Extending Protection Motivation Theory to Understand Security Determinants of Anti-virus Software Usage on Mobiles Devices

Waleed Al-Ghaith

Abstract— THIS study proposes and develops a theoretical model by adopting and extending the protection motivation theory to identify factors affecting mobile's users' anti-virus software adoption by considering subjective norm with threat appraisal and coping appraisal variables which have been rarely examined before. The results show that threat appraisal and coping appraisal variables with subjective norm are able to explain 94% of mobile's users' intention to adopt anti-virus software on their mobile's devices. The study findings show that perceived severity alone explains 50.7% of mobile's users' intention to adopt anti-virus on their mobile's devices followed by subjective norm which explains around 21.3% of intention, and then response cost that has the ability to lessening intention of mobile's users to adopt anti-virus on their mobile's devices by 20.6%. Perceived vulnerability, self-efficacy and response efficacy also have significant positive influence on mobile's users' intention to adopt anti-virus for their mobile's devices by 17.8%, 12.7% and 12% respectively.

Keywords— Antivirus Software, Protection Motivation Theory, Security, Smartphone.

I. Introduction

THIS decade, we have witnessed the evolution in production of mobile handheld devices such as smart phones and tablets in conjunction with emergence of a large variety of mobile operating system vendors, such as Apple, Google, and Microsoft. According to a February 2015 CISCO report "Globally, mobile devices and connections will grow to 11.5 billion by 2019" [1]. Actually, mobile phone penetration rates have reached over 100 percent per capita in most countries [2]. Google announced that more than 1.5 Million new Android-based devices are activated every day [3]. At its 2015 Worldwide Developers Conference (WWDC), Apple CEO Tim Cook says more than 100 billion app downloads from iTunes Store [4].

This growth in mobile usage which have led by an explosive growth in developments of mobile applications was not matched by similar growth in awareness of other important aspects of usage such as security of mobile systems.

According to Symantec, the most popular security firm, mobile users do not use adequate levels of security on their mobile devices as compared to desktops [5]. Moreover, mobile users did not know that antivirus software and other protection methods existed for mobile devices. The Norton Report showed that even with the use of antivirus software in the mobile devices; new platforms were emerging to bypass this security technique, thus mobile users need other security practices to support the antivirus software [5].

Same results have been reported by Trend Labs, another security firm, which found that mobile users did not use antivirus software and, in general, mobile users have a low level of awareness of the security and privacy threats associated with using mobile platforms thus, they did not focus on how to protect their mobiles [6]. Consequently, mobile users' behavior was the crucial factor contributing to mobile' lack of security [6].

Scholars are increasingly recognizing that people play essential role in the IS security [7], [8]. Scholars perceived people or IS users as weakest link in the security of a system, since that IS user can be tricked into doing something insecure like installing malicious software which causes that the security of an entire system can be compromised [7], [8]. Thus, hackers and cybercriminals are fully recognizing the fact that users represent the weakest link in the security chain and they are routinely using social engineering tactics to coax users into installing malwares or stopping technical security controls [9].

Given this reality, we need to understand how mobile users perceive and respond to their mobile security risks through installing and using antivirus software to protect them. This raises the following research question -What factors that effecting mobile's users' intention to adopt anti-virus software on their mobile's devices? The rest of this paper answers this question by presenting and extending the Protection Motivation Theory (PMT) as a potential theory to explain differences in security behavior, particularly using antivirus software on mobiles. In following section, we review viruses and infection strategies which raised security concerns and present the study theoretical framework which includes the PMT, as a main

Waleed Al-Ghaith is with Computer Science Department, Shaqra University, Riyadh, Saudi Arabia (corresponding author; e-mail: w.alghaith@su.edu.sa).

theory that guides the development of the study model. Moreover, section 2 also presents the proposed hypotheses along with the study model. In section 3, the methods of analysis are presented. The results of the study are then presented in Section 4. Thereafter, in section 5, the Al-ghaith's equation [10] has been used to calculate the participation of every model's construct in the model's explanatory power. The results are presented and discussed in Section 5. Section 6 is devoted to highlight the implications of the current study to theory and practice.

II. 2. Literature review and theoretical framework

A. Viruses and Infection Strategies

Viruses can be classified into two different classes: first, viruses that killing computers by causing a serious damage to operating systems by deleting operating system files, and then replicating themselves to other systems. Second, viruses that replicating themselves to any program files by altering their tasks to perform a certain functions and then replicating themselves to other systems via Internet, email or storage devices.

Viruses, in general, contain three core components: first, a replication mechanism that allows viruses to duplicate themselves and move to other computers. Second, a task or group of tasks that execute on a computer to perform a certain functions such as causing damage or altering setting or sending data. Third, a trigger that is designed to execute the previous two components: the replication mechanism and the task of the viruses [11].

Mobiles have more security issues than traditional PCs due to that mobiles equipped by more sensors and communication and networking functions compared to traditional PCs such as Wi-Fi, 3G or 4G, Bluetooth, EDGE, the SMS/MMS messaging system, and NFC in addition to the mobiles' apps. Thus, viruses programs have a variety of channels to enter the mobile device and distribute themselves, however, there are two main approaches are using as a distribution techniques. First one, self-propagation that virus can use different strategies to automatically install the payload into a device. Second, using social engineering to exploit the security unawareness of users to coax them into manually installing the application [9].

Suarez-Tangil, et al., [12] identified six different distribution vectors that can be used to infect devices: First, Market to Device (M2D): this happen if user install malicious application to his device. This malicious application has been uploaded to a market by an attacker with a stolen identity to trick markets to accept such malicious apps. Users get infected when they install this malicious application to their devices. Second, Application to Device (A2D): in this technique, an attacker use vulnerable application to spread itself such as Facebook to post links with a copy of the malicious code. Third, Web-browser to Device (W2D): this technique similar to A2D, however, malware can be downloaded instead of using a specific application. Fourth, SMS to Device (S2D): an attacker uses SMS or MMS to distribute a malicious payload. Fifth, Network to Device (N2D): here attackers rely on network to exploit vulnerabilities or misconfigurations of the device. Network to Device (N2D) also can be done by two techniques: a. Device to Device (D2D) when infection is done by another mobile device, and Cloud to Device (C2D): When infection is done by a powerful computer such as a workstation or a server. Sixth, USB to Device (U2D): malware can transfer from an infected PC to the mobile device through a port (typically a cable) when they connected to each other [12].

B. Protection Motivation Theory

Human' fear is an emotion or passion motivated by the expectation of evil or the worry of impending danger; as response of fear, individuals adopt an emotional state protecting one against danger or a motivational state leading one away from something [13]. Scholars found that this response of fear, which is widely renamed as a fear appeal, can change attitudes and, subsequently, change behavior. Rogers [13] proposed Protection motivation theory (PMT) in order to provide conceptual clarity in the area of fear appeals and to address the link between fear appeals and attitude change. PMT defined the components of a fear appeal with the aim of determining the common variables that produced attitude change. According to PMT, each component of a fear appeal would initiate a corresponding mental or cognitive mediating process. These processes have an impact on protection motivation, in the form of an intention to adopt the recommended behavior [13]. In 1983, Rogers showed that these cognitive mediational processes could be categorized into two forms: (1) threat appraisal and (2) coping appraisal [14].

Threat appraisal means the process of estimating the components of a fear appeal associated with individual's perception of threats (or danger). The PMT variables that form threat appraisal are perceived vulnerability and perceived severity. Perceived vulnerability is associated with an individual's evaluation of his probability of being exposed to the critical threat (or danger). Thus, when a person perceives high vulnerability; the probability of adopting the protective behavior is increased [14], [15], [16]. Perceived severity evaluates how serious the individual believes that negative consequences resulting from the threat would harm his own life. According to the PMT, the perceived severity variable has a positive significant effect on the individual's intention to follow protective actions [14], [15], [17].

Coping appraisal is associated with recommended preventive response, and evaluates an individual's ability to cope with and avoid the appraised threat. Coping appraisal is a summation of three appraisals: (1) response efficacy, (2) self-efficacy, and (3) any costs of adopting the recommended preventive response such as inconvenience, expense, and difficulty. Response efficacy means the beliefs regarding whether the recommended preventive response will be effective in avoiding or reducing threat. Self-efficacy is the belief that one is or is not capable of performing the recommended preventive response. Whereas, response costs means the beliefs regarding how costly performing the recommended preventive response will be to the individual [14].

C. Hypotheses development

This study proposes and develops a theoretical model by adopting and extending PMT. We use PMT as a core theoretical foundation to empirically test why individuals adopt anti-virus software for their mobile's devices. The research hypotheses are formulated and discussed in this section.

1) Security Threat Appraisal

Security threat appraisal means the process of estimating the components of a fear appeal associated with individual's perception of security threats (or danger). According to the PMT, two variables (perceived severity and perceived vulnerability) form this threat appraisal. The perceived severity variable has a positive significant effect on the individual's intention to follow protective actions [14], [15], [18]. It is supposed that the more seriously an individual perceives the level of the negative consequences resulting from current inadequate actions, the more he adopts recommended adequate actions. Similarly, we expect that mobile's users perceive viruses as a severe threat for their mobile systems and its negative consequences would extend to harm their life. For instance, viruses or malware such "DroidKungFu" for Android based mobiles and "FindAndCall" for iPhone mobiles are designed to steal a range of personal information stored in the mobile devices and transfer it through the network to a remote server [12]. In addition to a severe threat that would happened with "DroidKungFu" and FindAndCall", the worst can be seen in "Spybubble", "Nickispy", and "FinSpyMobile2" viruses, which work on Android based mobiles, with the ability to monitor, record and transfer the mobile device's location, ongoing and past phone calls and SMS logs [12], [19]. Given these threats, mobile's users are expected to intend to adopt anti-virus software for their devices.

Scholars found that perceived severity significantly influence the intention to adopt recommended adequate actions. In a study conducted to investigate factors that affecting small and medium-sized business (SMB) executives' decision to adopt anti-malware software for their organizations, Lee and Larsen found that perceived severity was the most influential factor, showing that the degree of expected harm from malware attacks is the strongest motivator of the software adoption [20]. Thus, the following hypothesis is proposed:

H1: Perceived severity positively influences mobile's users' intention to adopt anti-virus software for their mobile's devices.

The second PMT variable that form threat appraisal is perceived vulnerability [14]. Perceived vulnerability is associated with an individual's evaluation of his probability of being exposed to the critical threat (or danger). Thus, when a person perceives high vulnerability; the probability of adopting the protective behavior is increased [14], [15], [16]. Prior studies have found the Perceived vulnerability has a significant effect on the intentions to adopt protective behaviors [16], [20]. In the same way and in line with purpose of this study, it is assumed that mobile' users are expected to seriously consider the adoption of anti-virus software for their mobile's devices when they perceive that their mobile's devices have a high probability of being exploited by virus or malware attacks. Thus, the following hypothesis is proposed:

H2: Perceived vulnerability positively influences mobile's users' intention to adopt anti-virus software for their mobile's devices.

2) Security Coping Appraisal

Security coping appraisal is associated with recommended preventive response, and evaluates an individual's ability to cope with and avoid the appraised security threat. In this study, security coping appraisal is a summation of three appraisals: (1) response efficacy, (2) self-efficacy, and (3) any costs of adopting the recommended preventive response such as inconvenience, expense, and difficulty. Security response efficacy means the beliefs regarding whether the recommended preventive response will be effective in avoiding or reducing security threat. Anti-virus software has been reported as an effective and efficient solution for detecting and preventing virus threats. Thus, in this study, it is assumed that installing anti-virus software would give mobile's users a confidence that this solution will prevent or mitigate the security threat. Whereas, self-efficacy refers to an individual's belief in his or her own capability to perform a specific task within a particular domain [21], [22]. It is assumed that individuals with high confidence in their ability to conduct a recommended action, are more likely to adopt the action. Thus, this study proposes that the more mobile's users are convinced regarding their capability to learn, implement, and use anti-virus software, the stronger their intention to adopt anti-virus software for their mobile's devices. Prior studies have found that both the response efficacy and self-efficacy have a significant effect on the intentions to adopt protective behaviors. LaRose et al., [23] found that self-efficacy and response efficacy were most related to intentions to engage in safe online behavior [23]. Johnston and Warkentin investigate, in their study, the influence of fear appeals on the compliance of end users with recommendations to enact specific individual computer security actions toward the mitigation of threats. Results suggest self-efficacy, response efficacy influence end-user behavioral intentions [24]. Thus, the following hypotheses are proposed:

H3: Response efficacy positively influences mobile's users' intention to adopt anti-virus software for their mobile's devices.

H4: Self-efficacy positively influences mobile's users' intention to adopt anti-virus software for their mobile's devices.

According to PMT, cost of adopting the recommended response or the painfulness of the amount of work involved in implementing the recommended response has a significant negative impact on adaptive behaviors. Actually, individuals tend to not adopt the recommended response if they feel inconvenience or have to dedicate a high amount of effort, money, or time [20]. Scholar have found that response cost negatively influences individuals' intention to adopt adaptive behaviors. Wu and Wang investigate what factors behind user mobile commerce acceptance; they assert that cost is one of the important inhibitors of behavioral intention to use mobile commerce, and this has a significantly negative direct effect on behavioral intention to use [25]. Same findings have been confirmed by Reardon and Davidson; they examined factors contributing to low adoption of health information technologies such as electronic medical records and found that cost is one of the greatest inhibitors of behavioral intention to adopt electronic medical records [26]. In this study, it is assumed that same negative impact is expected to be found in anti-virus software adoption. Thus, mobile's users are less likely to adopt anti-virus software when they perceive high cost to adopt and operate that software and the following hypothesis is proposed:

H5: Response cost negatively influences mobile's users' intention to adopt anti-virus software for their mobile devices..

3) *Subjective norm*

The subjective norm can be defined as individuals' perception of social pressure particularly from their important referents to perform or not perform a behavior [27], [28]. In other words, persons usually become involved in actions or an object when they have a positive attitude toward it and when they believe that important individuals think they should do so [28]. The positive relation between the individual's intention to perform certain behavior and subjective norm has been confirmed by many IS theories such as the theory of reasoned action (TRA) [27] and the theory of planned behavior (TPB) [28]. Accordingly, a positive relationship between subjective norms and behavioral intentions has hypothesized in many prior studies and much support has been found. Peace, Galletta, and Thong, in their attempt to understand software piracy by individuals in the workplace, they assert that individual subjective norms was significant precursors to the intention to illegally copy software [18]. Similar findings have been confirmed by another study conducted by Chen, Huang and Chou to identify salient determinants that expand the intention to use mobile videophones, the findings show that the flow and the subjective norm are positively related to the expanded intention to use mobile videophones [29]. Hsien-Tung and Bagozzi, in their study to build and test a theory regarding member contribution behavior in virtual communities, found that subjective norm has a positive impact in encouraging contribution behavior [30]. Moreover, Lai, Chen, and Chang in their pursuit to determinant influential factors of knowledge seeking in professional virtual communities, they found that Knowledge-seeking intention is based on the attitude towards knowledge seeking and the subjective norm of knowledge seeking [31]. In Al-ghaith' recent study to examine individuals' intentions and behavior on Social Networking Sites (SNSs), he confirmed that subjective norm has positive significant direct effects on intention to use SNSs [10].

Although the information systems adoption literature and in the discipline theories suggest that subjective norm has a significant effect on individuals intentions to adopt behavior. Scholars have paid less attention to subjective norm impact in their theoretically based research in behavioral security. This study contributes to the behavioral security research by examining impact of subjective norm on mobile's users' intention to adopt anti-virus software for their mobile devices. Thus, we hypothesize the following:

H6: Subjective norm positively influences mobile's users' intention to adopt anti-virus software for their mobile's devices.

4) *User behavioral intention and Usage Behavior*

Behavioral intention has been seen as a dominant factor in predicting the decision to perform a particular behavior for many information systems theories such as the Theory of reasoned action model (TRA), the Theory of Planned Behavior Model (TPB), the Decomposed Theory of Planned Behavior Model (DTPB) and the Technology Acceptance Model (TAM). All these models have been widely and successfully applied in a range of situations and in a variety of subject areas for predicting and understanding the performance of actual behavior [32], [33], [34], [10], [35] and all of them proposed that behavioral intention has a significant direct influence on an actual behavior. As with prior studies, this study predicts that when mobile's users intend to adopt anti-virus software, they are more motivated to purchase or download and install the software which leads to the software adoption. Thus, the following hypothesis is proposed:

H7: Mobile's users' intention to adopt anti-virus software for their mobile's devices is positively related to actual adoption of anti-virus software on their mobile's devices.

III. Methodology

A. *Measurement*

Defining the constructs that study attempt to measure, and then select proper measuring methods to measure those constructs is critical and has a significant influence on the accuracy of findings [36]. In order to test the research hypotheses, the researcher developed the survey instrument. The items used in the survey instrument to measure the constructs were identified and adopted from previous research; particularly from the Communication field and IS research, with the aim to ensure the face (content) validity of the scale used. The items were widely used in the majority of previous studies indicating potential subjective agreement among researchers that these measuring instruments logically appear to reflect accurate measure of the constructs of interest. Table 1 lists the items developed for each construct in this study as well as set of prior studies where these items have been adopted from.

Table 1. List of items by construct

Construct	Items	Adapted from
Perceived Severity (PS)	How strongly do you disagree or agree with the following statements? PS1. Viruses pose a severe security risk to your mobile systems. PS2. Viruses can transmit sensitive data to third parties (e.g., passwords, usernames, and customer information). PS3. Viruses can allow remote access to your mobile. PS4. Viruses can be used to download and install malicious applications.	[37].
Perceived Vulnerability (PV)	How likely is viruses to affect your mobile in the following ways? PV1. Transmit sensitive data to third parties. PV2. Allow access to remote attackers. PV3. Install malicious applications.	[17].
Response Efficacy (RE)	RE1. Installing anti-virus software will successfully prevent viruses' attacks. RE2. Anti-virus software is the best solution for counteracting problems caused by viruses. RE3. If you install anti-virus software on your mobiles, you can minimize the threat of viruses.	[17].
Subjective Norm (SN)	SN1. Your friends would think that you should install and use anti-virus software on your mobile's device. SN2. Your colleagues/classmates would think that you should install and use anti-virus software on your mobile's device. SN3. People who are important to you would think that you should install and use anti-virus software on your mobile's device.	[33], [10], [35].
Self-efficacy (SE)	SE1. It is easy for you to install and manage anti-virus software on your mobile's device. SE2. You can perform system updates on anti-virus software by yourself. SE3. You have the capability to solve possible system requirements or problems during the installation and operation of anti-virus software. SE4. You would be able to use anti-virus software even if you had never used a system like it before.	[33], [10].
Response cost (RC)	RC1. Anti-virus software is expensive to purchase and operate. RC2. You have to upgrade you mobile's system to install anti-virus software. RC3. Anti-virus software can slow down your mobile's system.	[38], [20].
Behavioral intention (BI)	BI1. You intend to install and use anti-virus software on your mobile's device in next three months. BI2. You expect that your use of the anti-virus software to continue in the future.	[33], [10], [35].
Anti-virus software Usage (US)	US1. On average, each week you scan your mobile's device by using anti-virus software often. US2. Every morning, you check your anti-virus software	[39], [10], [35].

B. Data Collection Procedures

Data for this study were collected in four stages (3 months apart), from samples stratified into gender groups, by means of a survey conducted in Saudi Arabia in 2013. This type of sampling technique has been selected due to the difficulty of drawing an actual representative sample in Saudi Arabia. Most houses in Saudi Arabia have not their own mail boxes and postal services are not available for every house. Moreover, due to the conservative nature of Saudi Arabian society, it is inappropriate to approach females or talk with them. Therefore, stratified samples were drawn from a variety of areas in the country and female relatives were engaged to distribute questionnaires to the female strata besides using electronic means to guarantee reaching females as well as males. The survey questionnaires were distributed to 2500 participants (1250 male and 1250 female). A total of 832 responses were received from male participants and 717 from female participants. After checking the data for validity, 1523 were deemed fit for use in the analysis.

IV. Data analysis and results

A. Reliability and validity

A reliability and internal consistency have been tested by using data obtained from the pilot study of each construct in the instrument. The results shows that the alpha values ranged from .963 to .997 with an overall alpha value of .965. Results of the Cronbach's alpha reliability of constructs in the study have been presented in table 2. The results indicated that all constructs of the model were reliable. Hence, the internal consistency of the instrument was acceptable.

In order to examine the adequacy of the study sample and the validity of the study instrument, this study conducts Kaiser–Meyer–Olkin (KMO) and principal component factor analysis. As the value of KMO was 0.919 as in Table3, the study sample was considered adequate and the appropriateness of using principal component factor analysis on the collected data was assured.

Table 2. Cronbach's Alpha Reliability of Constructs

Construct	Number of Items	Cronbach's Alpha
Perceived Severity (PS)	4	.995
Perceived Vulnerability (PV)	3	.985
Response Efficacy (RE)	3	.979
Subjective Norm (SN)	3	.970
Self-efficacy (SE)	4	.994
Response cost (RC)	3	.997
Behavioral intention (BI)	2	.988
Anti-virus software Usage (US)	2	.963
Overall alpha value	24	.965

Table 3. KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.919
Bartlett's Test of Sphericity	Approx. Chi-Square	25232.802
	df	28
	Sig.	.000

Construct validity was measured by conducting factor analysis to calculate a principal components analysis with a Varimax rotation. This analysis helped in evaluating the convergent and discriminant validity of items. The convergent validity was evaluated by examining whether items of a variable converged together on a single construct [40], and whether the factor loading for every item was > 0.45, as suggested by Comrey and Lee [41]. Comrey and Lee [41] suggested that loadings in excess of 0.45 could be considered fair, whereas it might be considered as good if loadings were greater than 0.55, and those of 0.63 very good, and those of 0.71 as excellent. The discriminant validity was evaluated by examining the cross loading of items on different factors. As the factor pattern shows in Table 4, loadings on the target factor are in the excellent range (21 out of 24), and very good (3 out of 24). As Table 4 shows, no weak loading was found indicating the validity of constructs applied in this study.

Table 4. Factor Analysis of Items Sorted by Construct **(Rotated Component Matrix (a))**

	Component					
	1	2	3	4	5	**Its assessment**
PS1	**.728**	.561	.340	.104	-.010	*Excellent > 0.71*
PS2	**.779**	.474	.376	.070	.075	*Excellent > 0.71*
PS3	**.783**	.472	.372	.064	.074	*Excellent > 0.71*
PS4	**.781**	.470	.372	.065	.068	*Excellent > 0.71*
PV1	.499	**.752**	.291	.082	.226	*Excellent > 0.71*
PV2	.569	**.674**	.333	.096	.281	*Very good > 0.63*
PV3	.580	**.684**	.327	-.015	.229	*Very good > 0.63*
RE1	.402	**.845**	.248	.104	.095	*Excellent > 0.71*
RE2	.495	**.752**	.300	.132	.188	*Excellent > 0.71*
RE3	.505	**.767**	.296	-.031	.107	*Excellent > 0.71*
SN1	.346	**.879**	.197	.139	-.148	*Excellent > 0.71*
SN2	.451	**.791**	.265	.179	-.037	*Excellent > 0.71*
SN3	.467	**.805**	.257	-.034	-.131	*Excellent > 0.71*
SE1	**.726**	.580	.317	.063	-.052	*Excellent > 0.71*
SE2	**.771**	.506	.341	.027	.018	*Excellent > 0.71*
SE3	**.782**	.491	.345	.033	.033	*Excellent > 0.71*
SE4	**.782**	.493	.345	.012	.018	*Excellent > 0.71*
RC1	-.323	-.254	**-.905**	-.058	-.028	*Excellent > 0.71*
RC2	-.330	-.247	**-.905**	-.056	-.023	*Excellent > 0.71*
RC3	-.325	-.251	**-.907**	-.059	-.026	*Excellent > 0.71*
BI1	**.711**	.568	.348	.150	-.010	*Excellent > 0.71*
BI2	**.756**	.486	.389	.115	.054	*Excellent > 0.71*
US1	**.620**	.502	.353	.469	.018	*Very good > 0.63*
US2	**.730**	.378	.392	.329	.058	*Excellent > 0.71*

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.
a Rotation converged in 6 iterations.

B. Hypotheses testing

Assuming that the decision of mobile's users to adopt anti-virus software for their mobile's devices is strongly influenced by both threat and coping appraisals, this study proposes and develops a theoretical model by adopting and extending PMT (see Figure 1).

As shown in Figure 1, the study's model can be formed through test of 7 hypotheses. These hypotheses identify the relation between factors as independent variables that influence mobile's users' adoption behavior. Each accepted hypothesis represents an explanation of usage behavior as dependent variables. Explanations are nomothetic and advance through deductive reasoning. The simple correlation amongst all the study variables was conducted using Pearson's correlation analysis as shown in Table 5. As variables showed significant correlations ($p \leq 0.01$), we then utilized the regression model to test multicollinearity by examining collinearity statistics; i.e. Variance Inflation Factor (VIF) and tolerance.

To determine whether any multicollinearity effects existed, we checked whether there was any warning message produced by the AMOS output that signalled a problem of multicollinearity. The results showed that there was no evidence of multicollinearity. The potential problem of multicollinearity can be further examined formally in the context of regression analysis.

In Table 6, the tolerance values ranged from 0.865 to 0.310. One way to quantify collinearity is with variance inflation factors (VIF). Although a variance inflation factor (VIF) that is less than or equal to 10 (i.e. tolerance >0.1) is commonly suggested (Asher, 1983; lee, 2009). In this study, a variance inflation factor (VIF) greater than 4 is considered to indicate a serious problem of multicollinearity. However, as shown in Table 6, there were no VIF values over 4 in the model; since the VIFs values ranged from 1.157 to 3.229. Thus there was no evidence of multicollinearity.

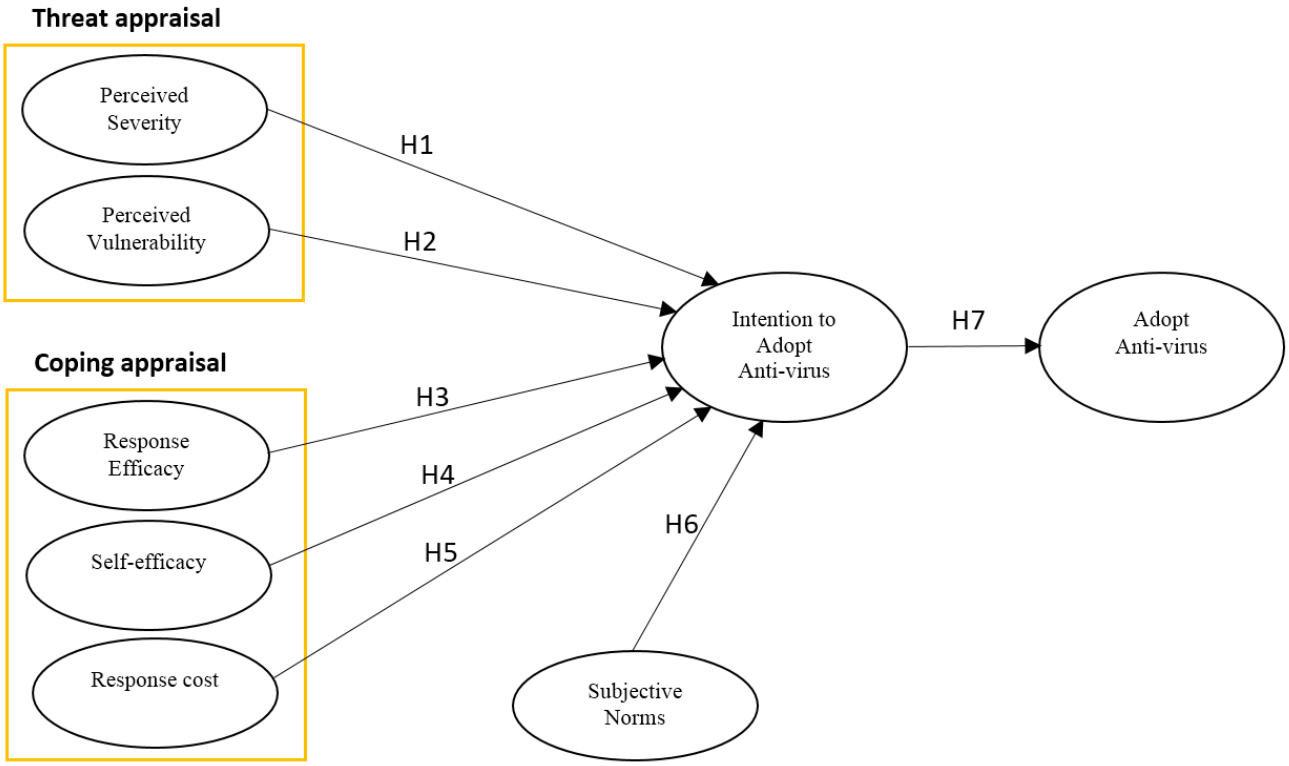

Figure 1. The study model

Table 5. Correlation analysis amongst the variables.

	US	BI	SN	RC	SE	RE	PV
BI	.923*						
SN	.801*	.855*					
RC	-.688*	-.727*	-.593*				
SE	.890*	.966*	.978*	-.681*			
RE	.821*	.883*	.958*	-.624*	.908*		
PV	.844*	.910*	.929*	-.650*	.929*	.966*	
PS	.903*	.979*	.875*	-.693*	.984*	.903*	.930*

US: Usage, BI: Behavioral intention, SN: Subjective Norm, RC: Response cost, SE: Self-efficacy, RE: Response Efficacy, PV: Perceived Vulnerability, PS: Perceived Severity.
* *p ≤ 0.01*

Table 6. Multicollinearity test

Dependent variable	Path direction	Independent variables (predictors)	Collinearity Statistics	
			Tolerance	VIF
Usage	←	Intention	.424	2.357
Intention	←	Perceived Severity (PS)	.318	3.143
Intention	←	Perceived Vulnerability (PV)	.865	1.157
Intention	←	Response Efficacy (RE)	.850	1.176
Intention	←	Self-efficacy (SE)	.310	3.229
Intention	←	Response cost (RC)	.516	1.936
Intention	←	Subjective Norm (SN)	.439	2.276

After assuring that necessary requirements are all adequately met, the study hypotheses were tested using multiple regression analysis.

First, “Intention” was regressed on “Usage”. As in Fig. 2, it was found that “Intention” (β = 0.923, Standardized path coefficient, $p < 0.05$) is significantly and positively related to “Usage” (adjusted R^2=0.85) (see Table 7, Table 8 and Fig. 2). Thus, H7 is supported.

Table 7 Coefficients for Proposed model

Dependent variable	Path direction	Independent variables (predictors)	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
			B	Std. Error	Beta		
Usage	←	Intention	.860	.009	.923	93.493	.000
Intention	←	Perceived Severity (PS)	.610	.025	.560	24.788	.000
Intention	←	Perceived Vulnerability (PV)	.221	.024	.197	9.089	.000
Intention	←	Response Efficacy (RE)	.150	.009	.133	15.837	.000
Intention	←	Self-efficacy (SE)	.148	.016	.141	9.147	.000
Intention	←	Response cost (RC)	-.265	.027	-.228	-9.696	.000
Intention	←	Subjective Norm (SN)	.275	.019	.235	14.833	.000

P values less than 0.05 were considered statistically significant

Table 8. Standardized Regression Weights

Criterion variable	Path direction	Criterion variable predictors	Estimate	(Significance)
Usage	←	Intention	.923	Significant
Intention	←	Perceived Severity (PS)	.560	Significant
Intention	←	Perceived Vulnerability (PV)	.197	Significant
Intention	←	Response Efficacy (RE)	.133	Significant
Intention	←	Self-efficacy (SE)	.141	Significant
Intention	←	Response cost (RC)	-.228	Significant
Intention	←	Subjective Norm (SN)	.235	Significant

Thereafter, the six independent variables (i.e. “Perceived Severity”, “Perceived Vulnerability”, “Response Efficacy”, “Self-efficacy”, “Response cost” and “Subjective Norm”) were regressed on “Behavioral Intention”. Results, as in Fig. 2, indicate that all six variables are significantly related to “Behavioral Intention” (adjusted R^2=0.94): “Perceived Severity” (β = 0.560, Standardized path coefficient, $p < 0.05$), “Perceived Vulnerability” (β = 0.197, Standardized path coefficient, $p < 0.05$) , “Response Efficacy” (β = 0.133, Standardized path coefficient, $p < 0.05$) , “Self-efficacy” (β = 0.141, Standardized path coefficient, $p < 0.05$) , “Response cost” (β = -0.228, Standardized path coefficient, $p < 0.05$) and “Subjective Norm” (β = 0.235, Standardized path coefficient, $p < 0.05$) (see Table 7, Table 8 and Fig. 2). Thus, H1, H2, H3, H4, H5 and H6 are supported.

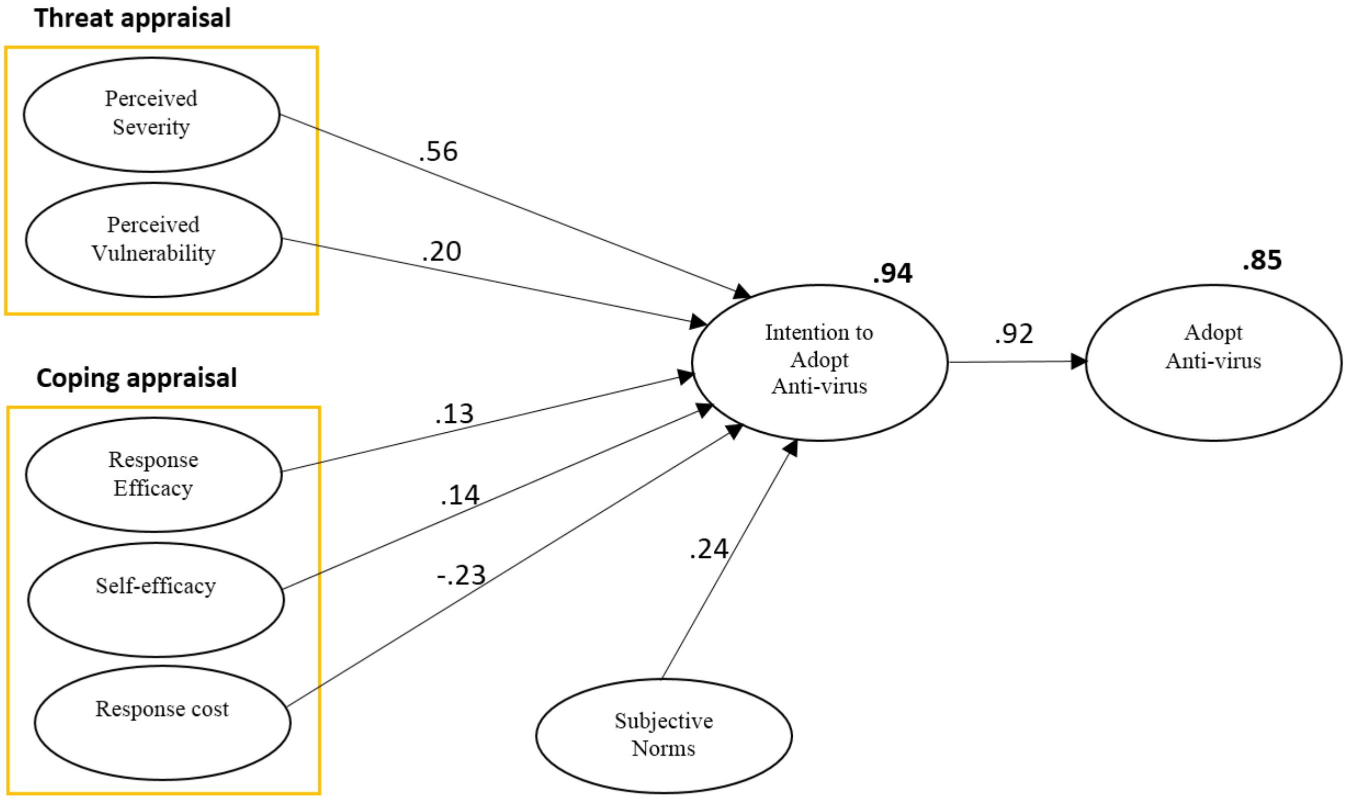

Figure 2. The study model (Results).

V. Discussion

This study proposes and develops a theoretical model by adopting and extending PMT to include subjective norm as a cognition, representing a person's perception of social pressure to perform or not perform a behavior under consideration. The study model investigate the factors affecting mobile's users' anti-virus software adoption. The study's findings show that a significant amount of variance in mobile's users' anti-virus software adoption was explained by the proposed model. All the research hypotheses are supported. Threat appraisal and coping appraisal variables were found to significantly affect mobile's users' anti-virus software adoption intention.

This suggests that mobile's users' anti-virus software adoption decision is effected by both the level of negative consequences from virus attacks and mobile's systems vulnerability to the attacks, as well as magnitude of beliefs regarding whether the installing and using anti-virus software, as a recommended preventive response, will be effective in avoiding or reducing security threat, degree of mobile's users beliefs regarding their capability to learn, implement, and use anti-virus software and the expected costs and consequences associated with adopting anti-virus software.

The results also show that threat appraisal and coping appraisal variables with subjective norm are able to explain the 94% of mobile's users' "intention" to adopt anti-virus software on their mobile's devices (see Figure 2).

Waleed Al-ghaith, in his study, developed an equation to calculate the participation of every model's construct in the model's explanatory power [10].

$$\boldsymbol{A_x} = \frac{\boldsymbol{\beta_x}^{\mathbf{2}}}{\sum_{\boldsymbol{k=1}}^{\boldsymbol{n}} \boldsymbol{\beta_x}^{\mathbf{2}}} \times \boldsymbol{R_{PC}}^{\mathbf{2}}$$

Where:

$\boldsymbol{A_x}$ = Participation of variable A_x in a model' explanatory power

$\boldsymbol{\beta_x}^{\mathbf{2}}$= Square of beta coefficients or standardized coefficients of variable

$\mathrm{R_{PC}}^2$= Model' explanatory power (perceived privacy concerns)

$\sum_{\boldsymbol{k=1}}^{\boldsymbol{n}} \boldsymbol{\beta_x}^{\mathbf{2}}$= Total of causal effects for the model's constructs

This study adopts the above equation to calculate the participation of each constructs and their antecedents in the model's explanatory power and to calculate rate of participation of every antecedents in their constructs' explanatory power.

The equation has been applied on the antecedents of the "Intention" to adopt anti-virus, the results have been summarized in Table 9. The result shows that "Perceived Severity" alone explains 50.7% of mobile's users "Intention" to adopt anti-virus on their mobile's devices followed by "Subjective Norm" which explains around 21.3% of "Intention", and then "Response cost" that has the ability to lessening "intention" of mobile's users to adopt anti-virus on their mobile's devices by 20.6%. "Perceived Vulnerability", "Self-efficacy" and "Response Efficacy" also have significant positive influence on mobile's users "Intention" to adopt anti-virus for their mobile's devices by 17.8%, 12.7% and 12% respectively.

Table 9. Participation of Intention's variables in its explanatory power

Antecedents	Intention to Adopt Anti-virus
Perceived Severity	50.7%
Subjective Norm	21.3%
Response cost	-20.6%
Perceived Vulnerability	17.8%
Self-efficacy	12.7%
Response Efficacy	12%
Total	94%

As aforementioned, perceived severity alone explains 50.7% of mobile's users "Intention" to adopt anti-virus on their mobile's devices, which indicating that perceived severity was the most influential factor and degree of harm that would happen as a result to the virus infection becomes the strongest motivator for mobile's users to adopt anti-virus software on their mobile's devices. This finding is consistent with Lee and Larsen study which found that perceived severity was the most influential factor, showing that the degree of expected harm from malware attacks is the strongest motivator of the software adoption [20].

The study findings also show that "Subjective Norm" was the second strongest factor by its ability to explain around 21.3% of mobile's users "intention" to adopt anti-virus on their mobile's devices, which indicating that degree of interpersonal pressure that caused by the felt expectations held by specific referents and the motivations to comply with their expectations is the second strongest motivator for mobile's users to adopt anti-virus software on their mobile's devices. In other words, mobile' users usually tends to install and use anti-virus software on their mobile's devices when they perceive important individuals do so. This result is consistent with most prior studies in other context of the information systems adoption literature and in the discipline theories which suggest that subjective norm has a significant effect on individuals intentions to adopt behavior (see [29], [30], [31], [10]). Scholars have paid less attention to subjective norm impact in their theoretically based research in behavioral security. This study contributes to the behavioral security research by showing that subjective norm has a significant impact on mobile's users' intention to adopt anti-virus software for their mobile devices.

The study findings also show that "Response cost" has the ability to lessening "intention" of mobile's users to adopt anti-virus software on their mobile's devices by 20.6%. Actually, individuals tend to not adopt the recommended response if they feel inconvenience or have to dedicate a high amount of effort, money, or time [20]. The significant negative influence of response cost on "intention" of mobile's users to adopt anti-virus software on their mobile's devices indicates that there is a need to develop different versions of anti-virus software to comply with the diversity of mobiles' systems requirements and not deteriorate mobile operating systems' performance which will help reduce the mobile's users' concerns regarding anti-virus software usage. This finding is consistent with most prior studies in other context of the information systems adoption literature such as Wu and Wang study that asserts that cost is one of the important inhibitors of behavioral intention to use mobile commerce, and this has a significantly negative direct effect on behavioral intention to use [25]. Same findings have been confirmed by Reardon and Davidson; they examined factors contributing to low adoption of health information technologies such as electronic medical records and found that cost is one of the greatest inhibitors of behavioral intention to adopt electronic medical records [26].

"Perceived Vulnerability", "Self-efficacy" and "Response Efficacy" also have significant positive influence on mobile's users "intention" to adopt anti-virus for their mobile's devices by 17.8%, 12.7% and 12% respectively.

The influence of perceived vulnerability was relatively weaker than expected however it still has a significant effect on intention" of mobile's users to adopt anti-virus software on their mobile's devices. The result means that mobile' users are expected to seriously consider the adoption of anti-virus software for their mobile's devices when they perceive that their mobile's devices have a high probability of being exploited by virus or malware attacks. This finding is consistent with most prior studies that have shown that when a person perceives high vulnerability; the probability of adopting the protective behavior is increased, which means that perceived vulnerability has a significant effect on the intentions to adopt protective behaviors [16], [20].

The significant effect of self-efficacy represents that more mobile's users are convinced regarding their capability to learn, implement, and use anti-virus software, the stronger their intention to adopt anti-virus software for their mobile's devices. In other words, mobile's users are willing to adopt anti-virus software for their mobile's devices when they are confident in their ability to adopt and operate it.

Response efficacy also has strong impact on adoption intention, with its 12% ability to explain mobile's users' intention to adopt anti-virus software for their mobile's devices. In other words, the result indicating that mobile's users are highly motivated to adopt anti-virus software when they predict high expected returns of adopting the recommended protective systems. Anti-virus software has been reported as an effective and efficient solution for detecting and preventing virus threats, thus, it is assumed that installing anti-virus software would give mobile's users a confidence that this solution will prevent or mitigate the security threat. These results are in line with LaRose et al., [23] and Johnston and Warkentin [24]'s studies that have found that both the response efficacy and self-efficacy have a significant effect on the intentions to adopt protective behaviors. LaRose et al., [23] found that self-efficacy and response efficacy were most related to intentions to engage in safe online behavior [23]. Johnston and Warkentin investigate, in their study, the influence of fear appeals on the compliance of end users with recommendations to enact specific individual computer security actions toward the mitigation of threats. Results suggest self-efficacy, response efficacy influence end-user behavioral intentions [24].

The results also show that "Intention" ($\beta = 0.923$, Standardized path coefficient, $p < 0.05$) is significantly and positively related to "Usage" (adjusted R^2=0.85), indicating intention was the only significant variable affecting adoption, which means that when mobile's users intend to adopt anti-virus software, they are more motivated to purchase or download and install the software which leads to the software adoption. This result is consistent with many information systems theories, that have been widely and successfully applied in a range of situations and in a variety of subject areas for predicting and understanding the performance of actual behavior , such as the Theory of reasoned action model (TRA), the Theory of Planned Behavior Model (TPB), the Decomposed Theory of Planned Behavior Model (DTPB) and the Technology Acceptance Model (TAM), that see behavioral intention as a dominant factor in predicting the decision to perform a particular behavior ([32], [33], [34], [10], [35]).

VI. Implications for Theory and Practice

A. Implications for theory and research

Theoretically, this study proposes and develops a theoretical model by adopting and extending PMT to include subjective norm as a cognition, representing a person's perception of social pressure to perform or not perform a behavior under consideration. The study model also identify factors affecting mobile's users' anti-virus software adoption by considering threat appraisal and coping appraisal variables which have been rarely examined before. The study's findings show that a significant amount of variance in mobile's users' anti-virus software adoption was explained by the proposed model. It suggests that the model expansion by incorporating subjective norm factor was valuable exploration. Further, the results also show that threat appraisal and coping appraisal variables with subjective norm are able to explain the 94% of mobile's users' "intention" to adopt anti-virus software in their mobile's devices (see Figure 2).

From a researcher's perspective, this study demonstrated that perceived severity alone explains 50.7% of mobile's users "Intention" to adopt anti-virus on their mobile's devices, which indicating that perceived severity was the most influential factor and degree of harm that would happen as a result to the virus infection becomes the strongest motivator for mobile's users to adopt anti-virus software on their mobile's devices. The study findings also show that "Subjective Norm" was the second strongest factor by its ability to explain around 21.3% of mobile's users "intention" to adopt anti-virus on their mobile's devices, which indicating that degree of interpersonal pressure that caused by the felt expectations held by specific referents and the motivations to comply with their expectations is the second strongest motivator for mobile's users to adopt anti-virus software on their mobile's devices.

B. Implications for Practice

From a practitioner's perspective, this study provides various valuable recommendations for anti-virus' vendors. The study's findings show that perceived severity was the most influential factor and degree of harm that would happen as a result to the virus infection becomes the strongest motivator for mobile's users to adopt anti-virus software on their mobile's devices, thus, vendors can prepare campaign programs and materials that raise mobile's users awareness regarding risks and harm that would happen as a result to the mobiles' virus infection. In addition, the findings also show that "subjective norm" was the second strongest influential factor on mobile's users "intention" to adopt anti-virus on their mobile's devices, vendors of anti-virus software can utilize this result by asking mobile's users when they install anti-virus software to nominate one or more relative or friend to get some sort of rewards or discount when their nominated friends install the same software on their mobiles. Furthermore, the study findings also show that "Response cost" has the ability to lessening "intention" of mobile's users to adopt anti-virus software on their mobile's devices by 20.6%. The significant negative influence of response cost on "intention" of mobile's users to adopt anti-virus software on their mobile's devices indicates that there is a need to develop different versions of anti-virus software to comply with the diversity of mobiles' systems requirements and not deteriorate mobile operating systems' performance which will help reduce the mobile's users' concerns regarding anti-virus software usage.

References

[1]. "CISCO," 2015. [Online]. Available: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.pdf. [Accessed 18 Oct 2015].

[2]. H. Hoehle and V. Venkatesh, "MOBILE APPLICATION USABILITY: CONCEPTUALIZATION AND INSTRUMENT

DEVELOPMENT," *MIS Quarterly,* vol. 39, no. 2, pp. 435-A12, 2015.

[3]. A. Cocotas, "Android Activations Top 1.5 Million A Day," 18 April 2013. [Online]. Available: http://www.businessinsider.com.au/android-activations-to-reach-1-billion-2013-4. [Accessed 17 June 2014].

[4]. T. Cook, "Apple's App Store has passed 100 billion app downloads," in *the Apple Worldwide Developers Conference*, SFrancisco, 2015.

[5]. M. Merrit, "2013 Norton Report. Internet Safety Advocate at Symantec," 7 October 2013. [Online]. Available: http://www.slideshare.net/marianmerritt/the-norton-report-2013. [Accessed 16 June 2015].

[6]. "Trend Micro," 9 Apr 2012. [Online]. Available: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt_security_in_the_age_of_mobility.pdf. [Accessed 2 Sep 2014].

[7]. S. Furnell and N. Clarke, "Power to the people? The evolving recognition of human aspects of security," *Computers & Security,* vol. 31, no. 8, pp. 983-988, 2012.

[8]. R. Willison and M. Warkentin, "Beyond deterrence: An expanded view of employee computer abuse," *MIS Quarterly,* vol. 37, no. 1, pp. 1-20, 2013.

[9]. S. Abraham and I. Chengalur-Smith, "An overview of social engineering malware: Trends, tactics, and implications," *Technology in Society,* vol. 32, no. 3, pp. 183-196, 2010.

[10]. W. Al-Ghaith, "Understanding Social Network Usage: Impact of Co-Presence, Intimacy, and Immediacy," *(IJACSA) International Journal of Advanced Computer Science and Applications,* vol. 6, no. 8, pp. 99-111, 2015a.

[11]. M. Erbschloe, Trojans worms, and spyware. A computer security professional's guide to malicious code, Burlington, MA: Elsevier Butterworth-Heinemann, 2005.

[12]. G. Suarez-Tangil, J. E. Tapiador, P. Peris-Lopez and A. Ribagorda, "Evolution, Detection and Analysis of Malware for Smart Devices," *IEEE Communications Surveys & Tutorials,* no. 16, p. 961–987, 2013.

[13]. R. W. Rogers, "A Protection Motivation Theory of Fear Appeals and Attitude Change," *Journal Of Psychology,* vol. 91, no. 1, pp. 93-114, 1975.

[14]. R. W. Rogers, "Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation," in *Social Psychophysiology*, New York, Guilford Press, 1983, p. 153–176.

[15]. S. Milne, P. Sheeran and S. Orbell, "Prediction and intervention in health-related behavior: a meta-analytic of protection motivation theory," *Journal of Applied Social Psychology,* vol. 30, no. 1, p. 106–143, 2000.

[16]. B. T. McClendon and S. Prentice-Dunn, "Reducing skin cancer risk: an intervention based on protection motivation theory," *Journal of Health Psychology,* vol. 6, p. 321–328, 2001.

[17]. C. Pechimann, G. Zhao, M. E. Goldberg and E. T. Reibling, "What to convey in antismoking advertisements for adolescents: the use of protection motivation theory to identify effective message theme," *Journal of Marketing,* vol. 67, no. April, p. 1–18, 2003.

[18]. A. G. Peace, D. F. Galletta and J. L. Thong, "Software Piracy in the Workplace: A Model and Empirical Test," *Journal of Management Information Systems,* vol. 20, no. 1, pp. 153-177, 2003.

[19]. Y. Zhou and X. Jiang, Android Malware. Springer Briefs in Computer Science, New York: Springer, 2013.

[20]. Y. Lee and K. R. Larsen, "Threat or Coping Appraisal: Determinants of SMB Executives' Decision to Adopt Anti-Malware Software," *European Journal of Information Systems,* vol. 18, pp. 177-187, 2009.

[21]. D. R. Compeau and C. A. Higgins, "Computer self-efficacy: development of a measure and initial test," *MIS Quarterly,* vol. 19, no. 2, pp. 189-211, 1995.

[22]. A. Bandura, "Self-efficacy: toward a unifying theory of behavioural change," *Psychol Rev.,* vol. 84, no. 2, pp. 191-215, 1997.

[23]. R. LaRose, N. J. Rifon and R. Enbody, "Promoting Personal Responsibility for Internet Safety," *Communications of the ACM,* vol. 51, no. 3, pp. 71-76, 2008.

[24]. A. C. Johnston and M. Warkentin, "Fear Appeals and Information Security Behaviors: An Empirical Study," *MIS Quarterly,* vol. 34, no. 3, pp. 548-566, 2010.

[25]. J. H. Wu and S. C. Wang, "What drives mobile commerce? An empirical evaluation of the revised technology acceptance model," *Information & Management,* vol. 42, no. 5, p. 719–729, 2005.

[26]. J. L. Reardon and E. Davidson, "An organizational learning perspective on the assimilation of electronic medical records among small physician practices.," *European Journal of Information Systems,* vol. 16, no. 6, pp. 681-694, 2007.

[27]. I. Ajzen and M. Fishbein, Understanding Attitudes and Predicting Social Behavior, Englewood Cliffs, NJ: Prentice-Hall, 1980.

[28]. I. Ajzen, "The theory of planned behavior," *Organizational Behavior and Human Decision Processes,* vol. 50, no. 2, pp. 179-211, 1991.

[29]. W. Chen, H. Huang and S. T. Chou, "Understanding what determines consumers' expanded use of mobile videophones," *Behaviour & Information Technology,* vol. 31, no. 10, pp. 953-967, 2012.

[30]. T. Hsien-Tung and R. P. Bagozzi, "CONTRIBUTION BEHAVIOR IN VIRTUAL COMMUNITIES: COGNITIVE, EMOTIONAL, AND SOCIAL INFLUENCES," *MIS Quarterly,* vol. 38, no. 1, pp. 143-A3, 2014.

[31]. H. Lai, C. Chen and Y. Chang, "Determinants of knowledge seeking in professional virtual communities," *Behaviour & Information Technology,* vol. 33, no. 5, pp. 522-535, 2014.

[32]. B. Sheppard, J. Hartwick and P. Warshaw, "The theory of reasoned action: a meta-analysis of past research with recommendations for modifications and future research," *Journal of Consumer Research,* vol. 15, no. 3, p. 325–343, 1988.

[33]. S. Taylor and P. A. Todd, "Understanding information technology usage: A test of competing models," *Information Systems Research,* vol. 6, no. 2, pp. 144-176, 1995.

[34]. L. Chen, L. M. Gillenson and L. D. Sherrell, "Consumer acceptance of virtual stores: a theoretical model and critical success factors for virtual stores," *ACM SIGMIS Database,* vol. 35, no. 2, pp. 8-31, 2004.

[35]. W. Al-Ghaith, "Using the Theory of Planned Behavior to Determine the Social Network Usage Behavior in Saudi Arabia," *International Journal of Research in Computer Science,* vol. 5, no. 1, pp. 1-8, 2015b.

[36]. W. G. Zikmund, Business research methods (7th ed.), Cincinnati, OH: Thomson, 2003.

[37]. I. M. Y. Woon, G. W. Tan and R. T. Low, "A protection motivation theory approach to home wireless security," in *The Twenty-Sixth International Conference on Information Systems (Avison, D., Galletta, D., & DeGross, J., Eds)*, Las Vegas, 2005.

[38]. V. Venkatesh, M. Morris, M. G. Rris, G. B. Davis and F. D. Davis, "User acceptance of information technology: toward a unified view," *MIS Quarterly,* vol. 27, no. 3, p. 425–478, 2003.

[39]. W. Al-Ghaith, L. Sanzogni and K. Sandhu, "Factors Influencing the Adoption and Usage of Online Services in Saudi Arabia," *Electronic Journal of Information Systems in Developing Countries (EJISDC),* vol. 40, no. 1, pp. 1-32, 2010.

[40]. G. Premkumar and K. Ramamurthy, "The role of Interorganizational and organizational factors of the decision mode for adoption of interorganizational systems," *Decision Science,* vol. 26, no. 3, pp. 303-336, 1995.

[41]. A. L. Comrey and H. B. Lee, A first course in factor analysis, L., NJ: Erlbaum Associates, 1992.

[42]. H. B. Asher, Causal modeling, Newbury Park: Sage University Press, 1983.

[43]. M. Lee, "Factors influencing the adoption of internet banking: An integration of TAM and TPB with perceived risk and perceived benefit," *Electronic Commerce Research and Applications,* vol. 8, no. 3, pp. 130-141, 2009.

[44]. M. Workman, W. Bommer and D. Straub, "Security Lapses and the Omission of Information Security Measures: An Empirical Test of the Threat Control Model," *Journal of Computers in Human Behavior,* vol. 24, no. 6, pp. 2799-2816, 2008.

Waleed Al-Ghaith is an Assistant Professor of Information systems at Shaqra University, Riyadh, Saudi Arabia. He holds a PhD in information systems from Griffith University, Australia. His areas of expertise are information technology research, internet research and organizational intelligence technologies. He currently works as Head of Information Systems Department, and as Dean of IT and eLearning deanship.