http://www.calsec.or.kr/jsebs
ISSN: 2288-3908

The Journal of Society for e-Business Studies
Vol.19, No.3, Aug 2014, pp.65-89
http://dx.doi.org/10.7838/jsebs.2014.19.3.065

위험지각과 효능감에 따른 인터넷 사용자의 개인정보 유출 예방행위 분석 : 위험지각태도 프레임웍을 기반으로

Analyzing the Privacy Leakage Prevention Behavior of Internet Users Based on Risk Perception and Efficacy Beliefs : Using Risk Perception Attitude Framework

장익진(Ickjin Jang)* 최병구(Byounggu Choi)**

초 록

개인정보 유출에 미치는 영향요인 및 유출의 결과와 관련된 다양한 연구가 진행되어 왔음에도 불구하고, 인터넷 사용자에 따라 개인정보 유출 예방행동에 어떠한 차이가 있는지에 대한 연구는 거의 이루어지지 않고 있다. 본 연구는 위험지각태도(risk perception attitude: RPA) 프레임웍을 기반으로 인터넷 사용자의 개인정보 유출 예방행동이 어떻게 달라지는가를 파악하고자 하였다. 보다 구체적으로 개인정보 유출에 대한 지각된 위험과 이의 예방을 위한 효능감을 기준으로 인터넷 사용자를 4가지 유형으로 분류할 수 있으며 각 그룹이 개인정보 보호동기, 정보탐색, 유출 예방행동에 있어 어떠한 차이가 있는지를 파악하고자 하였다. 276명의 인터넷 사용자로부터 수집된 자료를 분석한 결과 인터넷 사용자는 즉각대응(responsive), 회피(avoidance), 상황주도(proactive), 무관심(indifference)의 4가지 그룹으로 분류 가능하며 각 그룹 간 보호동기, 정보탐색, 예방활동에 있어 차이가 있음을 규명하였다. 본 연구는 개인정보 유출 예방전략 및 정책수립을 위한 가이드라인을 제시하였다는 점에서 그 의의가 있다.

ABSTRACT

Although many studies have focused on the influences and outcomes of personal information leakage, few studies have investigated how the personal information leakage prevention behavior differs depending on internet user. This study attempts to supplement the existing studies' limitations with the use of risk perception attitude (RPA) framework. More specifically, this study tries to show internet user can be classified into four groups based on perceived risk of personal information leakage and efficacy beliefs of personal information protection, and to identify how the groups differ in terms of motivation, information seeking, and behaviors for privacy leakage prevention. Analysis on survey data from 276 internet users reveals that the users can be classified into responsive, avoidance, proactive, indifference groups. Furthermore, there are differences between groups in terms of motivation, information seeking, and behaviors for personal information leakage prevention. This study contributes to expand existing literature by providing tailored guidelines for implementation of personal information protection strategies and policy.

키워드 : 위험인식태도 프레임웍, 온라인 프라이버시, 보호동기, 정보탐색, 예방활동
Risk Perception Attitude(RPA) Framework, Online Privacy, Privacy Protection Motivation, Information Seeking, Prevention Behavior

* Department of Data Science, Kookmin University(ijjang@kookmin.ac.kr)
** Corresponding Author, College of Business Administration, Kookmin University(h2choi@kookmin.ac.kr)
2014년 06월 26일 접수, 2014년 08월 11일 심사완료 후 2014년 08월 13일 게재확정.

1. 서 론

인터넷의 발전과 빠른 보급으로 인해 정확한 소비자 분류 및 서비스 응대를 위해 다량의 개인정보를 저장, 보관, 활용, 유통하는 기업이 증가하고 있다. 개인정보 수집 및 활용의 증가는 개인정보 유출 및 불법 유통과 같은 사고의 증가를 필연적으로 수반하게 된다[24]. 개인정보 유출로 인한 피해 방지를 위해 정부는 다양한 법적·제도적 장치를 마련해 왔다[25]. 또한 기업은 개인정보보호를 위해 개인보호정책 및 업무체계 수립, 최신 보안기술 도입 등과 같은 많은 투자와 노력을 기울여 왔다[42]. 그러나 정부와 기업의 제도적, 기술적 노력에도 불구하고 개인정보 유출로 인한 피해는 여전히 줄어들고 있지 않은 것도 사실이다[45]. 특히, 개인정보를 기반으로 형성되는 다양한 형태의 소셜 네트워크 서비스가 활성화되면서 개인정보 유출로 인한 피해는 점점 심화되고 있는 실정이다[32].

개인정보 유출로 인한 문제를 해결하기 위해 법적·제도적 방안을 마련하고 기술적 방안을 제공하는 것은 매우 중요하며 관련 문제를 어느 정도 해결할 수 있는 것도 사실이다[21]. 그러나 인터넷 서비스 사용자들이 자발적으로 개인정보의 중요성을 인식하고 행동을 변화시킴으로써 개인정보 유출로 인한 피해를 예방할 수 있는 조치를 적극적으로 취하는 것 또한 매우 중요하다. 다행히 최근 인터넷 사용자들은 그들의 개인정보보호에 책임을 다하지 못한 기업에게 법적인 책임을 묻고, 자신들의 개인정보 관리에 보다 많은 신경을 기울이고 있다[15, 25]. 이는 개인정보의 중요성에 대한 인식이 점점 증대함에 따라 개인정보에 대한 공개 및 제공, 그리고 개인정보의 유출에 대한 사용자의 인식이 크게 변화하고 있음을 시사한다.

지금까지 개인정보 유출과 관련하여 다양한 연구가 진행되어 왔다. 몇몇 연구는 개인정보 유출과 관련된 국가 간 법적·제도적 비교를 통해 효과적이고 효율적인 개인정보 유출 예방을 위한 절차 및 시스템 개발을 제안하였으며[3, 29, 49], 몇몇 연구는 개인정보보호를 위한 다양한 기술 및 이를 운용할 수 있는 전문 인력 양성방안을 제시함으로써 개인정보보호 연구에 기여하였다[4, 31, 48]. 또 다른 연구들은 개인정보 유출로 인한 비용을 체계적이고 합리적으로 측정함으로써 개인정보보호를 위한 투자의 근거를 마련하고자 하였다[5, 19, 23]. 또한 몇몇 연구는 인터넷에서 개인정보 유출 예방과 관련한 개인의 정보보호 행위에 대한 연구를 통해 개인정보 유출 예방 연구에 기여하였다[18, 27, 32].

하지만 기존 연구는 인터넷 사용자 개개인의 개인정보 유출에 대한 위험인식과 이의 예방에 대한 개인별 능력 차이에는 거의 주목하지 않았다. 인터넷 사용자들이 (1) 어떻게 위험을 인지하는가와[10] (2) 인터넷 활용에 대한 효능감에 있어 어떤 차이가 있는가를 이해하는 것은 매우 중요하다. 왜냐하면 사용자들의 인터넷 사용 행동양식은 위험에 대한 인식과 효능감의 차이에 따라 크게 달라지기 때문이다[41]. 그러나 이러한 중요성에도 불구하고 개인정보 유출에 대한 위험인식과 이의 예방에 대한 효능감의 차이에 따라 어떻게 인터넷 사용자를 분류할 수 있을 것인지 그리고 각 분류에 따라 개인정보 유출 예방행동이 어떻게 다른지에 대한 연구는 거의 이루어지지 않았다.

본 연구에서는 인터넷 사용자에 따른 개인정보 유출 예방행동의 차이를 규명함으로써

기존 연구의 한계를 보완하고자 한다. 보다 구체적으로 인터넷 사용자의 개인정보 유출에 대한 위험지각과 효능감에 초점을 두고 개인정보 유출과 예방행위에 대한 개인 간 차이를 규명하고자 한다. 이를 위해 개인의 질병예방 활동에 대한 태도를 설명하기 위해 개발된 위험지각태도(risk perception attitude : RPA) 프레임웍을 활용하고자 한다. 위험지각태도 프레임웍은 왜 인터넷 사용자들에 따라서로 다른 예방활동을 제공해야만 하는 가에 따른 이론적 기반을 제공할 수 있을 것이다. 본 연구에서는 위험지각태도 프레임웍을 기반으로 개인정보 예방과 관련된 인터넷 사용자의 유형을 분류하고 이러한 유형에 따라 온라인 개인정보 유출을 예방하기 위한 보호동기, 정보탐색, 예방활동이 어떻게 차이가 나는가를 파악하고자 한다. 이를 바탕으로 본 연구는 크게 다음 두 가지 질문에 답하고자 한다.

(1) 인터넷 개인정보 유출에 대한 인터넷 사용자의 태도는 지각된 위험과 효능감 정도에 따라 어떠한 차이가 있는가?

(2) 지각된 위험과 효능감 정도로 구성된 태도집단들은 인터넷 개인정보 유출 예방을 위한 보호동기, 정보탐색, 예방활동에서 어떠한 차이를 보이는가?

2. 이론적 배경

2.1 온라인 개인정보 유출 관련 기존 연구

인터넷과 이를 기반으로 한 소셜 네트워크 서비스의 발달은 온라인상에서의 개인정보 수집, 처리, 이용 범위의 확장을 가져왔다. 이로 인해 인터넷 사용자의 개인정보 유출 위험은 크게 증가하였으며 개인정보 유출 및 이를 방지하기 위한 다양한 연구가 진행되어 왔다. 정보보안(information security)이 승인되지 않은 접근, 사용, 유출, 훼손, 변조, 파괴 등으로부터 정보 및 정보시스템을 보호하는 것을 의미하는 반면 개인정보보호는 정보주체가 자신의 개인정보에 대한 공개 및 접근에 대한 통제권을 갖는 것을 의미한다는 점에서 차이가 있다[28, 33].

개인정보 유출과 관련한 기존 연구는 개인정보보호와 관련된 법적·제도적 장치에 초점을 둔 연구, 기술에 초점을 둔 연구, 경제적 비용에 초점을 둔 연구, 개인의 정보보호 행위에 초점을 둔 연구 등으로 분류할 수 있다. 법적·제도적 장치에 초점을 둔 연구들은 개인정보보호와 관련된 국가 간 법률 비교[29, 49], 효과적인 개인정보보호 체계[46] 등과 같은 법적·제도적 장치를 연구함으로써 개인정보보호 및 유출 예방과 관련된 우리의 이해를 증진시켜왔다. 예를 들면, Byun et al. [3]은 우리나라와 미국, 영국, 캐나다, 호주의 개인정보 유 노출 침해에 대한 사후조치 관련 법적 제도적 현황을 비교 분석함으로써 유노출 사고 대처방안에 대한 가이드라인을 제시하였다. Kim[20]은 개인정보보호 관리체계의 중요성을 강조하며, 이를 위한 정책수립, 개인정보 위험 관리, 개인정보 대책 구현, 평가/개선의 4단계로 구성된 개인정보보호 관리체계를 제시하였다.

개인정보보호 기술에 초점을 둔 연구들은 다양한 개인정보보호 기술, 관련 기술의 분류, 관련 기술의 향후 전망, 전문 인력 양성을 위한 기술수요 등을 제시함으로써 개인정

보보호 연구에 기여하여 왔다[4, 48]. 예를 들면, Nam et al.[31]은 개인정보보호 관련기술을 진단기술, 노출관리 기술, 통신기술, 저장기술, 정책기술, 정책관리기술의 6가지로 분류하고 각 기술의 현황과 향후 과제를 도출하였다. 또한 Yoo and Kim[47]은 문헌연구 및 델파이 방법을 활용하여 효율적인 정보보호 전문 인력 양성 및 관리를 위해 요구되는 71개 요소 지식 및 정보보호 기술을 도출하였다.

개인정보보호 및 유출과 관련된 경제적 비용에 초점을 둔 연구들은 합리적인 개인정보보호 투자를 위한 근거를 파악하기 위해 개인정보유출로 인해 발생하는 비용을 체계적으로 측정하고자 함으로써 개인정보보호 연구에 기여하였다[19, 23]. 예를 들면, Cavusoglu et al.[5]은 이벤트 방법론을 활용하여 1996년부터 2001년까지 개인정보 유출을 겪은 기업 주가의 평균누적비적상 수익률이 2.1% 하락하였음을 실증하였다. 또한 Han et al.[14]은 미국과 일본의 연구를 기반으로 개인정보 유출 피해산정을 위한 정보의 수집 방법과 범위, 그리고 이의 정량적 분석을 위한 프레임웍을 제시하고 이를 검증할 수 있는 방안을 제시하였다.

마지막으로 개인의 정보보호 행위에 초점을 둔 연구들은 온라인상에서 개인정보보호에 영향을 미치는 다양한 요인을 규명함으로써 개인정보 유출 예방 연구에 기여하였다[16, 18, 27]. 예를 들면, Kim and Kim[21]은 보호동기이론을 기반으로 신뢰와 개인정보 유출 위험 간의 관계를 분석하였다. 또한 신뢰와 개인정보 유출 위험에 영향을 미치는 요인으로 개인의 인지적 평가인 위협과 효능감을 설정하여 이들 간의 인과관계를 분석하였다. 또한 Park and Kim[32]은 소셜 네트워크 서비스를 사용하는 대학생들의 개인정보보호행동에 영향을 미치는 요인을 파악하고 이들 간의 관계를 실증적으로 분석하였다. 분석 결과 자기효능감, 반응효능감, 정보침해심각성은 개인정보보호 인식에 긍정적인 영향을 미치는 것으로 파악되었으며, 이러한 개인정보보호 인식은 개인정보보호 행동에 긍정적인 영향을 미치는 것으로 나타났다.

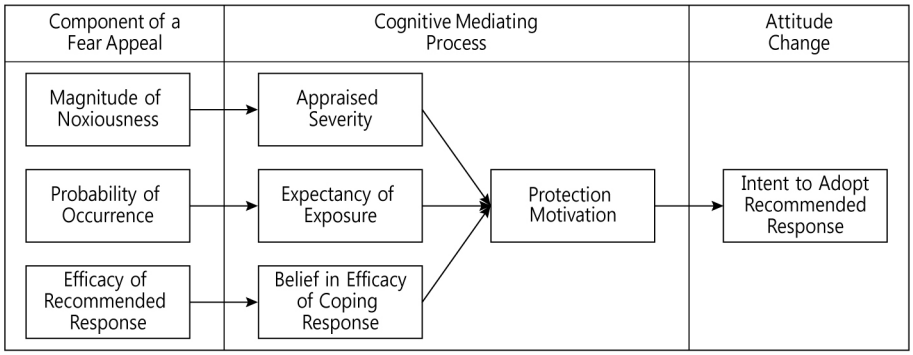
개인정보 유출과 관련된 기존 연구는 개인정보보호와 관련된 법적, 제도적, 기술적, 경제적 요인 등에 대한 다양한 관점을 제시하여 왔다. 나아가 개인정보 유출에 대한 위험인식 및 인터넷 사용에 대한 효능감 등과 같은 개인정보보호 행위를 설명할 수 있는 다양한 요인을 파악함으로써 개인정보 유출 예방에 대한 우리의 이해를 크게 넓힌 것도 사실이다[10, 41]. 그러나 개인정보 유출에 대한 개개인의 위험인식 및 이의 예방에 대한 능력이 개인별로 상이함에도 불구하고 인터넷 사용자에 따라 개인정보 유출 예방활동에 어떠한 차이가 있는지에 대한 연구는 거의 이루어지지 않은 것도 사실이다. 개인정보 유출을 예방하기 위한 활동은 개인정보 유출 예방에 대한 인터넷 사용자의 위험인식과 예방능력에 대한 효능감에 따라 크게 달라지기 때문에 이를 정확하게 이해하는 것은 효과적인 개인정보 유출 예방을 위한 전략 및 정책 마련에 매우 중요하다. 따라서 본 연구에서는 개인정보 유출에 대한 인지된 위험과 개인정보 유출 예방에 대한 효능감을 기준으로 인터넷 사용자를 그룹화하고 이를 간에 개인정보 유출 예방활동이 어떻게 차이가 나는지를 규명하고자 한다.

2.2 위험지각태도(RPA : Risk Perception Attitude) 프레임웍

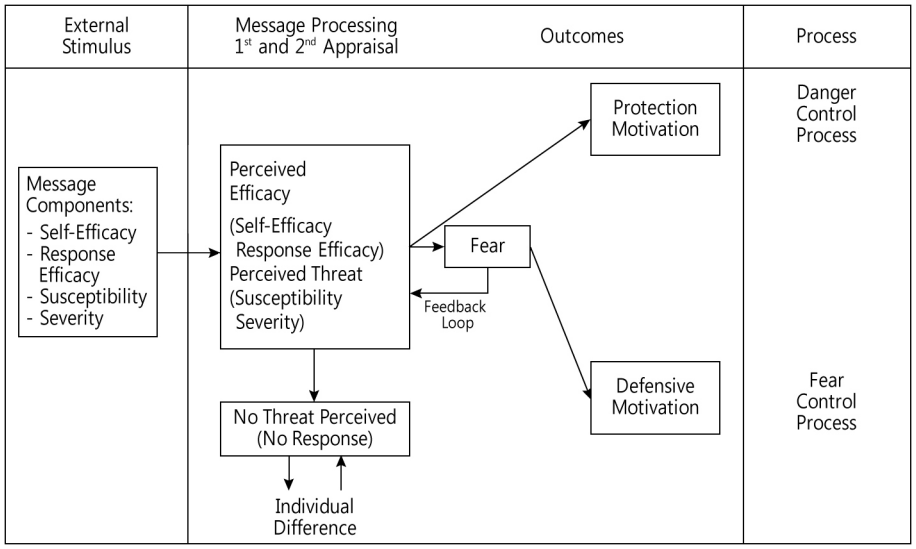
위험지각태도 프레임웍은 보호동기이론과 확장된 병행과정 모델을 기반으로 하고 있다. Rogers[39]가 발표한 논문에 의해 논의되기 시작한 보호동기이론은 개인이 건강위험 메시지에 반응하여 어떻게 태도와 행동을 바꾸는가를 설명하기 위한 이론으로 위험에 대한 개인의 인지 과정을 강조하고 있다. 보호동기이론의 기본 전제는 사람들이 건강에 대한 위험 신호 및 전문의의 위험 메시지를 심각하거나 위험한 신호로 받아들인다면, 이러한 위험을 회피하기 위해 행동에 변화를 가져올 것이라는 것이다. 즉, 위험을 회피하거나 감소시키기 위해 보호동기가 생성되고, 보호동기로 인해 위험으로부터 자신을 보호할 수 있다고 믿게 된다면, 필요한 행동 변화를 할 동기가 개인에게 부여된다는 것이다. 다음 <Figure 1>은 보호동기이론을 통해 질병 관련 메시지가 이용자의 태도 변화에 미치는 과정에서 보호동기의 생성과정과 요인의 구성에 대해서 설명하고 있다.

확장된 병행과정 모델은 Leventhal[26]의 초기 "병행과정 모델(parallel process model)"과 Rogers[39]의 "보호동기이론"의 이론적 관점을 통합하여 Witte[44]가 처음 제안하였다. 이 모델은 메시지의 위협에 대한 평가와 이를 해결하기 위한 권고 방안에 대한 효능감 평가의 두 가지 인지적 평가에 기반하고 있다(<Figure 2> 참조). 이 이론에 따르며 개인은 위협에 대한 두 가지 평가를 통해 무반응(no response), 위험 통제 과정(danger control process), 공포 통제 과정(fear control process) 가운데 한 가지 경로를 선택하여 개인이 직면한 위협에 대응하기 위한 행동을 결정한다.

보호동기이론과 확장된 병행과정 모델 연구들은 위험에 대한 개인의 인식을 개인의 행위 예측을 위한 신뢰할 만한 예측변수로 규정하고 있다[39, 44]. 위험지각태도 프레임웍은 이러한 주장을 바탕으로 위험에 대한 인식 정도와 사회인지이론(social cognitive theory : Bandura[1])에서 처음 제시한 효능감의 정도에 따라 질병을 예방하고자 하는 개인의 동기 및 예방활동에 차이가 있을 것이라는 가설 하에 개발되었다[38]. 이 프레임웍에서는 지각된 위험과 효능감의 정도에 따라 어떤 질병에 대한 개인의 예방활동 및 건강행동 결과에 차



〈Figure 1〉 Protection Motivation Theory(Adopted from[39])



〈Figure 2〉 Extended Parallel Process Model(Adopted from[44])

이가 있음을 주장하고 있다. 즉, 위험지각태도 프레임웍은 개인이 질병으로부터 자신의 건강을 보호하려는 예방활동은 단순히 위험을 지각하는 것만으로 이루어지지 않으며 질병을 예방할 수 있다는 효능감이 필수적임을 강조하고 있다. 질병에 대한 지각된 위험은 질병의 위협으로부터 벗어나기 위한 예방행위의 동기를 유발하지만 실제 어떤 예방활동을 통해 질병의 위협에 대응할 것인가는 개인의 효능감에 의해 조절된다는 것이다[44].

본 연구에서는 이러한 위험지각태도 프레임웍을 인터넷 개인정보 유출 분야에 적용하고자 한다. 개인정보 유출은 실제 질병과 마찬가지로 개인정보가 유출될 경우 개인에게 위험 및 상당한 손해를 초래할 수 있으며, 이러한 위험의 지각에 따라 개인정보를 보호하기 위한 동기가 생성되고 이를 예방할 수 있다는 효능감에 따라 실제 개인정보 유출 예방 행위로 이루어진다는 측면에서 정보화 시대의 질병이라 할 수 있다(<Table 1> 참조).

〈Table 1〉 Application of Risk Perception Attitude Framework to Personal Information Leakage

Criteria	Disease	Personal Information Leakage
Perceived Risk	Financial Risk Psychological Risk Time Risk Social Risk	Financial Risk Psychological Risk Time Risk Social Risk
Efficacy	Persons' recognized ability to take personal control over disease Perceived benefits from being involved in certain behavior, which is the actions taken to prevent disease	Persons' recognized ability to take personal control over the personal information leakage Perceived benefits from being involved in certain behavior, which is the actions taken to prevent personal information leakage

Rimal and Real[38]은 위험지각태도 프레임웍을 위험지각(risk perception)과 효능감(efficacy beliefs)을 기준으로 즉각대응 그룹(responsive group), 회피 그룹(avoidant group), 상황주도 그룹(proactive group), 무관심 그룹(indifference group)으로 분류하였다.

즉각대응 그룹(responsive group)은 인터넷 개인정보 유출에 대한 위험의 인식 수준이 높고, 이를 예방하기 위한 자신의 지식과 능력에 대한 믿음 또한 높은 그룹이다. 이 그룹은 위험의 발생 또는 새로운 위협에 대해 즉각적으로 반응하고 온라인 개인정보 유출로부터 자신을 보호하고 피해를 최소화시킬 수 있도록 조치를 취할 것으로 기대되는 그룹이다. 회피 그룹(avoidant group)은 인터넷 개인정보 유출에 대한 위험의 인식 수준은 높은 반면, 개인정보 유출을 예방하기 위한 자신의 지식과 능력에 대한 믿음이 낮은 그룹이다. 이 그룹은 자신들이 개인정보 유출에 직면할 경우의 위험에 대해서는 고려를 하지만 이러한 위험에 상응하는 조치를 취하지 못하거나, 위험 상황 자체를 회피하고자 하는 의도를 가지고 있는 그룹이다. 상황주도 그룹(proactive group)은 인지된 위험이 낮기 때문에 동기 부여가 되진 않지만 온라인 개인정보 유출을 예방하는데 필요한 자신의 지식과 능력에 대한 믿음의 수준이 높기 때문에 지속적으로 온라인 개인정보 유출 상황이 발생하기에 앞서 대책을 강구할 것으로 예측되는 그룹이다. 마지막으로 무관심 그룹(indifference group)은 인지된 위험과 효능감 모두가 낮은 수준의 그룹이다. 즉 온라인 개인정보 유출과 이로 인한 피해에 대해 아무런 관심이 없으며, 이에 대한 지식과 능력이 미미한 그룹이다.

2.3 위험지각태도 프레임웍을 활용한 기존연구

지금까지 위험지각태도 프레임웍은 자궁경부암[17], 심혈관[35], AIDS/HIV[36], 피부암[38], 당뇨병[43], 폐암[50] 등과 같은 질병과 관련한 건강행동을 연구함에 있어 널리 활용되어 왔다. 이러한 연구들은 주로 서베이 방법론[35, 38]이나 실험연구[38, 43]를 활용하여 개별 질병과 이에 대한 예방활동 간의 관계를 파악하는 데 중점을 두고 진행되어 왔다. 특히 서베이 방법론을 활용할 때 위험지각태도 프레임웍의 가설을 보다 지지하는 결과를 보여주고 있다[50].

위험지각태도 프레임웍을 활용한 기존 연구들은 위험지각이 높은 집단에 속하지만 효능감의 정도에 따라 구분되는 즉각대응 그룹과 회피 그룹 간에 차이가 있을 것이라는 가설에 대해 일치하지 않는 결과를 보여주고 있다. 몇몇 연구들은 즉각대응 그룹과 회피 그룹 간에 질병 예방활동에 차이가 있다는 결과를 보여주고 있으나[35, 38, 43] 다른 연구들은 두 집단 간에 통계적으로 유의한 차이가 없다는 결과를 보여주고 있다[36]. 반면 위험지각이 낮은 집단에 속하는 상황주도 그룹과 무관심 그룹 간에는 효능감 정도의 차이와 관련 없이 질병 예방활동에 차이가 있다는 위험지각태도 프레임웍의 가설을 지지하고 있다. 이러한 결과는 효능감의 효과가 위험지각이 높은 집단에만 존재하고 위험지각이 낮은 집단에는 존재하지 않을 것이라는 확장된 병행과정 모델의 가설을 기각하는 것으로 질병 예방과 관련된 행위에 있어 효능감의 중요성을 증명하는 것으로 해석해 볼 수 있다.

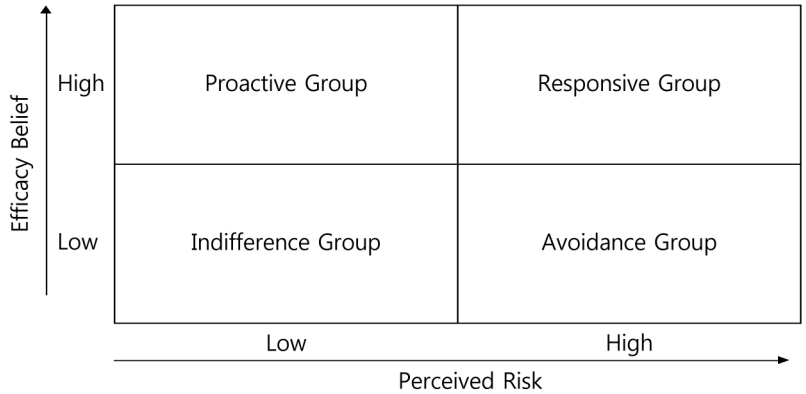
위험지각태도 프레임웍을 적용한 기존 연구를 통합적으로 분석해 보면 다음과 같은 사실을 파악할 수 있다. 첫째, 질병예방을 위한 사람들의 태도 및 행위는 4가지로 그룹으로 구분할 수 있다. 둘째, 4개의 그룹 간에는 정보탐색이나 예방활동에 있어 차이가 있다. 비록 몇몇 연구는 즉각대응 그룹과 상황주도 그룹 간에 유의미한 차이가 없음을 주장하고 있으나 대다수의 연구는 전반적으로 즉각대응 그룹이 가장 활발한 질병 예방을 한다는 것에 어느 정도 동의를 하고 있다[35, 38]. 또한 회피 그룹보다 무관심 그룹이 질병예방 활동에 있어 가장 좋지 못한 집단임을 주장하고 있다[38, 43]. 셋째, 효능감은 질병예방 활동에 직접적인 영향을 미칠 뿐 아니라 위험지각과 질병예방 활동 간의 관계에 대한 조절변수의 역할도 하고 있다[35].

본 연구에서는 위험지각태도 프레임웍을 활용하여 인터넷 사용자를 그룹화하고 이들 간의 개인정보 유출 예방 활동이 어떻게 차이가 있는지를 규명함으로써 개인정보 유출 예방 정책수립을 위한 가이드라인을 제시할 수 있을 것이다.

3. 연구모형 및 가설 수립

위험지각태도 프레임웍은 지각된 위험과 효능감의 정도에 따라 4개의 태도집단을 구분하고 있다(<Figure 3> 참조). 이때 지각된 위험은 질병에서 벗어나기 위한 행동을 하려는 동기유발 요인으로, 효능감은 행동변화의 촉진요인으로 개념화되고 있다[35].

인터넷 사용자의 개인정보 유출 예방행동을 위한 동기는 질병 예방행동과 마찬가지로 개인정보 유출로부터 발생할 수 있는 위험과 손해에 대한 지각에 의해 생성된다. 그러나 인터넷 사용자들은 위험에 대한 지각만으로 개인정보 유출 예방행동에 나서지 않는다. 왜냐하면 실제 행동을 추구하기 위해서는 개인정보 유출을 예방할 수 있다는 효능감이 반드시 필요하기 때문이다. 이러한 논의를 바탕으로 본 연구에서는 인터넷 사용자의 개인정보 유출 예방행동 역시 위험지각태도 프레임웍에 따라 4개의 태도집단으로 분류 가능할 것으로 추정하여 다음과 같은 가설을 설정하였다.



〈Figure 3〉 Risk Perception Attitude Framework(Adapted from[38])

가설 1 : 수집된 표본은 위험지각태도 프레임웍에서 제안한 바와 같이 개인정보 유출에 대한 위험 지각과 이를 예방할 수 있다는 효능감 정도에 따라 4개의 서로 다른 그룹으로 분류 될 것이다.

위험지각태도 프레임웍을 처음 제안하였던 Rimal and Real[38]의 연구 결과에 따르면 4개의 그룹은 보호동기(protective motivation), 정보탐색(intention to seek information), 예방활동(protective behavior)에서 각각 다른 특성을 나타내고 있다. 이후 Real[34]이 작업장의 근로안전에 관하여 위험지각태도 프레임웍을 적용한 연구에서도 정보이용능력(information availability), 정보탐색 의도(information seeking intentions), 행동(behavior), 행동의도(behavioral intention)에 따라 각 그룹별로 통계적으로 유의하게 다른 특성을 나타내고 있는 것으로 조사되었다. 이를 기반으로 본 연구에서는 다음과 같은 가설을 설정하였다.

가설 2 : 분류된 4개의 그룹은 보호동기, 정보탐색, 예방활동에 서로 다른 특성을 보일 것이다.

비록 몇몇 연구결과에서는 상황주도 그룹과 즉각대응 그룹 간에 유의한 차이가 없는 것으로 나타나기도 했으나[35, 38], 대다수의 연구결과에 따르면 즉각 대응 그룹이 다른 그룹에 비해 보호동기, 정보탐색, 예방활동, 활동의도 등 모든 기준에서 높은 점수를 보이는 것으로 나타났다[34, 37, 43]. 반면 무관심그룹은 모든 부분에서 가장 낮은 점수를 나타내는 것으로 분석되었다[35, 38, 43]. 이를 바탕으로 본 연구에서는 다음과 같은 가설을 설정하였다.

가설 3 : 즉각대응 그룹은 다른 그룹들보다 보호동기, 정보탐색, 예방 활동에서 보다 적극적인 태도를 보일 것이다.

가설 4 : 무관심 그룹은 다른 그룹들보다 보호동기, 정보탐색, 예방 활동에서 보다 소극적인 태도를 보일 것이다.

위험지각태도와 관련된 기존 연구 결과 가운데 불일치를 보이고 있는 부분은 효능감이 예방활동과 관련하여 조절변수(moderating effect)의 역할을 수행하느냐 아니면 주요인(main effect) 역할을 수행하는 가에 대한 부분이다[17]. 이를 파악하기 위해서는 위험에 대한 지각이 낮은 반면 효능감 정도가 다른 상황주도 그룹과 무관심 그룹 간의 개인정보 유출 예방행동 간의 차이를 분석할 필요가 있다. 이와 관련하여 Real[35], Rimal and Real[38] 등은 보호동기, 정보탐색, 예방활동, 활동의도 등에 있어 상황주도 그룹과 무관심 그룹 간에 효능감 정도의 차이뿐만 아니라 개인정보 유출 예방행동에도 차이가 있음을 지적함으로써 효능감의 주요인 효과를 주장하고 있다. 이를 바탕으로 본 연구에서는 다음과 같은 가설을 설정하였다.

가설 5 : 보호동기에 있어 상황주도 그룹은 무관심그룹에 비해 더 높은 값을 나타낼 것이다.

가설 6 : 정보탐색에 있어 상황주도 그룹은 무관심그룹에 비해 더 높은 값을 나타낼 것이다.

가설 7 : 예방활동에 있어 상황주도 그룹은 무관심그룹에 비해 더 높은 값을 나타낼 것이다.

4. 연구방법

4.1 자료수집 및 표본 특성

본 연구에서는 서울과 경기 지역에 거주하는 일반인 중 하루 1시간 이상 인터넷을 사용하는 사람을 대상으로 개인정보 유출과 관련된 위험 지각과 효능감에 대한 설문지를 배포하여 총 316개의 표본을 수집하였다. 이 가운데 하루 인터넷 이용 시간이 한 시간 미만인 40개의 표본을 제외하고 총 276개의 표본을 최종 분석에 사용하였다. 88%의 국민이 하루 1시간 이상 인터넷을 사용하는 우리나라 현실을 고려하여 표본을 한정함으로써 표본의 대표성을 확보하고자 하였다[22].

본 연구에서 수집한 276명의 응답자 가운데 남성이 113명(40.9%), 여성이 163명(59.1%)로 여성이 다소 높은 비율을 보였다. 연령에 따른 분포를 살펴보면, 20대가 184명(66.7%)로 가장 많았다. 학력에 따른 분포를 살펴보면, 대졸이 202명(73.2%)로 과반수를 차지하고 있으며, 고졸이 37명(13.4%), 대학원졸 32명(11.6%)로 나타났다. 연간 가계 수입에 따른 분포는 3000만원 미만이 115명(41.7%)로 가장 많았으며, 1억 이상도 41명(14.9%)이나 존재하였다. 일일 인터넷 사용 시간은 1~4시간이 103명(37.3%)으로 가장 많았다(<Table 2> 참조). 일일 인터넷 사용 시간의 경우 전반적으로 우리나라 평균 인터넷 이용시간에 비해 약간 높은 수치를 보이기는 하였으나 응답자의 대부분이 40대 미만인 점을 고려해 볼 때 크게 문제가 되지 않는 것으로 판단된다[22].

〈Table 2〉 Characteristics of Participants

Criteria		Frequency(percent)
Gender (N = 276)	Male	113(40.9%)
	Female	163(59.1%)
Age (N = 276)	10~19	31(11.2%)
	20~29	184(66.7%)
	30~39	37(13.4%)
	40 and above	24(8.7%)
Education (N = 276)	Elementary School	2(0.7%)
	Middle School	3(1.1%)
	High School	37(13.4%)
	University	202(73.2%)
	Graduate University	32(11.6%)
Annual Income (N = 275)	Less than $30000	115(41.7%)
	$30000~$50000	48(17.4%)
	$50000~$70000	40(14.5%)
	$70000~$100000	31(11.2%)
	More than $100000	41(14.9%)
Internet Usage Time per Day (N = 276)	1~4 hours	103(37.3%)
	4~7 hours	84(30.4%)
	7~10 hours	51(18.5%)
	10 hours and above	38(13.8%)

4.2 측정

위험지각태도 프레임웍에서 지각된 위험은 지각된 취약성(perceived susceptibility)과 지각된 심각성(perceived severity)으로 구성되어 있다. 먼저 지각된 취약성은 자신이 질병에 얼마나 취약한지에 대한 개인적인 생각이며, 지각된 심각성은 질병의 심각성에 대한 개인적인 생각을 의미한다. 본 연구에서는 이를 연구의 목적에 맞게 수정하여 지각된 취약성은 자신이 개인정보 유출에 얼마나 취약한지에 대한 개인적인 생각으로 정의하였고, 지각된 심각성은 개인정보 유출의 심각성에 대한 개인의 생각으로 정의하였다. 이러한 개념을 측정하기 위해서 Rimal and Juon[37]에 의해 개발된 인지된 취약성 측정문항 2개, 인지된 심각성 측정문항 2개를 포함한 총 4개의 측정문항을 연구 목적에 맞게 수정하여 활용하였다.

효능감은 사회인지이론을 바탕으로 자기효능감(self-efficacy)과 결과기대(outcome expectations)의 두 가지 항목으로 구성하였다[37]. 자기효능감은 질병 또는 질병을 예방하기 위해 자신을 통제할 수 있는 개인의 인지된 능력이며, 결과기대는 자신이 알고 있고, 실행할 수 있는 일들이 질병을 조기에 발견하거나 예방할 수 있을 것이라는 개인의 기대감을 의미한다. 본 연구에서는 이를 연구의 목적에 맞게 수정하여 자기효능감을 개인정보 유출을 예방하기 위해 자신이 가지고 있는 지식 및 능력으로 정의하였고, 결과기대는 자신이 알고 있고, 실행할 수 있는 일들이 개인정보 유출을 조기에 발견하거나 방지할 수 있을 것이라는 기대감으로 정의하였다. 이를 측정하기 위해 Beuningen et al.[2], Rimal and Juon[37], Siponen et al.[23] 등이 개발한 자기효능감 측정문항 5개, 결과기대 측정문항 2개를 연구 목적에 맞게 수정하여 활용하였다.

Rimal and Real[38]은 자기보호 동기를 질병을 예방하기 위한 개인의 욕구라고 정의하였다. 본 연구에서는 이를 개인정보 유출을 예방하기 위한 개인의 욕구라고 정의하고, Rimal and Real[38]이 개발한 자기보호 동기 측정문항 4개를 연구 목적에 맞게 수정하여 활용하였다. 질병예방 관련 연구에서 정보탐색은 환자들이 TV, 신문, 라디오, 인터넷 등의 미디어에서 질병과 관련된 이야기가 나올 때 관심을 기울이고자 하는 정도라고 정의된다[38, 43]. 본 연구에서는 이를 인터넷 사용자들이 TV, 신문, 라디오, 인터넷 등의 미디어에서 개인정보 유출과 관련된 이야기가 나올 때 관심을 기울이고자 하는 정도로 정의하고 이의 측정을 위해 Rimal and Real[38]이 개발한 측정문항 7개를 본 연구의 목적에 맞게 수정하여 활용하였다. 마지막으로 예방활동이란 인지된 위험을 통제하고, 감소 및 회피하기 위해 하는 행동일체를 의미한다[12]. 본 연구에서는 예방활동을 개인정보 유출을 예방하기 위해 개인이 실제 실시하는 행동으로 정의하고 Chan et al.[6], Chen and Guo[8], Duh et al.[12], Moon and Kim[30] 등이 개발한 측정문항 12개를 수정・활용하였다. 본 연구에서 사용된 모든 측정 항목은 Likert 7점 척도를 이용하였으며 이를 요약하면 다음 <Table 3>과 같다. 또한 전체 설문은 <부록 1>에 나타나 있다.

〈Table 3〉 Structure of Survey

Variables	Factors	Items Number	Source
Perceived Risk	Susceptibility	2	[37, 44]
	Severity	2	
Efficacy Belief	Self-Efficacy	5	[1, 2, 37, 40]
	Outcome Expectation	2	[3]
Motivation	Self-Protective Motivation	4	[38]
Information Seeking	Information Research	4	[38]
	Information Sharing	3	
Actual Behavior	Behavior	12	[6, 8, 12, 30]

본 연구에서 지각된 위험, 효능감, 정보탐색은 여러 하위개념의 측정항목들을 합산하여 단일항목으로 측정하였다. 이러한 방식은 다양한 연구에서 활용되고 있다[11]. 예를 들면, 서비스의 유형성(tangiblity), 신뢰성(reliability), 응답성(responsiveness), 확신성(assurance), 공감성(empathy) 등의 5개의 하위차원으로 구성된 서비스 품질을 측정함에 있어 Chang and Chen[7]은 하위 5개 측정항목을 단일항목으로 합쳐 활용할 수 있음을 실증하였다. 또한 Jo and Yoo[17]는 지각된 위험 및 효능감의 측정에 있어 하위개념의 측정항목을 합산하여 단일 항목으로 측정하여 연구에 활용하였다.

5. 자료 분석 및 결과

5.1 변수의 신뢰성 및 타당성 검사

본 연구는 기존 연구에 의해 타당성이 검증되고 사용된 문항의 준용과 개인정보보호 분야 전문가의 사전검토를 통해 변수의 내용타당성(content validity)을 확보하였다. 신뢰성(reliability) 검정을 위해 크론바 알파 (cronbach's alpha) 계수를 활용하였으며 0.7을 절단값(cutoff value)로 활용하였다. <Table 4>는 변수들에 관한 신뢰성과 타당성 분석결과를 보여주고 있다.

지각된 위험, 자기효능, 보호동기, 정보탐색, 예방활동의 타당성 검정을 위해 주성분 요인분석(principal component factor analysis)을 실시하였다. 이러한 방법은 상관관계가 높은 항목들을 하나의 요인으로 묶어내고 요인들 간에는 상호 독립성을 유지하도록 하기 위한 방법이다. 요인분석을 하는데 있어서 각 변수와 요인간의 상관관계 정도를 나타내는 요인 적재량(factor loading value)이 0.5 이상인 경우를 유의한 것으로 판단하였다. 각 요인의 요인분석을 실시한 결과는 다음 <Table 4>에서 보는 바와 같다. 또한 q23과 q30의 경우 요인적재량이 0.5 이하로 나타남에 따라 추가 분석을 위해 두 문항을 제거하였다.

〈Table 4〉 Reliability and Validity Test

Variables	Items	Factor 1	Factor 2	Factor 3	Factor 4	Factor 5	Cronbach Alpha
Perceived Risk	q1	.878					.869
	q2	.787					
	q3	.905					
	q4	.810					
Efficacy Belief	q5		.819				.863
	q6		.775				
	q7		.660				
	q8		.670				
	q9		.627				
	q10		.832				
	q11		.804				
Motivation	q12			.769			.728
	q13			.834			
	q14			.856			
	q15			.518			
Information Seeking	q16				.710		.838
	q17				.767		
	q18				.695		
	q19				.632		
	q20				.735		
	q21				.743		
	q22				.671		
Actual Behavior	q23					.291 (deleted)	.855
	q24					.682	
	q25					.624	
	q26					.571	
	q27					.688	
	q28					.660	
	q29					.634	
	q30					.328 (deleted)	
	q31					.653	
	q32					.672	
	q33					.661	
	q34					.550	

5.2 분석 결과

위험지각태도 프레임워크 유형 도출을 위해 군집 내 차이(within-cluster differences)를 최소화할 수 있는 계층적 군집분석 방법인 Ward's 기법을 활용하여 군집분석을 실시하였다. 군집분석에 있어 군집수의 결정은 군집화 일정표(agglomeration schedule)를 이용하였다[9]. 군집화 일정표는 군집화 과정의 각 단계에서 하나의 군집을 형성하기 위해 그룹화된 관측치 사이의 거리를 보여준다. 이 값이 작을수록 동질적인 관측치가 하나의 군집으로 묶여짐을 나타내며, 군집수를 결정하는데 중요한 지침을 제공한다. <Table 5>의 군집화 일정표를 살펴보면 군집계수가 4개에서 3개 구간(8.491-6.645 = 1.846), 3개에서 2개 구간(17.930-8.491 = 9.439), 2개에서 1개 구간(25.467-17.930 = 7.537)이 큰 차이를 보이는데 반해, 4개에서 5개 구간의 변화량이 0.025로 급격히 줄어드는 것으로 보아 적절한 군집의 수는 4개임을 알 수 있다.

계층적 군집분석 결과의 신뢰성 및 타당성 확보를 위해 비계층적 군집분석의 대표적 방법인 K-Means 방법을 추가적으로 활용하였다[13]. 대체적으로 군집의 번호가 바뀌고 사례 수에 있어 약간 차이가 날뿐 Ward's 방법에 의한 것과 비슷한 결과를 보여주고 있다. 따라서 본 연구의 군집분석 결과는 신뢰성 및 타당성을 확보하고 있다고 할 수 있다. 두 개의 분석결과 가운데 어떤 것을 활용해도 무방하기 때문에 본 연구에서는 계층적 군집분석 결과를 활용하였다.

분류된 각각의 그룹이 위험지각태도 프레임웍 상의 어떤 그룹에 해당하는지를 파악하기 위해 각 그룹을 요인변수로 하고 인지된 위험과 효능감을 종속변수로 하여 분산분석을 실시하였다. 분석결과 인지된 위험은 유의수준 0.01에서 ($F(3, 272) = 242.34$, $p = 0.000$) 유의미한 차이가 있는 것으로 나타났으며 효능감 또한 유의수준 0.01에서 ($F(3, 272) = 211.59$, $p = 0.000$) 유의미한 차이가 있는 것으로 나타났다(<Table 6> 참조).

〈Table 5〉 Analysis of Agglomeration Coefficients

Number of Clusters	Agglomeration Coefficient	Differences in Coefficient	Change in Coefficient in Next Level(%)
5	6.620	0.025	0.30
4	6.645	1.846	21.7
3	8.491	9.439	52.6
2	17.930	7.537	29.5
1	25.467		

〈Table 6〉 Clustering Analysis Results

	Responsive Group (n = 91)		Avoidance Group (n = 102)		Proactive Group (n = 57)		Indifference Group (n = 26)		Total (n = 276)
	Mean	*SD*	Mean	*SD*	Mean	*SD*	Mean	*SD*	*F*
Perceived Risk	6.57 High	.50	6.47 High	.59	4.52 Low	.93	3.22 Low	1.08	242.34***
Efficacy Belief	5.77 High	.76	3.32 Low	.729	4.71 High	.72	2.86 Low	.88	211.59***

***p < 0.01.

즉각대응 그룹에 속한 응답자는 91명으로 인지된 위험(평균 = 6.57)과 효능감(평균 = 5.77)이 모두 높은 값을 나타냈으며, 회피 그룹에 속한 응답자는 102명으로 인지된 위험(평균 = 6.47)은 높은 값을 나타낸 반면, 효능감(평균 = 3.32)은 낮은 값을 나타냈다. 상황주도 그룹에 속한 응답자는 57명으로 인지된 위험(평균 = 4.52)은 낮은 값을 보인 반면 효능감(평균 = 4.71)은 높은 값을 보였다. 무관심 그룹에 속한 응답자는 26명으로 인지된 위험(평균 = 3.22)과 효능감(평균 = 2.86) 모두 낮은 값을 나타냈다. 이러한 분석결과는 개인정보 유출에 대한 위험인식과 개인정보 유출 예방활동에 대한 효능감을 기준으로 인터넷 사용자를 위험지각태도 프레임웍의 4개 그룹으로 분류할 수 있음을 의미한다. 따라서 가설 1은 채택한다.

가설 2의 검증을 위해 4개 그룹 간에 보호동기, 정보탐색, 예방활동이 차이가 있는지를 분석하였다(<Table 7> 참조). 분석결과 4개의 그룹은 보호동기, 정보탐색, 예방활동에 있어 매우 유의한 차이를 보이고 있음을 알 수 있다($p < 0.00$). 따라서 가설 2는 채택한다.

<Table 7>에서 알 수 있듯이 개인정보 보호동기는 즉각대응 그룹(평균 = 6.41)이 가장 높은 값을 보였으며, 회피 그룹(평균 = 5.81), 상황주도 그룹(평균 = 5.36), 무관심 그룹(평균 = 4.16) 순으로 나타났다. 반면, 정보탐색의 경우 즉각대응 그룹(평균 = 5.33), 상황주도 그룹(평균 = 4.79), 회피 그룹(평균 = 4.48), 무관심 그룹(평균 = 3.47) 순으로 높은 값을 나타냈다. 예방활동의 경우 즉각대응 그룹(평균 = 5.12), 상황주도 그룹(평균 = 4.37), 회피 그룹(평균 = 3.87), 무관심 그룹(평균 = 3.41) 순으로 평균값을 보였다. 따라서 가설 3과 가설 4를 채택한다.

각 그룹간의 차이를 보다 정밀하게 파악하기 위해 Scheffe 방법을 이용하여 사후 검정을 실시하였다.

<Table 8>에 나타나 있듯이 보호동기에서 상황주도 그룹과 무관심 그룹 간에는 유의미한 차이가 있는 것으로 나타났으며($p = 0.000$) 이에 따라 가설 5를 채택한다. 정보 탐색에 있어서도 상황주도 그룹과 무관심 그룹 간의 유의한 차이가 파악되었으며($p = 0.000$) 가설 6을 채택한다. 마지막으로 예방활동에 있어 상황주도 그룹과 무관심 그룹 간에는 유의 수준 0.01에서 유의한 차이가 있는 것으로 나타났다($p = 0.002$). 따라서 가설 7 또한 채택한다.

〈Table 7〉 ANOVA Results for RPA Groups in terms of Motivation, Information Seeking, Behavior

	Responsive Group (n = 91)		Avoidance Group (n = 102)		Proactive Group (n = 57)		Indifference Group (n = 26)		Total n = 276
	Mean	*SD*	Mean	*SD*	Mean	*SD*	Mean	*SD*	*F*
Motivation	6.41	.70	5.81	1.00	5.36	1.15	4.16	1.18	38.40***
Information Seeking	5.33	1.28	4.48	1.07	4.79	1.00	3.47	1.47	19.57***
Actual Behavior	5.12	.98	3.87	.99	4.37	1.08	3.41	1.24	31.35***

*** $p < 0.01$.

〈Table 8〉 Multiple Comparison Test Results Using Scheffe Method

	Average Linkage (Between Group)	Significance Probability
Motivation	Proactive Group and Responsive Group	.000
	Proactive Group and Avoidance Group	.063
	Proactive Group and **Indifference Group**	**.000**
	Responsive Group and Avoidance Group	.001
	Responsive Group and Indifference Group	.000
	Avoidance Group and Indifference Group	.000
Information Seeking	Proactive Group and Responsive Group	.060
	Proactive Group and Avoidance Group	.470
	Proactive Group and **Indifference Group**	**.000**
	Responsive Group and Avoidance Group	.000
	Responsive Group and Indifference Group	.000
	Avoidance Group and Indifference Group	.002
Actual Behavior	Proactive Group and Responsive Group	.000
	Proactive Group and Avoidance Group	.037
	Proactive Group and **Indifference Group**	**.002**
	Responsive Group and Avoidance Group	.000
	Responsive Group and Indifference Group	.000
	Avoidance Group and Indifference Group	.264

6. 논의 및 함의

6.1 논의

인터넷 및 소셜 네트워크 서비스의 발달로 인해 사회 전반에 걸쳐 개인정보 유출 및 프라이버시 침해에 대한 우려가 확산되고 있음에도 불구하고 개인정보 유출과 관련된 법적, 제도적, 기술적, 경제적 연구에 비해 인터넷 사용자들의 인식이나 행동 변화와 관련된 연구는 상대적으로 부족하였다. 이를 보완하기 위해 본 연구는 인터넷 사용자의 따른 특성에 따른 개인정보 유출 예방행동 변화 전략 및 정책을 위한 가이드라인을 제시하고자 위험지각태도 모형을 기반으로 인터넷 사용자를 4개의 태도그룹으로 분류하고 보호동기, 정보탐색, 예방활동이 이들 그룹에 따라 어떻게 다른가를 분석하였다. 분석결과 첫째, 지각된 위험과 효능감을 기준으로 인터넷 사용자를 크게 4가지 형태로 구분할 수 있음을 파악하였다. 이를 통해 위험지각태도 프레임웍이 개인정보 유출 예방과 관련된 행위 변화를 예측할 수 있는 주요 모형으로 활용 가능함을 실증하였다. 둘째, 분류된 4개의 그룹은 보호동기, 정보탐색, 예방활동에 있어 유의한 차이가 있음을 파악하였다. 보호동기의 경우 즉각대응 그룹, 회피 그룹, 상황주도 그룹, 무관심 그룹 순으로 높은 값을 보인 반면

정보탐색의 경우 즉각대응 그룹, 상황주도 그룹, 회피 그룹, 무관심 그룹 순으로 높은 값을 보였으며 예방활동의 경우 즉각대응 그룹, 상황주도 그룹, 회피 그룹, 무관심 그룹 순으로 높은 값을 나타냈다. 즉, 즉각대응 그룹이 개인정보 유출과 관련하여 보호동기, 정보탐색, 예방활동에서 가장 적극적인 태도를 보이는 반면 무관심 그룹은 가장 소극적인 태도를 보이는 것으로 파악되었다. 셋째, 보호동기, 정보탐색, 예방활동의 경우 지각된 위험이 높은 그룹인 즉각대응 그룹과 회피 그룹 간에 유의한 차이가 있을 뿐만 아니라 지각된 위험이 낮은 그룹인 상황주도 그룹과 무관심 그룹 간에도 유의한 차이가 있는 것으로 나타났다. 이는 효능감이 개인정보 유출 위험에 대한 지각과 관련 없이 보호동기, 정보탐색, 예방활동에 영향을 미치고 있음을 의미하며 보호동기, 정보탐색, 예방활동에 있어 효능감이 조절효과가 아닌 주요인 효과가 있다는 것을 의미한다.

또한 본 연구에서는 응답자의 약 70%(회피 그룹 37%, 즉각대응 그룹 33%, 무관심 그룹 9%, 상황주도 그룹 21%)가 개인정보 유출에 대해 높은 수준의 위험을 인식하고 있다고 응답한 반면 약 54%의 응답자만이 높은 수준의 효능감을 보유하고 있다고 대답하였다. 이는 우리 사회가 대량의 개인정보 유출 사고 및 이메일, 메신저, 보이스피싱 등의 여러 가지 정보화 역기능 피해를 경험해 왔고 이로 인해 개인정보 유출 위험에 대해 많은 우려와 걱정을 하고 있는 반면 개인정보 유출을 예방하고 이에 상응하는 대처에는 상대적으로 취약하다는 것을 의미한다. 따라서 기업과 정부 정책에 이와 관련된 다양한 방안이 적극적으로 반영되어야 할 것이다.

6.2 함의

본 연구는 학문적·실무적으로 다음과 같은 효과가 기대된다. 먼저 학문적 기대효과를 살펴보면 다음과 같다. 첫째, 개인정보 유출 예방활동과 관련된 연구에 위험지각태도 프레임웍의 활용 가능성을 검증하였다. 그동안 위험지각태도 프레임웍은 질병과 관련된 현상에만 적용되었을 뿐 개인정보 유출과 같은 사회현상에는 활용된 예가 매우 드물었다. 본 연구에서는 위험지각태도 프레임웍을 개인정보 유출 예방이라는 사회현상에 적용함으로써 이의 적용가능성을 확대하였다. 둘째, 개인정보 유출의 원인 및 결과에 초점을 둔 기존 연구와 달리 개인정보 유출에 대한 지각된 위험과 이의 예방에 대한 효능감을 기준으로 인터넷 사용자를 분류하고 이를 기반으로 분류된 태도집단에 따라 개인정보 유출 예방과 관련된 보호동기, 정보탐색, 예방활동이 어떻게 달라지는가를 규명함으로써 개인정보와 관련된 연구의 지평을 일정 정도 넓힐 수 있었다. 셋째, 개인정보 유출 예방행위와 관련하여 효능감이 갖는 주요인 효과를 실증적으로 파악하였다. 몇몇 기존 연구는 효능감이 지각된 위험과 예방행동 간의 조절변수 역할을 할 뿐 주요인 효과는 없다고 주장하고 있다. 그러나 본 연구의 분석결과에 따르면 효능감이 지각된 위험과 관계없이 개인정보 유출 예방행동에 직접적인 영향을 주는 주요인 효과를 가지고 있는 것으로 나타났다. 즉, 지각된 위험에 관계없이 효능감은 독립적으로 개인정보 유출 예방행동을 높이는데 영

향을 주는 주요 변수라 할 수 있다.

실무적 관점에서 보면 본 연구는 첫째, 인터넷 사용자의 특성에 맞는 개인정보 유출 예방 방안을 마련할 수 있는 가이드라인을 제시할 수 있을 것이다. 기존 개인정보 유출 연구는 모든 인터넷 또는 온라인 사용자를 동일한 특성을 갖는 하나의 집단으로 간주하고 진행되었기 때문에 이를 해결하기 위한 정책 또한 모든 사용자를 전제로 제시되었다. 그러나 인터넷 사용자의 특성이 개인마다 다르다는 현실 상황을 고려해 볼 때 이러한 해결책 또는 정책은 그 한계가 뚜렷하다고 할 수 있다. 따라서 본 연구는 보다 현실적인 관점에서 개인정보 유출 예방을 위한 정책을 제시하고자 하는 정책개발자에게 일정 정도의 시사점을 줄 수 있을 것이다. 둘째, 개인정보 유출 예방행동에 있어 효능감의 중요성을 파악함으로써 개인정보 유출 예방을 위한 보다 세분화된 정책 수립에 도움을 줄 수 있을 것이다. 기존 개인정보 유출 예방정책과 함께 활용할 수 있는 효능감 증진 방안을 마련함으로써 개인정보 관리 담당자들이 보다 효과적인 개인정보 유출 예방 전략 및 정책을 수립하는데 도움을 줄 수 있을 것이다.

7. 결 론

본 연구는 인터넷 사용자의 특성에 따른 개인정보 유출 예방 행동변화를 위한 전략 및 정책에 도움을 주고자 위험지각태도 프레임웍을 활용하여 인터넷 사용자를 4개의 태도그룹으로 분류하고 이들 그룹 간의 보호동기, 정보탐색, 예방활동 간의 차이를 실증적으로 분석하였다. 분석결과 지각된 위험과 효능감에 의해 분류된 각 그룹에 따라 개인정보 유출 예방과 관련된 행위나 태도가 서로 상이하다는 것을 파악하였다. 본 연구의 결과는 기업 및 정부의 개인정보 유출 예방 담당자로 하여금 보다 세분화된 유출 예방활동 전략을 수립할 수 있는 가이드라인의 역할을 수행 할 수 있을 것으로 기대된다.

본 연구는 다음과 같은 한계점이 있으며 이를 해결할 수 있는 후속 연구가 필요하다. 첫째, 표본이 매우 제한적이다. 사용된 표본의 특성을 보면 20대가 과반수를 차지하고 있으며, 학력 또한 대졸이상이 과반수를 차지하고 있다. 따라서 보다 다양한 표본을 포함함으로써 연구 결과를 일반화 할 수 있을 것이다. 둘째, 개인정보 유출과 관련된 다양한 변수를 고려하지 못했다. 예를 들면, 어떤 상황 하에서 가장 많은 개인정보를 노출시키는지는 전혀 다루어지지 않았다. 따라서 향후 연구에서는 인터넷 사용 목적과 개인정보 공개 및 제공과 관련된 다양한 변수가 추가 될 필요가 있다.

References

[1] Bandura, A., Social Foundation of Thought and Action, Prentice-Hall, Englewood Cliffs, NJ, 1986.

[2] Beuningen, J. V., Ruyter, K., Wetzels, M., and Streukens, S., “Customer Self-Efficacy in Technology Based Self-Service,” Journal of Service Research, Vol. 11, No.

4, pp. 407-428, 2009.

[3] Byun, S.-J., Lee, G.-S., and Park, K.-J., "Current Status of Domestic and Foreign Personal Information Breach Notification Act," KIISC Review, Vol. 18, No. 6, pp. 35-42, 2008.

[4] Carpinter, J. and Hunt, R., "Tightening the Net : A Review of Current and Next Generation Spam Filtering Tools," Computers and Security, Vol. 25, pp. 566-578, 2006.

[5] Cavusoglu, H., Mishra, B., and Raghunathan, S., "The Effect of Internet Security Breach Announcements on Market Value : Capital Market Reactions for Breached Firms and Internet Security Developers," International Journal of Electronic Commerce, Vol. 9, No. 1, pp. 70-104, 2004.

[6] Chan, Y. E., Culnan, M. J., Greenaway, K.., Laden, G., Levin, T., and Smith, H. J., "Information Privacy : Management, Marketplace, and Legal Challenges," Communications of the Association for Information Systems, Vol. 16, No. 12, pp. 270-298, 2005.

[7] Chang, T.-Z. and Chen, S.-J., "Market Orientation, Service Quality and Business Profitability : A Conceptual Model And Empirical Evidence," Journal of Services Marketing, Vol. 12, No. 6, pp. 246-254, 1998.

[8] Chen, J. and Guo, C.-X., "Online Detection and Prevention of Phishing Attacks," IEEE Communication and Networking, China Com'06, pp. 1-7, 2006.

[9] Choi, B. and Lee, H., "An Empirical Investigation of KM Styles and Their Effect on Corporate Performance," Information and Management, Vol. 40, No. 3, pp. 403-417, 2003.

[10] Crespo, A. H., del Bosque, I. R., and Sanchez, M. M. G. D., "The Influence of Perceived Risk on Internet Shopping Behavior : A Multidimensional Perspective," Journal of Risk Research, Vol. 12, No. 2, pp. 259-277, 2009.

[11] Cronin, J. J. and Taylor, S. A., "Measuring Service Quality : A Reexamination and Extension," Journal of Marketing, Vol. 56, No. 3, pp. 55-67, 1992.

[12] Duh, R.-R., Sunder, S., and Jamal, K., "Control and Assurance in E-Commerce: Privacy, Integrity, and Security at eBay," Taiwan Accounting Review, Vol. 3, No. 1, pp. 1-27, 2002.

[13] Hair, J. F., Anderson, R., Tatham, R., Black, W., Multivariate Data Analysis with Readings, Prentice Hall, Englewood Cliffs, New Jersey, 1995.

[14] Han, C. H., Chai, S. W., Yoo, B. J., Ahn, D. H., and Park, C. H., "A Quantitative Assessment Model of Private Information Breach," The Journal of Society for e-Business Studies, Vol. 16, No. 4, pp. 17-31, 2011.

[15] Hui, K. L., Teo, H. H., and Lee, S. Y., "The Value of Privacy Assurance : A Field Experiment," MIS Quarterly, Vol.

31, No. 1, pp. 19-34, 2009.

[16] Jee, B., Fan, L., Lee, S.-C., and Suh, Y.-H., "Personal Information Protection Behavior for Information Quality : Health Psychology Theory Perspectives," Journal of the Korean Society for Quality Management, Vol. 39, No. 3, pp. 432-443, 2011.

[17] Jo, S. E. and Yoo, S. W., "A Study on the Effects of Risk Perception Attitudes and Subjective Norm on the Preventive Behaviors of Cervical Cancer Testing RPA Framework on Korean College Women," Journal of Public Relations Research, Vol. 15, No. 1, pp. 58-98, 2011.

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

[19] Kim, J., "Analyzing Effects on Firms' Market Value of Personal Information Security Breaches," The Journal of Society for e-Business Studies, Vol. 18, No. 1, pp. 1-12, 2013.

[20] Kim, J.-D., "Personal Information Security Management System and Governance," KIISC Review, Vol. 18, No. 6, pp. 1-5, 2008.

[21] Kim, J. and Kim, S., "Privacy Behavioral Intention in Online Environment : Based on Protection Motivation Theory," Informatization Policy, Vol. 20, No. 3, pp. 63-85, 2013.

[22] Korea Internet and Security Agency, 2013 Survey on the Internet Usage Executive Summary, Korea Internet and Security Agency, 2013.

[23] Kwon, Y. O. and Kim, B. D., "The Effect of Information Security Breach and Security Investment Announcement on the Market Value of Korean Firms," Information Systems Review, Vol. 9, No. 1, pp. 105-120, 2007.

[24] Lee, D., "Self-disclosure and Privacy in the Age of Web 2.0 : A Case Study," Journal of Communication and Information, Vol. 46, pp. 556-589, 2009.

[25] Lee, S. K., "An Infringement of private Information Right and Its protection in an Information Society," Chung-Ang Law Review, Vol. 11, No. 1, pp. 51-83, 2009.

[26] Leventhal, H. I., "Finding and Theory in the Study of Fear Communications," Advances in Experimental Social Psychology, Vol. 5, pp. 119-186, 1971.

[27] Liang, H. and Xue, Y., "Understanding Security Behaviors in Personal Computer Usage : A Threat Avoidance Perspective," Journal of the Association for Information Systems, Vol. 11, No. 7, pp. 394-413, 2010.

[28] Mayer-Schönberger, V., "The Internet and Privacy Legislation : Cookies for a Treat?" Computer Law and Security Review, Vol. 14, No. 3, pp. 166-174, 1998.

[29] Moon, S., "An International Trend in Online Individual Information Protection -Focusing on American System-," Journal of Comparative Law, Vol. 3, pp. 57-81,

2004.

[30] Moon, J.-W. and Kim, Y. G., "Extending the TAM for a World-Wide-Web Context," Information and Management, Vol. 38, No. 4, pp. 217-230, 2001.

[31] Nam, K., Park, S., Kang, H.-S., Nam, K., and Kim, S., "The Latest Trends and Future Prospects on Personal Information Protection Technologies," KIISC Review, Vol. 18, No. 6, pp. 11-19, 2008.

[32] Park, H.-S. and Kim, S., "An Empirical Study on SNS Users' Privacy Protection Behaviors," Management and Economics, Vol. 46, No. 2, pp. 69-91.

[33] Park, C. and Lee, S.-W., "A Study of the User Privacy Protection Behavior in Online Environment : Based on Protection Motivation Theory," Journal of Internet Computing and Services, Vol. 15, No. 2, pp. 59-71, 2014.

[34] Real, K., "Information Seeking and Workplace Safety : A Field Application of the Risk Perception Attitude Framework," Journal of Applied Communication Research, Vol. 36, No. 3, pp. 339-359, 2008.

[35] Rimal, R. N., "Perceive Risk and Self-efficacy as Motivators : Understanding Individuals' Long-term Use of Health Information," Journal of Communication, Vol. 51, No. 4, pp. 633-654, 2001.

[36] Rimal, R. N., Bose, K., Brown, J., Mkandawire, G., and Folda, L., "Extending the Purview of the Risk Perception Attitude Framework : Findings from HIV/AIDS Prevention Research in Malawi," Health Communication, Vol. 24, No. 3, pp. 210-218, 2009.

[37] Rimal, R. N. and Juon, H., "Use of the Risk Perception Attitude Framework for Promoting Breast Cancer Prevention," Journal of Applied Social Psychology, Vol. 40, No. 2, pp. 287-310, 2010.

[38] Rimal, R. N. and Real, K., "Perceived Risk and Efficacy Beliefs as Motivators of Change Use of the Risk Perception Attitude(RPA) Framework to Understand Health Behaviors," Human Communication Research, Vol. 29, No. 3, pp. 370-399, 2003.

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

[40] Siponen, M., Pahnila, S. M., and Adam, M. A, "Compliance with Information Security Policies : An Empirical Investigation," Computer, Vol. 43, No. 2, pp. 64-71, 2010.

[41] Soh, P.-H. and Subramanian, A. M., "Is Usage a Missing Link in Explaining the Perceived Learning Outcome of Technology-Mediated Learning," IEEE Transactions on Engineering Management, Vol. 55, No. 1, pp. 50-66, 2008.

[42] Song, Y.-J. and Lee, D.-H., "Web Services-Adaptable Privacy-Aware Digital Rights Management Architecture," The Journal of Society for e-Business Studies, Vol. 10, No. 4, pp. 53-81, 2005.

[43] Turner, M. M., Rimal, R. N., Morrison, D., and Kim, H., "The Role of Anxiety in Seeking and Retaining Risk Information : Testing the Risk Perception Attitude Framework in Two Studies," Human Communication Research, Vol. 32, No. 2, pp. 130-156, 2006.

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

[45] Woo, J., "From Information Privacy to Identity Privacy Reconsidering the Concept of Network Privacy," Press and Society, Vol. 13, No. 4, pp. 110-145, 2005.

[46] Yoo, J., "Comparison of Information Security Controls by Leadership of Top Management," The Journal of Society for e-Business Studies, Vol. 19, No. 1, pp. 63-78, 2014.

[47] Yoo, H.-W. and Kim, T.-S., "Considering Information Security Professionals' Career to Analyze Knowledge and Skills Requirements," Journal of The Korea Institute of Information Security and Cryptology, Vol. 19, No. 4, pp. 77-89, 2009.

[48] Youm, H. Y., "The Present and Future of IT839 Information Security Technologies," KIISC Review, Vol. 15, No. 3, pp. 1-12, 2005.

[49] Yun, S.-Y., "Coping Strategy for Environment Changes in Personal Information Protection Regulations due to Personal Information Protection Law Enforcement," Korea Information Processing Society Review, Vol. 17, No. 2, pp. 3-9, 2010.

[50] Zhao, X. and Cai, X., "The Role of Risk, Efficacy, and Anxiety in Smokers' Cancer Information Seeking," Health Communication, Vol. 24, No. 3, pp. 259-269, 2009.

〈부록 1〉 설문서

항목 1: 인구통계

학력수준 : 초졸 ( ) 중졸 ( ) 고졸 ( ) 대졸 ( ) 대학원졸 ( )
성별 : 남자 ( ), 여자 ( )
나이 :
가계소득수준 :
1일 인터넷 사용시간 :

본 설문에서 **개인정보 유출**이란 개인이 회원가입 등의 목적으로 개인정보를 제공한 포털, 특정 기업 또는 개인이 개설한 웹 사이트 등에서 해킹 또는 개인정보의 불법 유통 등으로 개인이 허가하지 않은 제 3자에게 개인정보가 무단 도용되는 것을 말합니다. 이러한 개인정보 유출은 무분별한 스팸메일, 이메일 및 보이스피싱, 명의 도용, 사기 등의 2차 피해를 초래하여 금전적, 정신적, 시간적 피해를 야기할 수 있습니다.

항목 2 : 다음은 개인정보 유출에 대한 당신의 지각된 위험 정도에 대한 항목입니다.

1. 나는 개인정보 유출로 인한 피해를 입을 가능성이 있다고 생각한다.
2. 나도 언젠가는 개인정보 유출로 인한 피해를 입을 수 있는 가능성이 있다고 생각한다.
3. 개인정보 유출로 인한 피해는 나와 내 가족 모두에게 피해를 줄 것이다.
4. 개인정보 유출로 인한 피해 복구는 매우 어려울 것이다.

항목 3 : 다음은 개인정보 유출 예방에 대한 당신의 능력과 그에 대한 믿음 정도에 대한 항목입니다.

1. 나는 개인정보가 유출되지 않도록 잘 관리할 자신이 있다.
2. 나는 개인정보가 유출되면 이를 파악하고 이에 상응하는 조치를 할 능력이 있다.
3. 나는 개인정보 유출을 정기적으로 체크 하거나 보안 전문기업의 서비스를 이용하는 것이 개인정보 유출을 조기에 차단하는 효과적인 방법이라고 믿는다.
4. 나는 개인정보 유출을 정기적으로 체크 하거나 보안 전문기업의 서비스를 이용하는 것이 개인정보 유출 피해를 예방해줄 것이라고 믿는다.
5. 나는 웹사이트의 개인정보보호 정책을 잘 따를 수 있다.
6. 나는 개인정보 유출 예방을 위해 내가 할 수 있는 일들이 많이 있다고 생각한다.
7. 나는 개인정보 유출 예방 방법이 실천하기 쉽다고 생각한다.

항목 4 : 다음은 개인정보 유출 예방에 대한 당신의 보호행동 동기 정도에 대한 항목입니다.

1. 나는 개인정보 유출을 막기 위해 적극적으로 노력할 것이다.
2. 나는 개인정보 유출을 막을 수 있는 능력을 갖고 싶다.
3. 나는 개인정보 유출을 예방하고 싶다.
4. 나는 개인정보 유출에 아무런 관심이 없다. (역진코드)

항목 5 : 다음은 개인정보 유출 예방을 위한 당신의 정보탐색 정도에 대한 항목입니다.

1. 내가 만약 개인정보 유출에 관한 정보를 TV에서 접한다면, 주의 깊게 시청할 것이다.
2. 내가 만약 개인정보 유출에 관한 정보를 신문에서 접한다면, 주의 깊게 정독할 것이다.
3. 내가 만약 개인정보 유출에 관한 정보를 인터넷에서 접한다면, 주의 깊게 살펴볼 것이다.
4. 내가 만약 개인정보 유출에 관한 정보를 라디오에서 접한다면, 주의 깊게 청취할 것이다.
5. 나는 개인정보 유출에 대해 가족들과 함께 대화할 것이다.
6. 나는 개인정보 유출에 대해 친구, 지인들과 함께 대화할 것이다.
7. 나는 개인정보 유출에 대해 관련 기관 및 업체에 문의할 것이다.

항목 6 : 다음은 개인정보 유출 예방을 예방활동 정도에 대한 항목입니다.

1. 나는 내가 개인정보를 제공한(회원가입 등) 웹사이트의 개인정보보호정책을 필독한다.
2. 나는 방화벽, 사이트 가드 등의 인터넷 보안 프로그램을 사용한다.
3. 나는 V3, 노턴 고스트, 알약 등 백신 및 안티 스파이웨어 프로그램을 사용한다.
4. 나는 웹 사이트에 회원 가입 시 영문과 숫자가 혼합된 비밀번호를 사용한다.
5. 나는 웹 사이트에 회원 가입 시 되도록 긴 비밀번호를 사용한다.
6. 나는 개인정보보호 및 관리 전문기업 (사이렌 24 등) 또는 I-PIN 등 제 3자가 제공하는 서비스를 이용한다.
7. 당신은 1년 동안 몇 회나 개인정보 유출 및 예방 방법 등과 관련된 정보 탐색을 위해 시간을 할애 하십니까?
8. 당신은 개인정보 유출 및 예방 방법에 대한 정보를 탐색할 때 얼마나 많은 시간을 사용하십니까?
9. 당신은 얼마나 자주 개인정보 유출 및 예방 방법에 대한 정보를 탐색 하십니까?
10. 당신은 얼마나 자주 바이러스, 스파이웨어를 검사 및 치료 하십니까?
11. 당신은 얼마나 자주, 이용 중인 웹 사이트의 비밀번호를 변경 하십니까?
12. 당신은 1년 동안 몇 회나, 이용 중인 웹 사이트의 비밀번호를 변경 하십니까?

저 자 소 개

장익진 (E-mail : ijjang@kookmin.ac.kr)
2008년~2010년 국민대학교 경영대학 e-비즈니스학과 (석사)
2010년~2013년 국민대학교 경영대학 e-비즈니스학과 (박사과정 수료)
2013년~현재 국민대학교 경영대학 데이터사이언스 학과 (박사과정)
관심분야 인터넷비지니스, Supply Chain Management

최병구 (E-mail : h2choi@kookmin.ac.kr)
1990년~1994년 고려대학교 정경대학 통계학과 (학사)
1994년~1996년 KAIST 경영대학원 경영공학전공 (석사)
1996년~2002년 KAIST 경영대학원 경영공학전공 (박사)
2002년~2003년 University of Minnesota Carlson School of Management (방문연구원)
2004년~2008년 University of Sydney, School of Information Technologies 조교수
2008년~2009년 국민대학교 경영대학 조교수
2010년~현재 국민대학교 경영대학 부교수
관심분야 지식경영, 인터넷비지니스, 데이터사이언스