韓國IT서비스學會誌
第13卷 第2號
2014年 6月, pp.113-131
http://dx.doi.org/10.9716/KITS.2014.13.2.113

스마트폰 이용자의 악성코드용 모바일 백신 이용 의도에 영향을 미치는 요인

장재영* · 김지동* · 김범수*

The Factors Affecting Smartphone User's Intention to use Mobile Anti-Malware SW

Jaeyoung Jang* · Jidong Kim* · Beomsoo Kim*

■ Abstract ■

Smartphone security threat has become an important issue in Information Science field following the wide distribution of smartphones. However, there are few studies related to such. Therefore, this study examined the factors affecting the intention of smartphone users to use the mobile vaccine against malware with the Protection Motivation Theory. To secure the reliability of the study, a surveying agency was commissioned. A total of 263 respondents, excluding 37 respondents who are users of iOS, which does not have mobile vaccine in the smart phone, or who gave invalid responses, were surveyed. The results showed that perception of the installed mobile vaccine significantly affected the Response Efficacy and Self-efficacy, and that the Perceived Severity, Perceived Vulnerability, Response Efficacy, and Self-efficacy significantly influenced the intention to use the mobile vaccine. On the other hand, Installation Perception of mobile vaccine itself did not affect the Perceived Severity and Perceived Vulnerability. This study is significant since it presented the new evaluation model of threat evaluation and response evaluation in the Protection Motivation Theory in accepting the security technology and raised the need for the promotion and exposure of mobile vaccine, since perception of mobile vaccine installation affects the response evaluation. It also found that the promotion must consider the seriousness of smartphone security, outstanding attribute of mobile vaccine, and user-friendliness of mobile vaccine above all.

Keyword : Protection Motivation Theory, Smartphone, Mobile Anti-Malware SW

논문투고일 : 2013년 11월 12일 논문수정완료일 : 2014년 05월 10일 논문게재확정일 : 2014년 05월 12일
* 연세대학교 정보대학원

1. 서 론

해킹 등 보안 관련 위협이 해마다 증가하고 있다. 2012년 한 해 동안 해킹 등 보안 공격은 전년 대비 42%, 웹 기반 공격은 30%, social networking site에 대한 피싱(phishing) 공격은 125%가 증가했다[49]. 해킹 등으로 인한 보안 사고는 개인적 · 사회적으로 막대한 비용을 유발한다[25, 33]. 이에 따라 이용자들은 대부분 해킹, 웜/바이러스, 악성코드, 애드웨어/스파이웨어용 백신 등을 설치하여 자신들의 PC나 스마트폰 등을 보호하고 있다[44].

최근에는 스마트폰의 보급 확산에 따라 새로운 보안 위협이 제기 되고 있다. 그러나 한국인터넷진흥원[17]의 「2012년도 정보보호 실태조사」 결과에 따르면 한국의 모바일 백신 이용률은 31.1%에 불과하다고 한다. 뱅킹 서비스를 위해 자동적으로 실행되는 건수를 제외하면 자발적인 이용률은 이 수치보다 적을 것으로 보인다. 이는 PC 이용자의 백신 이용률인 88.2%와 비교하면 절반에도 못 미치는 수치이다.

스마트폰은 기능적으로 PC와 유사하여 PC에서 문제가 되고 있는 해킹, 웜/바이러스, 악성코드 문제를 동일하게 가지고 있다[50]. 더욱이 스마트폰은 이용자가 원하지 않는 과금 또는 결제 등 금전적인 피해를 야기할 수 있다는 측면과 위치정보서비스(Location based service)를 이용할 경우 개인의 위치 정보가 노출될 수 있고, 전화번호 등이 들어있는 단말기를 분실하면 사회생활에 커다란 지장을 초래할 수 있다는 측면에서 프라이버시 보호를 위해 PC보다 높은 수준의 보안이 요구된다.

스마트폰의 보급 확산과 보안 위협의 증가에도 불구하고 현재까지 IS 분야에서의 관련 연구는 거의 이루어지 않고 있다. 현재까지 진행된 관련 연구로는 anti-virus 이용 행동에 관한 Larose and Rifon[34]과 Lee[36]의 연구, anti-malware에 관한 Lee and Larsen[35]의 연구, anti-spyware 이용 의도에 관한 Lee and Kozar[37]와 Johnston and Warkentin[32]의 연구 정도가 있다. 그러나 이들 연구 모두 PC 이용자를 대상으로 하고 있어서 모바일 이용자나 모바일 환경에 적용하기에는 한계가 있다.

이러한 연구의 한계를 극복하기 위해 본 연구는 스마트폰 이용자를 대상으로 하고 있다. 이 연구는 스마트폰 이용자가 악성코드용 모바일 백신이용 의도에 영향을 미치는 요인을 도출하는 것을 목적으로 하고 있다. 또한 백신 설치 지각이 보호동기 변인에 미치는 인과 관계와 이들 변인들이 백신 이용 의도에 미치는 영향을 밝히고자 한다.

스마트폰 이용자의 악성코드용 모바일 백신 이용 의도는 보호동기이론(PMT : Protection Motivation Theory)으로 설명이 가능하다. 보호동기이론은 보건 분야에서 발전하여 보안, 안전, 보호 분야에서 보편적으로 이용되고 있는 이론으로 IS 영역에서도 보안 분야를 중심으로 활용이 점차적으로 증가하고 있다.

본 연구를 통해 학문적으로나 실무적으로 다음과 같은 기여가 예상된다. 학문적으로는 스마트폰 악성코드용 모바일 백신 이용 의도 분야에 보호동기이론을 처음 적용하여 모바일 백신의 이용 의도, 백신의 설치 지각, 보호 동기 이론의 변인간의 관계를 규명할 수 있을 것이다. 실무적으로는 이용자의 악성코드용 모바일 백신 이용 의도를 분석함으로써 백신의 이용률을 제고할 수 있고, 스마트폰 이용자들이 백신을 이용하지 않는 원인을 찾아 이용 활성화에 기여할 수 있을 것으로 보인다. 이를 통해 스마트폰 보안 수준을 제고하여 모바일 관련 보안사고 및 사이버 범죄를 예방할 수 있을 것으로 기대된다.

이 논문은 다음과 같이 구성되어 있다. 첫째, 이 장에서는 이 논문의 배경, 문제점, 필요성, 관련 이론 및 시사점을 간략하게 소개한다. 제 2장에서는 선행 연구, 배경 이론, 연구 가설, 이론적 프레임워크를 제시한다. 제 3장에서는 연구를 위한 설문의 작성, 데이터 수집 등 연구 방법을 설명한다. 제 4장에서는 설문 결과 및 연구 결과를 검증한다. 제 5장에서는 연구의 결과에 대한 토의, 시사점, 연구

의 제약과 향후 연구 방향을 제시한다. 그리고 마지막 제 6장에서는 결론을 제시한다.

2. 이론적 배경 및 가설

2.1 모바일 악성코드와 모바일 백신

모바일 악성코드(mobile malicious code)란 모바일 단말기를 대상으로 개인정보 유출, 시스템 파괴, 원격지 접속 등의 악의적인 행위를 수행하기 위해 제작된 악성 프로그램을 말한다[3]. 악성코드에 감염되면 인터넷 기반의 PC 환경에서의 보안 위협과 같이 감염 후에 디바이스의 성능저하뿐만 아니라 정보유출, 금전적, 손실, 공격지로의 활용 등이 가능하다[13]. 모바일 악성코드는 모바일 디바이스의 진화와 더불어 블루투스, Wi-Fi 등의 무선 접속 기술의 발전과 함께 증가하고 있고[12], 피싱, 스파이웨어, DDos(Distributed Denial of Service), 인터넷 뱅킹 보안 위협 등으로 발전될 가능성이 높다[14]. 모바일 악성코드의 대표적인 특징은 <표 1>과 같다.

〈표 1〉 모바일 악성코드의 특징

유형	피해 현상
파일 조작	◦ 파일 실행 차단 ◦ 파일 감염 및 덮어 쓰기 ◦ 응용 프로그램 혹은 아이콘 변경
정보 유출	◦ 휴대폰 원격 제어 ◦ 휴대폰 정보 유출 ◦ 이용자의 SMS 훔쳐보기 ◦ 이용자의 데이터 은닉 및 도난
서비스 과금	◦ SMS 메시지 전송을 통한 부당 요금 발생 ◦ 프리미엄 서비스 무단 접속 및 국제전화 무단 발신으로 부당 요금 발생

출처 : [2, 5] 자료 일부 수정.

모바일 악성코드는 안드로이드 OS, iOS 모두에서 발견되고 있다. 특히 안드로이드 OS의 경우 앱스토어가 단말기 제조사나 이동통신 사업자들에 의해 분산되어 있고 블랙마켓들도 활성화되어 있어 모바일 악성코드가 많이 나타나고 있다[17].

모바일 악성코드의 종류로는 바이러스, 웜, 트로이목마, 스파이웨어, 가짜 소프트웨어, 서비스 거부 공격이 있다. 모바일 악성코드의 종류는 내용에 있어서는 차이가 있으나 종류에 있어서는 PC의 악성코드와 커다란 차이가 없다.

이처럼 모바일 악성코드의 증가에 따라 악성코드용 모바일 백신의 필요성이 증대되고 있다. 현재 삼성, LG, 팬택 등 국내 안드로이드 계열의 스마트폰에는 악성코드용 모바일 백신이 기본 프로그램으로 설치되어 있다. 이 외에도 안드로이드 마켓인 '구글플레이'나 통신사 마켓을 통해 국내·외의 모바일 백신 제품을 설치할 수 있다.

2.2 모바일 악성코드용 백신 설치 지각

지각(perception)이란 개인이 환경 내에서 특정 사물이나 대상을 인지하는 것을 말하며, 인간은 촉각·미각·후각·청각·시각 등의 감각을 이용하여 환경에 대한 정보를 통합적으로 받아들인다[1]. 감각 기능이 환경에 대한 정보를 처리하기 위해서는 자극 선택성, 자극 강도, 시간적 제약, 시각의 내적 특성 등이 고려 요소가 된다. 특히 지각은 자극의 정도가 일정 수준을 넘어야 지각할 수 있는 임계치(Threshold) 이상이어야 발생한다.

지각은 대상이 무엇인지 모르지만 무엇인가의 존재를 발견(detection)하는 단계부터 그것이 무엇인지를 알게(cognition)되는 단계까지를 포함한다. 이 경우 지각과 인지 간의 개념상의 혼란이 발생하게 된다. 지각은 외부로부터 들어온 자극이 감각기관을 통해 입력되어 뇌까지 전달되어 그 자극이 무엇인지를 해석하여 행동이나 태도에 영향을 주는 과정으로 외부 자극을 강조하는 개념이다. 반면 인지는 이 보다는 조금 넓은 개념으로 감각정보가 입력, 변형, 축소, 정교화, 저장, 인출되는 모든 과정을 의미한다. 따라서 자극을 통해 입력된 정보가 일정한 과정을 거쳐 처리되는 것을 강조하는 개념이다. 인지는 형태인식, 주의집중, 기

억, 문제해결, 창의적인 사고 등 거의 모든 사고 과정을 포함한다[11]. 지각의 연구 영역은 대상의 형태, 공간, 색채, 시간 및 운동 등의 하위 영역으로 세분되며, 지각 연구는 감각, 주의, 의식, 형태 재인 및 기억 등과 밀접한 관련이 있다[11].

스마트폰 제조사들은 제조 단계에서 다양한 기능의 모바일 어플리케이션을 번들 형태로 설치 후 시장에 출시하고 있다. 번들형 어플리케이션 중에는 스마트폰의 안전을 위한 악성코드용 모바일 백신도 설치되어 있다. 이것은 공급 과정에서 스마트폰에 자동으로 설치된 것이므로 스마트폰 이용자는 초기에는 모바일 백신이 설치된 것을 인식하지 못할 수도 있다. 그러나 이용자가 필요한 스마트폰 어플리케이션을 이용하기 위해서는 스마트폰의 어플리케이션이 모여 있는 화면을 순차적으로 이동해야 된다. 이는 스마트폰 화면 어딘가에 위치하고 있는 악성코드용 모바일 백신에 자연스럽게 지속적으로 노출됨을 의미한다. 따라서 이용자는 스마트폰을 이용하면서 자신의 스마트폰에 악성코드용 모바일 백신이 설치되어 있다는 것을 자연스럽게 지각하게 된다. 또한 모바일 뱅킹 시에 모바일 백신이 동작하기 때문에 스마트폰 이용자는 본인의 스마트폰에 모바일 백신이 설치되어 있다는 것을 지각하게 된다.

2.3 보호동기이론

로저스(Rogers[46])에 의해 처음 개발된 보호동기이론은 개인이 건강과 관련한 위험 메시지를 인지했을 때 자신의 태도와 행동이 어떻게 변하는지를 설명하는 이론이다. 보호동기이론은 특정 개인은 외부의 위협을 인지하면 이로 인해 태도나 행동이 직접적으로 변화하지는 않지만, 심리적 요인에 의한 위협 평가(threat appraisal)와 대응 평가(copying appraisal)를 통해 위협을 회피하거나 대처하기 위한 보호동기가 생성된다고 한다[47]. 이러한 보호 동기는 직접적이지는 않지만 행위의도에 영향을 준다고 한다[45, 51]. 또한 계획된 행동이론(Theory of Planned Behavior)에 의하면 특정 개인의 행위는 개인의 의도를 통해 예측 가능하다고 한다[26]. 따라서 개인의 보호동기와 의도를 파악하면 특정 개인의 보호행동을 예측할 수 있게 된다[19]. 보호동기이론은 다양한 보호행동의 중요한 사회 인지적 설명력을 제공함으로써 가치 있는 이론적 프레임을 제공하고 있다[38].

Rogers[46]가 제시한 초기의 보호동기이론에 따르면 보호 동기는 위협의 정도를 의미하는 심각성(severity), 자신이 그 위협에 노출될 가능성을 의미하는 취약성(vulnerability), 위협 대처 방안이 얼마나 효과적인지 판단하는 대응 효능감(response efficacy)으로 구성되어 있었다. 초기 보호동기이론은 선행 연구들을 통해 행위의도(behavioral intention)에 영향을 미치는 것으로 밝혀졌으나 사회인지이론에 따르면 개인의 행위 의지는 독립적이고 자기 통제적인 상황 하에서 발생하기 때문에[22], Rogers[47]는 이를 감안하여 특정한 영역 속에서 자신이 수행할 수 있는 능력에 대한 신념을 의미하는 자기 효능감(self-efficacy) 변수를 보호동기이론에 새로 추가했다. 메타 분석 결과에 의하면 보호동기이론의 모든 위협 및 대응 평가 변수들은 보호행동을 이해하고 예측하는데 유의한 영향력이 있다고 한다[30].

보호동기이론은 보건의료 분야에서 처음 개발되었으며[27, 40, 43], 식품 안전[48], 환경 보호[42]와 핵 확산 방지[21] 등 다양한 분야에서 적용되고 있다. IS 분야에서도 최근 보안 분야를 중심으로 보호동기이론을 활용하는 연구 사례가 증가하고 있다. 최근 연구로는 가정집 무선랜 보안[55], 온라인 이용자의 강력한 비밀번호 사용 의도[57], 표절 방지 소프트웨어 이용 의도[36] 등의 연구가 있다.

2.4 연구 모형

본 연구는 악성코드용 모바일 백신 이용 의도에 영향을 미치는 요인을 알아보기 위해 보호동기이론을 활용했다. 또한 스마트폰의 모바일 백신 설치에

대한 지각이 백신 이용 의도에 영향을 미치는 요인을 살펴보고자 한다.

2.4.1 백신 설치 지각

인지 심리학에서는 자극 반응 과정은 자극(stimulus), 지각(perception), 인지(cognition), 태도(attitude), 반응(reaction) 순으로 나타난다고 한다. 따라서 스마트폰 이용자가 모바일 악성코드 백신의 설치를 지각하게 되면 인지 과정을 거쳐 태도 등에 일정부분 영향을 준다고 가정할 수 있다[8].

지각이 인지에 영향을 미치지만 지각과 인지 간의 영향 관계가 항상 일정한 방향으로 나타나는 것은 아니다[4]. 지각과 인지와의 관계를 살펴보면 지각은 특정 위협 요인과 관련된 지식이나 경험과 상관성을 가지나[29, 53], 지각이 인지와 반드시 일정한 방향성을 가지는 것은 아니라고 한다[23]. 예를 들어 만성질환자의 신종 만성질환 보도에 대한 공포인식 연구에서는 이용자의 보호동기 추구 가운데 심각성과 취약성에 양(+)의 영향을 준다는 연구 결과[11]와 텔레비전 뉴스에 많이 노출된 시청자는 질병에 대한 공포가 높게 나타난다는 연구 결과가 있다[9]. 반면 경찰의 순찰 활동에 관한 연구에서는 시민이 경찰의 순찰 활동 또는 순찰차만 보더라도 범죄 위협에 음(-)의 영향을 준다는 연구 결과도 있다[6, 8].

선행 연구 결과를 바탕으로 하면 스마트폰 이용자에게 악성코드 백신의 설치 지각은 악성코드로부터 자신의 스마트폰을 보호할 수 있는 수단이 있다고 인식될 수도 있으며, 반대로 스마트폰도 PC와 같이 보안 공격의 대상이 될 수도 있다고 느낄 수도 있을 것이다.

따라서 다음과 같은 가설을 제시할 수 있다.

H1a : 스마트폰 이용자의 악성코드 제거용 모바일 백신 설치 지각은 스마트폰 악성코드 피해로 인한 지각된 심각성에 정(+)의 영향을 미칠 것이다.

H1b : 스마트폰 이용자의 악성코드 제거용 모바일 백신 설치 지각은 스마트폰 악성코드 피해로 인한 지각된 심각성에 음(-)의 영향을 미칠 것이다.

H2a : 스마트폰 이용자의 악성코드 제거용 모바일 백신 설치 지각은 스마트폰 악성코드 피해로 인한 지각된 취약성에 정(+)의 영향을 미칠 것이다.

H2b : 스마트폰 이용자의 악성코드 제거용 모바일 백신 설치 지각은 스마트폰 악성코드 피해로 인한 지각된 취약성에 음(-)의 영향을 미칠 것이다.

지각은 취약성과 심각성 외에 대응 효능감과 자기 효능감에도 영향을 미친다(Rogers[46]). 예를 들면 신종 감염질환 관련 매체별 뉴스 이용량에 따른 질병 공포는 대처 효율성과 자기 효능감에 영향을 미치고[10], 신종플루 뉴스 이용은 대응 효능감에는 영향을 미치지 않지만 자기 효능감에는 영향을 미친다고 한다[2].

선행 연구 결과를 바탕으로 하면 스마트폰 이용자에게 악성코드 백신의 설치 지각은 악성코드로부터 자신의 스마트폰을 보호할 수 있다는 믿음과 관련한 자기 효능감에 유의한 영향을 미칠 수 있다고 가정할 수 있다. 대응 효능감의 경우는 연구 결과가 일관되게 나오고 있지 않으나 보안 분야에는 선행연구가 없고, 다수의 연구 결과가 반영된 보호동기이론 중 하나의 변수이므로 백신 설치 지각이 대응 효능감에 영향을 준다고 가정하고 연구하여 지각과 대응 효능감의 유의성 여부를 검증할 필요가 있다.

따라서 선행 연구를 종합적으로 검토하여 다음과 같은 가설을 제시할 수 있다.

H3 : 스마트폰 이용자의 악성코드 제거용 모바일 백신 설치 지각은 스마트폰 악성코드 피해에 대한 대응 효능감에 정(+)의 영향을 미칠 것이다.

H4 : 스마트폰 이용자의 악성코드 제거용 모바일

백신 설치 지각은 스마트폰 악성코드 피해에 대한 위협 자기 효능감에 정(+)의 영향을 미칠 것이다.

또한 앞의 가설을 고려했을 때 특정한 상황 또는 대상의 지각으로 인해 지각된 취약성과 지각된 심각성, 대응 효능감과 자기 효능감을 느낀다면 행위 의도에 간접적으로 영향을 미친다는 연구가 있다[24, 52, 55]. 그러나 일부 연구에서는 직접적으로 영향을 미칠 수 있다는 주장도 있다[2].

따라서 선행 연구를 바탕으로 다음과 같은 가설을 제시할 수 있다.

H5 : 악성코드용 모바일 백신 설치 지각은 모바일 백신 사용 의도에 정(+)의 영향을 미칠 것이다.

2.4.2 지각된 심각성

지각된 심각성이란 특정 상황이나 대상에 대해 그 위협이 얼마나 심각한 지에 대한 지각된 정도를 의미한다[46]. 지각된 심각성은 외부의 위협에 대한 평가 과정에서 물리적, 사회적, 심리적 상호작용에 의해 발생하며 심각성이 지각되는 경우 이용자의 불안감이 유발된다. 이용자는 이러한 불안감을 제거하기 위해 자신의 태도를 바꾸거나 행동을 수정하려 한다고 한다[9]. 관련 선행 연구들을 살펴보면 지각된 심각성은 대학 교직원을 대상으로 한 표절 방지 소프트웨어 도입[36], 가정의 무선 네트워크의 보안 설정[55], IS 보안 정책 준수[52] 등의 의도에 영향을 미친다고 한다.

선행 연구 결과를 활용하면 스마트폰 이용자가 백신 설치 지각을 통해 자신의 스마트폰에 보안 문제가 발생할 수 있다는 심각성을 지각하게 되면 해당 모바일 백신을 사용하려는 의도가 발생할 수 있다는 것을 가정할 수 있다.

따라서 다음과 같은 가설을 제시할 수 있다.

H6 : 모바일 악성코드의 피해에 대한 지각된 심각성은 악성코드용 모바일 백신 이용 의도에 정(+)의 영향을 미칠 것이다.

2.4.3 지각된 취약성

지각된 취약성이란 위협이 발생할 경우 그 위협이 자신에게 발생할 가능성을 의미한다[46]. 취약성의 지각은 해당 위협에 대해 노출될 가능성에 대한 자신의 평가를 기반으로 한다[36]. 지각된 취약성이 증가하는 경우 대처 행위를 취할 가능성 또한 증가하게 된다. 선행 연구를 살펴보면 지각된 취약성은 가정의 무선 네트워크의 보안 설정[55], 안티-멀웨어 소프트웨어 설치[38], 바이러스 보호 행동[35] 등의 의도에 영향을 미친다고 한다.

선행 연구 결과를 활용하면 스마트폰 이용자가 백신 설치 지각을 통해 자신의 스마트폰에 보안 문제가 노출될 수 있다는 취약성을 지각하게 되면 해당 모바일 백신을 사용하려는 의도가 발생할 수 있다고 가정할 수 있다.

따라서 다음과 같은 가설을 제시할 수 있다.

H7 : 모바일 악성코드의 피해에 대한 지각된 취약성은 악성코드용 모바일 백신 이용 의도에 정(+)의 영향을 미칠 것이다.

2.4.4 대응 효능감

대응 효능감이란 권고된 보호행동 또는 보호 기술 등의 대처 방안이 효과적으로 작용하여 위협을 통제할 수 있다는 믿음이다[46]. 대응 효능감은 위협을 제거할 수 있도록 제안된 권고 또는 기술 등에 대한 신뢰를 의미한다[9]. 이용자가 높은 대응 효능감을 가지고 있다면 이용자가 대응 행동을 할 가능성 또한 증가하게 된다. 선행 연구들을 살펴보면 대응 효능감은 스파이웨어에 대한 보호 행동[32], 보안 사고에 대비한 데이터 백업[28], 대학 교직원을 대상으로 한 표절 방지 소프트웨어 도입[36], 직장인의 IS 보안 정책 준수[52] 등의 의도에 영향을 미친다고 한다.

선행 연구 결과를 활용하면 스마트폰 이용자가 백신 설치 지각을 통해 자신의 스마트폰에 설치된 백신이 보안 문제에 대한 높은 대응 효능감을 가지고 있다고 개인이 인식하면 개인의 모바일 백신 사용 의도가 높을 것이라는 것을 가정할 수 있다.

따라서 다음과 같은 가설을 제시할 수 있다.

H8 : 모바일 악성코드의 피해에 대한 대응 효능감은 악성코드용 모바일 백신 이용 의도에 정(+)의 영향을 미칠 것이다.

2.4.5 자기 효능감

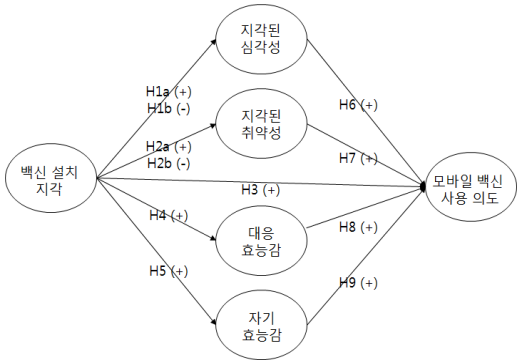
자기 효능감이란 Bandura[22]에 의해 고안된 개념으로 특정한 영역 또는 분야에서 자신이 대응 행동을 수행할 수 있는 능력에 대한 그 자신에 대한 신념이다. 이용자가 권고된 행동을 수행할 수 있고 충분히 통제할 수 있다는 자신의 능력에 대한 자신감을 가지고 있다면 이용자는 대응 행동을 수행할 가능성이 증가하게 된다. 선행 연구들을 살펴보면 대응 효능감은 스파이웨어에 대한 보호 행동[32], 보안 사고에 대비한 데이터 백업[28], 대학 교직원을 대상으로 한 표절 방지 소프트웨어 도입[36], 온라인 이용자의 강력한 비밀번호 사용 의도[57] 등의 의도에 영향을 미친다고 한다.

선행 연구 결과를 활용하면 스마트폰 이용자가 백신 설치 지각을 통해 자신의 스마트폰에 설치된 백신이 보안 문제에 대한 높은 자기 효능감을 가지고 있다고 개인이 인식하면 개인의 모바일 백신 사용 의도가 높을 것이라는 것을 가정할 수 있다.

따라서 다음과 같은 가설을 제시할 수 있다.

H9 : 모바일 악성코드의 피해에 대한 자기 효능감은 악성코드용 모바일 백신 이용 의도에 정(+)의 영향을 미칠 것이다.

보호동기이론과 선행 연구 결과를 바탕으로 제시한 가설들을 정리하면 [그림 1]과 같은 연구 모형을 제시할 수 있다.



[그림 1] 연구 모형

3. 연구 방법

3.1 변수의 조작적 정의 및 측정 항목 개발

각 변수의 조작적 정의 및 변수별 측정 항목은 <표 2>와 같다. 백신 설치 지각을 제외한 나머지 변수들은 보호동기 이론과 관련한 선행 연구들에서 검증된 변수들을 기반으로 본 연구의 목적에 맞게 수정했다. 다만 백신 설치 지각은 적절한 선행 연구를 발견하지 못해서 모바일 환경을 고려하여 자체 개발했다.

측정 항목은 본 조사에 앞서 산・학・연의 50명을 대상으로 파일럿 테스트를 실시했다. 파일럿 테스트에는 대학원 석・박사 과정 재학생들과 보안 전문 기관 및 보안업체의 보안 전문가, 스마트폰을 이용하는 일반 유저(직장인, 대학생, 가정 주부 등)가 참여했다. 파일럿 테스트 결과 일부 측정 항목들의 가독성에 문제가 있어 질문지를 수정했다.

각각의 문항들은 1점('전혀 그렇지 않다')에서 7점('매우 그렇다')까지 응답할 수 있는 리커트(Likert) 7점 척도를 이용했다. 인구 통계학적 통계를 위한 문항은 질문 항목에 따라 2점부터 7점의 명목 척도를 사용했다.

3.2 표본추출

본 연구는 표본의 신뢰성 확보를 위해 설문 대

〈표 2〉 연구 변수의 조작적 정의 및 측정 항목

변수	조작적 정의	측정 항목		출처
PS	모바일 악성 코드로부터 스마트폰이 위협에 노출되어 피해를 입을 수 있는 유해성의 크기	PS1	만약 스마트폰이 악성코드(웜, 바이러스, 해킹툴 등)에 감염되면 치명적인 문제를 야기할 것이다.	[32]
		PS2	만약 스마트폰이 악성코드(웜, 바이러스, 해킹툴 등)에 감염되면 심각한 문제를 야기할 것이다.	
		PS3	만약 스마트폰이 악성코드(웜, 바이러스, 해킹툴 등)에 감염되면 중요한 문제를 야기할 것이다.	
PV	자신의 스마트폰이 모바일 악성 코드 감염 및 피해 위협에 노출될 수 있는 가능성의 크기	PV1	내 스마트폰은 악성코드(웜, 바이러스, 해킹툴 등)에 감염 될 수 있다.	[32]
		PV2	내 스마트폰은 악성코드(웜, 바이러스, 해킹툴 등)에 감염될 수 있을 것 같다.	
		PV3	내 스마트폰은 악성코드(웜, 바이러스, 해킹툴 등)에 감염될 가능성이 있다.	
RE	모바일 악성 코드로부터 피해 위협에 대처하는 방안이 얼마나 효과적인지의 정도	RE1	악성코드(웜, 바이러스, 해킹툴 등) 제거용 모바일 백신은 스마트폰을 보호할 수 있을 것이다.	[32]
		RE2	악성코드(웜, 바이러스, 해킹툴 등) 제거용 모바일 백신은 스마트폰 보호에 효과적일 것이다.	
		RE3	악성코드(웜, 바이러스, 해킹툴 등) 제거용 모바일 백신을 이용하면 스마트폰 보호가 더욱 잘 될 것이다.	
SE	자신이 악성코드 제거용 모바일 백신을 수행할 수 있는 능력에 대한 신념의 정도	SE1	나는 내 스마트폰에 대한 보호 조치를 취하는 것이 편하다.	[20, 32]
		SE2	일반적으로 나는 다른 사람의 스마트폰에 대한 보호 조치를 취하는 것이 편하다.	
		SE3	나는 내 책임 하에 나에게 필요한 보호 조치를 취할 수 있다.	
		SE4	나는 보호 조치에 필요한 자원과 지식을 가지고 있다.	
		SE5	나는 필요한 보호 조치를 취하는 것이 쉽다.	
IP	스마트폰에 악성코드 제거용 모바일 백신이 설치되어 있다는 것을 지각하는 정도	IP1	나는 내 스마트폰에 악성 코드(웜, 바이러스, 해킹툴 등) 제거용 모바일 백신이 기본으로 설치되어 있다는 것을 알고 있다.	자체 개발
		IP2	나는 내 스마트폰에 악성 코드(웜, 바이러스, 해킹툴 등) 제거용 모바일 백신이 설치되어 있다는 것을 알고 있다.	
UI	악성코드 제거용 모바일 백신 이용 의도에 대한 정도	UI1	나는 스마트폰용 악성 코드(웜, 바이러스, 해킹툴 등) 제거용 모바일 백신을 이용할 의도가 있다.	[36]
		UI2	나는 가까운 미래에 스마트폰용 악성 코드(웜, 바이러스, 해킹툴 등) 제거용 모바일 백신을 이용할 것으로 예상된다.	
		UI3	나는 가까운 미래에 스마트폰용 악성 코드(웜, 바이러스, 해킹툴 등) 제거용 백신을 이용할 계획이 있다.	

행 기관을 활용했다. 연구자는 연구 결과를 토대로 설문지를 작성하여 전문기관에 설문을 의뢰했다. 전문 기관에서는 자신들의 사이트를 방문한 온라인 패널들을 대상으로 무작위로 설문 조사를 실시한 후 설문 결과를 연구자에 제공했다. 설문 대행 기관은 자사 기준에 따라 설문 응답자에게 보상을 실시했다. 설문 조사는 2013년 9월 5일~9월 9일까지(5일간) 300명을 대상으로 이루어졌다. 원천 데이터를 분석한 결과 스마트폰에 악성코드용 모바일 백신이 설치되어 있지 않은 iOS 계열 이용자 및 설문에 오류가 발견된 37명의 응답을 제외하고 총 263부를 통계에 활용했다. 응답자의 인구통계학적 특성은 <표 3>과 같다.

본 연구에 활용된 자료의 인구 통계학적 특성을

〈표 3〉 인구통계학적 특성

구 분		설문자 수	비율(%)
성별	남자	128	48.7%
	여자	135	51.3%
연령	10대 이하	30	11.4%
	20대	66	25.1%
	30대	88	33.5%
	40대	61	23.2%
	50대 이상	18	6.8%
소득	2천만 원 이하	80	30.4%
	2천~4천만 원	72	27.4%
	4천~6천만 원	73	27.4%
	6천~8천만 원	24	9.1%
	8천~1억 원	14	5.3%
학력	중졸	26	9.9%
	고졸	40	15.2%
	대재 및 대졸	155	58.9%
	석사	40	15.2%
	박사	2	0.8%

살펴보면 남성이 128명(48.7%), 여성이 135명(51.3%)으로 나타났다. 연령은 30대 68명(33.5%), 20대 66명(25.1%), 40대 61명(23.2%) 순으로 나타났다. 소득의 경우 2천만 원 이하가 80명(30.4%)으로 제일 많았고, 4천~6천만 원이 73명(27.4%), 2천~4천만 원이 72명(27.4%) 순을 나타났다. 마지막으로 학력의 경우 대재 및 대졸이 155명(58.9%), 석사와 고졸이 각각 40명(15.2%)으로 나타났다.

4. 연구 결과

본 연구를 위한 모형 및 가설 검정 도구로 SPSS 18.0과 AMOS20.0을 사용했다. 연구 결과는 측정 항목의 신뢰성과 수렴타당성, 판별타당성을 검정한 후 가설 검정 순으로 진행했다.

〈표 4〉 신뢰성 분석

항목	평균	편차	성분						Cronbach'α
			1	2	3	4	5	6	
PS1	5.87	1.082	0.078	0.134	0.266	**0.856**	0.093	0.041	0.906
PS2	5.96	1.046	0.036	0.170	0.288	**0.866**	0.109	-0.005	
PS3	5.99	1.045	0.041	0.162	0.237	**0.834**	0.124	0.006	
PV1	5.55	1.180	0.109	0.111	**0.859**	0.231	0.008	0.035	0.910
PV2	5.52	1.172	0.058	0.151	**0.888**	0.229	0.043	0.033	
PV3	5.47	1.232	0.081	0.081	**0.853**	0.303	0.066	-0.009	
RE1	4.76	1.171	0.197	0.108	0.034	0.199	**0.870**	0.086	0.911
RE2	4.84	1.163	0.211	0.189	0.025	0.091	**0.882**	0.046	
RE3	4.85	1.162	0.175	0.218	0.062	0.033	**0.873**	0.014	
SE1	4.85	1.145	**0.750**	0.245	-0.083	0.167	0.104	0.022	0.872
SE2	4.61	1.137	**0.781**	0.146	-0.023	0.067	0.154	0.000	
SE3	4.74	1.092	**0.810**	0.143	0.023	0.098	0.206	0.147	
SE4	4.68	1.086	**0.801**	0.023	0.223	0.013	0.078	0.090	
SE5	4.60	1.167	**0.786**	0.077	0.173	-0.135	0.129	0.109	
UI1	5.16	1.328	0.177	**0.879**	0.072	0.182	0.181	0.057	0.933
UI2	5.06	1.337	0.207	**0.885**	0.155	0.133	0.176	0.041	
UI3	5.08	1.227	0.170	**0.868**	0.148	0.159	0.184	0.073	
IP1	4.30	1.646	0.152	0.065	0.024	-0.013	0.119	**0.928**	0.887
IP2	4.55	1.819	0.102	0.064	0.023	0.044	0.000	**0.941**	

주) 요인추출 방법 : 주성분 분석.
회전 방법 : Kaiser 정규화가 있는 베리맥스.
a. 6 반복계산에서 요인회전이 수렴되었습니다.

4.1 신뢰성 분석

신뢰성 평가에 앞서 탐색적 요인 분석을 실시했다. 요인추출은 주성분 분석법을 이용하였고, 요인회전은 요인들 간의 상호독립성 검정에 유용한 직교회전(Varimax) 방식을 사용했다. 요인의 고유치는 1.0 이상인 것을 추출하였다. 요인 분석 결과 <표 4>와 같이 6개의 요인이 추출되었고, 요인들의 설명력은 81.784%로 나타났으며, 모든 변수에 대한 측정 항목의 요인 적재량은 0.750 이상이었다. 따라서 본 연구의 요인들의 설명력은 유의미한 수준이라고 판단할 수 있다. 요인으로 묶이지 않는 설문항목은 없었다.

다음으로는 요인 분석을 통해 추출된 각 요인에 대한 신뢰성을 분석했다. 신뢰성 분석에는 일반적으로 가장 많이 사용하는 Cronbach's α를 사용했다. 확인 결과 <표 4>와 같이 모든 변수가 0.872~0.933의 분포를 보였다. 일반적으로 0.8~0.9 이상이면 바람직하고 0.6~0.7이면 수용할 만한 수준이라 한다. 따라서 본 연구에 사용된 척도들은 신뢰성이 있다고 할 수 있다. 평균과 편차의 경우 평균은 4.60~5.99, 편차는 1.045~1.337사이를 나타냈다.

4.2 수렴 타당성 분석

잠재변수를 측정하는 관측변수들의 일치성 정도를 알아보기 위해 수렴 타당성을 조사했다. 검정을 위해서 요인 부하량(factor loading), 유의성(critic ratio), 평균 분산추출(AVE : Average Variance Extract), 개념 신뢰도(CR : Composite Reliability)를 분석했다.

요인적재량은 비표준화 계수와 표준화 계수를 모두 조사했다. 본 연구의 표준화 계수는 0.720~0.955로 나타났다. 유의성은 7.507~20.042로 나타났다. 요인 적재량은 표준화 계수가 최소 0.5 이상이어야 하며 0.7 이상이면 바람직하다고 한다. 유의성은 1.965 이상이어야 한다. 평균 분산추출은 0.521~0.748로 나타났으며, 개념 신뢰도는 0.731~0.899로 나타났다. 일반적으로 평균 분산추출은 0.5 이상, 개념 신뢰도는 0.7 이상이면 타당성이 있다고 간주한다[31]. 따라서 본 연구에 사용된 척도들의 수렴 타당성은 확보됐다고 간주할 수 있다. 수렴 타당성 검정에 대한 사항은 <표 5>와 같다.

모형의 적합도는 χ^2 = 250.228, SRMR = 0.0387, GFI = 0.910, AGFI = 0.876, NFI = 0.932, TLI = 0.960, CFI = 0.968, RMSEA = 0.056로 나타났다. AGFI와 RMSEA를 제외하고는 모두 기준치 이내로 나타났다. AGFI와 RMSEA도 양호한 수준의 적합도를 나타냈다. 일반적인 적합도는 χ^2는 0.05 이상, GFI, AGFI, NFI, CFI는 0.9 이상이면 적합, 0.8 이상이면 양호, SRMR과 RMSEA는 0.05 이하면 적합 0.08 이하면 양호한 것으로 본다. 따라서 확인적 요인 분석을 통한 수렴 타당성 조사를 위한 모형 적합도는 적합한 수준이라 간주할 수 있다.

4.3 판별 타당성 분석

두 변인의 상관계수 제곱값보다 각 변인에 대한 AVE 값이 크면 두 변인 간에는 판별타당도가 있다. 이는 수학적으로 각 변인에 대한 AVE 제곱값(the square root of AVE)이 상관 계수보다 작으면 판별타당도가 있다는 것과 같은 의미가 된다. <표 6>은 상관 계수와 AVE 제곱값을 비교한 수치이다. 표를 보면 상관 계수 중 가장 커다란 값이 0.52이고 AVE 제곱값은 0.854로 나타나 어떠한 상관 계수도 AVE 제곱값보다 높지 않다. 따라서 본 연구에서 사용된 문항들의 판별타당성은 확보되었다고 간주할 수 있다.

4.4 연구 모형의 적합도 분석

연구 모형의 적합도를 분석한 결과 χ^2 = 403.297, SRMR = 0.161, GFI= 0.866, AGFI = 0.822, NFI = 0.891, TLI = 0.901, CFI = 0.926, RMSEA = 0.078로 나타났다. 적합도는 χ^2는 0.05 이상, GFI, AGFI, NFI, CFI는 0.9 이상, SRMR은 0.05 이하면 적합

〈표 5〉 수렴 타당성 검증

항목	비표준화 계수	표준화 계수	S.E	유의성	P	평균 분산추출	개념신뢰도
PS1	1.112	0.864	0.068	16.450	***	0.748	0.899
PS2	1.187	0.955	0.068	17.570	***		
PS3	1.000	0.805			-		
PV1	0.976	0.858	0.056	17.311	***	0.705	0.877
PV2	1.058	0.937	0.056	18.790	***		
PV3	1.000	0.842			-		
RE1	1.018	0.869	0.057	17.979	***	0.716	0.883
RE2	1.055	0.908	0.056	18.876	***		
RE3	1.000	0.861			-		
SE1	0.945	0.720	0.084	11.308	***	0.521	0.845
SE2	0.958	0.735	0.083	11.554	***		
SE3	1.054	0.842	0.080	13.203	***		
SE4	0.942	0.757	0.079	11.910	***		
SE5	1.000	0.748			-		
UI1	1.091	0.888	0.054	20.042	***	0.735	0.892
UI2	1.134	0.921	0.054	21.166	***		
UI3	1.000	0.880			-		
IP1	1.116	0.994	0.149	7.507	***	0.578	0.731
IP2	1.000	0.805			-		

χ^2 = 250.228, df = 138, p = 0.000, χ^2/df = 1.813.
SRMR = 0.0387, GFI = 0.910, AGFI = 0.876, NFI = 0.932, TLI = 0.960, CFI = 0.968, RMSEA = 0.056.

〈표 6〉 판별 타당도 분석

Construct	1	2	3	4	5	6
PS	**0.95**					
PV	0.52	**0.94**				
RE	0.25	0.18	**0.94**			
SE	0.14	0.20	0.40	**0.92**		
UI	0.38	0.39	0.50	0.41	**0.94**	
IP	0.06	0.12	0.35	0.41	0.31	**0.85**

주) 대각 행렬에 있는 값들은 각 변수의 평균 추출 분산의 제곱근 값들임.

한 것으로 본다. RMSEA이 경우는 0.05 이하면 적합, 0.08 이하면 양호한 것으로 본다. 연구모형 적합도를 나타내는 지수 수치 중 절대적합지수를 나타내는 SRMR을 제외하고는 모델 적합도가 좋거나 양호한 것으로 나타났다. 선행 연구에서는 구조방정식 모형의 적합도 기준들은 상대적 지수이고 표본의 크기와 측정 변인의 수에 민감하므로 다른 지수들과 통합적으로 고려하여 살펴보아야 한다고 지적하고 있다[31]. 따라서 본 연구에서 설정한 연구모형은 SRMR 지수가 양호하지는 않지만 SRMR을 제외한 다른 수치들이 적합하거나 양호하므로 종합적으로 판단하였을 때 본 모형은 수용할 만한 적합도 수준을 가지고 있다고 판단된다.

4.5 구조모형 분석

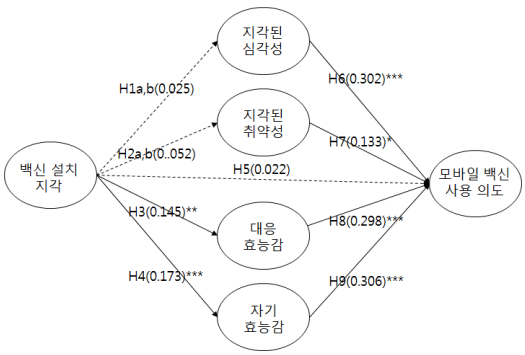
스마트폰 이용자의 악성코드 제거용 모바일 백신 이용 의도에 미치는 요인을 검증한 결과 <표 7>과 같이 나타났다. 백신 설치 지각은 대응 효능감과 자기 효능감에는 (+)의 영향을 미치는 것으로 나타났다. 지각된 심각성, 지각된 취약성, 대응 효능

감, 자기 효능감은 스마트폰 보호 의도에 (+)의 영향을 주는 것으로 드러났다. 그러나 백신 설치 지각은 지각된 심각성, 지각된 취약성, 그리고 보호 의도에 영향을 준다는 근거는 찾을 수 없었다.

〈표 7〉 가설 검증 결과

가설	경로	계수값	t-값	p-값	채택 여부
H1a	IP→PS	0.025	0.691	0.490	기각
H1b	IP→PS	0.025	0.691	0.490	기각
H2a	IP→PV	0.052	1.134	0.257	기각
H2b	IP→PV	0.052	1.134	0.257	기각
H3	IP→RE	0.145	.3.275	0.001	채택
H4	IP→SE	0.173	4.344	***	채택
H5	IP→UI	0.022	0.504	0.614	기각
H6	PS→UI	0.302	4.142	***	채택
H7	PV→UI	0.133	2.279	0.023	채택
H8	RE→UI	0.298	4.697	***	채택
H9	SE→UI	0.306	3.992	***	채택

연구 모형 분석의 결과는 [그림 2]와 같다.



[그림 2] 연구 모형 분석 결과

5. 논의, 한계, 향후 연구 방향 및 기여

5.1 연구 결과 논의

이 연구 모형의 검정 결과 스마트폰 보호동기이론은 이용자의 모바일 악성코드용 백신 이용의도에 대해 양호한 설명력을 보였다. 연구 결과 스마트폰 이용자가 모바일 악성코드용 백신 설치를 지각하는 경우 대응 효능감과 자기 효능감에 유의한 영향을 미치고, 지각된 심각성, 지각된 취약성, 대응 효능감, 자기 효능감은 스마트폰 보호 동기에 유의한 영향을 미친다는 가설이 채택됐다. 반면 모바일 악성코드용 백신 설치 지각만으로는 지각된 심각성, 지각된 취약성에 유의한 영향을 준다는 가설 및 백신 설치 지각이 악성코드용 모바일 백신 이용 의도에 영향을 준다는 가설은 기각됐다.

본 연구 결과를 분석하면 다음과 같은 설명이 가능하다. 첫째, 백신 설치 지각은 지각된 심각성과 지각된 취약성을 감소시킨다는 가설이 기각됐다. Johnston and Warkentin[32]의 연구에 따르면 위협에 대한 지각은 보안 소프트웨어 이용 동기에 필수적 요소라고 한다. 또한 Loch et al.[39]의 주장에 따르면 이용자는 위협은 자신이 아닌 다른 사람에게 더 잘 나타날 것으로 믿는 경향이 있다고 한다. 또한 Croog and Richards[27]의 연구에 따르면 부정적 경험에 노출된 사람은 부정적인 결과가 나타날 가능성에 대한 지각이 높다고 한다. 그럼에도 불구하고 백신 설치 지각과 지각된 심각성과 지각된 취약성의 유의성이 검증되지 않은 것은 스마트폰이 보급된 지 아직 오래되지 않아 스마트폰 사용 중에 보안 위협을 직접 경험 또는 피해 사례를 미디어 또는 주변의 지인 등을 통해 습득한 이용자가 적어 백신 설치 지각이 보안 위협 평가(심각성, 취약성)에 영향을 주지 못한 것으로 보인다.

둘째, 백신 설치 지각은 모바일 백신 이용 의도에 직접적인 영향을 준다는 가설이 기각됐다. 이는 인지 과정에서 지각이 바로 의도에 영향을 주는 것이 아니라 인지 과정을 통해 백신 이용 의도에 영향을 주기 때문이라 판단된다. 이는 Rogers[47]가 주장한 위협의 인지는 태도나 행동에 직접 변화를 주지 않지만 위협 평가와 대응 평가를 통해 보호동기가 생성된다는 것을 뒷받침해 주는 근거라고 판단된다. 따라서 이용자가 백신 설치를 지각하면

이는 모바일 백신 이용 의도에 직접 영향을 주기보다는 대응 효능감과 자기 효능감을 중심으로 매개적으로 영향을 준다고 보는 것이 타당해 보인다.

셋째, 모바일 백신 설치 지각은 대응 평가(대응 효능감과 자기 효능감)에 유의한 영향을 주는 것으로 나타났다. 이는 이용자가 백신의 효능감에 대한 지식을 사전에 습득한 상태에서 모바일 어플리케이션을 이용하면서 모바일 악성코드용 백신에 지속적이고 반복적으로 노출되기 때문에 노출 효과에 의해 이용자들이 유의한 영향을 받을 것으로 보인다. 이는 단순 노출 효과로도 설명이 가능하다. 한자(Chinese character)에 익숙하지 않은 미국 대학생들을 대상으로 의미를 알 수 없는 한자를 노출시켰을 때 한자에 가장 많이 반복해서 노출된 집단이 한자의 의미를 더 호의적으로 평가했다고 한다[56]. 따라서 스마트폰 이용자의 경우 백신이 위협과 취약점에 대응하기 위한 수단이라는 것을 알고 있는 상태에서 악성코드용 모바일 백신에 노출 및 지각되어 효능감이 발생한 것으로 보인다.

넷째, 보호동기이론의 주요 변수(지각된 심각성, 지각된 취약성, 대응 효능감, 자기 효능감) 모두 스마트폰 백신 이용 의도에 영향을 준다는 가설이 채택됐다. 이는 본 연구 결과가 Floyed et al.[30]의 보호동기이론의 모든 위협 및 대응 평가 변수들은 보호 행동을 이해하고 예측하는데 유의한 영향력이 있다는 연구 결과를 뒷받침해 주는 결론을 의미한다. 또한 Johnston and Warkentin[32], Lee[36], Lee and Larsen[38]의 연구와 같이 보호동기이론이 IS 분야 및 정보보호(information security)의 설명에 있어서 적합하다는 것 외에 스마트폰의 모바일 악성코드용 백신 이용과 관련한 연구에도 적합하다는 것을 보여준다. 그러나 보호동기이론이 IS 분야의 모든 연구에서 지지를 받는 것은 아니다. 예를 들면 Zhang and McDowell[57]의 온라인 이용자의 강한 비밀번호 사용 의도 연구에서는 심각성, Mohamed and Ahmad[41]의 SNS에서의 개인정보 노출 의도 연구에서는 대응 효능감, Larose and Rifon[34]의 개인 컴퓨터의 데이터 백업 의도 연구에서는 자기 효능감이 각각 유의성이 검증되지 않았다. 따라서 보호동기이론도 연구 분야와 대상에 따라 일부 상이한 결과가 나올 수 있다.

5.2 연구의 기여

본 연구는 다음과 같은 기여가 있다. 학문적으로는 첫째, 보호동기이론을 스마트폰 백신 이용 의도에 처음 적용했다. 이 이론은 최근 IS 분야에서 활발히 활용하고 있지만 아직 전통적인 PC 환경에만 적용되고 있다. 따라서 본 연구는 보호동기이론의 연구 영역을 스마트폰 영역으로 확장시켰다는 학문적 기여가 있다. 또한 아직까지 국내에서는 IS 분야에서 보호동기이론을 사용한 연구 사례가 알려지지 않고 있다. 보호동기이론은 위협과 대응 평가(appraisal)가 가능한 분야에서 적용 가능성이 높은 이론이다. IS 분야에서는 정보 보안과 사이버 불링(Cyber Bulling) 분야가 대표적 연구 영역이 될 것으로 판단된다. 위의 두 분야는 최근 급격히 발달해 학문적으로 연구가 많이 필요한 분야이므로 보호동기이론을 활용한 연구가 증가할 것으로 보이며, 본 연구가 정보보안 또는 사이버 불링 분야의 연구에 보호동기이론을 적용하는 데에 있어서 학문적으로 기여하는 바가 있다고 하겠다.

둘째, 이 연구는 보안 제품의 기술 수용에 대한 새로운 관점을 제시했다. 기술 수용에 관한 연구는 일반적으로 기술수용이론(Technology Acceptnce Model), 합리적행동이론(Theory of Reasoned Action), 계획된행동이론(Theory of Planned Behavior), 기술확산이론(Innovation Diffusion Theory) 등을 활용해 왔다. 그러나 보안 제품 및 서비스는 기존의 IT 제품과 다른 위협과 관련한 가치(value)가 있다. 따라서 기존의 유용성, 편의성 등으로는 설명이 되지 않는 요소들이 있다. 이러한 연구의 한계에 대해서 보호동기이론의 위협평가 및 대응평가는 보안 관련 기술 수용에 있어서 새로운 평가 모델을 제시할 수 있다고 판단된다.

셋째, 스마트폰의 백신 설치 지각은 위협 평가

보다는 대응 평가와 관련이 있음을 밝혔다. 현재까지 IS 분야에서 백신 설치 지각에 대한 연구들은 위협 평가가 보호 의도에 더 많은 영향력을 주는 것으로 나타났다[143]. 그러나 본 연구에서는 대응 평가가 보호 의도에 더 많은 영향력을 주는 것으로 나타났다. 이에 따라 위협 평가와 대응 평가에 대한 추가적인 연구 필요성이 있음을 도출했다. 향후 연구에서는 Floyed et al.[30]의 보호동기 이론의 전체 모형의 내적 · 외적 보상과 비용을 함께 고려한 연구가 필요해 보인다.

실무적으로는 첫째, 스마트폰의 백신 설치 지각이 대응 평가 관련 변수(대응 효능감 및 자기 효능감)에 영향을 미치는 것으로 밝혀짐에 따라 모바일 백신에 대한 홍보 및 노출을 지속적할 필요성이 있다. 스마트폰 어플리케이션에서 악성코드용 백신의 지각을 높이기 위해서는 스마트폰에 모바일 백신이 설치되어 있다는 것을 TV, 신문 등 언론을 통해 홍보하고 내용에 모바일 백신의 기능, 사용 방법 등을 포함할 필요가 있다. 이 외에 백신 어플리케이션의 초기 화면 디자인을 다른 어플리케이션들과 차별화하는 것을 고려해야 한다. 이 외에 온라인, 오프라인의 악성코드용 백신들과 동일한 브랜드 이미지를 사용함으로써 스마트폰 이용자가 이를 쉽게 지각할 수 있도록 해야 한다.

둘째, 스마트폰 이용자들에게 홍보할 내용으로는 연구 결과 경로 계수가 높은 스마트폰 보안의 심각성, 모바일 백신의 우수성, 모바일 백신의 사용 편의성 등을 고려해야 한다. 경로 계수는 독립변수가 종속변수에 미치는 영향력의 세기를 의미한다. 따라서 본 연구 결과에 의하면 동일한 조건하에서 모바일 백신의 이용 의도에 영향을 주기 위한 심각성(0.302)에 관한 홍보는 취약성(0.133)에 관한 홍보 보다 약 2.3배의 효과가 있게 된다.

셋째, 스마트폰 이용자들에게 취약점에 대한 인식을 높일 필요가 있다. 연구 결과 스마트폰 이용자들은 스마트폰 보안 위협에 대한 심각성, 대응 효능감, 자기 효능감은 높게 나타났지만 취약성은 상대적으로 낮은 것으로 나타났다. 따라서 스마트폰 악성코드용 백신 이용 의도를 높이기 위해서는 스마트폰 이용자의 취약성에 대한 인식을 높이는 방안을 찾아야 한다. 이를 위해서는 스마트폰 이용자들 대상 취약성 교육, 홍보, 피해 사례 홍보 등이 필요해 보인다.

6.3 연구의 한계 및 향후 연구 방향

이 연구는 다음과 같은 한계가 있다. 첫째, 이 연구는 스마트폰 이용 환경을 대상으로 하고 있어서 백신 설치 지각을 포함한 본 연구 모형을 다른 분야에 적용하는 것에 한계가 있을 수 있다. 따라서 연구 모형의 일반화를 위해 향후에는 다른 환경과 다른 맥락에서 동일한 연구를 진행할 필요가 있다. 특히, 기업들에서 종사자를 대상으로 백신을 설치하는 환경 또는 서비스 이용 중에 은행, 보험사 등에서 자동으로 설치하는 PC 및 모바일 백신 등에 대해 백신 설치 지각과 보호 행위 의도에 대한 연구가 가능할 것으로 보인다.

둘째, 이 연구는 스마트폰이 출시될 때 자동으로 백신을 설치해서 출고하는 안드로이드 계열만을 대상으로 진행했다. 스마트폰 시장을 양분하고 있는 IOS 계열의 경우 백신을 자동으로 설치하지 않고 있어서 현재로서는 연구 대상이 되지 못하고 있다. 따라서 향후 애플이 악성코드용 모바일 백신을 자동을 설치한 스마트폰을 출시한다면 연구의 일반화를 위해 IOS 계열의 스마트폰 이용자를 대상으로 추가적인 연구를 진행할 필요가 있다.

셋째, 악성코드용 모바일 백신 이용 의도에 관한 연구에서는 대응 평가 변수들이 위협 평가 변수들과 비교해서 영향력의 강도가 높은 것으로 나타났다. 이는 선행 연구인 Lee[36], Mohamed and Ahmad[41]의 연구 결과와 반대되는 결론이다. Lee [36]의 연구에서는 심각성과 취약성의 경로 계수(path coefficients)가 각각 0.340, 0.367로 나왔으며, 대응 효능감과 자기 효능감은 각각 0.224, 0.177로 나타났다. Lee and Larsen[38]의 연구는 위협 평가와 대응 평가가 비슷한 경로 계수값(심각성 : 0.252,

취약성 : 0.120, 대응 효능감 : 0.215, 자기 효능감 : 0.114)을 나타냈다. 따라서 향후에는 보호동기이론에서 독립변수가 종속변수에 미치는 영향력의 강도를 나타내는 경로 계수값이 상이하게 나타나는 원인을 밝히는 연구를 진행할 필요가 있다.

넷째, 가설이 기각되긴 했지만 백신 설치 지각이 지각된 심각성과 취약성에 (+) 또는 (-)의 영향을 줄 것이라는 가정과 다르게 연구 결과 어떠한 유의성도 검증되지 않았다. 따라서 향후에 백신 설치 지각이 심각성과 취약성에 어떠한 방향으로 영향을 미치는 지에 대한 추가연구의 필요성이 있다.

마지막으로 백신 설치 지각과 관련한 선행 연구 부족으로 인해 측정 항목을 자체 개발하여 측정 항목에 대한 신뢰성과 타당성의 검증이 미흡했다. 따라서 향후 연구에서는 백신 설치 지각이 다른 변수에 미치는 영향 요인에 대한 후속 연구가 필요해 보인다.

6. 결 론

본 연구에서는 스마트폰 이용자의 악성코드용 모바일 백신 이용 의도에 대해서 연구했다. PC 이용자들은 보안 위협의 심각성을 인식하여 다양한 보안 대책을 강구하고 있지만 스마트폰 이용자들은 모바일 백신을 거의 사용하지 않고 있다. 따라서 스마트폰에 자동으로 설치되어 있는 악성코드용 모바일 백신의 이용을 제고하기 위한 연구를 진행했다.

연구 결과에 따르면 스마트폰 이용자가 모바일 악성코드용 백신 설치 지각은 대응 효능감과 자기 효능감에 유의한 영향을 미치고, 지각된 심각성, 지각된 취약성, 대응 효능감, 자기 효능감은 스마트폰 보호 동기에 유의한 영향을 미치는 것으로 나타났다. 반면 모바일 악성코드용 백신 설치 지각은 지각된 심각성, 지각된 취약성에 유의한 영향을 주지 않으며, 백신 설치 지각은 악성코드용 모바일 백신 이용 의도에도 영향을 주지 않는 것으로 나타났다.

따라서, 국내 스마트폰 이용자의 악성코드용 모바일 백신의 이용을 증가시키기 위해서는 연구결과 도출된 바와 같이 백신 설치 지각을 높이고 경로 계수값이 높게 나타난 심각성, 대응 효능감, 자기 효능감을 높이기 위한 지속적인 홍보가 필요해 보인다.

본 연구는 위의 연구를 수행하기 위해 보호동기이론을 활용했다. 최근 국외에서는 IS 분야의 보호동기이론 관련 연구가 증가하고 있으나 국내에서는 아직까지 연구가 거의 이루어지지 않고 있다. 따라서 본 연구가 국내의 IS 분야에서 보호동기이론을 활용한 연구의 활성화에 조금이나마 기여할 수 있기를 바란다.

참 고 문 헌

[1] 김예진, 이규백, “시지각적 특성에 따른 경계의 모호성에 관한 연구”, 「기초조형학연구」, 제13권, 제5호(2012), pp.57-67.

[2] 김여라, “신종플루 뉴스 이용 정도가 개인 및 공중에 대한 건강보호 행위의도에 미치는 영향에 관한 연구 : 보호동기이론을 중심으로”, 「한국언론정보학회」, 통권51호(2010), pp.5-25

[3] 김익수, 정진혁, 이형찬, 이정현, “모바일 악성코드 분석방법과 대응방안”, 「한국통신학회논문지」, 제35권, 제4호(2010), pp.599-609.

[4] 김준홍, “범죄피해 위협과 보호행동을 예측하는 요인들의 성차”, 「한국공안행정학회보」, 제40호(2010), pp.72-113.

[6] 김지훈, 조시행, “사이버 환경에서의 보안위협”, 「한국정보보호학회논문지」, 제20권, 제4호(2010), pp.11-20.

[7] 노성호, 김지선, “범죄의 두려움에 대한 경험적 연구”, 「피해자학연구」, 제6권(1998), pp. 169-205.

[8] 박철현, “범죄피해경험, 이웃통합 그리고 범죄의 두려움 : 대학생에 대한 심층면접결과를 중심으로”, 「피해자학연구」, 제13권, 제1

호(2005), pp.51-77.

[9] 양호일, 「환경디자인 행태학」, 유림문화사, (1990), p.39.

[10] 우형진, "텔레비전 뉴스 시청이 시청자의 건강증진의지에 미치는 영향에 관한 연구", 「한국언론학보」, 제51권, 제2호(2007), pp.308-320.

[11] 이민규, 김영은, "질병 관련 인터넷 정보 이용 효과 연구", 「언론과학연구」, 제9권(2009), pp. 506-539.

[12] 이정모 외, 「인지심리학」, 학지사, (1999), pp. 24-32.

[13] 정만경, 서희석, "과거 및 현재의 모바일 악성코드 증상에 따른 향후 전망 모바일 악성코드 연구", 「2011년 한국컴퓨터교육학회 하계 학술발표논문지」, 제15권, 제2호(2011), pp.179-184.

[14] 정훈영, 서희석, "스마트폰 통신환경 변화에 따른 모바일 악성코드 감염경로 연구", 「한국컴퓨터교육학회 하계 학술발표논문지」, 제15권, 제2호(2011), pp.173-176.

[15] 장상근, "모바일 악성코드의 전략과 사례 분석을 통한 모바일 악성코드 진단법", 「정보보호학회지」, 제23권, 제2호(2013), pp.14-20.

[16] 한국인터넷진흥원, 「모바일 접속환경을 위한 웹사이트 침해예방 연구」, 2010.

[17] 한국인터넷진흥원, 「2012년도 정보보호실태 조사」, 2012.

[18] Ahnlab, "악성코드 분석 특집, 2012 Vol.26", *ASEC REPORT*, 2012.

[19] Ajzen, I. and M. Fishbein, *Understanding Attitudes and Predicting Social Behavior*, Prentice-Hall, 1980.

[20] Anderson, C. L. and R. Agarwal, "Practicing Safe Computing : A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions", *MIS Quarterly*, Vol.34, No.3(2010), pp.613-643.

[21] Axelrod, L. J. and J. W. Newton, "Preventing Nuclear War : Beliefs and attitude of Disarmist and Deterrentist Behavior", *Journal of Applied Psychology*, Vol.21, No.1(1991), pp.29-40.

[22] Bandura, A., "Self efficacy : toward a unifying theory of behavioral change", *Psychological Review*, Vol.84(1977), pp.191-215.

[23] Barden-O'Fallon, J. L., J. deGraft-Johnson, T. Bisika, S. Sulzbach, A. Benson, and A. O. Tsui, "Factors Associated with HIV/AIDS Knowledge and Risk Perception in Rural Malaw", *AIDS and Behavior*, Vol.8, No.2(2009), pp.131-140.

[24] Boer, H. and E. R. Seydel, "Protection motivation theory. In Predicting health behavior : Research and practice with social cognition models (ed)", *Open University Press*, (1996), pp.95-120.

[25] Campbell, K., L. A. Gordon, M. P. Loeb, and L. Zhou, "The Economic Cost of Publicly Announced Information Security Breaches : Empirical Evidence from the Stock Market", *Journal of Computer Security*, No.11(2003), pp.431-448.

[26] Chau, P. Y. K. and P. J. H. Hu, "Investigating healthcare professionals' decisions to accept telemedicine technology : an empirical test of competing theories", *Information and Management,* Vol.39(2002), pp.297-311.

[27] Croog, S. H. and N. P. Richards, "Health Beliefs and Smoking Patterns in Heart Patients and Their Wives : A Longitudinal Study", *American Journal of Public Health*, Vol.67, No.10(1977), pp.921-930.

[28] Crossler, R. E., "Protection Motivation Theroy : Understanding Determinants to Backing Up Personal Data", *Proceedings of the 43rd hawaii International conference on Sys-*

tem Sciences, (2010), pp.1-10.

[29] Doria, M. F., N. Pidgeon, and P. Hunter, "Perceptions of Drinking Water Quality and Risk and Its Effects on Behaviour : A Cross-national Study", *Science of the Total Environment*, Vol.407(2009), pp.5455-5464.

[30] Floyed D. L., S. Prentice-Dunn, and R. W. Rogers, "A meta-analysis of research on protection motivation theory", *Journal of Applied Social Psychology*, Vol.30(2000), pp. 407-429.

[31] Hair, J. F., B. Black, B. Babin, R. E. Anderson, and R. L. Tatham, *Maltivariate data analysis(6th ed.)*, Pearson Prentice Hall, 2006.

[32] Johnston, A. C. and M. Warkentin, "Fear appeals and information security behaviors : An empirical study", *MIS Quarterly*, Vol. 34, No.3(2010), pp.549-566.

[33] Krebs, B., "Hacking Home PCs Fueling Rapid Growth in Online Fraud", *Washington Post*, Technology Section, Special Reports, Cyber-Security, 2005.

[34] LaRose, R. and N. Rifon, "You Privacy Is Assured of Being Invaded", *New Media and Society*, Vol.8, No.4(2006), pp.1009-1030.

[35] Lee, D., R. Larose, and N. Rifon, "Keeping our network safe : a model of online protection behaviour", *Behaviour and Information Technology*, Vol.27, No.5(2008), pp.445-454.

[36] Lee, Y., "Understanding anti-plagiarism software adoption : An extended protection motivation theory perspective", *Decision Support Systems*, Vol.50(2011), pp.361-369.

[37] Lee, Y. and K. Kozar, "Investigating factors affecting the adoption of anti-spyware systems", *Communications of the ACM*, Vol.48, No.8(2005), pp.72-77.

[38] Lee, Y. 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, No.2(2009), pp.177-187.

[39] Loch, K. D., H. H. Carr, and M. E. Warkentin, "Threats to Information Systems : Today's Reality, Yesterday's Understanding", *MIS Quarterly*, Vol.16, No.2(1992), pp.173-186.

[40] Milne, S. E., S. Orbell, and P. Sheeran, "Combining motivational and volitional interventions to promote exercise participation : Protection motivation theory and implementation intentions", *British Journal of Health Psychology*, Vol.7(2002), pp.163-184.

[41] Mohamed, N. and I. H. Ahmad, "Information privacy concerns, antecedents and privacy measure use in social networking sites : Evidence from Malaysia", *Computer in Human Behavior*, Vol.28. No.6(2012), pp.2366-2375.

[42] Obermiller, C., "The Baby Is Sick/The Baby Is Well : A Test of the Environmental Communication Appeals", *Journal of Advertising*, Vol.24, No.2(1995), pp.55-71.

[43] Prentice-Dunn, S. and R. W. Rogers, "Protection motivation theory and preventive health : Beyond the health belief model, Health Education Research", *Theory and Practice*, Vol.1(1986), pp.153-161.

[44] Richardson, R., *2011 CSI Computer Crime and Security Survey*, Computer Security Institute, 2012.

[45] Rippetoe, P. A. and R. W. Rogers, "Effects of Components of Protection-Motivation Theory on Adaptive and Maladaptive Co-

ping With a Health Threat", *Journal of Personality and Social Psychology*, Vol.52(1987), pp.596-604.

[46] Rogers, R., "Protection motivation theory of fear appeal and attitude change", *Journal of Psychology*, Vol.91, No.1(1975), pp.93-114.

[47] Rogers, R. W., "Cognitive and Physiological Processes in Fear Appeals and Attitude Change : A Revised Theory of Protected Motivation", *Social Psychophysiology : A Sourcebook*, The Guilford Press, 1983.

[48] Schafer, R. B., E. Schaefer, G. Bultena, E. Hoiberg, "Coping with a health threat : a study of food safety", *Journal of Applied Social Psychology*, Vol.23(1993), pp.386-394.

[49] Symantec, *Internet Security Threat Report*, Vol.18(2013).

[50] Symantec, *Norton Report*, 2013.

[51] Tanner, J. F., J. B. Hunt, and D. R. Eppright, "The protection motivation model : A normative model of fear appeal", *Journal of Marketing*, Vol.55(1991), pp.36-45.

[52] Vance, A., M. Siponen, and S. Pahnila, "Motivation IS security compliance : Insights from Habit and Protection Motivation Theory", *Information and Management*, Vol.49 (2012), pp.190-198.

[53] Walker, E. A., A. Caba, C. B. Schechter, C. E. Basch, E. Blanco, T. DeWitt, M. R. Kalten, M. S. Mera, and G. Mojica, "Measuring Comparative Risk Perceptions in an Urban Minority Population : The Risk Perception Survey for Diabetes", *The Diabetes Educator*, Vol.33(2007), pp.103-110.

[54] Weinstein, N. D., "Testing four competing theories of health-protective behavior", *Health Psychology*, Vol.12(1993), pp.324-333.

[55] Woon, M. Y., G. W. Tan, and R. T. Low, "A protection motivation theory approach to home wireless security", *Proceedings of the Twenty-Sixth International Conference on Information Systems*, 2005.

[56] Zajonc, R. B., "Attitudinal effects of mere exposure", *Journal of Personality and Social Psychology*, Vol.9(1968), pp.1-27.

[57] Zhang, L. and W. C. McDowell, "Am I Really at Risk? Determinants of Online Users' Intentions to Use Strong Passwords", *Journal of Internet Commerce*, Vol.8, No.3/4(2009), pp.180-197.

◈ 저 자 소 개 ◈

장 재 영 (jyjang31@gmail.com)

현재 연세대학교 정보대학원 박사과정에 재학 중이며, 한국인터넷진흥원 책임연구원으로 근무하고 있다. 영국의 웨스트민스터대학교에서 정보통신 정책과 규제를 전공했다. 주요 관심분야는 프라이버시 보호, 위치정보 보호, 스팸 대응 정책 및 기술, 디지털비즈니스 전략이다.

김 지 동 (jidongkim@yonsei.ac.kr)

현재 연세대학교 지식서비스보안 석사 과정 중이다. 주요 관심분야는 개인정보보호, 금융정보보호, IT서비스 등이다.

김 범 수 (beomsookim@gmail.com)

현재 연세대학교 정보대학원 부원장으로 재직 중이며, 한국정보시스템감사협회(Information Systems Audit and Control Association) 회장직을 맡고 있다. 미국의 시카고 일리노이대학교에서 교수로 재직했으며, 한글과컴퓨터의 감사를 역임했다. 연구 관심분야는 프라이버시 법률과 정책, 정보 보안과 프라이버시 보호의 모범 사례, 클라우드 컴퓨팅 서비스의 보안과 프라이버시 관리, 기업의 보안과 프라이버시 보호 정책, IT 산업에서의 경제적인 이슈이다.