attacks carried out through OSNs. The paper is structured thus; section 2 presents a review of TTAT and identified gaps. Section 3 reviews

the newly added construct to TTAT; section 4 presents the research hypothesis and the theoretical justifications.

## 2. TECHNOLOGY THREAT AVOIDANCE THEORY (TTAT)

The development of this research is based on the technology threat avoidance theory (TTAT) proposed by Liang and Xue (2009) which explains the motivation for technology threat avoidance by users of computer systems. The fundamental principle of TTAT is that when computer users perceive a malware threat they are motivated to use a safeguarding measure to avoid the threat if they perceive that it would be effective for threat avoidance. In the process of avoiding malware threats by users of computer systems, Liang and Xue (2009) proposed a set of key factors that demonstrates the perceptions, motivations, and behavior of users. According to their proposed model, users' malware threat perceptions are affected by the perceived likelihood of the threat's occurrence as well as the perceived severity of its negative consequences. By drawing from previous studies on health protective behaviour (Janz and Becker, 1984; Rosenstock, 1974), Liang and Xue (2009) argue that there are three main factors considered by computer users when evaluating the degree of avoidance of a malware threat – the effectiveness of the safeguard, the self-confidence in applying the safeguard and the costs of applying the safeguard.

TTAT also suggests that users normally perform emotion-focused coping to passively avoid the malware threat. Emotion-focused coping creates a false sense of the situation without essentially modifying one's needs or importance of needs so that negative emotions connected to malware threat are avoided. Thus, it reduces perceived threat or motivation of coping with the threat without altering the reality of the threat.

Liang and Xue (2009) conducted their survey on 152 US college students within the business department and found out that users' malware threat avoidance behavior is predicted by their motivation to avoid the threat. Additionally, they argue that avoidance motivation of malware threat is determined by perceived threat, safeguard effectiveness, safeguard cost and self-efficacy or self-confidence. Therefore, their findings suggest that users develop a perception of malware threat when they feel that a malware has the possibility of attacking them (perceived susceptibility or perceived vulnerability) and the corresponding consequences would be severe (perceived severity).

Furthermore, when faced with a malware threat, they suggest that users are motivated to use a safeguard measure if they perceive the degree of its effectiveness; the inexpensiveness and convenience of using it (safeguard cost); and their confidence in using it (self-efficacy). They identified that perceived threat and safeguard effectiveness have a negative interactive effect on the motivation for malware threat avoidance. This implies that an increase in users' perception of malware threat is correlated with a decrease in the relationship between safeguard effectiveness and avoidance motivation. Also, their findings suggest that an increase in users' perception of a safeguarding measure is correlated with a decrease in the relationship between perceived threat and avoidance motivation. Their research model developed and tested is shown in figure 1.

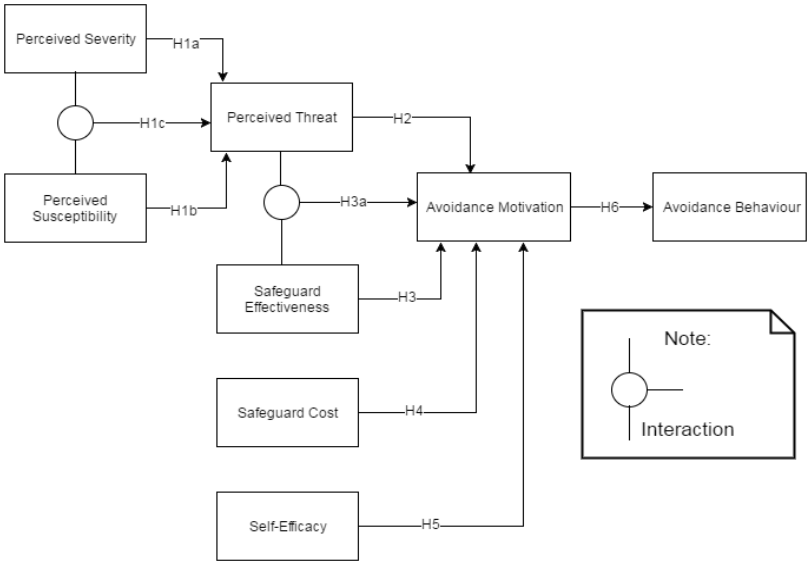


Figure 1. Research model developed and tested by Liang & Xue (2009)

## 2.1 Limitations of Technology Threat Avoidance Theory

Firstly, their findings cannot be generalized to a larger population of computer users due to the niche convenience sample of Business College Students used for their study. Business College Students do not adequately represent the population of general computer users and as such including other students in various academic departments may have produced more demographically diverse views and understanding on the perception of malware threats by computer users.

Secondly, the use of general computer users to explain the security behaviours of IT users regarding a complex issue as malware threats may not provide in-depth information that can be representative of diverse computer users who normally utilise some specific technological platforms more than the others and thus may encounter varied forms and techniques of malware threats (Bayuk et al. 2011; Reavis 2012; Sophos 2014).

A study conducted by Hampton *et al,* (2011) found that the typical internet user is more than twice as likely as others to feel that people can be trusted. The research found that Facebook users are even more likely to be trusting and engage in using the platform multiple times per day; precisely 43% more likely than other internet users and more than three times as likely as non-internet users to feel that most people can be trusted. More enriched information on the IT security behavior of computer users would have been identified if the narrative of their study was focused on the use of a more specified information technology platform (e.g. online social networks, electronic banking, and aviation industries). This idea is also due to the fact that previous studies have shown that the degree of malware threat varies from platform to platform (Bayuk et al., 2011; Reavis, 2012; ). For instance, the core computing practices and behaviours' of traffic air controllers would be entirely different from that of online social media marketers.

# 3. MODIFYING THE TECHNOLOGY THREAT AVOIDANCE THEORY FOR OSN USERS

## 3.1 Mass Interpersonal Persuasion (MIP)

Fogg & Hall (2008), highlighted a distinct characteristic of online social network termed – Mass Interpersonal Persuasion (MIP). MIP is the biggest factor that influences users of online social networks to perform certain behaviors on a massive scale. According to Fogg & Hall (2008), MIP is a unique characteristic of online social networks which makes it possible for users to reach and influence millions of their direct and indirect connections (friends/followers and friends of friends) within the shortest possible time. MIP is focused on changing users' behaviors and not simply disseminating information to them.

MIP works effectively when a social network platform has millions of users with multiple interpersonal connections. For instance, regardless of how compelling a persuasive experience may be, MIP cannot occur if all the social network users are merely 50 people. Fogg, (2009) argues that MIP is defined by its calculated impact, which implies that a user needs to know how many users have been engaged with the persuasive system in the last 24 hours, or how many users have installed the system on a daily or weekly basis.

A systematic review by (Ikhalia & Serrano, 2015), highlighted some of the challenges faced by IT practitioners in developing effective security awareness systems to assist users in avoiding malware attacks. One of the significant issues identified was the lack of a contextual knowledge whilst deploying security awareness. For OSN users, having a security awareness system deployed through MIP could be very effective in presenting contextual security awareness information because of their tendency to trust content from their interpersonal social network connections.

Based on the unique characteristic – MIP, of online social networks; we argue that the mass interpersonal persuasive (MIP) attribute of a malware safeguarding measure would likely be a key factor that may influence the coping appraisal process of users when evaluating a potential malware threat. This implies that users of online social networks are more likely to use a safeguard measure to identity a malicious threat if they are motivated through interpersonal persuasions on a massive scale. Consequently, in modifying the TTAT model for OSN users, this research posits that MIP positively affects avoidance motivation. In addition, we posit that MIP positively moderates the relationship between safeguard effectiveness and avoidance motivation, further theoretical justification for this argument is presented in the hypothesis section of this paper. Figure 2 shows our proposed research model.

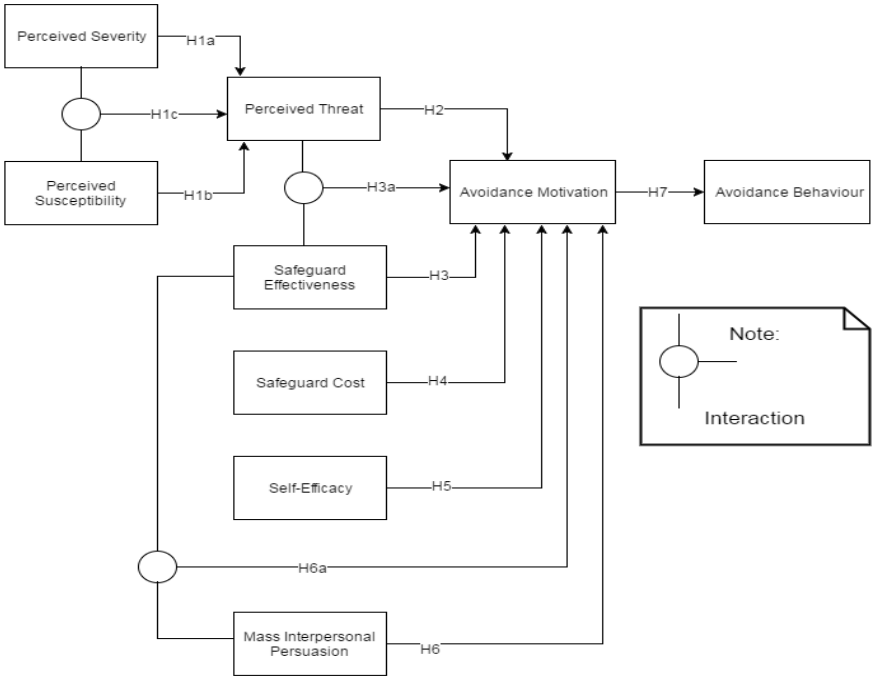


Figure 2. The proposed new model - TTAT-MIP (Liang & Xue 2009; Fogg & Hall 2008)

# 4. RESEARCH HYPOTHESIS

'Perceived threat' can be defined as, the degree to which a user perceives that a malware threat can be dangerous. According to TTAT, threat perception is developed by perceived susceptibility and perceived severity. Perceived susceptibility is simply defined as, the subjective belief that a user will be negatively affected by malware threat. Meanwhile, perceived severity is the degree to which a user perceives that the negative consequences of a threat will be severe (McClendon 2012; Stretcher & Rosenstock 1997). For this reason, this research posits that the combination of perceived susceptibility and severity positively affects threat perception.

***H1a: Perceived susceptibility of being attacked by malware positively affects perceived threat.***

***H1b: Perceived severity of being attacked by malware positively affects perceived threat.***

When users' perceived susceptibility of a threat increase, the relationship between perceived severity and perceived threat will consequently increase in strength.

***H1c: Perceived susceptibility and perceived severity have a positive interaction effect on perceived threat.***

When social network users perceive a malware threat, they are usually motivated to avoid it. Avoidance motivation is defined as the degree to which computer users are motivated to avoid malware threats using safeguarding measures (Rippetoe *et al,* 1987; Weinstein, 1993).

***H2: Perceived threat positively affects avoidance motivation.***

The effectiveness of a safeguard is defined as the subjective assessment of a safeguarding measure on how effective it can be applied to avoid the malware threat. This theory was drawn from the concept of perceived benefits of health belief model as postulated by Janz & Becker (1984) and the concept of response efficacy in protection motivation theory (Rogers, 1997), which predicts behavior motivation.

***H3: Safeguard effectiveness positively affects avoidance motivation***

This paper proposes a new safeguard measure based on video animation system that provides useful guidelines through dramatized storytelling on how social network users can avoid malware attack. Therefore, based on the context of our proposed safeguard this research posits that safeguard effectiveness positively moderates the relationship between perceived threat and avoidance motivation. As a result, when the level of safeguard effectiveness increases social network users will feel more motivated to avoid the threat.

***H3a: Perceived threat and Safeguard effectiveness have a positive interaction effect on avoidance motivation.***

Safeguard cost is defined as the physical and cognitive efforts – such as money, time, comprehension and inconvenience needed to make use of given safeguard measure (Lang & Xue 2009). This means that users are more likely to use a safeguard if it takes less time, money and effort to adopt. Earlier research by Ikhalia & Serrano (2015) identified a key element needed for creating effective security awareness systems – ***Timeboxing***. This means that security awareness solutions for users must ensure strict time boundaries when disseminating instructional guidelines to the user. Therefore the cost of using the safeguard would be relatively less and then the avoidance motivation would increase.

***H4: Safeguard cost negatively affects avoidance motivation***

Self-efficacy has been studied in previous research (Ng et al., 2009; Woon et al., 2005; Workman et al., 2008) and found to have a positive influence on IT security related behaviors of computer users. Hence, the higher the self-efficacy on using a safeguarding measure the stronger the motivation to avoid a malware threat.

***H5: Self-efficacy positively affects avoidance motivation***

In order to comprehend the social influence on persuasive experience, it is important to consider how social media such as Facebook, LinkedIn, and WhatsApp or Twitter invitations are modelled. When a Facebook user is invited by his/her friend to use a third party application (e.g. a malware threat awareness video system), Facebook sends an invitation request with messages such as;

***"Here is Joseph's IT security awareness score on this Video APP, you can get your score too by viewing the Video APP and together we can become aware on how to stop the spread of malware on Facebook".***

MIP as the process of creating persuasive experiences deployed using automated software tools within a small amount of time in a highly socially distributed technological platform embedded with capabilities to measure its impact. MIP focuses on changing users' thoughts and behaviors and only informing them. Foster et al, (2009) carried out research that focused on determining peoples' attitudes on domestic electricity usage, through a Facebook application termed 'Watts Up'. Their application presented visualizations of users' own electricity consumption as well as that of their friends; which positively affected their energy consumption leading to reduced energy consumption by users of the application. This work argues that the motivation to avoid malware threats by OSN users would be positively and significantly affected by the mass interpersonal persuasiveness of a given safeguard.

***H6: MIP positively affects avoidance motivation***

MIP can positively moderate the relationship between safeguard effectiveness and avoidance motivation. Interpersonal influence theory and research postulates that individuals are normally inclined to conform to the expectations of others regarding purchase decisions (Bearden *et al*, 1989). Oftentimes users demonstrate the tendency to learn about products and services by observing or seeking information from others (Bearden *et al*, 1989). Empirical studies by (Bullee *et al*, 2015; Hutter *et al*, 2013; Lee *et al*, 2014) suggest that online social influence not only can affect consumer perception of quality of a sports brand but also consumer buying intention. Therefore MIP positively moderates the relationship between safeguard effectiveness and avoidance motivation. This implies that the higher the mass interpersonal persuasive attribute of the safeguard, the higher the motivation to avoid malware threats by OSN users.

***H6a: MIP and safeguard effectiveness have a positive interaction effect on avoidance motivation***

# 5. A FACEBOOK ANIMATION VIDEO APP TO CREATE SECURITY AWARENESS FOR OSN USERS

This section focuses on explaining the architecture of the proposed Facebook animation video App to create awareness for users of online social networks to avoid malware attacks. A Facebook App is an interactive software application developed to use the fundamental technologies of the Facebook platform to create a broad social media framework for the app. Facebook Apps integrates Facebook's News Feed, Notifications, several social channels and other features to create awareness and interest in the app by Facebook users (Wang et al. 2011). To prevent the spread of malware through OSNs, user awareness about the nature and dynamics of malware distribution within a social network context needs to be considered (Sood 2011). An animation video App embedded on a social networking platform can be effective in facilitating user engagement and a more proactive online social network security behaviours (Ikhalia & Serrano 2015).

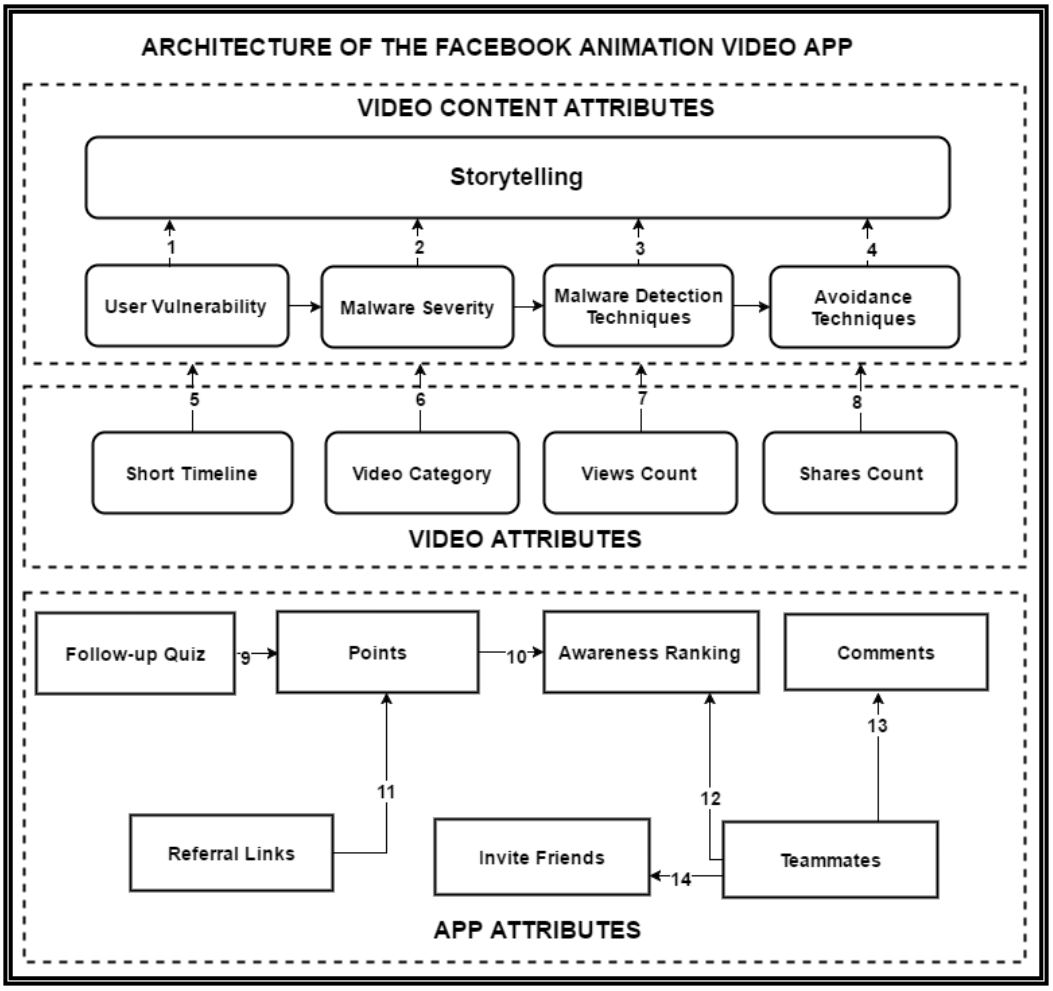


Figure 3. The Architecture of the Proposed Facebook Animation Video App
(Liang & Xue 2009; Fogg & Hall 2008)

As shown in **Figure 3**. The architecture of the proposed Facebook Animation Video App system consists of three layers; Video Content Attributes, Video Attributes and App Attributes. The Video Content Attributes describes the manner through which the security awareness would be disseminated to the user. The main idea of the video content is to present a dramatic clip on security awareness through storytelling of previous incidents of malware attacks on OSN users (Ikhalia & Serrano 2015). The story would include information on users' vulnerability, the severity of the attack, the potential detection techniques and how users could avoid such attacks in future.

Also, **Figure 3** shows the video attributes contained in the second layer of the architecture. The video attributes describes the unique features of the videos such as; short timeline, video category, views count and shares count. The short timeline attribute simply implies that each video would be timeboxed to effectively focus on the most important message (Zhang et al.

2016). By having a video disseminate security awareness within a short timeframe, the problems of information overload would be avoided (Zhang et al. 2016).

The Video Category attribute would allow users effectively select videos that are suitable to their interests (Lin & Lu 2011). For example, the stories of malware attacks contained in the videos of our proposed App could be categorized based on the type of social network platform (e.g. Facebook, Twitter, LinkedIn), or based on type of OSN social engineering technique (e.g. Accepting fake friend requests, Installing malicious Social Network Apps, Clicking on malicious links on a friends timeline) used to attack users (Yan et al. 2007). The Views Count and Share Count attributes would allow users to examine the reach of the videos and may have a huge impact on their engagement on the App (Diffley & Kearns 2011).

In **Figure 3,** the App Attributes shown in the third layer of the architecture presents the features that would be included in the App development to ensure users of online social networks are regularly and actively engaged. In addition, the components of the App attributes may also have a huge impact on the viral propagation of security awareness amongst interconnected users.

The 'Follow-up Quiz' is an extremely important part of the App, when a user has completed watching a video, a pop-up menu would be presented with questions about the video content. Again, the Quiz would have a short timeframe of about 60secs. The aim of the quiz is to test whether the user has been able to retain the knowledge gain from watching the video. At the end of the 60 seconds countdown or after the user has answered the questions correctly, points are automatically allotted which would contribute to their security awareness rank on the App. One correctly answered question attracts 15 points for the user.

The Awareness Ranking attribute implies than when a user has accumulated a specific number of points by regularly watching videos and providing answers to the corresponding quizzes, the App automatically ranks them in the following fashion;

1. When users' accumulate 200 points they are ranked - 1 Star Security General
2. When users accumulate 400 points they are ranked – 2 Star Security General
3. When users accumulate 600 points they are ranked – 3 Star Security General
4. When users accumulate 800 points they are ranked = 4 Star Security General

And the cycle continues when they increase their points by 200. If a user has more than 2 weeks of inactiveness, they will lose ranking points (i.e. they need to regularly watch videos to retain/increase their ranking).

Furthermore, the 'Referral Links' attributes, implies that the App would contain links to external website/blogs which extends the knowledge about the subject of social network security for the user. When a user clicks on a referral link, they gain 2 points extra automatically.

As with other Facebook apps, the users would be able to automatically send App requests and/or receive App requests from other users. The App would allow users to form a list of 'teammates' whenever they send personal invitations to their Facebook friends and such invitations get acknowledged. Moreover, users can share their thoughts and comments on each video which may enhance the engagement on the App. In the next section we attempt to connect the theoretical constructs of our proposed TTAT-MIP model with the three layers of the proposed Facebook animation video App.

## 5.1 Relationship Between the Proposed Facebook Video Animation App and Ttat-Mip

**Table 1. Relationship Between The Proposed Facebook Video Animation App and TTAT-MIP (**(Ikhalia & Serrano 2015; Ikhalia & Serrano 2016; Liang & Xue 2009)**)**

| TTAT-MIP Constructs | Attributes of the Proposed Facebook Video Animation APP |
|---|---|
| **1. Perceived Susceptibility**<br>Perceived susceptibility is defined as a user's subjective belief that he or she will be negatively affected by a malware attack (Lang & Xue 2009; McClendon, 2012; Stretcher & Rosenstock, 1997). | **Video Content Attributes:**<br>Based on the first layer of the architecture which describes the attributes of the video content. When users' watch a video that addresses problems of the vulnerable behaviour of other users we theorize that users' perceived susceptibility could be influenced when they watch a video that reports on a previous case of social network malware attack. |
| **2. Perceived Severity**<br>Perceived severity is the degree to which a user perceives that the negative consequences of a threat will be severe (McClendon, 2012; Stretcher & Rosenstock, 1997). | **Video Content Attributes:**<br>When users' watch a video that addresses problems of the severity of malware attacks faced by other users, we argue that it would have a significant impact on their perceived severity. |
| **3. Perceived Threat**<br>Perceived threat can be defined as, the degree to which a user perceives that a malware threat can be dangerous (Lang & Xue 2009; Rippetoe et al, 1987; Weinstein, 1993). | **Video Content Attributes:**<br>When users' watch a video that addresses problems of both the severity of malware attacks faced by other users as well as the problems of the vulnerable behaviour of other users and we argue that it would have a significant impact on perceived threat. |
| **4. Safeguard Effectiveness**<br>The effectiveness of a safeguard is defined as the subjective assessment of a safeguarding measure on how effective it can be applied to avoid the malware threat (Lang & Xue 2009; Carver & Scheier, 1982). | **Video Content Attributes:**<br>When users' watch a video that addresses malware threat detection techniques as well as threat avoidance techniques, their perception of the effectiveness of using a given safeguard would be significantly influenced. |

| | |
|---|---|
| **5. Safeguard Cost**<br>Safeguard cost is defined as the physical and cognitive efforts – such as money, time, comprehension and inconvenience needed to make use of given safeguard measure (Lang & Xue 2009). | **Video Attributes:**<br>When users' watch a video that addresses threat avoidance techniques, their perception of the cost of using a given safeguard would be significantly influenced. |
| **6. Self-Efficacy**<br>Self-efficacy as the confidence of users in taking a safeguarding measure to avoid malware threat (Lang & Xue 2009). | **App Attributes:**<br>When users' are extremely successful in providing answers to the quiz questions and consequently attain high security awareness ranks on our proposed App, their Self-efficacy in dealing with malware threats would significantly improve overtime. |
| **7. Mass Interpersonal Persuasion (MIP)**<br>MIP is defined as the ability of online social network users to influence the behaviour of their direct connections into performing similar behaviours. It involves the creation of persuasive experiences deployed using automated software tools within a small amount of time in a highly socially distributed technological platform embedded with capabilities to measure its impact (Fogg & Hall 2008). | **App Attributes:**<br>When users receive massive personal requests from their inter-personal connections on a given social networks, we theorize that they would be persuaded to watch the security awareness video and also use the safeguarding measures recommended. |

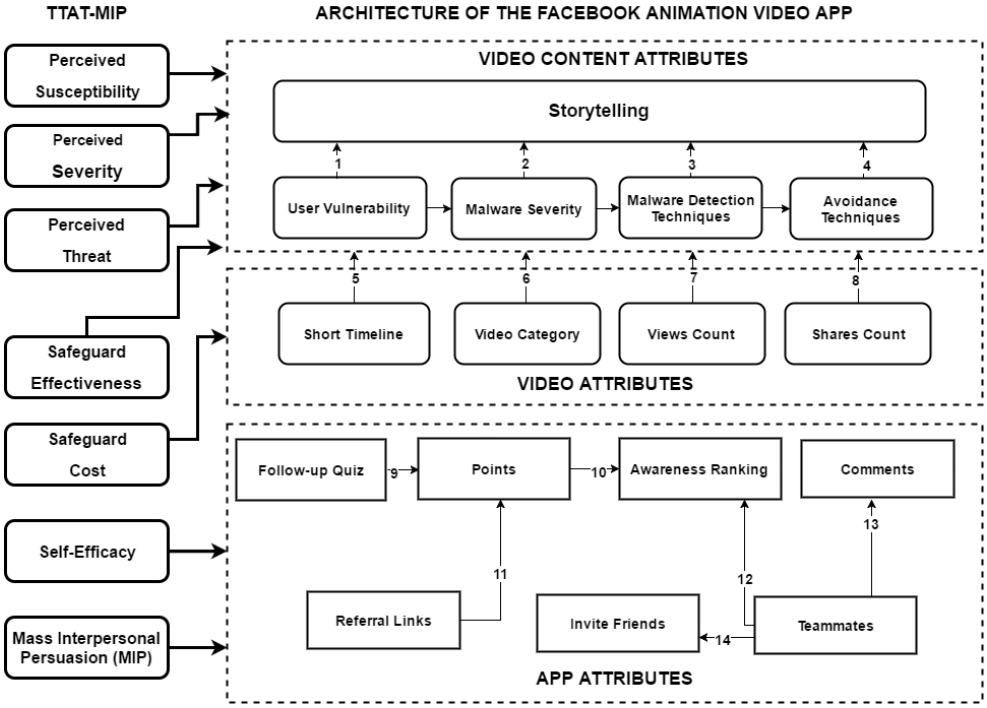


Figure 4. TTAT-MIP and The Architecture of the Proposed Facebook Animation Video App (Liang & Xue 2009; Fogg & Hall 2008)

## 6. DISCUSSION & FURTHER WORK

This paper explored the technology threat avoidance theory (TTAT) proposed by Liang & Xue (2009), in order to study the motivating factors needed for users to avoid IT malicious threats. The TTAT model is relatively useful in helping general computer users understand and avoid malware threats; however, some obvious gaps have been highlighted in its application within online social networking contexts. Online social networks have unique attributes in terms of user behavior and structural design which should be carefully considered when developing a model for malware threat avoidance for its users.

Due to the complexities of IT security, there exists no single solution that can effectively address all the unique threats faced by various technological platforms, and especially its users. Our work is a hypothetical model drawn from TTAT and a unique attribute of online social networks – Mass interpersonal persuasion (MIP). Similar to the works of Liang & Xue (2009), we suggest the elements that need to be considered in order to motivate users of OSNs to avoid malware attacks. By synthesizing previous works on social influence theory, the theory of persuasion and consumer buying decisions, we rationalize the argument that the mass interpersonal persuasive attribute of a safeguarding measure can effectively affect the avoidance motivation of social network users against IT malicious threats. One of the main contribution of this paper is the proposed Facebook animation video App as a tool to created security awareness for users of online social networks. Although the ideas of our proposed

App have not been empirically validated, we were able to show how the constructs of TTAT-MIP are related to the three levels of the App's architecture which has a huge impact for researchers in IS field. In addition, our findings show a significant contribution for practitioners who intend to develop softwares that has sufficient and coherent theory-base.

In order to empirically validate our theory, we recommend a questionnaire survey to gather quantitative data about the security threat perception of online social network users and a potential safeguarding measure developed through a Facebook animation video APP. The measured items of each constructs in the model should reflect the context of online social networks and then such data could be analysed using structural equation modelling (SEM) technique.

# REFERENCES

Abdullah Algarni, Yue Xu, Taizan Chan, Y.-C.T., 2013. Social Engineering in Social Networking Sites: Affect-Based Model. *International Journal of e-Education, e-Business, e-Management and e-Learning*, 3(6), pp.456–463.

Abrams, R., Pathak, J. & Barrera, O., 2013. Socially Engineered Malware Blocking. , pp.1–18.

Aggarwal, A., 2012. Detection of Spam Tipping Behaviour on Foursquare.

Balasubramaniyan, V.A. et al., A Crow or a Blackbird ?: Using True Social Network and Tweeting Behavior to Detect Malicious Entities in Twitter.

Baltazar, J., Costoya, J. & Flores, R., 2009. The real face of koobface: The largest web 2.0 botnet explained. *Trend Micro Research*, 5(9), p.10.

Bayuk, J. et al., 2011. Malware Risks and Mitigation Report. *Bits a Division of the Financial Services Roundtable*, (June).

Braun, R. & Esswein, W., 2013. Towards a Conceptualization of Corporate Risks in Online Social Networks: A Literature Based Overview of Risks. *Proceedings of the 2013 17th IEEE International Enterprise Distributed Object Computing Conference*.

Bullee, J.W.H. et al., 2015. The persuasion and security awareness experiment: reducing the success of social engineering attacks. *Journal of Experimental Criminology*, 11(1), pp.97–115.

Diffley, S. & Kearns, J., 2011. Consumer behaviour in social networking sites: implications for marketers. *Irish Journal Of …*, pp.47–66. Available at: http://iamireland.ie/wp-content/uploads/2012/05/IJM_30_2_Final_crop.pdf#page=57.

Doostari, M.A. et al., 2013. Anomaly Detection in Cliques of Online Social Networks Using Fuzzy Node-Fuzzy Graph. , 3(8), pp.614–626.

Faghani, M.R., Matrawy, A. & Lung, C.H., 2012. A study of Trojan propagation in online social networks. *2012 5th International Conference on New Technologies, Mobility and Security - Proceedings of NTMS 2012 Conference and Workshops*, pp.6–10.

Fire, M., Goldschmidt, R. & Elovici, Y., 2013. Online Social Networks: Threats and Solutions Survey. , 16(4), pp.1–20.

Fogg, B., 2009. A behavior model for persuasive design. *Proceedings of the 4th International Conference on Persuasive Technology - Persuasive '09*, p.1.

Fogg, B.J. & Hall, C., 2008. Mass Interpersonal Persuasion : An Early View of a New Phenomenon 2 Facebook Makes a New Form of Persuasion Possible 3 A Stanford Course Leverages Mass Interpersonal Persuasion. *Persuasive Technology*, (2008), pp.23–34.

Foster, D. et al., 2009. Social networking sites as platforms to persuade behaviour change in domestic energy consumption. *Communication*.

Gao, H. et al., 2011. Security issues in online social networks. *IEEE Internet Computing*, 15(4), pp.56–63.

Hampton, K.N. et al., 2011. Social networking sites and our lives. *Pew Research Center's Internet & American Life Project*, 47(9), p.85.

Hutter, K. et al., 2013. The impact of user interactions in social media on brand awareness and purchase intention: The case of MINI on Facebook. *Journal of Product and Brand Management*, 22(5), pp.342–351.

Ikhalia, E. & Serrano, A., 2015. A Framework for Designing an Effective Security Awareness System for Online Social Network Users. *European, Mediiterranean & Middle Eastern Conference on Information Systems*, 2015, pp.1–16.

Ikhalia, E. & Serrano, A., 2016. Developing a New Model for the Avoidance of Malware Threats through Online Social Networks. In *15th International Conference WWW/Internet 2016*.

Lee, D., Hosanagar, K. & Nair, H.S., 2014. The Effect of Social Media Marketing Content on Consumer Engagement: Evidence from Facebook. *Working Papers (Faculty) -- Stanford Graduate School of Business*, (Summer 2013), pp.1–51.

Liang, H. & Xue, Y., 2009. Avoidance of Information Technology Threats: A Theoretical Perspective. *MIS Quarterly*, 33(1), pp.71–90.

Lin, K.Y. & Lu, H.P., 2011. Why people use social networking sites: An empirical study integrating network externalities and motivation theory. *Computers in Human Behavior*, 27(3), pp.1152–1161.

McClendon, D., 2012. Perceived susceptibility of cardiovascular disease as a moderator of relationships between perceived severity and cardiovascular health promoting behaviors among female registered nurses. *Dissertation Abstracts International: Section B: The Sciences and Engineering*, 72(7–B), p.3955.

Palmer, D., 2013. Social media malware rising significantly, says McAfee report - 03 Jun 2013 - Computing News. *http://www.computing.co.uk/*. Available at: http://www.computing.co.uk/ctg/news/2272203/social-media-malware-rising-significantly-says-mcafee-report [Accessed June 4, 2015].

Reavis, J., 2012. The Ongoing Malware Threat: How Malware Infects Websites and Harms Businesses — and What You Can Do to Stop It. *Symantec*, p.11.

Sood, A.K., 2011. Chain Exploitation — Social Networks Malware. *ISACA Journal*, 1, pp.1–6. Available at: http://www.cse.msu.edu/~enbody/ISACA_JAN_2011_Chain_Exploitation.pdf.

Sophos, 2014. Internet Security Threat Report , SOPHOS. *Sophos*, pp.1–34.

Stretcher, V. & Rosenstock, I.M., 1997. The Health Belief Model. *Health Behavior and Health Education: Theory, Research and Practice*, pp.31–36.

Thomas, K. & Nicol, D.M., 2010. The Koobface botnet and the rise of social malware? *Proceedings of the 5th IEEE International Conference on Malicious and Unwanted Software, Malware 2010*, pp.63–70.

Tidwell, C.L., 2011. Testing The Impact Of Training With Simulated Scenarios For Information Security Awareness On Virtual Community Of Practice Memebers.

Turkanović, M. & Polančič, G., 2013. On the security of certain e-communication types: Risks, user awareness and recommendations. *Journal of Information Security and Applications*, 18(4), pp.193–205.

Wang, N., Xu, H. & Grossklags, J., 2011. Third-Party Apps on Facebook : Privacy and the Illusion of Control. *Proceedings of the 5th ACM Symposium on Computer Human Interaction for Management of Information Technology. ACM*, p.10. Available at: http://dl.acm.org/citation.cfm?id=2076448.

Wilson, M., Hash, J. & Division, C.S., 2003. Building an Information. , (October).

Yan, G. et al., 2007. Malware Propagation in Online Social Networks : Nature , Dynamics , and Defense Implications Categories and Subject Descriptors. *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security*, pp.196–206.

Zhang, S. et al., 2016. Do you get tired of socializing? An empirical explanation of discontinuous usage behaviour in social network services. *Information & Management*, 53(7), pp.904–914. Available at: http://dx.doi.org/10.1016/j.im.2016.03.006.