韓國IT서비스學會誌
第16卷 第3號
2017年 9月, pp.147-165

Journal of Information Technology Services
https://doi.org/10.9716/KITS.2017.16.3.147

온라인 사용자의 비밀번호 보호행위 : 공포 소구와 메시지 프레이밍 효과, 그리고 비밀번호 보호행위의 동기요인*

박재영** · 김전도*** · 김범수****

Online Users' Password Security Behavior : The Effects of Fear Appeals and Message Framing, and Mechanism of Password Security Behavior*

Jaeyoung Park** · Jeondo Kim*** · Beomsoo Kim****

■ Abstract ■

Recently, there have been numerous issues about password breaches and it is becoming important for the users to manage their passwords. In practice, the online service provider are asking the online users to change their passwords periodically. However, majority of the users are not changing their passwords regularly, and this can increase the risk of password breach. The purpose of this study is to investigate whether 'fear appeals' and 'message framing' enhance the behavior of changing passwords by the online users. Furthermore, we identify the mechanism on how the behavior of changing passwords is enabled using protection motivation theory. The results of an online experiment show that the online users who are exposed to 'fear appeals' perceived a more vulnerability and severity of password breaches, which in turn, increased the intention of changing their password. In addition, we found that perceived severity of password breaches affect fear positively. Moreover, we found that fear has significant impact on the willingness of changing passwords. Finally, Message framing plays a moderating role between fear and change intentions. That is, in a situation where 'fear appeal' is presented, it means that 'gain framing' is more effective than 'loss framing' These findings suggest that the online service providers may need to use 'fear appeals' to the online users. Security managers can address issues related to the password breaches by carefully designing 'fear appeals'.

Keyword : Fear Appeals, Message Framing, Password, Password Breach, Password Security Behavior, Protection Motivation Theory, Warning Message

Submitted : March 27, 2017 1st Revision : July 7, 2017 Accepted : August 14, 2017

* 본 논문은 박재영의 석사학위(연세대 정보대학원) 논문을 일부 수정하여 작성한 것임을 밝힙니다.

** 연세대학교 정보대학원 박사과정
*** 연세대학교 정보대학원 석사과정
**** 연세대학교 정보대학원 교수, 교신저자

1. 서 론

오늘날 정보통신기술의 발전으로 개인들 간 정보 교류는 물론이고, 쇼핑, 금융 등 일상생활에서 필요한 거의 모든 행위들이 온라인 환경에서 가능하게 되었다. 통계청에 따르면, 전체 소매 판매에서 온라인 쇼핑이 차지하는 비중이 2012년 9.7%에서 매년 상승하여 2015년에는 14.7%로 치솟았다.[1] 이렇게 환경이 변화함에 따라 대부분의 사람이 온라인 환경에서의 대표적인 인증 수단이라고 할 수 있는 비밀번호를 최소한 하나 정도는 가지고 있다고 해도 무방할 것이다.

최근 들어, 비밀번호가 유출되는 사고가 급증하고 있다. 2013년 야후(Yahoo), 2015년 뽐뿌 사이트와 같이 해킹으로 인한 대규모 비밀번호 유출 사건이 발생했는가 하면, 개인의 비밀번호 관리 미숙으로 인한 계정 도용 사례도 속출하고 있다. 비밀번호 유출은 금전적 피해는 물론, 사생활 침해로까지 이어질 수가 있다.

따라서 사용자의 철저한 비밀번호 관리가 요구되는데, 기업에서는 비밀번호를 주기적으로 변경하라고 안내하고 있다. 하지만, 대다수가 비밀번호를 변경하지 않는 것으로 나타나고 있다. 한국인터넷진흥원에 따르면, 공인인증서 비밀번호 변경주기에 대해 물어본 결과, 응답자 중 33.2%가 변경하지 않는다고 하였다(KISA, 2015). 그리고 국내 보안담당자 대상으로 설문조사를 실시한 결과, 응답자 중 26.15%가 잘 바꾸지 않는다고 하였다.[2] 이와 같은 사실은 사용자들의 비밀번호 관리 의식이 상당히 미흡한 수준인 것을 나타내며, 이를 향상시키기 위한 노력이 필요하다고 볼 수 있다.

지금까지 비밀번호와 관련된 연구가 다수 진행되어 왔다. 우선, 비밀번호 보호수준을 끌어올릴 수 있는 방안으로 공포 소구(Fear Appeals)가 활용되어 왔다. 공포 소구는 특정 위협의 취약성과 심각성, 그리고 권고행동의 효능감(반응 효능감, 자기 효능감)에 대한 메시지를 통해 수용자들이 바람직한 행동을 하게끔 유도하는 설득적 메시지라고 할 수 있다(Witte, 1992). 공포 소구를 통해 사용자들이 보다 강한 비밀번호를 사용하는 것으로 나타났으며(Vance et al., 2013; Zhang and McDowell, 2009), 공포 소구는 비밀번호 가이드라인 준수의도를 향상시킬 수 있는 효과적인 방법이라고 하였다(Mwagwabi et al., 2014). 이처럼 공포 소구는 개인들의 태도, 인식 그리고 행동까지 변화시킬 수 있는 효과적인 설득 커뮤니케이션 수단이라고 할 수 있다. 또한, 일부 연구에서는 보호동기이론(Protection Motivation Theory)을 바탕으로 비밀번호 보호행위에 영향을 미치는 요인들이 무엇인지 설명하였다(Mwagwabi et al., 2014; Park, 2015; Zhang and McDowell, 2009).

위에서 살펴봤듯이, 공포 소구와 보호동기이론을 활용하여 비밀번호와 관련된 행위를 설명한 연구가 일부 진행되어 왔다. 하지만 공포 소구와 보호동기이론을 모두 적용한 연구는 아직 부족하다고 할 수 있으며, 비밀번호 변경행위에 초점을 맞춘 연구는 극히 일부에 불과한 것으로 파악된다. 따라서 비밀번호 변경행위에 대한 실증적 분석이 추가적으로 필요한 실정이라고 볼 수 있다.

특정 상황에서 개인들의 선택과 판단이 달라지는지를 알아보기 위해 적용되는 또 다른 이론으로 메시지 프레이밍이 있다. 이것에 의하면, 동일한 행동을 유도하는데 있어서 메시지 제시 방식에 따라 사람들의 태도와 의사결정이 달라진다고 한다. 따라서 메시지 프레이밍은 비밀번호 변경행위를 설명하는데 적용될 수 있다고 판단된다. 이를 통해 비밀번호 변경행위가 변화하는지를 밝혀낸다면, 학문적으로 의의가 있을 뿐 아니라, 실무적으로도 의미하는 바가 있다고 볼 수 있다.

---

1) 매일경제, “패더라임 확 바뀌는 유통街…매장에서 아이쇼핑 구매는 온라인서”, [online], [cited 2016. 04. 08], Available at http://vip.mk.co.kr/news/view/21/20/1388129.html.

2) 보안뉴스, “보안담당자들, 비밀번호 변경 얼마나 자주 할까?”, [online], [cited 2014. 11. 12.], Available at http://www.boannews.com/media/view.asp?idx=51108.

종합하자면, 본 연구에서는 비밀번호 변경행위를 증대시킬 수 있는 방안에 대해 알아보고, 추가적으로 그 동기요인이 무엇인지 찾고자 한다. 즉, 다음과 같은 목적을 지닌다. 첫째, 공포 소구가 효과적으로 발휘되는지 보고자 한다. 공포 소구 유무에 따라 비밀번호 변경의도가 달라지는지 알아보는 것이다. 둘째, 메시지 프레이밍 효과를 살펴보고자 한다. 메시지 프레이밍에 따라 비밀번호 변경의도가 다르게 나타나는지 확인하는 것이다. 셋째, 공포 소구와 메시지 프레이밍 간 상호작용 효과가 발생하는지 알아보고자 한다. 마지막으로 비밀번호 변경행위가 이루어지는 메커니즘(Mechanism), 즉, 인과관계를 규명하고자 한다.

2. 이론적 배경

2.1 공포 소구(Fear Appeals)

2.1.1 공포 소구의 개념

공포(Fear)는 높은 수준의 자극과 함께 오는 부정적 정서를 말하며, 심각하고 자신과 관련이 있다고 여겨지는 위협으로부터 발생된다(Easterling and Leventhal, 1989; Ortony and Turner, 1990; Witte, 1992). 일반적으로 '위협 기법(Scare Tactic)'이라고도 불리는 공포 소구(Fear Appeals)는 "만약 수용자들이 메시지에서 권고한 행동을 하지 않게 되면, 끔찍한 일이 발생할 것이라고 경고함으로써, 수용자들에게 두려움을 심어주는 설득적 커뮤니케이션"이라고 정의된다(Witte, 1992). 보건, 광고, 마케팅 등과 같은 설득 커뮤니케이션 분야에서 사람들의 행동을 변화시키기 위한 수단으로 널리 사용되고 있으며, 에이즈 예방, 금연 캠페인, 비듬방지 샴푸 광고 등에 대해서 살펴본 연구가 대표적이다. 사람들은 일반적으로 자신에게 부정적인 결과가 발생하는 것을 원하지 않을 뿐 아니라, 그런 끔찍한 경험 자체를 두려워하기 때문에 메시지에서 권고된 방향대로 행동하려는 경향이 있다(Witte et al., 2001).

2.1.2 보호동기이론(Protection Motivation Theory)

보호동기이론(Protection Motivation Theory)은 공포 소구에 의해 수용자들의 태도가 어떻게 변화되는지를 규명하기 위해 제안되었다(Rogers, 1975). 이것에 의하면, 공포 소구는 유해성 크기(Magnitude of Noxiousness), 발생 가능성(Probability of Occurrence), 권고반응의 효능감(Efficacy of Recommended Response)과 같은 세 가지 요소들로 구성되어 있다. 수용자들은 인지적 매개 과정(Cognitive Mediating Process)을 통해 세 가지 요소들을 평가하고, 이러한 과정을 거쳐 보호동기 수준이 형성된다. 그리고 이것에 의해 최종적으로 권고방안을 따르려는 의도가 결정된다는 것이 초기 보호동기이론이다.

이후에 Rogers는 자기 효능감(Self-efficacy)과 반응 비용(Response Cost)을 추가하여 수정된 이론을 고안하였다(Rogers, 1983; Maddux and Rogers, 1983). 여기에서 자기 효능감은 Bandura(1995)가 제시한 개념으로 "어떠한 행위 및 영역 안에서 자신이 수행할 수 있는 능력에 대한 개인의 신념"으로 정의된다. 달리 말하면, 자신이 어려움과 장애에 잘 대처할 수 있는 능력이 있다고 믿는 정도를 의미하다고 볼 수 있다. 수정된 이론에는 두 가지 인지적 매개 과정, 위협평가(Threat Appraisal Process)와 대처평가(Coping Appraisal Process)가 있다. 위협평가는 보상에서 위협의 심각성과 취약성을 뺀 값으로 나타낼 수 있다. 즉, 보상이 위협보다 클 경우에는 부적응 반응으로 이어지는 것이다. 반면, 대처평가는 효능감에서 반응 비용을 뺀 값으로 효능감이 반응 비용보다 높을 때 적응 반응이 나타난다. 이러한 인지적 매개 과정을 거치고 난 후에 보호동기가 형성되고, 이것이 보호행동으로 이어진다.

2.1.3 공포 소구와 보호동기이론에 관한 연구

공포 소구는 보건, 공익 캠페인과 같은 설득 커뮤니케이션 분야에서 많이 활용되어 왔는데, 최근

정보 시스템 분야에서도 공포 소구를 바탕으로 한 연구가 일부 진행되었다. 특히, 정보보안 행위를 증대시키기 위한 방안으로 활용되었으며, 대다수의 연구에서 그 효과가 입증되었다. Johnston and Warkentin(2010)의 연구를 살펴보면, 스파이웨어(Spyware)에 대한 공포 소구를 보여주자, 개인들의 태도가 변화하였다. 즉, 공포 소구를 제시하기 전과 비교하여 위협 요소인 지각된 심각성과 지각된 취약성이 더 높게 나타났다. 구체적으로 말하자면, 수용자들은 공포 소구를 보고나서 스파이웨어를 더 심각한 위협으로 느끼게 되었고, 그것에 감염될 가능성이 더 크다고 인지하게 되었다. 또한, 공포 소구의 강도(위협 수준 낮음 VS. 위협 수준 높음)에 따라 백업행위와 안티 멀웨어(Anti-Malware) 소프트웨어 사용행위에 대한 인과관계가 달라짐을 보였고(Boss et al., 2015), 공포 소구 제시 방식이 공포 소구의 설득력에 영향을 주는 것으로 나타났다(Park, 2015). Mwagwabi et al.(2014)는 공포 소구가 비밀번호 가이드라인 준수 의도를 향상시키는 효과적인 방법임을 입증했으며, 일부 연구자는 사용자들이 공포 소구로 인해 보다 강한 비밀번호를 사용하게 된다고 하였다(Vance et al., 2013; Zhang and McDowell, 2009).

보호동기이론 역시 대체적으로 보건 분야에서 사용되어 왔는데, 점차적으로 그 적용분야가 확대되고 있는 추세이다. 정보 시스템 분야에서도 보호동기이론을 활용하여 개인들의 행위를 규명하는 연구가 다수 진행되었다. 안티 스파이웨어 소프트웨어나 안티 멀웨어 소프트웨어 등과 같은 백신 소프트웨어 사용행위를 규명했으며(Boss et al., 2015; Johnston and Warkentin 2010), 표절 방지 소프트웨어 사용행위에 대한 연구도 진행되었다(Lee, 2011). 비밀번호 사용에 초점을 맞춘 연구도 있었으며(Mwagwabi et al., 2014; Park, 2015; Zhang and McDowell, 2009), 포괄적으로 정보보호 행위를 다루기도 하였다(Chen and Zahedi, 2016; Hanus and Wu, 2016; Tsai et al., 2016; Workman et al., 2009).

정보 시스템 분야에서 공포 소구와 보호동기이론을 모두 적용하여 개인들의 행위를 살펴본 연구도 일부 진행되었다. 하지만, 공포 소구 효과를 입증한 후에 정보보안 행위에 대한 메커니즘까지 규명한 연구는 드물었다. 다시 말해, 대부분의 연구가 실험을 통한 공포 소구 효과 입증 없이 공포 소구를 제시한 경우에 어떠한 인과관계를 가지는지만 분석하였다(Johnston and Warkentin, 2010; Mwagwabi et al., 2014; Zhang and McDowell, 2009). 또한, Boss et al.(2015)는 멀웨어와 관련하여 공포 소구 수준(위협 수준 높음 VS. 위협 수준 낮음)에 따라 심각성, 취약성, 두려움, 의도, 행동이 달라진다고 밝혔으나, 공포 소구 유무에 대해서는 아무런 언급이 없었다. 따라서 공포 소구 유무에 따라 개인들의 행위가 달라지는지를 밝힐 뿐 아니라 그 행위들이 어떻게 이루어지는지에 대한 메커니즘까지 규명할 필요성이 있어 보인다.

2.2 메시지 프레이밍(Message Framing)

메시지 프레이밍(Message Framing)은 어떤 메시지를 표현하는데 있어서 긍정적 혹은 부정적 구성형식을 갖는 것이라고 할 수 있다(Lee, 2006). 즉, 긍정적(이득)으로 프레이밍 된 메시지는 특정 행동을 할 경우에 긍정적 결과 혹은 이득을 얻을 것이라고 강조한다. 반면, 부정적(손실) 프레이밍 메시지는 특정 행동을 하지 않았을 경우에 부정적 결과 혹은 손실이 발생될 것이라고 말한다. 앞서 살펴본 공포소구와는 개념적으로 상이하다고 볼 수 있다. 즉, 공포 소구는 비밀번호 유출 자체가 가지고 있는 위협을 나타낸 것이라고 할 수 있다. 반면, 메시지 프레이밍, 특히, 부정적 메시지 프레이밍은 비밀번호를 변경하지 않았을 때 발생되는 손실을 말한다.

Meyerowitz and Chaiken(1987)는 개인들이 지니고 있는 부정성 편향(Negativity Bias)과 손실혐오(Loss Aversion)로 인해 일반적으로 손실 프레이밍이 이득 프레이밍보다 더 설득적이라고 하였다. 이를 자세히 알아보면, 유방암 자가 검진에

대한 광고를 긍정적 메시지("유방암 자가 검진을 할 경우, 치료 가능한 초기 상태의 종양을 발견할 가능성이 높다.")와 부정적 메시지("유방암 자가 검진을 하지 않을 경우, 치료 가능한 초기 상태의 종양을 발견할 가능성이 낮다.")로 나눠서 보여준 결과, 부정적 메시지에 더 반응하는 것으로 나타났다(Meyerowitz and Chaiken, 1987). 구강청정제 광고에서도 부정적인 손실을 강조하는 메시지가 더 효과적인 것으로 드러났다(Homer and Yoon, 1992). 또한, 신용카드사용에 대한 연구에서도 마찬가지로 부정적으로 프레이밍 된 메시지가 소비자들의 행동에 더 큰 영향을 미치는 것으로 나타났다(Ganzach and Karsahi, 1995).

반면, 일부 연구에서는 긍정적 프레이밍이 더 효과적인 것으로 밝혀졌다. 쇠고기를 평가하는 경우, 실험 참여자들은 부정적으로 나타낸 메시지(25% 지방)보다 긍정적으로 표현된 메시지(75% 육질)에 더 호의적인 태도를 보였다. Gaeth et al.(1990)의 연구에서도 마찬가지로 워드프로세스를 통해 성적이 올라간 학생들의 비율을 제시하는 것이 그것을 사용하지 않아 성적이 낮아진 학생들의 비율을 제시하는 것보다 더 설득적인 것으로 나타났다.

위에서 살펴본 것처럼 메시지 프레이밍을 바탕으로 많은 연구가 진행되었지만, 정보 시스템 분야에서는 그 활용이 다소 적었다고 볼 수 있다. 그 간 진행된 연구를 살펴보면, 비밀번호 변경에 있어서 손실을 강조한 메시지를 더 설득적이라고 느끼는 것으로 밝혀졌으며(Park, 2015), 모바일 뱅킹 서비스의 경우에는 메시지 프레이밍 효과가 없는 것으로 나타났다(Kurila et al., 2016). 즉, 이득 프레이밍과 손실 프레이밍 간 종속변수의 차이가 유의미하지 않았다. 그리고 다른 연구들의 경우, 부정적 프레이밍만 살펴보거나(Shropshire et al., 2010) 긍정 프레이밍과 중립 프레이밍만 알아보았다는 점(Angst and Agarwal, 2009)에서 일부 한계점이 존재한다. 이처럼 정보 시스템 분야에서는 메시지 프레이밍을 적용한 연구가 아직 부족한 실정이라고 볼 수 있으며, 그 효과가 제대로 나타나고 있지 않는 것이 현재 상황이다.

3. 연구모형과 연구가설

3.1 공포 소구와 메시지 프레이밍 효과

공포 소구와 같은 설득 커뮤니케이션은 인간의 태도, 의도, 그리고 행동을 변화시키는데 효과적인 수단이라고 하였으며(Fishbein and Ajzen, 1975), 정보 시스템 분야에서 이와 같은 공포 소구의 효과를 입증한 연구가 일부 존재한다. Johnston and Warkentin(2010)는 스파이웨어 관련 공포 소구를 처치요인으로 하여 집단 내 실험설계를 통해 진행한 결과, 그 효과가 있음을 입증하였다. 공포 소구를 보기 전보다 본 후에 위협 요소인 지각된 취약성과 지각된 심각성이 높게 나타난 것이다. 이것은 공포 소구를 통해서 지각된 위협이 증가된 것으로 볼 수 있다. 또한, 현장 실험을 통해 공포 소구와 상호작용성이 비밀번호 선택에 어떠한 영향을 미치는지 알아본 결과, 상호작용성이 있는 공포 소구(Interactive Fear Appeal Treatment)가 가장 효과적인 것으로 드러났다(Vance et al., 2013). Boss et al.(2015)의 연구에서는 공포 소구 수준에 따라 개인들의 태도와 의도가 다르게 나타났다. 즉, 공포 소구가 강한 경우에 위협을 더 심각하고 발생 가능성이 높다고 지각했으며, 행위의도도 더 높은 것으로 드러났다. 이와 같은 선행연구들을 통해 공포 소구로 인해 특정 위협에 대한 인식이 바뀌게 될 뿐 아니라, 행위 역시 달라질 수 있다는 것을 알 수 있다. 따라서 다음과 같은 H1을 설정하였다.

H1 : 온라인 사용자가 비밀번호를 변경하는데 있어서 공포 소구가 영향을 줄 것이다. 즉, 공포 소구가 제시된 집단의 비밀번호 변경의도가 더 높게 나타날 것이다(공포 소구 효과).

앞서 살펴본 바와 같이 메시지 프레이밍은 다양한 분야에서 활용되어 왔으며, 부정적 프레이밍이 대체적으로 더 설득적인 것으로 나타났다. 즉, 사람들은 부정적인 메시지에 더 민감하게 반응한다는

것으로(Meyerowitz and Chaiken, 1987) 이는 부정편향성 이론에 의한 것이라고 볼 수 있다. 정보시스템 분야에서 진행된 비밀번호 변경 관련된 연구에서도 손실을 강조한 메시지가 공포 소구 설득력에 영향을 미치는 것으로 나타났다(Park, 2015). 따라서 본 연구에서도 손실 프레이밍이 더 효과적일 것이라고 보고, 아래와 같이 H2를 세웠다.

H2 : 온라인 사용자가 비밀번호를 변경하는데 있어서 메시지 프레이밍이 영향을 줄 것이다. 즉, 손실 프레이밍이 제시된 집단의 비밀번호 변경의도가 더 높게 나타날 것이다(메시지 프레이밍 효과).

공포 소구 효과를 살펴본 연구에 따르면, 공포 소구가 다른 요인과 상호작용하여 그 효과가 더욱 증대되는 것으로 나타났다. Vance et al.(2013)는 공포 소구 효과가 상호작용성(Static VS. Interactive)에 따라 달라진다고 하였다. 즉, 공포 소구가 상호작용적(Interactive Fear Appeals)으로 제시되었을 때, 실험 대상자들은 강한 비밀번호를 설정하는 것으로 나타난 것이다. 이를 바탕으로 본 연구에서도 공포 소구와 다른 요인 간의 상호작용 효과가 나타나는지 살펴보기로 하고, 다음과 같은 H3을 설정하였다.

H3 : 공포 소구와 메시지 프레이밍 간 상호작용 효과가 발생할 것이다.

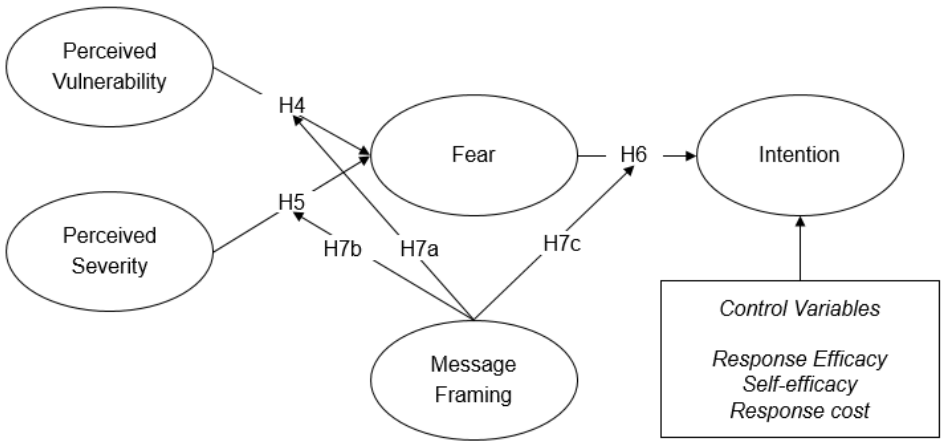
3.2 비밀번호 변경행위의 동기요인

다음으로 비밀번호 변경행위가 이루어지는 메커니즘을 규명하기 위하여 보호동기이론을 바탕으로 아래와 같은 연구모형을 설정하였다. 본 연구는 비밀번호 유출에 대한 위협(지각된 취약성, 지각된 심각성)에 초점을 맞추어 진행하였다. 이에 따라 개인의 정보보호 행위에 영향을 줄 수 있는 다른 요인들. 즉, 반응 효능감, 자기 효능감, 반응 비용은 통제변수로 설정하였다.

Boss et al.(2015)가 정리한 보호동기이론에 의하면, 지각된 취약성과 지각된 심각성이 두려움에 영향을 미친다고 하였다. 다른 연구에서도 비밀번호 유출에 대한 취약성과 심각성을 높게 인지할수록 그것에 대한 두려움이 커지는 것으로 밝혀졌다(Park, 2015). 따라서 보호동기이론과 기존 문헌을 바탕으로 아래와 같은 가설을 설정하였다.

H4 : 지각된 취약성이 두려움에 정(+)의 영향을 줄 것이다.

H5 : 지각된 심각성이 두려움에 정(+)의 영향을 줄 것이다.



〈Figure 1〉 Research Model

위와 같이 위협(지각된 취약성, 지각된 심각성)으로 형성된 두려움이 개인의 행위에 어떠한 영향을 미치는지를 살펴본 연구가 다수 존재한다. Mwagwabi et al.(2014)는 비밀번호 유출에 대한 위협이 비밀번호 가이드라인 준수의도에 긍정적인 영향을 준다는 것을 밝혔다. 또한, 비밀번호가 해킹당할 수 있다고 느끼는 두려움이 커질수록 비밀번호를 주기적으로 변경하며 안전한 비밀번호를 사용하는 것으로 나타났다(Zhang and McDowell, 2009). 따라서 본 연구에서는 비밀번호 유출에 대한 두려움이 비밀번호 변경의도에 긍정적인 영향을 준다고 가정하였다.

H6 : 두려움이 비밀번호 변경의도에 정(+)의 영향을 줄 것이다.

본 연구에서는 집단별로 각각 이득(긍정적) 프레이밍과 손실(부정적) 프레이밍을 제시하였다. 따라서 메시지 프레이밍에 따라 집단 간 인식 차이가 발생할 수 있다. Jeon et al.(2013)는 희소성 메시지 유형이 소비자의 충동구매에 미치는 영향에서 긍정적 프레이밍 효과가 더 크다고 밝혔다. 즉, 부정적 프레이밍에 노출된 소비자는 심리적 위협을 더 느끼게 되고, 이에 따라 내적 긴장이 증가하게 되므로 결과적으로 광고 메시지를 회피하게 된다는 것이다. 이와 같은 맥락으로 본 연구에서는 공포 소구가 제시된 집단의 경우, 이미 공포 소구로 인해 비밀번호 유출에 대한 위협 인식이 높아진 만큼 손실 프레이밍은 심리적 반발감을 일으킬 수 있다. 따라서 이득 프레이밍이 손실 프레이밍보다 더 효과적으로 작용할 수 있다고 보고, 아래와 같은 가설을 설정하였다.

H7a : 지각된 취약성과 두려움 간에 메시지 프레이밍이 조절역할을 할 것이다.

H7b : 지각된 심각성과 두려움 간에 메시지 프레이밍이 조절역할을 할 것이다.

H7c : 두려움과 비밀번호 변경의도 간에 메시지 프레이밍이 조절역할을 할 것이다.

4. 연구방법

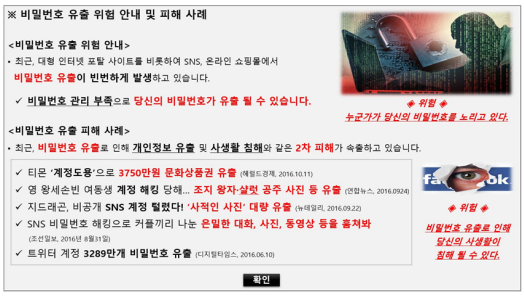
4.1 실험 설계

본 연구의 목적 중 하나는 비밀번호 변경행위에 대한 공포 소구와 메시지 프레이밍의 효과를 알아보는 것이다. 이에 2×2(공포 소구 : 없음/있음, 메시지 프레이밍 : 이득/손실) 집단 간 요인설계(Between-subject Factorial Design) 실험을 실시하였다. 총 4개 집단으로 진행하였으며, 집단 1(집단 2)에게는 공포 소구 없이 이득(손실) 프레이밍만 제시하였고, 집단 3(집단 4)에게는 공포 소구를 노출 시키고, 이득(손실) 프레이밍을 보여주었다.

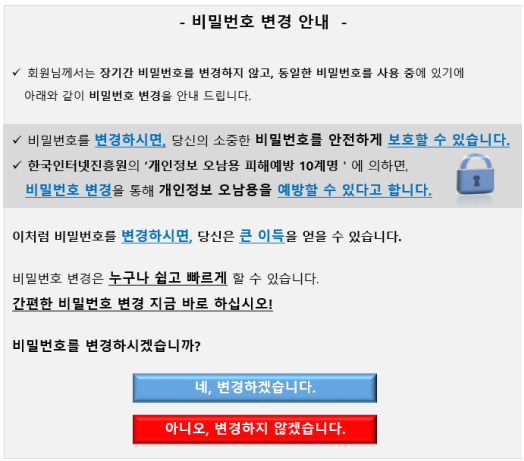
본 설문조사를 실시하기에 앞서 연세대학교 정보대학원 석/박사 과정 20명을 대상으로 파일럿 테스트를 수행하였다. 일부 의견을 수렴하여 실험 처치물과 설문문항을 수정하였다. 성실히 참여한 응답자들에 한해 추첨으로 5,000원 상당의 기프티콘을 제공하였다. 다음으로 설문조사 전문기관 엠브레인을 통해 웹사이트 로그인 경험이 있는 20대~40대를 대상으로 본 설문조사를 진행하였다. 설문지는 무작위로 배포되었으며, 집단 별로 서로 다른 시나리오를 읽고 난 후, 설문문항에 응답하였다. 이때, 별도의 보상을 제공하지 않았다. 설문 응답지 303부를 회수하였으며, 불성실 응답 및 조작 점검에 의해 일부 탈락한 응답자를 제외한 152명(집단 1 : 35명, 집단 2 : 34명, 집단 3 : 39명, 집단 4 : 44명)을 최종적으로 분석에 활용하였다.

본 연구는 처치요인(Treatment)으로 공포 소구와 메시지 프레이밍을 활용하였으며, <Figure 2>~<Figure 4>와 같이 실험 처치물(Stimulus)을 설계하였다. <Figure 2>는 공포 소구에 대한 처치물로 비밀번호 유출에 대한 취약성과 심각성을 인지하게 만들 수 있는 내용을 담았다. <Figure 3>은 이득 프레이밍에 대한 처치물로 사용자가 비밀번호를 변경했을 때, 긍정적 결과를 얻을 수 있다고 강조하였다. 반면, <Figure 4>와 같이 손실 프레이밍에는 비밀번호를 변경하지 않으면, 부정적

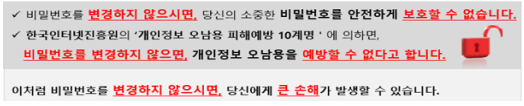
결과가 발생할 것이라는 메시지를 담았다. 다른 사항은 이득 프레이밍과 모두 동일하였다.



〈Figure 2〉 Fear Appeals Stimulus



〈Figure 3〉 Gain Framing Stimulus



〈Figure 4〉 Loss Framing Stimulus

4.2 변수의 조작적 정의

<Table 1>과 같이 기존 연구를 토대로 지각된 취약성, 지각된 심각성, 두려움, 비밀번호 변경의도에 대한 조작적 정의를 설정하였다. 각 변수에 대한 측정항목 역시 기존 문헌을 토대로 개발하였으며, 자세한 사항은 <Appendix A>에 기술하였다.

5. 연구 결과

5.1 표본의 특성

본 연구에서 사용된 표본은 <Table 2>에서 보는 바와 같이 152명으로 남성이 77명(50.7%), 여성이 75명(49.3%)이다. 대학(교) 졸업 이상이 92.8%로 대다수를 차지했으며, 직장인이 49.3%로 가장 많았다.

〈Table 2〉 Sample Characteristics

Category		N	%
Gender	Male	77	50.7
	Female	75	49.3
Age	20~29	60	39.5
	30~39	47	30.9
	40~49	45	29.6
Education	Below College	11	7.2
	College or above	141	92.8
Job	Student	33	21.7
	Employee	75	49.3
	Professional	18	11.8
	Self-employee	7	4.6
	etc.	19	12.5
Total		152	100

〈Table 1〉 Operational Definitions of Latent Variables

Variables	Operational Definitions	Sources
Perceived Vulnerability (지각된 취약성)	Internet users' belief about the degree of vulnerability to password breach	Johnston and Warkentin(2010) Witte et al.(1996)
Perceived Severity (지각된 심각성)	Internet users' belief about the significance or magnitude of potential harm caused by password breach	Johnston and Warkentin(2010) Witte et al.(1996)
Fear(두려움)	Internet users' degree of worry/fear about password breach	Boss et al.(2015)
Intention (비밀번호 변경의도)	Internet users' willingness to change passwords	Johnston and Warkentin(2010)

5.2 조작 점검(Manipulation Check)

본 연구에서는 앞에서도 기술했다시피 공포 소구와 메시지 프레이밍에 대한 실험 처치물을 제작하였다. 공포 소구 처치물에는 비밀번호 유출이 발생할 수 있으며, 그 피해가 심각하다는 내용을 담았다(<Figure 2> 참고). 따라서 실험 대상자가 공포 소구 처치물을 보고나서 비밀번호 유출에 대한 취약성과 심각성을 실제로 지각했는지에 대한 조작 점검(Manipulation Check)이 필요하다. 즉, 실험자의 의도대로 조작이 잘 이루어졌는지 검정 절차를 거쳐야 하는 것이다. 공포 소구를 보여준 집단과 보여주지 않은 집단 간에 지각된 취약성과 지각된 심각성의 차이가 통계적으로 유의한지 확인하기 위해 독립표본 t-검정을 실시하였다. 검정 결과, <Table 3> 상단에서 보는 바와 같이 공포 소구를 보여준 집단의 지각된 취약성($M_{\text{공포 소구 있음}}$ = 5.30, $M_{\text{공포 소구 없음}}$ = 4.96; t = 2.040, $p < .05$)과 지각된 심각성($M_{\text{공포 소구 있음}}$ = 5.07, $M_{\text{공포 소구 없음}}$ = 4.51; t = 3.019, $p < .01$)이 더 높게 나타났다.

공포 소구에 이어서 메시지 프레이밍 처치물에 대한 조작 점검도 실시하였다. 앞서 살펴본 바와 같이 메시지 프레이밍 처치물의 경우, 비밀번호 변경에 대한 이득을 강조한 '이득 프레이밍'과 비밀번호를 변경하지 않았을 때, 손실이 발생할 것이라는 내용에 초점을 맞춘 '손실 프레이밍'으로 제작하였다(<Figure 3>, <Figure 4> 참고). 실험 참여자가 이득 프레이밍에 대한 내용을 정말로 이득이라고 생각했는지를 측정하기 위해 "이 메시지는 비밀번호 변경을 통해 얻을 수 있는 긍정적 결과(이득)를 말하고 있다."라고 물어보았다. 그리고 손실 프레이밍에 대해서는 "이 메시지는 비밀번호를 변경하지 않았을 때, 발생되는 부정적 결과(손해)를 말하고 있다."라는 항목을 측정하였다. 공포 소구 조작 점검과 마찬가지로 독립표본 t-검정을 실시했으며, 그 결과는 <Table 3> 하단과 같다. '긍정적 결과(Gain)' 항목을 보면, 이득 프레이밍이 제시된 집단($M_{\text{이득 프레이밍}}$ = 4.27, $M_{\text{손실 프레이밍}}$ = 3.73; t = 2.313, p < .05)이 더 높게 나타났다. 반면, '부정적 결과(Loss)' 항목을 보면, 손실 프레이밍이 제시된 집단($M_{\text{손실 프레이밍}}$ = 4.56, $M_{\text{이득 프레이밍}}$ = 3.66; t = 3.693, p < .01)이 더 높게 나타났다. 즉, 이득 프레이밍이 제시된 집단은 비밀번호 변경을 통해 긍정적 결과를 얻을 수 있다고 평가한 것이며, 손실 프레이밍에 노출된 집단은 비밀번호를 변경하지 않으면, 부정적 결과가 발생할 것이라고 인식한 것이다. 따라서 메시지 프레이밍에 대한 조작 역시 성공적이라고 할 수 있다.

반면, 메시지 프레이밍에 따라 지각된 취약성($M_{\text{이득}}$ = 5.26, $M_{\text{손실}}$ = 5.04; t = 1.320, $p > .05$)과 지각된 심각성($M_{\text{이득}}$ = 4.83, $M_{\text{손실}}$ = 4.80; t =

〈Table 3〉 Manipulation Check

Treatment	Group	N	Perceived Vulnerability	Perceived Severity
Fear Appeals	No Fear Appeals	69	4.96(1.11)	4.51(1.18)
	Fear Appeals	83	5.30(.92)	5.07(1.12)
	t-value		2.040*	3.019**

Treatment	Group	N	Positive(Gain)	Negative(Loss)
Message Framing	Gain Framing	74	4.27(1.39)	3.66(1.48)
	Loss Framing	78	3.73(1.48)	4.56(1.53)
	t-value		2.313*	3.693**

*$p < .05$, **$p < .01$.
n1(n2) : The first number n1 represents mean. The second number n2 represents S.D.

.178, $p > .05$)이 유의미한 차이가 발생하지 않았다. 즉, 손실 프레이밍으로 제시된 메시지를 보았다고 비밀번호 유출의 취약성과 심각성을 더 높게 인지한 것은 아니라는 것이다. 따라서 공포 소구와 메시지 프레이밍은 개별적인 속성을 지니고 있다고 볼 수 있다.

5.3 연구 결과

본 연구가설을 검정하기 위해 SPSS 23.0을 활용하여 이원배치 분산분석(two-way ANOVA)을 실시하였으며, 추가적으로 SmartPLS 3.4를 사용하여 구조방정식모델 분석 및 다중집단분석을 수행하였다.

5.3.1 공포 소구와 메시지 프레이밍 효과

공포 소구 효과를 살펴본 결과, 공포 소구 유무에 따라 비밀번호 변경의도($F(1,148) = 14.92$, $p < .001$)가 달라졌다. 즉, 공포 소구를 본 집단의 비밀번호 변경의도가 더 높은 것으로 드러났다. 따라서 H1은 채택되었다. 반면, H2와 H3은 기각되었다. 메시지 프레이밍에 따라 변경의도가 달라지지 않았으며, 공포 소구와 메시지 프레이밍 간 상호작용 효과도 나타나지 않았다. 이에 대한 결과를 <Table 4>에 정리하였다.

〈Table 4〉 Results of Two-Way ANOVA

DV : Intention				
Source	SS	df	MS	F
Corrected Model	33.12	3	11.04	5.27**
Fear Appeals	31.23	1	31.23	**14.92*** **
Message Framing	1.61	1	1.61	.77
Fear Appeals× Message Framing	.75	1	.75	.36
Error	309.81	148	2.09	-

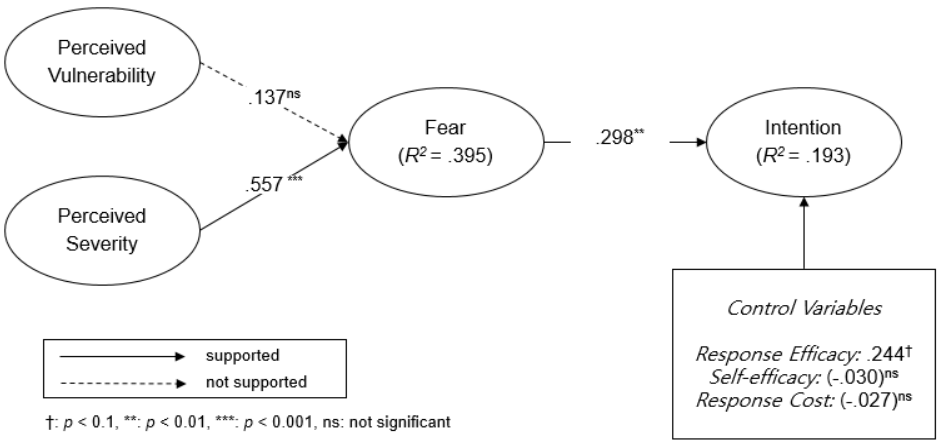
*** $p < .001$.

5.3.2 비밀번호 변경행위의 동기요인

본 연구는 공포 소구와 메시지 프레이밍의 효과 분석에 더하여 추가적으로 비밀번호 변경행위의 메커니즘까지 규명하고자 했다. 이에 공포 소구를 제시한 집단(집단 3, 4; N = 83)을 대상으로 앞서 제시한 연구모형에 대해 구조방정식모델 분석을 실시하였다.

가설 검정에 앞서 연구모형의 각 변수에 대한 신뢰성 및 타당성 검정을 수행하였다. 모두 적합한 수준으로 판명되었으며, 이에 대한 결과는 부록 B에 수록하였다.

연구모형의 경로분석 결과를 <Figure 5>에 나타냈다. 자세히 살펴보면, 지각된 심각성은 두려움($\beta = .557$, $t = 3.793$, $p < .001$)에 긍정적인 영향을 주는 것으로 나타났다. 또한, 두려움이 비밀번호



〈Figure 5〉 Results of Path Analysis(Group 3, 4; N = 83)

변경의도에 미치는 영향 역시 유의하게 나타났다 (β = .298, t = 2.272, p < .01). 이에 H5와 H6은 채택되었다. 반면, 지각된 취약성이 두려움에 유의한 영향을 미친다는 근거는 찾을 수 없었다. 따라서 H4는 기각되었다.

5.3.3 조절효과 검정

조절효과 검정을 위하여 Henseler et al.(2009)이 제안한 다중집단분석(MGA, Multi-group analysis)을 실시하였다.

분석 결과는 <Table 5>와 같다. 자세히 살펴보면, 두려움과 변경의도 간 메시지 프레이밍이 조절역할을 하는 것으로 나타났다($\beta_{\text{Gain farming}}$ = .498, $\beta_{\text{Loss farming}}$ = .118; diff. = .380, p < .05). 즉, 두려움이 변경의도에 주는 영향이 부정적 프레이밍보다 긍정적 프레이밍일 때, 더 크다고 할 수 있는 것이다. 따라서 H7c를 채택하였다. 반면, 지각된 취약성과 두려움, 지각된 심각성과 두려움 간에 메시지 프레이밍이 조절역할을 한다는 결과를 얻지 못하였다. 이에 H7a와 H7b를 기각하였다.

〈Table 5〉 Results of MGA

Path	β(GF)	β(LF)	*diff.*	p value
PV → FEAR	.069	.203	.134	.690
PS → FEAR	.602	.511	.091	.360
FEAR → INT	.498	.118	.380	**.048**

PV : Perceived Vulnerability, PS : Perceived Severity, INT : Intention, GF : Gain Framing, LF : Loss Framing.

6. 결 론

6.1 연구결과 토의

본 연구에서는 웹사이트 사용자들이 비밀번호를 변경하는데 있어서 공포 소구와 메시지 프레이밍이 효과적으로 작용하는지 살펴보았다. 즉, 비밀번호 유출에 대한 메시지가 담긴 공포 소구가 개인들의 비밀번호 변경행위에 어떠한 영향을 미치는지 알아본 것이다(공포 소구 효과). 그리고 비밀번호 변경을 권고하는 메시지를 서로 다르게 표현할 때, 즉, 비밀번호 변경에 대한 이득을 강조할 경우와 비밀번호를 변경하지 않았을 시에 발생되는 손실에 초점을 맞출 경우에 개인들의 선택과 판단이 달라지는지 확인하였다(메시지 프레이밍 효과). 또한, 비밀번호 변경행위가 어떠한 동기요인으로 이루어지는지, 즉, 메커니즘을 추가적으로 규명하였다.

실험 기반의 설문조사를 통해 수집한 데이터를 분석한 결과, 공포 소구를 보여준 집단의 비밀번호 변경의도가 더 높은 것으로 나타났다. 이는 비밀번호 변경행위에 있어서 공포 소구가 효과적으로 작용했다는 것을 의미한다. 한편, 손실 프레이밍이 제시된 집단의 비밀번호 변경의도가 더 높을 것으로 가정했으나, 이에 대한 유의한 결과를 얻지 못했다. 따라서 메시지 프레이밍은 비밀번호 변경행위에 특정 효과를 준다고 볼 수 없다. 그리고 손실 프레이밍이 제시 되었을 때, 공포 소구와 메시지 프레이밍의 상호작용으로 공포 소구 효과가 더욱 증대될 것으로 보았으나, 이 역시 통계적으로 유의한 값을 얻지 못하였다.

추가적으로 구조방정식모델 분석을 통해 비밀번호 변경행위에 대한 메커니즘을 밝혔다. 우선, 지각된 취약성이 두려움에 아무런 영향을 주지 못하는 것으로 나타났다. 기존 연구를 살펴보면, 특정 위협에 대해 취약하다고 지각할수록 그 위협을 두렵게 느낀다고 하였지만(Boss et al., 2015; Chen and Zahedi, 2016; Liang and Xue, 2010; Park, 2015), 본 연구에서는 그러한 결과가 나오지 않았다. 즉, 온라인 사용자가 비밀번호 유출의 발생 가능성을 높게 인지할지라도 이것이 두려움이라는 감정을 형성함은 아니라는 것이다. 따라서 향후 연구에서 지각된 취약성이 어떠한 심리적 반응을 통해서 비밀번호 변경의도로 이어지는지를 살펴볼 필요가 있다.

반면, 지각된 심각성은 다른 연구(Boss et al., 2015; Chen and Zahedi, 2016; Liang and Xue, 2010; Park, 2015)와 마찬가지로 두려움에 영향을 주는 것으로 나타났다. 즉, 비밀번호 유출에 대한 피

해를 심각하다고 느낄수록 비밀번호 유출을 두려워한다는 것이다. 다만, Boss et al.(2015)에서 언급한 바 있듯이, 지금까지의 연구는 두려움을 배제한 채 두 위협 요소(지각된 취약성, 지각된 심각성)와 행위의도 간에만 초점을 맞추어 진행되었다. 이처럼 지각된 취약성과 지각된 심각성을 두려움의 선행요인으로 살펴본 연구가 아직 부족한 만큼 추가적인 연구를 통해 그 관계를 자세히 규명할 필요가 있어 보인다.

그리고 이렇게 형성된 두려움은 비밀번호 변경의도에 긍정적인 영향을 미치는 것으로 나타났으며, 이는 기존 연구와 동일한 결과다(Boss et al., 2015; Chen and Zahedi, 2016; Liang and Xue, 2010; Park, 2015; Zhang and McDowell, 2009). 비밀번호 변경행위를 이끌어내기 위해서는 두려움을 자극시켜야 한다는 것인데, 이는 궁극적으로(두려움의 선행요인인) 지각된 심각성을 높여야 됨을 말한다. 따라서 비밀번호 유출 피해에 대한 심각성을 사용자들에게 각인시키는 것이 중요하다고 할 수 있다.

또한, 메시지 프레이밍에 대해 조절효과를 살펴본 결과, 두려움과 변경의도 간에 이득 프레이밍이 더 큰 영향을 주는 것으로 나타났다. 이는 공포 소구가 제시된 비밀번호 변경 상황에서는 이득 프레이밍이 손실 프레이밍보다 효과적이라고 해석할 수 있다.

6.2 연구의 시사점

본 연구가 학술적으로 기여하는 바는 다음과 같다. 기존 연구에서는 다루지 않았던 메시지 프레이밍을 활용하여 정보보안 행위, 더 정확하게는 비밀번호 변경행위를 살펴보았다는 점이다. 지금까지의 연구를 살펴보면, 정보보안 행위를 증대시키는 방안으로 공포 소구를 많이 활용해왔다(Boss et al., 2015; Johnston and Warkentin, 2010; Mwagwabi et al., 2014; Park, 2015; Vance et al., 2013; Zhang and McDowell, 2009). 그 효과가 백신 사용행위 등에서 어느 정도 입증되었지만, 실험설계 자체가 실제 환경과는 약간 동떨어진 감이 없지 않아 있었고, 비밀번호 변경행위에 초점을 맞춰 그 효과를 제대로 살펴본 연구는 없었다. 이에 본 연구에서는 실제 온라인 환경에서 접할 수 있는 '비밀번호 변경 안내문'을 바탕으로 실험설계를 하였고, 이 때, 기존과는 다른 새로운 접근 방식인, 하지만 다른 분야에서는 그 효과가 이미 입증된 메시지 프레이밍을 활용하였다. 비록 본 연구에서는 메시지 프레이밍 효과를 보지는 못했지만, 기존 방식에서 벗어난 새로운 관점으로 비밀번호 변경행위를 알아보았다는 점에서 그 의의가 있다고 할 수 있다. 향후에도 이를 활용한 연구가 이루어지기를 기대해 본다.

다음으로 실무적 시사점은 기업에서 공포 소구를 적극적으로 활용해야 한다는 것을 의미한다. 현재 웹사이트에서 제공하는 '비밀번호 변경 안내문'을 보면, 단순히 비밀번호 보호 차원에서 비밀번호를 변경하라는 내용이 대다수를 차지하고 있다. 이런 방식은 사람들의 행동을 바꾸기가 힘들고, 실제로 설문조사를 보아도 비밀번호 변경을 하는 사람이 극히 적다는 것을 알 수 있다. 따라서 기업들은 공포 소구를 바탕으로 비밀번호 변경행위를 이끌어낼 필요성이 있다. 이를 잘 적용한다면 사용자들이 비밀번호를 변경하게 될 것이고, 이에 따라 비밀번호 유출에 대한 위험이 다소 낮아질 수 있을 것으로 본다.

6.3 한계점 및 향후 연구방향

본 연구는 아래와 같은 한계점이 존재한다.

첫째, 실험설계에 있어서 일부 한계점이 존재한다고 볼 수 있다. 공포 소구와 메시지 프레이밍에 대한 실험 처치물을 만들었으나, 조작 점검을 통해 많은 설문지가 제외되었다. 이는 곧 조작이 다소 미흡하여 실험 참여자의 이해도가 떨어진 것으로 볼 수 있다. 따라서 향후에는 보다 엄밀한 설계를 바탕으로 연구가 진행되어야 한다. 특히, 메시

지 프레이밍 처치물 제작에 있어서 이득 측면을 잘 고려할 필요가 있다. 본 연구에서는 비밀번호 변경에 대한 이득으로 비밀번호를 안전하게 보호할 수 있음을 제시하였고, 조작 점검을 통해 실제로 이득이라고 인지했다는 것을 확인하였지만, 이것은 표면상에 불과할 수도 있다는 것이다. 달리 말하면, 다른 연구에서 다루었던 것, 예를 들면, 에이즈를 예방할 수 있다는 혹은 금연을 통해 건강해질 수 있다는 이득보다 그 강도가 약할 수가 있다는 것으로 이득을 체감하기 어렵다는 것을 의미한다. 따라서 비밀번호 변경을 통해 얻을 수 있는, 다시 말해, 사용자에게 실질적인 이득으로 다가올 수 있는 메시지를 고민해봐야 한다.

둘째, 공포 소구 효과를 그 유무에 대해서만 알아보았다는 점이다. 공포 소구를 활용한 다른 연구를 살펴보면, 공포 소구 제시 방식 혹은 강도에 따라 개인들의 인식, 태도 그리고 의도가 달라진다는 결과가 나타났다(Boss et al., 2015; Park, 2015). 따라서 비밀번호 변경행위에 있어서도 공포 소구 유무만 볼 것이 아니라 어떻게 제시하느냐에 따라 혹은 그 수준에 따라 사람들의 반응이 다르게 나타나는지를 알아보는 연구가 진행될 필요가 있다.

셋째, 웹사이트 유형에 따라 결과가 달라질 수 있을 것이다. 본 연구에서는 실험 참여자가 자주 방문하는 쇼핑몰 사이트라고 가정하고, 실험을 진행하였다. 하지만 웹사이트의 사용빈도 혹은 웹사이트의 특성(쇼핑몰 사이트 또는 포털사이트 등)에 따라 사용자들의 비밀번호 변경행위가 다르게 나타날 수 있다. 따라서 향후 연구에서는 이에 대해 살펴볼 필요가 있다.

마지막으로 비밀번호 변경에 대해 실제행동이 아닌 행위의도를 측정했다는 점을 들 수 있다. 의도와 행동이 일치하다는 연구가 지배적이지만, 이와 상반된 연구결과도 나오고 있는 만큼, 실제 변경여부를 측정할 필요가 있어 보인다. 따라서 다음에는 현장 실험(Field Experiment)을 통해 사용자가 실제로 비밀번호를 변경했는지에 대해 알아볼 필요가 있다.

References

Angst, C.M. and R. Agarwal, "Adoption of Electronic Health Records in the Presence of Privacy Concerns : The Elaboration Likelihood Model and Individual Persuasion", *MIS Quarterly*, Vol.33, No.2, 2009, 339-370.

Bandura, A., *Self-efficacy in Changing Societies*, Cambridge University Press, 1995.

Chen, Y. and F.M. Zahedi, "Individuals' Internet Security Perceptions and Behaviors : Polycontextual Contrasts between the United States and China", *MIS Quarterly*, Vol.40, No.1, 2016, 205-222.

Boss, S.R., D.F. Galletta, P.B. Lowry, G.D. Moody, and P. Polak, "What Do Users Have to Fear? Using Fear Appeals to Engender Threats and Fear that Motivate Protective Security Behaviors", *MIS Quarterly*, Vol.39, No.4, 2015, 837-864.

Easterling, D.V. and H. Leventhal, "Contribution of Concrete Cognition to Emotion : Neutral Symptoms as Elicitors of Worry about Cancer", *Journal of Applied Psychology,* Vol.74, No.5, 1989, 787.

Fishbein, M. and I. Ajzen, *Belief Attitude, Intention and Behavior*, Reading, MA : Addison-Wesley, 1975.

Gaeth, G.J., I.P. Levin, D.A. Cours, and S. Combs, "Framing of Attribute Information in Product Description", *Advances in Consumer Research*, Vol.17, No.2, 1990, 531-534.

Ganzach, Y. and N. Karsahi, "Message Framing and Buying Behavior : A Field Experiment", *Journal of Business Research*, Vol.32, No.1, 1995, 11-17.

Gefen, D., D. Straub, and M. Boudreau, "Structural Equation Modeling and Regression :

Guidelines for Research Practice", *Communications of the Association for Information Systems*, Vol.4, No.7, 2000, 1-77.

Ha, S.W. and H.J. Kim, "The Effects of User's Security Awareness on Password Security Behavior", *Digital Contents Society*, Vol.14, No.2, 2013, 179-189.

(하상원, 김형중, "정보보안의식이 패스워드 보안행동에 미치는 영향에 관한 연구", *한국디지털콘텐츠학회논문지*, 제14권, 제2호, 2013, 179-189.)

Hanus, B. and Y.A. Wu, "Impact of Users Security Awareness on Desktop Security Behavior : A Protection Motivation Theory Perspective", *Information Systems Management*, Vol.33, No.1, 2016, 2-16.

Henseler, J., C.M. Ringle, and R.R. Sinkovics, "The Use of Partial Least Squares Path Modeling in International Marketing", *In New Challenges to International Marketing*, Emerald Group Publishing Limited, 2009, 277-319.

Homer, P.M. and S.G. Yoon, "Message Framing and the Interrelationships among Ad-based Feelings, Affect, and Cognition", *Journal of Advertising*, Vol.21, No.1, 1992, 19-33.

Jeon, J.O., Q. Le, and H.H. Park, "The Influence of Scarcity Message Type and Message Framing on Impulse Buying Effect in Online Pice Discount Advertising : Focusing on the Moderating Effect of Need for Cognitive Closure", *The Korean Journal of Consumer and Advertising Psychology*, Vol.14, No.4, 2013, 549-574.

(전중옥, 이 금, 박현희, "희소성 메시지 유형과 메시지 프레이밍에 따른 온라인 광고의 충동구매 효과", *한국심리학회지 : 소비자 · 광고*, 제14권, 제4호, 2013, 549-574.)

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

KISA, "A Survey on the Use of Digital Signatures by the Public in 2015", 2015.

(한국인터넷진흥원, "2015년 대국민 전자서명 이용실태 조사", 2015.)

Kurila, J., L. Lazuras, and P.H. Ketikidis, "Message Framing and Acceptance of Branchless Banking Technology", *Electronic Commerce Research and Applications*, Vol.17, 2016, 12-18.

Lee, J.R., "A Study on the Effect of Persuasion on Attitude and Framing", *Korean Journal of Social Science*, Vol.28, No.2, 2006, 125-144.

(이재록, "태도와 프레이밍 및 설득과의 관계에 관한 연구", *한국사회과학연구*, 제28권, 제2호, 2006, 125-144.)

Lee, Y., "Understanding Anti-plagiarism Software Adoption : An Extended Protection Motivation Theory Perspective", *Decision Support Systems*, Vol.50, No.2, 2011, 361-369.

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

Maddux, J.E. and R.W. Rogers, "Protection Motivation and Self-efficacy : A Revised Theory of Fear Appeals and Attitude Change", *Journal of Experimental Social Psychology*, Vol. 19, No.5, 1983, 469-479.

Meyerowitz, B.E. and S. Chaiken, "The Effect of Message Framing on Breast Self-examination Attitudes, Intentions, and Behavior", *Journal of Personality and Social Psycho-*

logy, Vol.52, No.3, 1987, 500-510.

Mwagwabi, F., T. McGill, and M. Dixon, "Improving Compliance with Password Guidelines : How User Perceptions of Passwords and Security Threats Affect Compliance with Guidelines", *System Sciences(HICSS), 2014 47th Hawaii International Conference on,* 2014.

Ortony, A. and T.J. Turner, "What's Basic about Basic Emotions?", *Psychological Review*, Vol.97, No.3, 1990, 315-331.

Park, J.P., "Users' Security Protection Through Fear Appeal : A Behavioral Economics Approach", Ph.D Thesis, Yonsei University, South Korea, 2015.

(박종필, "공포소구를 통한 온라인 사용자들의 보안 강화 : 행동경제학적 접근으로", 박사학위논문, 연세대학교, 2015.)

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

Rogers, R.W., "Cognitive and Physiological Processes in Fear Appeals and Attitude Change : A Revised Theory of Protection Motivation", *Social Psychophysiology*, 1983, 153-176.

Shropshire, J.D., M. Warkentin, and A.C. Johnston, "Impact of Negative Message Framing on Security Adoption", *Journal of Computer Information Systems*, Vol.51, No.1, 2010, 41-51.

Tsai, H.Y.S., M. Jiang, S. Alhabash, R. LaRose, N.J. Rifon, and S.R. Cotten, "Understanding Online Safety Behaviors : A Protection Motivation Theory Perspective", *Computers and Security*, Vol.59, 2016, 138-150.

Vance, A., D. Eargle, K. Ouimet, and D. Straub, "Enhancing Password Security Through Interactive Fear Appeals : A Web-based Field Experiment", *2013 46th Hawaii International Conference on System Sciences,* 2988-2997.

Witte, K., "Predicting Risk Behaviors : Development and Validation of a Diagnostic Scale", *Journal of Health Communication*, Vol.1, 1996, 317-341.

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

Witte, K., G. Meyer, and D. Martell, "Effective Health Risk Messages : A Step-by-Step Guide", *Sage Publications*, 2001.

Woon, I., G.W. Tan, and R. Low, "A Protection Motivation Theory Approach to Home Wireless Security", *International Conference on Information on Systems*, 2005, 367-390.

Workman, M., W.H. Bommer, and D. Straub, "The Amplification Effects of Procedural Justice on a Threat Control Model of Information Systems Security Behaviours", *Behaviour and Information Technology*, Vol.28, No.6, 2009, 563-575.

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

〈Appendix A〉 Measurement Items

Variables	Operational Definitions	Measurement Instruments	Sources
Perceived Vulnerability (지각된 취약성)	웹사이트 이용 시, 비밀번호가 유출 될 가능성의 정도	1) 비밀번호가 유출 될 수 있을 것이다. 2) 비밀번호 유출이 발생할 수 있을 것 같다. 3) 나는 비밀번호 위험이 존재한다고 생각한다.	Johnston and Warkentin (2010) Witte et al. (1996)
Perceived Severity (지각된 심각성)	웹사이트 이용 시, 비밀번호가 유출되어 피해를 입을 수 있는 유해성의 크기	1) 만약 비밀번호가 유출된다면, 그것은 나에게 심각한 문제를 초래할 것이다. 2) 만약 비밀번호가 유출된다면, 그것은 나에게 치명적일 것이다. 3) 만약 비밀번호가 유출된다면, 그것은 나에게 큰일이다.	Johnston and Warkentin (2010) Witte et al. (1996)
Fear (두려움)	웹사이트 이용 시, 비밀번호 유출에 대한 두려움의 정도	1) 나는 내 비밀번호가 유출되는 것이 두렵다. 2) 나는 내 비밀번호가 유출되는 것이 무섭다. 3) 나는 내 비밀번호가 유출되는 것이 끔찍하다.	Boss et al. (2015)
Response Efficacy (반응 효능감)	웹사이트 이용시, 비밀번호 유출로부터 비밀번호 변경이 얼마나 효과적인지의 정도	1) 만약 비밀번호를 변경한다면, 내 비밀번호를 보다 안전하게 보호할 수 있을 것이다. 2) 만약 비밀번호를 변경한다면, 내 계정을 보다 잘 보호할 수 있을 것이다. 3) 비밀번호 변경을 통해 비밀번호를 좀 더 효과적으로 보호할 수 있을 것이다.	Johnston and Warkentin (2010); Maddux and Rogers (1983); Witte et al. (1996); Zhang and McDowell (2009)
Self Efficacy (자기 효능감)	웹사이트에서 비밀번호 변경을 할 수 있는 자신의 능력에 대한 믿음의 정도	1) 비밀번호 변경하는 것은 나에게 쉬운 일이다. 2) 비밀번호를 변경하는 것은 나에게 간단한 일이다. 3) 나는 비밀번호를 변경하는 방법에 대해서 잘 알고 있다.*	Johnston and Warkentin (2010); Witte et al. (1996)
Response Cost (반응 비용)	웹사이트에서 비밀번호를 변경하기 위해 발생되는 손해 혹은 노력의 정도	1) 비밀번호 변경은 귀찮은 일이다. 2) 비밀번호를 자주 변경하면, 비밀번호를 기억하기 어려워진다. 3) 비밀번호를 변경하는 것은 번거롭다.	Woon et al. (2005); Zhang and McDowell (2009)
Intention (비밀번호 변경의도)	웹사이트에서 비밀번호를 변경하고자 하는 의지의 정도	1) 나는 비밀번호를 변경할 것이다. 2) 나는 비밀번호를 변경하겠다. 3) 나는 지금 비밀번호를 바꿀 것이다.	Johnston and Warkentin (2010)

주) 1. 리커트 7점 척도(1. 전혀 그렇지 않다~7. 매우 그렇다).
2. *탐색적 요인 분석 후, 요인 적재량 0.6 미만으로 제외됨.

〈Appendix B〉 Measurement Analysis

우리는 본 연구에서 비밀번호 변경행위의 메커니즘을 규명하였는데, 이에 대한 측정항목의 신뢰성 및 타당성 검정 결과는 아래와 같다.

1. 탐색적 요인 분석 결과

Construct	Item	Component						
		1	2	3	4	5	6	7
두려움	FEAR1	**.905**	.023	.158	.208	.056	.151	.029
	FEAR2	**.898**	.040	.246	.258	-.001	.114	.109
	FEAR3	**.847**	.173	.230	.309	-.033	.012	.075
반응 효능감	RE1	.081	**.902**	.190	.041	-.116	.096	.113
	RE2	.043	**.929**	.174	.073	-.027	.073	.141
	RE3	.069	**.857**	.238	.073	-.074	.095	.137
변경의도	INT1	.217	.197	**.851**	.257	-.110	.060	.162
	INT2	.250	.271	**.877**	.190	-.051	.080	.124
	INT3	.219	.284	**.874**	.178	-.028	.105	.104
지각된 심각성	PS1	.212	.099	.183	**.801**	.014	.327	.006
	PS2	.280	.129	.262	**.850**	.004	.163	-.005
	PS3	.379	-.007	.181	**.811**	.011	.166	.120
반응 비용	RC1	-.180	-.048	-.004	.036	**.905**	-.020	-.051
	RC2	.114	.009	-.116	.003	**.855**	.221	-.045
	RC3	.095	-.170	-.028	-.021	**.865**	.150	-.132
지각된 취약성	PV1	.085	.092	.116	.171	.019	**.925**	-.083
	PV2	.140	.197	.104	.151	.179	**.874**	.010
	PV3	.043	-.021	-.023	.275	.260	**.714**	.305
자기 효능감	SE1	.074	.218	.148	.049	-.105	.040	**.926**
	SE2	.092	.148	.142	.029	-.122	.048	**.947**
초기 고유값		7.152	3.417	2.252	1.564	1.475	1.107	.883
분산 (%)		14.386	14.054	13.676	12.523	12.324	12.227	10.060
누적 (%)		14.386	28.440	42.115	54.639	66.962	79.189	89.250

주) 1. 요인추출방법 : 주성분 분석.
2. 회전방법 : Kaiser 정규화가 있는 직교회전(Varimax) 방식.
3. SE3의 경우, 요인 적재량 0.6 이하로 삭제함.

2. 확인적 요인 분석 결과

Construct	Item	Std. Loading	AVE	CR	Cronbach's α
두려움	FEAR1	.961	.921	.972	.957
	FEAR2	.971			
	FEAR3	.947			
변경의도	INT1	.959	.941	.979	.969
	INT2	.983			
	INT3	.967			
지각된 심각성	PS1	.875	.870	.952	.925
	PS2	.963			
	PS3	.957			
지각된 취약성	PV1	.912	.829	.935	.896
	PV2	.942			
	PV3	.875			
반응 비용	RC1	.949	.755	.902	.857
	RC2	.797			
	RC3	.854			
반응 효능감	RE1	.966	.919	.972	.956
	RE2	.965			
	RE3	.945			
자기 효능감	SE1	.986	.965	.982	.964
	SE2	.979			

3. 기술통계량과 상관분석

Construct	Mean	S.D	FEAR	INT	PS	PV	RC	RE	SE
FEAR	5.05	1.15	**.960**						
INT	3.61	1.60	.356	**.970**					
PS	5.07	1.12	.594	.403	**.933**				
PV	5.30	0.92	.342	.236	.361	**.910**			
RC	5.72	0.96	.222	.086	.155	.290	**.869**		
RE	4.68	1.10	.272	.304	.264	.271	.152	**.959**	
SE	4.70	1.37	.231	.136	.077	.267	-.007	.414	**.983**

주) 1. 대각행렬에 있는 굵게 표시한 값들은 AVE 제곱근임.
2. FEAR : 두려움, INT : 변경의도, PS : 지각된 심각성, PV : 지각된 취약성, RC : 반응 비용, RE : 반응 효능감, SE : 자기 효능감.
3. FEAR와 PS간 상관계수가 .594로 다중공선성이 의심되어 VIF 분석한 결과, 그 값이 1.150으로 다중공선성 문제는 없는 것으로 확인하였음.

About the Authors

Jaeyoung Park (inyourface33@gmail.com)

Jaeyoung Park is currently a Ph.D candidate in the Graduate School of Information at Yonsei University. His current research interests include Economics of Information Systems, Information Security Policy, IT value, Privacy and etc.

Jeondo Kim (zzang20044@naver.com)

Jeondo Kim is currently a M.S. candidate in the Graduate School of Information at Yonsei University. His current research interests include Privacy, Cyberbulling, IoT security, Bigdata analytics and etc.

Beomsoo Kim (beomsoo@yonsei.ac.kr)

Beomsoo Kim is currently a Professor at the Graduate School of Information, and the Executive Director, Barun ICT Research Center, Yonsei University, Korea. He also serves as a Vice-Chair, Working Party on Security and Privacy in the Digital Economy (SPDE), at OECD. He received his Ph.D. in Information Systems from the University of Texas at Austin. His current research interests include privacy laws and policies, information security and privacy best practices, security and privacy management in cloud computing and IoT services, IT values and ethics, knowledge management, and economic issues in IT industry.