「정보시스템연구」 제24권 제3호
한국정보시스템학회
2015년 9월, pp. 01~19
http://dx.doi.org/10.5859/KAIS.2015.24.3.1

스마트폰 사용자의 보안수칙 실천 부족에 관한 연구 : 효능감의 역할을 중심으로

김 재 현* · 김 종 기**

〈목 차〉

Ⅰ. 서 론

스마트폰 보안문제는 사용자가 상황을 명확히 인식하지 못한 상태에서 발생한다. 스마트폰은 절전기능으로 인해 탐지기능이 낮아져 몰래 요금이 차감되거나 악성코드가 설치된다. 사용자는 편리한 서비스 사용을 위해 스스로 위치정보를 활성화해 놓고 출처가 확인되지 않은 와이파이에 자동 접속되도록 설정해두는 경우가 많다. 이는 해킹과 악성코드 감염 위험에 노출돼 심각한 문제가 된다.

스마트폰 사용자의 보안수칙 실천 방법은 다양하다. 사용자는 보안프로그램을 설치해 악성코드를 정기적으로 검사하고 최신버전 업데이트를 통해 보안문제를 통제할 수 있다. 또한, 보안이 취약한 자동로그인과 자동접속 기능 등의 사용을 자제하고 의심이 되는 URL을 함부로 클릭하지 않도록 주의해야 한다. 의심스러운 애플리케이션은 내려받지 않고, 발신인이 의심스러운 메시지나 이메일은 삭제해야 한다. 특수문자가 포함된 강력한 비밀번호를 사용하고 수시

* 부산대학교 경영학과 박사과정, 주저자, kjh5315@pusan.ac.kr
** 부산대학교 경영학과 교수, 교신저자, jkkim1@pusan.ac.kr

로 변경하는 노력도 필요하다. 특히 와이파이, 위치정보, 블루투스 등의 기능을 켜놓지 않고 필요할 경우에만 켜놓아야 한다. 사용자는 보안위협에 대처하기 위해 많은 시간을 투자하고 노력하는 지속적인 보안관리가 필요하다(김종기 외, 2008).

보안의 가장 기본적인 기조는 예방이다. 스마트폰 사용자는 예방을 위한 기본적인 보안수칙을 실천하지 않는 경우가 많다. Furnell(2005)은 상당수의 사용자가 보안문제와 대처기능을 명확히 알지 못하여 어려워하고, 사용자가 보안을 하지 않는 이유에 대해 보안기능이 시스템에 내제되어 있고 고급 단어와 기술용어를 사용하는 문제에 대해 지적했다. 사용자는 어렵고 생소한 용어의 보안문제가 매번 새롭게 등장하고, 공격형태가 계속 진화하는 환경에 적응하는 것은 쉽지 않다. 사용자 대부분은 보안기술을 효율적으로 이용하지 않고, 보안문제를 정확히 인지하지 못하고 있다(김종기 외, 2009). 해당 위협에 대처하는 보안영역을 전문가의 영역이라고만 생각한다. 이러한 상황임에도 불구하고 기존 보안 분야 연구자들은 단순히 보안위협 인식이 보안행동을 유발하는가에 대한 설명에 중점을 둔다. 그러나 사용자의 보안위협 인식만으로 보안수칙 실천을 하지 않는 현상을 설명하는 데 한계가 있다. 보안문제에 대처하는 자기대처신념에 따라 보호동기 유발 과정은 다를 수 있다(Witte, 1992). 단순히 보안위협 인식과 보안문제를 스스로 해결할 수 있는 자기신념의 기제를 고려해 사용자 스스로 보안수칙을 실천하는 메커니즘의 논의가 필요하다.

최근 보안문제는 어려운 용어 사용과 복잡성으로 인해 사용자가 적절히 대응하기 어렵다(김종기, 2006). 따라서 언론매체를 통해 전문가가 제안하는 보안권고사항을 따르는 것이 매우 중요하다. 그러나 사용자들은 보안권고사항(보안수칙)을 따르지 않는다. 왜 스마트폰 사용자는 보안이 취약하다고 생각하지만, 보안권고사항을 따르지 않는가? 이러한 모순된 현상은 다음의 세부 질문으로 이어진다. 첫째, 보안문제에 적절히 대처할 수 있다고 판단할 때 보안권고사항을 따르고자 하는가? 둘째, 보안문제를 스스로 통제할 수 없다고 판단할 때 공포가 유발돼 보안문제를 부정(보안권고사항을 따르지 않고 정서적 거부)하는가? 본 연구는 이러한 스마트폰 사용자의 모순된 현상을 밝히기 위해 개별 사용자의 자기(Self) 인식수준을 논의한다. 자기 인식수준은 보안문제에 적절히 대처하는 자기신념으로 효능감(Efficacy)의 측면을 고려했다. 본 세부 연구 질문을 바탕으로 사용자가 위협에 대처하는 자신감의 정도에 따라 다른 평가과정(위험통제과정과 공포통제과정)이 유발되는가를 밝힌다(Witte, 1992). 본 검정결과는 스마트폰 보안 권고사항을 이행하지 않는 사용자의 인식 과정을 설명한다. 연구과정은 다음과 같다. 첫째, 문헌연구를 통해 위협평가요인, 대처평가요인, 그리고 보안권고사항을 이행하지 않는 감정적 대처과정 요인을 확인해 모형을 구성한다. 둘째, 사용자의 대처평가를 좀 더 명확하게 측정하기 위해 다른 척도구성과 실험방법(메시지 자극)을 이용해 자료수집 후 모형을 검증한다.

Ⅱ. 선행연구

2.1 확장된 병행과정모델

확장된 병행과정모델(Extended Parallel Process Model)은 효능감의 인식 수준에 따라

위협인식이 두 방향의 결과변수로 분류된다. 두 방향은 위험통제과정과 공포통제과정이며, 결과변수를 보호동기(Protection Motivation)와 방어동기(Defensive Motivation)로 설명한다(Witte, 1992). 보호동기는 실제 보안권고사항 실천을 의미하고, 방어동기는 직접 행동하지 않고 스스로 공포만을 통제하여 위협의 존재를 부정한다. 확장된 병행과정모델은 인지된 위협과 인지된 효능감의 상호작용을 논의한다. 효능감이 낮을 경우 공포가 유발되며, 공포는 감정적 방어동기인 공포통제과정을 유발한다(Witte, 1992, 1994). 공포통제과정은 합리화, 부정, 방어적 회피, 메시지 축소, 메시지 거부 등을 포함한다(Witte, 1992; Liang and Xue, 2009). 특히 공포통제과정은 절망으로 표현되며(Leventhal, 1971), 이 공포과정에 빠지면 위협에 직접 대응하지 않고 오로지 감정통제에 집중한다(Witte, 1992, 1994). 반면, 효능감이 높은 경우 긍정적 보안태도와 보안행위의도를 포함하는 위험통제과정이 유발된다(Witte, 1992, 1994).

2.2 통제이론과 대처평가

통제이론(Control Theory)은 인간이 매 순간마다 얻기를 바라는 참조가치(Reference Value)와 실제 결과를 비교기(Comparator)라는 메커니즘으로 비교해 인간 스스로 행동을 어떻게 통제하는가를 설명한다(Carver and Scheier, 1982; Carver, 2001). 이 이론은 스스로 행동을 통제하는 피드백 과정(Feedback Processes)에서 자기행동 결과를 다음 행동(이후 행동)의 통제정보로 사용하기 때문에 동기와 정서가 유발된다고 주장한다. 즉, 주어진 상황에 효과적으로 대처 가능한지 자신을 평가해 향후 행동의 방향을 결정하는 것이다. Carver and Scheier(1982)는 성공적으로 해당 상황에 대처할 수 있다 판단될 경우 더 많은 노력을 기울이고, 성공적으로 대처할 수 없다고 판단되는 경우에 통제과정을 이탈한다 했다. 이들은 성공할 수 있는 주관적 믿음의 기대수준이 낮아 개선노력을 하지 않는 행동이탈 또는 심리적 이탈로 통제과정을 설명한다. Lazarus and Folkman(1984)은 대처과정(Coping Process)을 제안했다. 이들은 인간이 직면한 상황에서 스스로 대처할 수 있는가에 대한 피드백과정을 통해 그 상황을 외면하고 감정통제를 할 것인가 또는 적극적으로 대처해 상황을 통제할 것인가를 결정한다 했다. 이들은 스스로 대처가 가능하다고 판단될 때 상황을 통제하고, 대처할 수 없다고 판단될 때는 감정을 통제하는 것으로 보았다. 대처평가는 대처의 다차원적 기능으로 문제중심대처와 감정중심대처를 제안한다. 문제중심대처는 객관적 현실을 변화시켜 문제 해결을 하는 방식으로 대응한다. 예를 들어, 문제중심대처는 사용자가 스마트폰 보호를 위해 보안조치를 수행해 위협의 원천을 직접 다룬다. 반면 감정중심대처는 현실의 변화를 위해 노력하지 않고 부정적 감정인 공포와 스트레스를 조정해 감정을 통제한다. 사용자가 적극적으로 보안위협에 대응하지 않고 거짓된 인식으로 감정의 안정을 유도하는 것이다. Carver and Scheier(1982)와 Lazarus and Folkman(1984)이 제시한 통제(자기조절)와 대처의 메커니즘 이해는 인간이 실체적 문제에 직면했을 때 어떻게 그 문제를 통제하고 대처하는가를 설명한다. 본 이론은 보안위협의 자극에 반응하는 자기조절 메커니즘을 탐구하는 데 참고했다. 본 연구는 스마트폰 사용자가 보안문제에 대해 자신의 행동을 통제하거나 감정을 통제하는가를 탐구

하는 데 중점을 둔다. 통제와 대처를 할 수 없는 상황에서 행동의 결핍과 감정중심대처 반응이 유발된다고 보았다. 본 논의를 바탕으로 문제를 직접 통제하는 위험통제과정과 감정을 통제하는 공포통제과정의 메커니즘을 설명한다.

2.3 기술위협회피이론

Witte(1992)는 확장된 병행과정모델에서 공포통제과정의 결과변수가 다양한 형태로 나타난다 했다. 공포통제과정은 부정, 방어적 회피, 메시지 무시, 그리고 메시지 거부 등 공포를 통제하는 정서적 반응이다. Liang and Xue(2009)는 이러한 정서적 반응을 정보기술수용모델로 단순화해 적용하는 것은 바람직하지 않다고 했다. 이들이 제안한 기술위협회피이론(Technology Threat Avoidance Theory)은 악의가 있는 정보기술인 해킹과 악성코드의 위협을 회피하는 행위에 대해 논의한다. 이 이론은 위협을 수용하는 관점과 회피하는 관점 간의 명확한 차이를 설명하고 있다. 기존 정보기술수용이론으로 정보기술위협의 회피를 설명하는 것은 한계가 있음을 강조한다. Liang and Xue(2009)는 수용과 회피의 이론적 입증과정이 기본적으로 다르며, 회피는 다양한 형태로 나타난다 했다. 회피와 수용은 반대되는 개념이 아니며, 회피는 수용을 제외한 다양한 방향인 합리화, 부정, 방어적 회피, 메시지 축소, 메시지 거부 등으로 나타난다(Liang and Xue, 2009; Carver, 2006). 이들은 문헌연구를 바탕으로 수용과 회피의 차이를 다음과 같이 설명한다. 첫째, 강화이론(Reinforcement Theory)은 보상을 증가시키고 후속 행동의 처벌을 감소시키면 행동 가능성이 커진다 했다. 바람직한 행동에 대한 바람직한 결과인 적극적 강화를 제공해 행동빈도를 높이고 바람직하지 않은 결과를 회피해(부정적 강화) 바람직한 행동의 빈도를 높이는 것은 서로 다르다고 주장한다(Pavlov, 1927; Skinner, 1953). 둘째, 생물학적으로 뇌의 구조 차이가 존재한다 했다. 수용동기와 회피동기는 다른 대뇌반구와 관련돼 있다. 왼쪽 전두엽 피질은 수용행동과 관련되어 있고, 오른쪽 전두엽 피질은 회피행동과 관련되어 있다(Sutton and Davidson, 1997). 셋째, 누적전망이론(Cumulative Prospect Theory)에 따르면 인간은 이익을 수용하려 하고 손실은 회피하는 경향이 있어 수용과 회피는 다른 평가과정을 거친다 했다. 확률이 낮은 상황일 때 이익에 대해 위험을 추구하고 손실 위험은 회피한다(Tversky and Kahneman, 1992). 이러한 자극의 수용과 회피 간의 차이는 명확히 구분된다. 대처효능감이 낮은 스마트폰 사용자가 보안문제를 회피하는 동기(감정통제)를 고려하기 위해 기술위협회피이론을 참고했다.

2.4 자기효능감

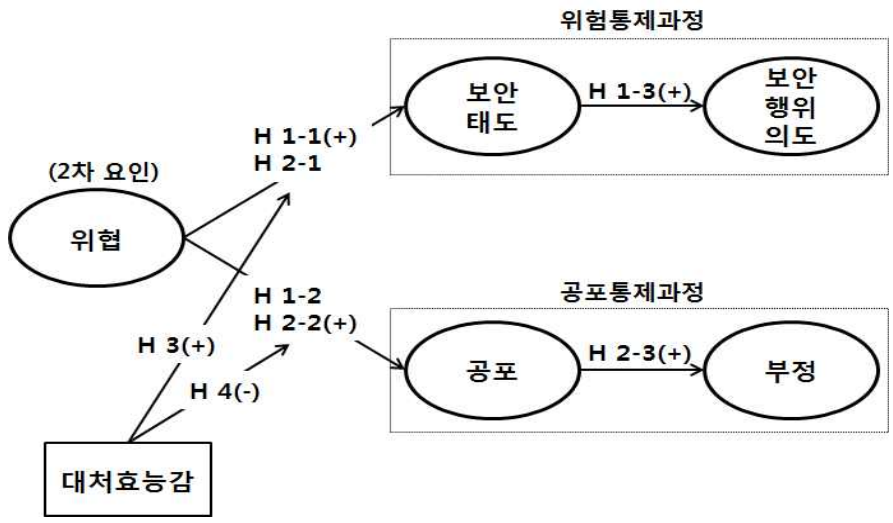
확장된 병행과정모델에서 제안하는 두 방향의 통제과정은 효능감 인식 수준에 의해 결정된다(Witte, 1992). 따라서 효능감에 대한 명확한 이해와 효능감의 차원을 밝힐 필요가 있다. Bandura(1997)는 효능감의 차원을 사회효능감, 자기조절효능감, 학습효능감, 수행효능감, 성취효능감, 관계효능감, 준비효능감, 대처효능감 등으로 세분하여 설명했다. 이들은 자기효능감과 다른 개념 간의 차이를 명확히 구분해 설명한다. 자기효능감은 개인적 수단인 노력과 능력으로 어느 특정 상황을 스스로 통제하는 힘의 정도를 평가되며, 반응효능감은 행동이 결과에 영향을 미치는지에 대한 개인의 신념으로 평가

된다. 반응효능감은 행위에 대한 결과 기대를 평가하여 자기효능감과 의미상으로 명확히 구별된다. 자기효능감은 자기의 능력에 대한 신념이지만, 자기개념(Self Concept)과 자기평가(Self Appraisal)는 자신의 존재를 어떻게 지각하고 해석하는가를 설명한다. Bandura(1997)는 자기효능감이 자신에 대한 복합적 견해로 효능감을 포괄하여 반영한다 했다. 효능감의 개념은 그 수준에 따라 나타나게 되는 인간의 행위를 설명한다. 자기효능감의 수준은 공포의 경험과 각성을 다르게 받아들이는 인간의 행위를 추론한다(Bandura, 1997). 자기효능감이 높은 사람은 정서적 각성(공포)을 에너지 촉진요인으로 받아들이지만, 자기효능감이 낮은 사람은 각성을 에너지의 쇠퇴요인으로 받아들인다(Harris, 1989; Bandura, 1997). 따라서 효능감의 수준에 따라 보안위협에 대처하는 사용자의 일반적 반응과 정서적 각성을 해석하는 데 차이가 있다(Leventhal, 1970, 1971; Carver and Scheier, 1982; Bandura, 1997; Witte, 1992).

Ⅲ. 연구모형과 가설

3.1 연구모형

본 연구는 Witte(1992)의 확장된 병행과정모델을 이용해 스마트폰 사용자의 보안수칙 실천 부족에 관한 현상을 설명하고자 한다. 확장된 병행과정모델의 구성 개념과 개념 간의 관계를 참고해 <그림 1>의 연구모형을 제안했다. 위험통제과정은 보안태도와 보안행위의도를 포함하고, 공포통제과정은 공포와 부정을 포함한다. 본 연구모형은 대처효능감의 수준에 따라 영향관계의 차이를 설명한다. 대처효능감의 수준이 높은 경우, 위협은 위험통제과정을 유발하고 공포를 유발하지 않을 것이다(가설 1-1, 1-2, 1-3). 반면 대처효능감의 수준이 낮은 경우, 위협은 공포통제과정을 유발하고 보안태도를 유발하지 않을 것이다(가설 2-1, 2-2, 2-3).



<그림 1> 연구모형

<표 1> 조작적 정의 및 측정항목

요인		조작적 정의	측정항목	관련 연구
위협	발생가능성	스마트폰 보안문제의 발생 가능성을 인지하는 정도	• 스마트폰이 보안위협에 노출될 가능성 • 스마트폰이 보안문제가 발생할 가능성 • 스마트폰이 악성코드에 감염될 가능성	Rogers(1975) Witte(1992, 1994) Johnston and Warkentin(2010)
	심각성	스마트폰 보안문제의 심각성을 인지하는 정도	• 스마트폰 보안문제는 위협적 • 스마트폰 보안문제는 심각 • 스마트폰 보안문제는 치명적	Rogers(1975) Witte(1992, 1994) Johnston and Warkentin(2010)
보안태도		스마트폰의 보안설정 사용에 대해 사용자가 긍정적으로 평가하는 정도	• 스마트폰 보안기능이 중요하다고 생각 • 스마트폰 보안설정이 현명하다고 생각 • 스마트폰 보안기능 이용이 바람직하다고 생각	Fishbein(1975) Witte(1992, 1994) Johnston and Warkentin(2010)
보안행위 의도		스마트폰을 보호하고자 하는 행동에 대한 의도	• 스마트폰 보안기능을 이용할 의도 • 스마트폰 보안설정을 관리할 생각 • 스마트폰 보안 상태를 점검할 의향	Fishbein(1975) Witte(1992, 1994) Johnston and Warkentin(2010)
공포		스마트폰 보안문제로 자극되어 두려운 정도	• 스마트폰 보안위협에 노출될까 무서움 • 스마트폰 악성코드에 감염되는 두려움 • 스마트폰 해킹공격을 당할 수 있어 불안	Leventhal(1971) Witte(1992, 1994) Witte et al.(1996)
부정		스마트폰 보안문제에 대한 메시지를 인정하지 않는 정도	• 스마트폰 보안문제가 왜곡된 느낌 • 스마트폰 보안문제가 과장된 느낌 • 스마트폰 보안문제가 부풀려진 느낌	Brehm(1966) Witte(1992, 1994) Witte et al.(1996)
대처 효능감		스마트폰 보안과 관련된 자신의 대처능력에 대한 자신감의 정도	• 파밍에 대한 대처 • 스미싱에 대한 대처 • 좀비폰에 대한 대처 • 스파이웨어에 대한 대처 • 애드웨어에 대한 대처 • 키 로깅에 대한 대처 • 제로데이 공격에 대한 대처 • 악성코드가 포함된 앱에 대한 대처 • 악성코드가 포함된 와이파이에 대한 대처 • 트로이 목마 바이러스에 대한 대처	Bandura(1997) Pajares and Urdan(2006)

위협은 개인이 외부로부터 발생한 자극의 존재를 인식하는 것으로(Witte, 1992), 심각성과 발생 가능성으로 평가된다(Rogers, 1975). 발생 가능성과 심각성의 조작적 정의는 <표 1>에 제시되어 있다. 본 연구모형에서 위협은 측정변수를 포함하지 않은 2차 요인인 고차요인모델(Higher-order Factor Model)로 구성했다. 위협은 발생 가능성과 심각성으로부터 형성된 2차 요인이다. 1차 잠재요인은 반영지표(Reflective Indicators)로 구성하고, 1차 잠재요인(발생 가능성, 심각성)과 2차 잠재요인(위협) 간의 관계는 형성 구조(Formative Constructs)관계로 구성했다. 기존연구는 위협평가의 구성요인으로 발생 가능성과 심각성을 고려한다(Rogers, 1975; Liang and Xue, 2009; Johnston and Warkentin, 2010). 따라서 기존의 위협평가 연구를 참고해 일차적 구조를 형성구조인 다차원 구조로 구성했다(Petter et al., 2007; Diamantopoulos, 2011).

3.2 연구가설

3.2.1 위협과 위험통제과정

보안을 위협하는 부정적 정보는 사용자의 보호동기를 자극한다(Liang and Xue, 2009; Johnston and Warkentin, 2010). 많은 연구자는 사용자의 위협인식이 보호동기를 유발하는 것으로 보았다. 위협 메시지는 보안권고사항 수행에 영향을 미치며 위협정보의 양이 증가할수록 설득에 도움이 된다(Leventhal, 1970, 1971). 위협은 보호동기를 유발하며 보호동기의 강도에 영향을 미친다(Rogers, 1975; Witee, 1992). 사람들은 위험에 직면했을 때 효과적으로 상황을 통제하고자 한다(Leventhal, 1970, 1971). 스스로 문제를 통제할 수 있는 신념을 지닌 사람은 위험상황을 스스로 통제하기 위해 노력한다(Bandura, 1997). 즉, 개인의 대처효능감이 높아야만 위협 메시지를 통해 보호동기가 유발된다(Carver and Scheier, 1982, Witte, 1992). 위험통제과정에 포함된 보안태도와 보안행위의도 간의 긍정적 영향관계는 Fishbein(1975)의 합리적행동이론(Theory of Reasoned Action)을 기반으로 기존연구에서 빈번하게 검증됐다. 높은 위협은 스마트폰 보호를 위한 보안권고사항 실천에 대한 긍정적 태도를 유발하며, 스마트폰의 보안권고사항 실천에 대해 사용자가 긍정적 태도를 가질수록 스마트폰을 보호하고자 하는 보안행위의도가 높아진다. 본 논의에 대한 가설은 다음과 같다.

H 1-1: 대처효능감이 높은 집단은 위협이 보안태도에 정(+)의 영향을 미칠 것이다.

H 1-2: 대처효능감이 높은 집단은 위협이 공포에 영향을 미치지 않을 것이다.

H 1-3: 대처효능감이 높은 집단은 보안태도가 보안행위의도에 정(+)의 영향을 미칠 것이다.

3.2.2 위협과 공포통제과정

위협과 효능감의 상호작용은 높은 공포를 유발한다(Witte, 1992). 즉, 위협수준이 높고 효능감의 수준이 낮은 경우 높은 공포가 유발된다. 공포는 문제의 근원을 직접 통제하는 위험통제과정과 영향관계가 존재한다(Hovland et al., 1953; Janis, 1967). 따라서 공포는 권고사항 메시지 수용에 영향을 미칠 수 있다(Bandura, 1997). 다만 기존 공포소구 연구에서 공포의 각성 수준이 매우 높을 때 오히려 메시지 수용에 부정적 영향을 미친다 했다(Hovland et al., 1953). 공포와 행동 사이에 역 U자형 관계를 제안한 Hovland et al.(1953)은 적절한 수준의 공포가 가장 큰 행동변화를 유발하고, 공포의 수준이 매우 높을 경우 오히려 행동변화가 적어진다 했다. 대처효능감이 낮은 상황에서 유발된 공포는 높은 수준의 공포이기 때문에 사용자는 무기력한 상태에 빠질 수 있다(Leventhal, 1971). 위협의 수준이 높고 위협에 대처할 수 있는 효능감이 낮은 상황에서 스마트폰 사용자는 큰 공포를 느끼며, 이는 위험통제과정이 아닌 공포통제과정의 유발 원인이 된다(Witte, 1992). 즉, 효능감의 수준이 낮은 경우 부정적 사고와 불안이 높아져 공포가 유발되며, 이러한 공포로 인해 감정적 통제가 유발된다고 보았다(Bandura, 1997; Witte, 1992). Witte(1992)의 확장된 병행과정모델은 공포요인과 보호동기 간의 인과적 관계를 고려하지 않는다. 다만 공포와 위협 간의 피드백 루프를 제안하고, 모형에서 공포요인을 위험통제과정과 공포통제과정의 중간에 위치시켜 공포의 역할을 설명하고 있다.

인간은 스스로 대처효능감을 평가해 상황을 통제할 수 있는 신념이 낮을수록 문제를 회피한다(Liang and Xue, 2009). 예를 들어, 스마트폰 사용자가 보안위협을 적절히 통제할 수 없을 것이라 믿으면 사용자는 보안위험을 직접 통제하기보다는 부정과 방어적 회피 등 감정을 통제한다. 부정(Denial)은 특정 상황이나 생각, 그리고 느낌을 있는 그대로 받아들이는 것이 고통스럽기 때문에 인정하지 않으려 하는 기제이다(Siponen and Vance, 2010). Leventhal(1971)은 두려움이 높고 권고사항이 효과적이지 않을 때 메시지에 대한 부정과 회피 반응이 일어나며, 이를 통해 두려움이 감소한다고 보았다. 본 논의에 대한 가설은 다음과 같다.

H 2-1: 대처효능감이 낮은 집단은 위협이 보안태도에 영향을 미치지 않을 것이다.
H 2-2: 대처효능감이 낮은 집단은 위협이 공포에 정(+)의 영향을 미칠 것이다.
H 2-3: 대처효능감이 낮은 집단은 공포가 부정에 정(+)의 영향을 미칠 것이다.

3.2.3 대처효능감의 조절효과

대처효능감은 해당 상황에서 개인의 능력과 노력으로 적절히 대처할 수 있는가를 판단하는 평가요인이다(Rogers, 1975; Witte, 1992). 따라서 대처효능감은 어떤 행동을 할 수 있는 신념으로 자신의 대처능력에 대한 자신감 정도로 정의된다(Bandura, 1997). 인간은 실제로 행동을 하기 전에 목표를 이루는 데 필요한 행동을 할 수 있는가를 평가한다. 기존 공포소구 관련 연구에서 위협평가와 대처평가는 계속 강조됐다. Witte(1992)는 위협인식과 대처인식의 상호작용을 통해 보호동기 또는 방어동기가 유발될 수 있다 했다. 공포메시지에 노출된 개인은 해당 위협과 대처를 평가해 보안문제에 대응한다. 개인은 대처평가를 통해 위협에 적극적으로 대응할 것인가 또는 위협을 외면하고 회피할 것인가를 판단한다. 효능감의 수준이 높고 낮음에 따라 서로 다른 통제과정이 유발된다(Carver and Scheier, 1982; Lazarus and Folkman, 1984; Witte, 1992). 본 논의에 대한 가설은 다음과 같다.

H 3: 위협과 보안태도 간의 관계는 대처효능감의 수준에 따라 차이가 있을 것이다.
H 4: 위협과 공포 간의 관계는 대처효능감의 수준에 따라 차이가 있을 것이다.

IV. 연구방법

4.1 자료수집

본 연구에서 발생 가능성, 심각성, 보안태도, 보안행위의도, 공포, 부정 등은 모두 5점 리커트 척도로 측정했다. 대처효능감은 기존문헌을 참고해 100점 척도에 10단위의 간격으로 신념강도를 표시하게 했다(Bandura, 1997; Compeau and Higgins, 1995; Pajares and Urdan, 2006). 대처효능감의 질문문항은 구체적인 보안사항의 대처 여부와 관련된 내용으로 구성했다(Bandura, 1997). 대처효능감을 명확히 평가하기 위해 구체적인 보안위협 10가지를 제시하고, 각 보안위협에 대한 대처의 자신감 정도를 직접 기재하도록 문항을 구성했다. 일반 사용자가 알지 못할 수도 있는 보안 관련 용어는 설명 정보를 각주에 제시하고, 의문이 있는 용어에 대해 진행자에게 자유롭게 질문하도록

했다.

설문조사는 스마트폰을 사용하는 대학생을 대상으로 했다. 연구모형을 검증하기 위해 기존 연구요인과 설문항목을 참고해 연구목적에 맞게 일부를 수정하고 보완했다. 연구의 취지를 설명하고 협조를 구한 후 약 10분 동안 스마트폰 보안위협 메시지와 보안위협에 대처하는 보안권고사항을 제시했다. 총 178부의 설문지를 회수했으며, 불성실하게 응답한 설문이 없어 모두 분석에 사용했다. 수집된 자료의 분석은 SPSS 18과 AMOS 18버전을 이용했다. 구성개념의 조작적 정의와 측정항목은 다음 <표 1>과 같다.

4.2 표본의 특성

스마트폰의 OS유형은 아이폰 OS 사용자가 35명(19.7%)이며, 구글 안드로이드 사용자가 140명(78.7%)이다. 스마트폰의 보안침해 경험에 대한 질문에서 보안침해 경험이 없다고 응답한 사용자는 125명(70.2%), 주변 사람이 보안침해 경험이 있고 직접 보안침해를 경험한 사용자는 모두 53명(29.8%)으로 나타났다. 스마트폰 백신프로그램을 사용하는 사용자는 132명(74.2%)이며, 백신프로그램을 사용하지 않는 스마트폰 사용자는 46명(25.8%)이다.

V. 실증분석 및 결과

5.1 측정모델의 분석

위협은 발생 가능성과 심각성으로부터 형성된 고차요인모델(Higher-order Factor Model)로 측정변수를 포함하지 않는다(Petter et al., 2007; Diamantopoulos, 2011). 2차 요인으로 구성된 위협은 2차 확인적 요인분석(Second-order Confirmatory Factor Analysis)을 수행해 측정모델의 타당성을 확인했다. 분석결과, 표준화 추정치가 모두 0.5 이상으로 나타나 집중타당성이 있음을 확인했다(Segars and Grover, 1993). 개념 신뢰도와 평균분산추출 값은 측정지표의 신뢰성을 검정한다(Fornell and Larcker, 1981). 개념 신뢰도는 0.7 이상으로 나타났고, 평균분산추출 값은 기준치인 0.5 이상으로 나타나 내적 일관성에 문제가 없는 것으로 나타났다(Hair et al., 2010). 판별타당성은 개별 요인 간의 상관계수와 평균분산추출 값의 제곱근 값으로 평가된다(Hair et al., 2010). 평균분산추출 제곱근 값이 상관계수보다 높게 나타나 측정모델의 판별타당성을 확보했다(Fornell and Larcker, 1981). 본 측정모형의 신뢰성, 집중타당성, 판별타당성은 문제가 없다. 확인적 요인분석 결과와 판별타당성 분석 결과는 다음 <표 2>와 <표 3>과 같다.

<표 2> 확인적 요인분석 결과

요인		측정항목	표준화 추정치	표준 오차	임계치	평균 분산 추출값	개념 신뢰도
2차 요인	위협	발생 가능성	0.689	-	-	-	-
		심각성	0.834	0.249	4.531		
1차 요인	발생 가능성	발생 가능성1	0.885	-	-	0.840	0.940
		발생 가능성2	0.968	0.053	19.866		
		발생 가능성3	0.829	0.060	15.222		
	심각성	심각성1	0.767	-	-	0.715	0.882
		심각성2	0.922	0.092	12.487		
		심각성3	0.840	0.103	11.714		
보안태도		보안태도1	0.761	-	-	0.825	0.934
		보안태도2	0.848	0.086	11.304		
		보안태도3	0.858	0.086	11.399		
보안행위의도		보안행위의도1	0.882	-	-	0.797	0.921
		보안행위의도2	0.916	0.069	15.960		
		보안행위의도3	0.738	0.075	11.754		
공포		공포1	0.873	-	-	0.753	0.901
		공포2	0.945	0.063	17.076		
		공포3	0.821	0.063	14.198		
부정		부정1	0.732	-	-	0.839	0.939
		부정2	0.934	0.118	12.397		
		부정3	0.952	0.129	12.376		

<표 3> 판별타당성 분석 결과

요인	평균	표준 편차	발생 가능성	심각성	보안 태도	보안 행위의도	공포	부정
발생 가능성	3.65	0.83	**0.917**					
심각성	2.71	0.90	0.523**	**0.846**				
보안태도	4.36	0.59	0.089	0.148*	**0.908**			
보안행위의도	4.03	0.74	0.069	0.078	0.614**	**0.893**		
공포	3.30	1.00	0.327**	0.383**	0.150*	0.150*	**0.868**	
부정	2.16	0.80	-0.036	-0.092	-0.295**	-0.371**	-0.068	**0.916**

주) 1. 대각선은 AVE제곱근

5.2 동일방법편의

동일방법편의(Common Method Bias)는 체계적 오차 분산(Systematic Error Variance)이 구조관계에서 대안설명을 제공해 심각한 문제를 일으킨다. 일반 행동연구에서 측정분산의 25%가 체계적 오차 분산일 수 있고, 이러한 체계적 오차 분산은 구조 간의 관계를 수축시키거나 팽창시켜 1종 오류와 2종 오류 모두를 유발한다(Podsakoff et al., 2003). 체계적 오차 분산은 실증분석 결과에 심각한 혼란을 주어 잘못된 결과해석의 원인이 된다. 체계적 오차 분산을 유발하는 근원은 매우 다양하다. 동일방법편의는 기본적으로 연구절차의 설계과정에서

통제해야 한다. 본 연구는 설문조사 이전에 연구 설계과정에서 질문순서의 균형을 바로잡고 모호한 문항을 제거하기 위해 노력했다. 또한, 설문 이후 데이터의 분석과정에서 통계적 기법을 이용해 잠재적 동일방법편의를 통제했다.

먼저 하만의 단일 요인 검사(Harman's Single-factor Test)로 동일방법편의의 존재를 확인했다. 탐색적 요인분석에서 회전되지 않은 결과의 설명된 분산수치가 하나의 요인에 집중됐는지 확인했다. 분석결과, 설명된 분산 28.847~5.641, 고유값 6.058~1.185으로 나타나 동일방법편의 문제가 없음을 확인했다.

두 번째로 동일잠재요인(Common Latent Factor)을 이용해 체계적 오차분산을 확인하고 통제했다. 동일잠재요인 방법은 체계적 오차분산의 구체적 원인은 식별하지 못하지만, 체계적 오차분산의 존재 여부를 밝히고 기술적으로 통제가 가능하다(Podsakoff et al., 2003). 분석을 위해 구조모형에 포함된 모든 측정변수와 연결된 동일잠재요인을 개입시켰다. 분석결과의 해석은 동일잠재요인이 개입된 모형의 표준화 추정치를 검토해 동일방법분산의 비율을 확인하여 평가된다. 동일방법요인 적재치가 유의하지 않고, 지표분산이 방법분산보다 상당히 크면 동일방법편의를 우려하지 않아도 된다(Williams et al., 2003; Liang et al., 2007). 분석결과, 관측된 지표에 의해 설명되는 평균분산은 0.74로 나타났으며, 동일잠재요인에 의해 설명되는 평균분산은 0.02로 나타났다. 지표에 의해 설명되는 평균분산 대비 동일방법분산의 평균비율은 30 : 1이다. 또한, 대부분의 방법요인 적재치는 각 측정지표에 통계적으로 유의하지 않았다. 따라서 본 연구모형은 동일방법편의를 심각하게 염려하지 않아도 된다.

세 번째 동일방법편의의 원인으로 사회적 바람직성 편의(Social Desirability Bias)를 확인했다. 사회적 바람직성 편의는 응답자가 실제 생각과 느낌을 사실대로 응답하지 않고 사회적으로 바람직하게 응답하는 것을 말한다(Podsakoff et al., 2003). 사회적 바람직성은 사회적 인정, 사회적 수용, 그리고 사회적 신념을 위해 필요하며 문화적으로 허용된 적절한 행동으로 성취된다(Crowne and Marlowe, 1964). 사회적 바람직성 편의는 거짓된 관계를 생성해 변수 간의 진정한 관계를 방해한다(Podsakoff et al., 2003). 또한, 설문지법 연구에서 인위적인 분산의 잠재적 원인이 된다. 일반적으로 부정적 행동은 사회적 바람직성 편의에 부분적으로 기인하며, 응답자는 자기보고에 의한 설문지 작성과정에서 그들의 부정적 특성과 행동을 과소평가하는 경향이 있다(Turel et al., 2011). 본 연구는 부정적 행동 경향을 묘사하는 문항(부정요인)을 포함하고 있어 사회적 바람직성 편의의 영향을 평가했다. 평가를 위해 가장 최근에 개발된 Stober(2001)의 사회적 바람직성 척도-17을 이용했으며, 국내 상황에 부적절한 항목 2개(마약 관련 항목)를 제외한 15개의 척도를 이용했다. 사회적 바람직성 편의의 영향은 Spearman's의 상관관계 분석으로 평가된다. 부(-)의 상관관계는 응답자가 사회적으로 바람직한 방향으로 응답해 자신을 바람직하게 보이도록 묘사하는 경향이 있다는 것으로 해석된다(Lindell and Whitney, 2001; Turel et al., 2011). 분석결과 사회적 바람직성은 모든 개별요인과 상관관계가 매우 낮았다. 발생 가능성 -0.094, 심각성 0.035, 보안태도 0.083, 보안행위의도 0.128, 공포 -0.174, 부정 -0.177의 상관관계를 보였다. 따라서 본 연구는 사회적 바람직성 편의의 영향이 심각한 문제가 되지 않는다.

<표 4> 구조모델의 적합도 분석 결과

모형 적합도 지수	χ^2 (df, p)	χ^2/df	SRMR	GFI	CFI	IFI	TLI	RMSEA
평가기준	-	3.0 이하	0.08 이하	0.8 이상	0.9 이상	0.9 이상	0.9 이상	0.08 이하
기본모형	385.300 (300, 0.001)	1.284	0.083	0.836	0.964	0.965	0.954	0.040
대처효능감 추가모형	380.911 (298, 0.001)	1.278	0.079	0.838	0.965	0.966	0.955	0.040

5.3 구조모델의 분석

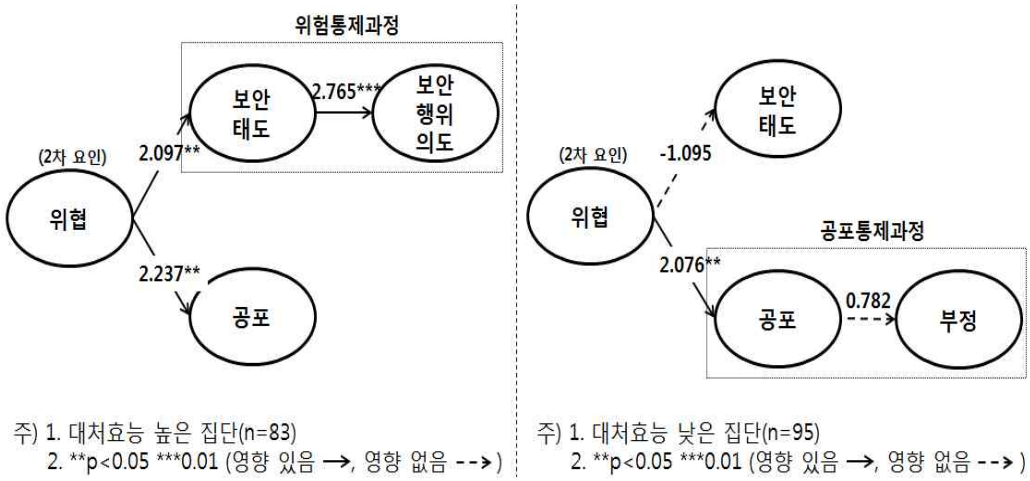
구조모델의 적합도 평가는 χ^2, GFI, CFI, TLI, SRMR, RMSEA 등의 적합지수를 선택해 제시했다(Hair et al., 2010). χ^2값은 자유도의 3배를 넘지 않는 것으로 나타나 구조모델 수용기준을 충족한다(Hair et al., 2010). CFI, IFI, TLI는 모두 수용기준을 충족하고, GFI의 경우 일반적인 수용기준 0.9를 충족하지 못했으나, 0.8 이상의 적합지수를 수용기준으로 하는 문헌을 참고했다(Etezadi-Amoli and Farhoomand, 1996). RMSEA 값은 기준치인 0.05보다 작아 모델의 적합도가 좋은 것으로 나타났다(Browne and Cudeck, 1993). SRMR은 0.08 이하를 기준치로 제시하는 기존연구를 참고해 적합지수 수용 여부를 판단했다(Hu and Bentler, 1999). 본 구조모델의 전반적인 적합도 수치는 수용기준을 만족한다. 구조모델 적합도 분석 결과는 <표 4>와 같다.

5.4 가설검정

대처효능감의 수준을 두 집단으로 분류하기 위해 K-평균 군집분석을 이용했다. 군집분석 결과 대처효능감이 높은 집단(n=83)과 낮은 집단(n=95)으로 분류됐다. 대처효능감이 높은 집단의 평균중심은 59.71이며, 낮은 집단의 평균중심은 27.21이다. 집단 간의 차이를 평가하기 위해 분산분석 결과를 확인한 결과 F값이 325.298(0.000)로 나타나 집단 간의 평균 차이가 통계적으로 유의했다. 군집분석으로 분류된 대처효능감 수준에 따라 개념 간의 인과관계를 확인했다. 분석결과, 첫째, 대처효능감이 높은 집단은 위협과 보안태도 간의 영향관계, 보안태도와 보안행위의도 간의 영향관계가 통계적으로 유의했다. 또한, 스마트폰 사용자가 보안문제에 대처하는 효능감이 높은 경우에 인지된 위협이 공포를 유발할 수 없을 것이라 보는 기존 귀무가설을 대립가설 받아들여 검증하고자 했으나 위협과 공포 간의 영향관계는 통계적으로 유의했다. 따라서 가설 1-1과 가설 1-3은 채택되고, 가설 1-2는 기각됐다. 둘째, 대처효능감이 낮은 집단은 위협과 공포 간의 영향관계가 유의하고, 위협과 보안태도 간의 영향관계가 유의하지 않았다. 스마트폰 사용자가 보안문제에 대처하는 효능감이 낮은 경우에 인지된 위협은 공포를 유발하지만, 보안에 대한 긍정적 태도를 유발하지 않을 것이라 보는 기존 귀무가설을 받아들여 검증했다. 가설 2-1과 가설 2-2는 채택됐다. 그러나 공포와 부정 간의 영향관계는 없는 것으로 나타났다. 공포가 보안문제 관련 메시지를 인정하지 않는 부정의 정도에 영향을

미치지 않았다. 따라서 가설 2-3은 기각됐다. 가설검정 결과는 <그림 2>과 같다.

대처효능감 수준에 따른 모수차이검정 결과는 다음과 같다. 첫째, 위협과 보안태도 간의 영향관계는 대처효능감의 수준에 따라 차이가 있다. 대처효능이 높은 사용자는 보안위협과 보안태도 간의 영향관계가 통계적으로 유의했다. 그러나 상대적으로 대처효능이 낮은 사용자는 보안위협과 보안태도 간의 영향관계가 없었다. 이러한 결과는 기존 Witte(1992)의 확장된 병행과정모델에서 논의된 결과를 지지한다. 반면, 위협과 공포 간의 영향관계는 대처효능감의 수준에 따라 차이가 없었다. 대처효능이 높은 사용자와 낮은 사용자 모두 보안위협과 공포 간의 영향관계가 통계적으로 유의했다. 대처효능이 낮은 집단과 마찬가지로, 대처효능이 높은 집단도 위협은 공포를 유발했다. 따라서 가설 3은 채택되고 가설 4는 기각됐다. 대처효능감의 조절효과 검정결과는 <표 5>와 같다.



<그림 2> 구조모델 분석결과

<표 5> 대처효능감 수준에 따른 모수차이검정 결과

가설	경로	대처효능높은집단 (n=83)		대처효능낮은집단 (n=95)		z값(p)	결과
		표준화 추정치	임계치 (유의수준)	표준화 추정치	임계치 (유의수준)		
H 3	위협 → 보안태도	0.119	2.097(0.036)	-0.025	-1.095(0.274)	2.137(0.032)	채택
H 4	위협 → 공포	0.313	2.237(0.026)	0.255	2.076(0.038)	1.295(0.195)	기각

VI. 토론과 결론

본 연구결과는 세 가지로 요약된다. 첫째, 대처효능감의 수준에 따라 위협과 보안태도 간의 영향관계는 명확히 차이가 있다. 대처효능감이 높은 집단은 위협의 인식수준이 보안수칙 이행에 긍정적 영향을 미친다. 반면에 대처효능감이 낮은 집단은 위협의 인식 수준이 보안수칙 이행에 영향을 미치지 않는다. 이러한 결과는 Witte(1992)의 확장된 병행과정모델의 논점과 일치하며, 사용자가 보안문제의 발생 가능성과 심각성을 인지하지만, 보안권고사항을 이행하지 않는 문제를 설명한다. 보안문제에 대처하는 자신감 정도가 낮으면 위협메시지를 통해 보안권고사항 이행의 긍정적 태도를 유발하는 것이 어렵다. 따라서 스마트폰 사용자가 보안문제를 직접 통제하는 보안수칙 이행을 유발하기 위해 보안문제에 대처하는 효능감의 수준을 높여 주어야 한다. 둘째, 대처효능감의 수준에 따라 위협과 공포 간의 영향관계의 차이는 없다. 대처효능감이 높은 집단과 낮은 집단 모두 공포에 영향을 미친다. 효능감이 상대적으로 높은 집단도 위협인식의 수준이 높을수록 공포가 유발됐다. 또한, 대처효능감이 낮은 집단도 위협과 공포 간의 영향관계가 존재했다. Bandura(1997)는 효능감이 높은 경우에 위협인식이 공포를 유발한다 했다. 이들은 자기효능감의 수준에 따라 정서적 각성인 공포를 받아들이는 차이를 제안했다. 즉, 인간은 효능감의 수준이 높은 경우 공포를 에너지의 촉진요인으로 받아들이고, 효능감의 수준이 낮은 경우 공포를 에너지의 쇠퇴요인으로 받아들인다는 것이다. 대처효능감이 낮은 사용자에게 위협메시지는 긍정적 보안태도를 유발하지 못하고, 오직 정서적 기제인 공포만을 유발한다. 대처효능감이 높은 사용자는 위협을 통해 공포가 유발되지만, 공포를 에너지의 각성요인으로 받아들이기 때문에 보안수칙 실천을 할 가능성이 크다. 반면에 대처효능감이 낮은 사용자는 위협을 통해 보안태도를 유발하지 않는다. 따라서 기존연구에서 빈번하게 논의되고 있는 위협을 통해 보호동기를 유발하는 메커니즘이 통하지 않는 것이다. 효능감이 낮은 사용자는 위협인식이 높다 해서 보안문제를 직접 다루지 않는다. 효능감이 낮은 사용자는 위협인식이 높을수록 공포가 유발되며, 이들은 공포를 에너지의 쇠퇴요인으로 받아들여(Bandura, 1997) 보안수칙을 실천하지 않는다(Witte, 1992). 셋째, 대처효능감이 낮은 집단의 경우 공포가 높아질수록 보안문제의 권고사항을 인정하지 않는 부정이 있을 것이라 보았다. 그러나 공포와 부정 간의 영향관계는 통계적으로 유의하지 않았다. Witte(1992)는 공포통제과정 내에서 공포의 후행요인으로 부정, 합리화, 방어적 회피, 메시지 축소와 메시지 거부 등을 제안했다. 보안위협을 회피하는 기제는 다양한 방향으로 나타난다(Liang and Xue, 2009). 본 연구는 건강보건 분야 연구인 확장된 병행과정모델을 이용해 스마트폰 사용자의 보안수칙 실천부족을 설명하고자 했다. 그러나 스마트폰 보안문제와 건강보건 분야의 문제는 다르다. 따라서 정보통신분야의 보안문제와 관련해 정서적 기제인 공포를 통제하는 과정에 대해 연구해야 한다. 향후 연구에서 공포통제과정의 논리적 인과 구조를 연구할 필요가 있다.

본 연구의 한계점은 다음과 같다. 첫째, 본 연구는 위험통제과정과 공포통제과정 간의 관계에 대한 논의가 부족하다. Leventhal(1971)과 Witte(1992)는 위험통제과정과 공포통제과정 간의 관계를 독립된 것으로 보았다. 그러나 Bandura(1997)는 적절한 정서적 각성

(Activation)은 주의력을 높여주고 행위를 촉진하지만, 낮은 정서적 각성 수준은 기능의 질을 파괴한다 했다. 적절한 공포가 보안권고사항 이행을 촉진할 수 있음을 의미한다. 따라서 대처효능감이 높은 집단의 경우 공포와 보안행위의도 간의 영향관계를 확인할 필요가 있다. 둘째, 대처효능감이 낮은 상황에서 공포의 내생요인을 밝히는 탐색연구가 필요하다. 수용과 회피의 이론적 입증이 다르고, 회피행위가 다양한 형태로 나타나(Liang and Xue, 2009), 공포통제과정 내에서 회피행위를 결과요인으로 고려할 필요가 있다. 셋째, 본 연구는 보안침해

경험과 백신프로그램 사용 여부를 통제변수로 포함했다. 보안침해 경험이 있는 스마트폰 사용자의 경우 상대적으로 보안위협을 높게 인식할 수 있다. 높은 위협인식은 보안태도에 미치는 영향 강도를 높인다(Rogers, 1975; Witee, 1992). 따라서 보안침해 경험이 없는 스마트폰 사용자를 대상으로 보안수칙 실천 부족에 관한 연구를 진행해야 한다.

본 연구의 시사점은 다음과 같다. 첫째, 사용자의 대처효능감 수준이 높으면 보안수칙 실천 가능성이 커진다. 대처의 효능감 수준에 따라 보안과 관련된 인식 차이가 명확히 존재하는 것이다. 사용자의 대처효능감 수준은 보안수칙 실천 교육을 통해 성취된다. 보안위협 관련 소식을 전하는 관련 기관은 부정적인 보안위협 정보만을 전할 것이 아니라 보안문제에 적절히 대처할 수 있는 보안수칙 실천의 중요성과 그 효과의 긍정적인 부분도 함께 보도해야 한다. 이는 스마트폰 사용자의 보안수칙 실천 의도를 유발한다. 본 연구 결과는 보안문제에 대처하는 사회적 대응방안과 정책 수립에 유용한 참고자료가 된다. 또한, 보안수칙을 이행하지 않는 조직구성원과 개인의 보호동기 연구에 다양한 시사점을 제공한다. 둘째, 기존 보안 관련 연구는 보안권고사항 이행과 관련된 기제만을 설명하고 있으나, 본 연구는 보안권고사항을 이행하지 않고 보안수칙을 실천하지 않는 기제를 설명한다. 공포통제과정의 설명은 향후 정서와 관련된 연구에 다양한 시사점을 제공한다.

참고문헌

김종기, 강다연, 전진환, “패스워드 선택을 위한 사용자의 보안행위의도에 영향을 미치는 요인,” 정보시스템연구, 제17권, 제1호, 2008, pp. 23-43.

김종기, 강다연, 전진환, “인터넷뱅킹 사용자의 보안의도에 영향을 미치는 요인에 관한 연구,” 정보시스템연구, 제18권, 제2호, 2009, pp. 1-18.

김종기, 전진환, 임호섭, “정보보안정책, 보안통제 및 사용자특성이 정보보안효과에 미치는 영향: 컴퓨터 바이러스를 중심으로,” 정보시스템연구, 제15권, 제1호, 2006, pp. 145-168.

Bandura, A., *Self-efficacy: The Exercise of Control,* Worth Publishers, 1997.

Browne, M. W. and Cudeck, R., *Alternate Ways of Assessing Model Fit, In Bollen,* Sage Publications; Newbury Park(CA), 1993.

Carver, C. S. and Scheier, M. F., *On the Self-regulation of Behavior,* New York: Cambridge University Press, 2001.

Carver, C. S. and Scheier, M. F., “Control Theory: A Useful Conceptual Framework for Personality-Social, Clinical, and Health Psychology,”

Psychological Bullentin, Vol. 92, No. 1, 1982, pp. 111-135.

Carver, C. S., "Approach, Avoidance, And the Self-regulation of Affect and Action," *Motivation and Emotion,* Vol. 30, No. 2, 2006, pp. 105-110.

Compeau, D. R. and Higgins, C. A., "Computer Self-Efficacy: Development of a Measure and Initial Test," *MIS Quarterly,* Vol. 19, No. 2, 1995, pp. 189-211.

Crowne, D. and Marlowe, D., *The Approval Motive: Studies in Evaluative Dependence,* New York: Wiley, 1964.

Diamantopoulos, A., "Incorporating Formative Measures into Covariance-Based Structural Equation Models," *MIS Quarterly,* Vol. 35, No. 2, 2011, pp. 335-358.

Etezadi-Amoli, J. and Farhoomand, A. R., "A Structural Model of end User Computing Satisfaction and User Performance," *Information & Management,* Vol. 30, No. 2, 1996, pp. 65-73.

Fishbein, M. and Ajzen, I., *Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research,* Addison-Wesley Publishing, 1975.

Fornell, C. and Larcker, D. F., "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error," *Journal of Marketing Research,* Vol. 18, No. 1, 1981, pp. 39-50.

Furnell, S., "Why Users Cannot Use Security," *Computers & Security,* Vol. 24, No. 4, 2005, pp. 274-279.

Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., *Multivariate Data Analysis,* 7th Edition., Prentice Hall International., 2010.

Harris, P. L., *Children and Emotion: The Development of Psychological Understanding,* Oxford: Basil Blackwell, 1989.

Hovland, C. I., Janis, I. L., and Kelly, H. H., *Communication and Persuasion: Psychological Studies of Opinion Change,* New Haven, CT: Yale University Press, 1953.

Hu, L. and Bentler, P. M., "Cutoff Criteria Fit Indexes in Covariance Structure Analysis: Conventional Criteria Versus New Alternatives," *Structural Equation Modeling,* Vol. 6, No. 1, 1999, pp. 1-55.

Janis, I. L., "Effects of Fear Arousal on Attitude Change: Recent Developments in Theory and Experimental Research," *In Advances in Experimental Social Psychology,* Vol. 3, 1967, pp. 166-244.

Johnston, A. C. and Warkentin, M., "Fear Appeals and Information Security Behaviors: An Empirical Study," *MIS Quarterly,* Vol. 34, No. 3, 2010, pp. 549-566.

Lazarus, R. S. and Folkman, S., *Stress, Appraisal, and Coping,* New York: McGraw-Hill, 1984.

Leventhal, H., "Findings and Theory in the Study of Fear Communications," *Advances in Experimental Social Psychology,* Vol. 5, 1970, pp.119-186.

Leventhal, H., "Fear Appeals and Persuasion: The Differentiation of Motivational Construct," *American Journal of Public Health,* Vol. 61, No. 6, 1971, pp. 1208-1224.

Liang, H., Saraf, N., Hu, Qing., and Xue, Y., "Assimilation of Enterprise Systems: The Effect of Institutional Pressures and the Mediating Role of Top Management," *MIS Quarterly,* Vol. 31, No. 1, 2007, pp. 59-87.

Liang, H. and Xue, Y., "Avoidance of Information Technology Threats: A Theoretical Perspective," *MIS Quarterly,* Vol. 33, No. 1, 2009, pp. 71-90.

Lindell, M. K. and Whitney, D. J., "Accounting for Common Method Variance in Cross-sectional Research Designs," *Journal of Applied Psychology,* Vol. 86, No. 1, 2001, pp. 114-121.

Pajares, F. and Urdan, T., *Self-efficacy Beliefs of Adolescents,* Information Age Publishing, 2006.

Pavlov, I., *Conditioned Reflexes: An Investigation into the Physiological Activity of the Cortex,* New York: Dover, 1927.

Petter, S., Straub, D., and Rai, A., "Specifying Formative Constructs in Information systems Research," *MIS Quarterly,* Vol. 31, No. 4, 2007, pp. 623-656.

Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., and Podsakoff, N. P., "Common Method biases in Behavioral Research: A Critical Review of the Literature and Recommende Remedies," *Journal of Applied Psychology,* Vol. 88, No. 5, 2003, pp. 879-903.

Rogers, R. W., "A Protection Motivation Theory of Fear Appeals and Attitude Change," *Journal of Psychology,* Vol. 91, No. 1, 1975, pp. 93-114.

Segars, A. H. and Grover, V., "Re-Examining Perceived Ease of Use and Usefulness: A Confirmatory Factor Analysis," *MIS Quarterly,* Vol. 17, No. 4, 1993, pp. 517-525.

Siponen, M. and Vance, A., "Neutralization: New Insights into Problem of Employee Information Systems Security Policy Violations," *MIS Quarterly,* Vol. 34, No. 3, 2010, pp. 487-502.

Skinner, B. F., *Science and Human Behavior,* New York: Macmillan, 1953.

Stober, J., "The Social Desirability Scale-17," *European Journal of Psychological Assessment,* Vol. 17, No. 3, 2001, pp. 222-232.

Sutton, S. K. and Davidson, R., "Prefrontal Brain Asymmetry: A Biological Substrate of the Behavioral Approach and Inhibition Systems," *Psychological Science,* Vol. 8, No. 3, 1997, pp. 204-210.

Turel, O., Serenko, A., and Giles, P., "Integrating Technology Addiction and Use: An Empirical Investigation of Online Auction Users," *MIS Quarterly,* Vol. 35, No. 4, 2011, pp. 1043-1061.

Tversky, A. and Kahneman, D., "Advances in Prospect Theory: Cumulative Representation of Uncertainty," *Journal of Risk and Uncertainty,* Vol. 5, No. 4, 1992, pp. 297-323.

Williams, L., Edwards, J. R., and Vandenberg, R. J., "Recent Advances in Causal Modeling Methods for Organizational and Management Research," *Journal of Management,* Vol. 29, No. 6, 2003, pp. 903-936.

Witte, K., "Putting the Fear Back into Fear Appeals: The Extended Parallel Process Model," *Communication Monographs,* Vol. 59, No. 4, 1992, pp. 329-349.

Witte, K., "Fear Control and Danger Control: A Test of the Extended Parallel Process Model(EPPM)," *Communication Monographs,* Vol. 61, No. 2, 1994, pp. 113-134.

김재현(Kim, Jea-hyun)

경상대학교 경영정보학과에서 학사학위와 석사학위를 취득하고, 현재 부산대학교에서 경영학 박사과정 재학 중이다. 주요 관심분야는 정보보안관리, 프라이버시 등이다.

김종기(Kim, Jong-ki)

부산대학교 경영학과에서 경영학 학사학위를 취득하고, Arkansas State University에서 경영학 석사학위, Mississippi State University에서 경영학 박사학위를 취득했다. 현재 부산대학교 경영학과 교수로 재직 중이다. 주요 관심분야는 정보보안관리, 전자상거래, 기술경영 등이다.

<Abstract>

A Study on Disconfirmity to Security Practices of Smart-phone : Focused on Roles of Efficacy

Kim, Jea-hyun · Kim, Jong-ki

Purpose

This study discusses the contradictory behavior of smart-phone users who consider security is important, but they do not follow the security recommendations. We found through literature research that this contradictory behavior is resulted from a low level of efficacy.

Design/methodology/approach

Research hypotheses were set based on Extended Parallel Process Model, Control Theory, and Self Efficacy Mechanism. The data were collected from undergraduate students. Total of 178 data were used for the analysis.

Findings

Results of the analysis, first, showed that the relationship between threat and security attitude varies with the level of coping efficacy. Second, showed that the relationship between threat and fear does not vary with the level of coping efficacy. Both the groups with high coping efficacy and low coping efficacy had a statistically significant effect on the relationship between threat and fear.

Keywords: Smart-phone Security, Coping Efficacy, Danger Control Process, Fear Control Process, Security Recommendations, Security Attitude

* 이 논문은 2015년 6월 8일 접수, 2015년 7월 22일 1차수정, 2015년 8월 17일 게재 확정되었습니다.