연구논문 정보화정책 제25권 제1호, 2018년 봄호, pp. 99–114

보안교육 및 보안서비스가 조직구성원의 정보보안정책 준수에 미치는 영향*

김 보 라**, 이 종 원***, 김 범 수****

요 약

조직의 정보보안은 물리적, 기술적, 관리적 영역에서 균형적으로 이뤄져야 한다. 그러나 과거 기업의 정보보안 대책은 주로 물리적, 기술적 영역에 집중되는 경향이 있었다. 최근 조직구성원에 의한 보안사고가 늘어남에 따라 기업에서도 인적 보안 관리나 정보보안 교육에 관심이 점차 높아지는 추세이다. 본 연구는 현장실험을 통해 보안교육이나 보안서비스 제공이 조직구성원의 보안정책 준수 행동에 어떤 영향을 미치는지 알아보았다. 연구 1에서 국내 대기업 임직원을 대상으로 스팸 이메일 대응교육을 실시한 후 교육 효과를 알아보기 위해 스팸 이메일 열람 여부를 측정했고, 3개월이 지난 후에도 효과가 지속되는지 알아보았다. 연구 2에서는 보안서비스의 효과를 알아보기 위해 보안경고 알림 메시지를 제공한 후 그 효과를 측정하였다. 실험 결과, 보안교육은 보안정책 준수 행동에 긍정적인 영향을 미치는 것으로 나타났다. 보안교육 직후 교육 이수집단이 미이수집단에 비해 스팸 이메일 열람률이 낮았다. 그러나 3개월 후 이러한 집단 간 차이는 사라졌다. 또한 보안위험 경고 알림 메시지는 스팸 이메일을 열람률을 낮추는 데 효과가 큰 것으로 나타나 보안정책 준수 행동에 긍정적인 영향을 미쳤다. 이 결과는 조직의 인적보안 관리를 위해서는 지속적인 보안교육이 필요하고, 보완적으로 보안서비스를 활용할 필요가 있음을 시사한다.

주제어: 정보보안, 보안교육, 보안서비스, 보안정책준수, 현장실험, 스팸 이메일

Effect of Information Security Training and Services on Employees' Compliance to Security Policies

Kim, Bo-ra, Lee, Jong-Won, Kim, Beom-Soo

Abstract

In the past, organizations tended to focus on physical and technical aspects of managing corporate's information security (IS), rather than the aspect of human resources related to IS. Recently, increasing security incidents caused by organization members raise the issue of how to improve employees' compliance with security policies. This study conducted a field experiment to examine the effect of security awareness training and technical security services on employee's security behaviors. In Study 1, the number of spam opening cases were measured right after the IS training and re-measured three months later. In Study 2, a spam warning message was provided and then the number of employees' spam opening cases were counted to find out the effect of security services. It was found that both the IS training and the technical IS service were effective; they significantly decreased spam opening rates. However, the training effect did not last longer than three months. These findings suggest that organizations need to consider providing regular training programs and supplementary technical services to improve employees' compliance with security policies.

Keywords: information security, security awareness training, technical security service, security policy compliance, field experiment, spam

2018년 2월 6일 접수, 2018년 2월 8일 심사, 2018년 2월 23일 게재확정

* 본 논문은 (사내 보안교육 및 보안서비스가 구성원의 기업 보안정책 준수에 미치는 영향, 2014 이종원)의 데이터를 활용하여 재분석한 것임

** 바른 ICT연구소 연구교수(bora.kim@barunict.kr)

*** GS 칼텍스 팀장(jwl@gscaltex.com)

**** 교신저자, 연세대학교 정보대학원 교수(beomsoo@yonsei.ac.kr)

Ⅰ. 연구 배경

조직의 정보보안 유형은 여러 학자들에 의해 다양한 분류가 시도되어 왔으며(Da Veiga & Eloff, 2007) 일반적으로는 기술적, 물리적, 관리적 유형으로 나눌 수 있다(김상훈·이갑수, 2015). 물리적 혹은 기술적 보안영역에서는 출입관리, 방화벽 설치, 백신프로그램 사용, 저장매체 차단, 특정 웹사이트 및 메신저의 차단 등 주로 시스템 통제를 통하여 조직구성원의 의도적인 행동을 제어하거나 기술적 방어체계를 구축한다. 반면 관리적 보안영역에서는 이러한 물리적, 기술적 통제로는 한계가 있는, 개인에 의해 발생하는 보안 사고를 방지하기 위해 보안정책을 수립하거나 보안교육을 실시하는 등의 노력을 통해 조직의 인적자원을 관리한다. 정보보안을 위한 기업의 노력은 이미 1960년대부터 시작되었으며 주로 물리적 설비 투자나 보안기술 개발에 집중되었고, 1990년대 들어서야 인적 보안에 대한 관심이 생기기 시작했다(Trček, et al., 2007). 최근 빅데이터 관련한 보안 분야의 연구 역시 기술 연구 중심으로 진행되고 있는 상황이다(박서기 · 황경태, 2016). 기술 중심의 보안이 주를 이루는 현상에 대하여 Dhillon & Backhouse(2000)는 이 방법이 가장 효과적이라서 그렇다기보다 다른 방법에 비해 통제가 상대적으로 용이하기 때문이라고 보았으며, 근본적으로는 시스템을 사용하는 '사람'이 중요하다고 강조하였다. 최근 들어 조직구성원에 의한 보안 사고가 늘어나며, 외부의 보안위협 뿐만 아니라 내부의 보안위협도 주목을 받기 시작했고, 관리적 정보보안에 대한 관심도 함께 높아지고 있다. 사실 조직구성원은 정보보호 분야에서 오랫동안 가장 취약한 고리(Weakest Link)로 간주되어 왔다(Mitnick & Simon, 2002; Warkentin & Willison, 2009).

조직구성원의 보안위반 행위는 사적인 목적을 위해 의도적으로 기업의 기밀정보를 유출하는 경우와 일상적인 업무 수행 중 의도치 않게 보안 사고를 일으키는 경우(예: 저장매체나 이메일 등을 통하여 바이러스 또는 악성코드에 감염)로 나뉠 수 있다. 국가정보원 산업기밀보호센터에 따르면 2009년부터 2014년까지 적발된 총 253건의 해외 기술유출 사건의 피의자 중 전직, 현직 직원의 비율이 79%를 넘는 것으로 나타났다(머니투데이, 14/11/24). 관계자에 의해 발생한 기술유출과 같은 보안 사건들은 의도적 보안위반 행위라 볼 수 있다. 의도적 보안위반은 개인이 목적과 의지를 가지고 저지르는 것이므로 조직 수준에서 일괄적으로 통제 및 관리하기가 쉽지 않다. 이와 달리 후자의 경우는 조직구성원이 부당한 이득을 취하기 위해 의도를 가지고 저지른 위반 행위가 아닌 경우가 많아 조직의 입장에서는 보안인식교육 등을 통해 상황을 개선할 수 있는 여지가 있다. 따라서 조직의 인적자원 관리의 측면에서 조직구성원의 보안의식 강화 등 정보보안과 관련된 교육 및 훈련이 실무적으로 중요해진다.

그러나 2015년도 국내 정보보호산업 실태조사(한국인터넷진흥원, 2015)에 따르면 정보보안 관련 기업 중 교육/훈련 서비스를 제품으로 제공하는 업체는 전체의 0.6%에 불과하고, 교육 훈련 서비스 매출은 전체의 0.4%밖에 되지 않는 것으로 나타났다. 직종별 인력 현황을 보아도 일본의 경우 전체 정보보안 산업 인력의 7.5%가 정보보안 교육에 관여하고 있으나, 한국은 0.2% 정도만 교육에 종사하고 있는 것으로 조사되었다. 즉, 현재로서는 한국 기업에서 직원을 대상으로 한 보안 교육 및 훈련에 집중하고 있다고 보기 어려운 상황이다. 그럼에도 불구하고 향후 정보보안 서비스 사업에서 교육훈련 분야의 매출은 크게 늘어날 것으로 예측된다. 일각에서는 2020년까지 매출이 약 30.98% 증가할 것이라는 전망도 있어(한국인터넷진흥원, 2015), 정보보안 교육의 필요성에 대한 공감대는 점차 높아질 것으로 예상된다.

정보보안과 관련하여 조직 내 인력관리의 중요성이 점차 높아지면서 조직구성원의 보안정책 준수에 대한 연구들도 늘어나고 있는데, 많은 연구들이 보안정책을 따르거나 위반하는 '행동' 자체보다는 보안정책에 대한 '태도'나 보안정책 준수 '의도'를 다룬다는 한

계가 계속 지적되어 왔다(Straub, 1990; Workman & Gathegi, 2007). 그러나 행동 의도와 행동이 반드시 일치하는 것은 아닌 만큼(Sheeran, 2002) 실제 조직 환경에서 보안교육이 조직구성원의 정보보호 정책 준수 행동에 어떤 영향을 미치는지 알아보는 실증 연구가 요구된다.

본 연구는 실제 조직구성원의 보안정책준수 행위에 초점을 맞춰 실험연구를 진행하였다. 현장실험을 통해 보안교육이 조직구성원의 보안 행동에 어떠한 영향을 미치는지, 교육의 효과는 얼마나 지속되는지, 보안서비스를 제공하는 것이 보안정책준수 행동 향상에 도움이 되는지를 실증적으로 검증하였다.

Ⅱ. 연구 주제

1. 정보보안 정책과 보안교육

정보보안 정책이란 조직의 정보와 기술 자원을 보호하기 위한 조직원의 역할과 책임에 대한 요구사항들을 명시해 놓은 것이다(Bulgurcu, et al., 2010). 기업의 입장에서 물리적/기술적 정보보안도 물론 중요하지만 관리적 정보보안 차원에서 보았을 때 보안 활동을 직접 행하는 주체인 조직구성원에게 초점을 맞추어 정보보안 정책 준수가 제대로 이루어지도록 하는 것 역시 중요하다(김상훈·박선영, 2011). 따라서 기업의 정보보안 정책은 우선 조직구성원들이 쉽게 이해할 수 있어야 하고 정책을 이행하는데 혼선이 없도록 행동지침이 구체적이고 명확해야 한다(김종기·강다연, 2008; 임명성, 2012). 또한 기업이 수립한 정보보안 정책이 효과를 보기 위해서는 지속적인 정보보안 인식교육이 요구된다(박철주·임명성, 2012).

보안교육이란 조직의 정보 자원에 대한 인식과 그에 대한 책임 의식을 높이고 정보자원을 이용하는 데 필요한 기술을 제공하는 데 목적을 둔 활동이다(Fornell & Larcker, 1989). 교육을 통해 정책 미준수 행동을 억제하기 위한 노력은 정보보호 정책 분야에서 오래 전부터 시행되어 왔다. Desman(2002)은 정보보호 정책 준수를 위한 효과적인 방법으로 사용자의 보안 행동 개선을 위한 4단계 인식 프로그램을 제안하였는데 먼저 현재의 상황을 파악하고 문서, 절차, 프로세스, 교육내용과 같은 프로그램을 개발하여야 한다고 하였다. 다음으로는 조직의 정보보안 의식 수준을 높이고 직원들이 정보보안 프로토콜을 따르도록 소통이 이뤄져야 하며, 마지막으로 교육 인식 프로그램의 평가 및 업데이트가 필요하다고 하였다.

정보보안 교육 효과의 지속성에 대해 다룬 연구는 많지 않다. 보안교육을 정기적으로 지속적으로 시행해야 교육 효과가 지속된다는 연구는 있었으나(박철주·임명성, 2012) 정보보안 분야에서 일회성 교육이 단기적으로 얼마 동안 지속되는지에 대해 초점을 맞춘 연구는 찾아보기 어렵다. 참고로 심폐소생술 교육 연구 결과들을 살펴보면 교육 후 1~2개월 간 효과가 지속되다가 3~4개월 후에는 효과가 감소하는 것으로 나타난다(김수홍 외, 2007; 채명정 외, 2015). 정보보안 교육에 있어서도 교육 효과의 감소, 즉 보안정책 준수 행동의 감소가 교육 후 얼마 뒤에 발생하는지 확인한다면 재교육 시점 및 교육 횟수 등 보안교육 시행에 관한 정책 수립에 도움이 될 것이다. 따라서 보안교육의 단기적 효과에 관한 연구 뿐 아니라 교육의 지속성에 관한 연구도 함께 이뤄질 필요가 있다.

2. 보안서비스

보안과 관련된 기술지원 서비스는 기술적 보안영역에서 주로 다루었기 때문에 인적보안 관리의 차원과 연계해 진행된 연구는 거의 없으며 대부분의 연구들이 해킹이나 보안침입 공격에 대해 효과적으로 대응하는 시스템 개발 및 보안에 집중하고 있다(김기영 외, 2001; 박수진 외, 2002). 또한 보안교육에 관한 연구 역시 대부분 교육이 정보보안 정책 준수 의도 및 행동에 어떤 영향을 미치는지 다루고 있을 뿐(박철주·임명성, 2012; Straub, 1990; Workman &

Gathegi, 2007) 기술적 지원을 통한 시너지 효과나 교육 효과 향상의 측면에서 살펴본 연구는 거의 없다. 임명성(2014)에 따르면, 보안교육이 직접적으로 정보보안 위반 행위를 억제한다기보다 조직구성원이 교육을 통해 정보보안 위반 행위에 대한 심각성을 인지했을 때 위반 행위 가능성이 낮아진다. 또한 Straub & Welke(1998)는 조직에서 보안교육을 실시하면 이는 조직구성원에게 조직이 보안위반 행위에 대해 얼마나 심각하게 여기는지 암묵적으로 메시지를 전달하는 것과 같다고 말했다. 따라서 보안교육과 함께 정보보안 위반 가능성에 대한 사전 경고 및 알림 서비스를 제공한다면 정보보안 정책에 관해 교육을 이수한 후 교육 효과를 오래 지속시키고 보안위반 행동에 대한 심각성을 지속적으로 일깨울 수 있을 것이다.

3. 스팸 이메일

정보보안 정책은 고의나 악의를 가지고 벌어지는 정보보안 위반사고에 대처하기 위한 것이라기보다는 의도치 않게 생길 수 있는 보안 사고에 대비하기 위한 지침이라고 볼 수 있다. 가장 흔한 예로 조직구성원이 일상 업무에서 이메일이나 이동저장매체 등을 부주의하게 사용하다 바이러스 또는 악성코드에 감염되는 경우가 있다. 김종기·전진환(2006)에 따르면 바이러스와 관련된 사용자의 보안태도는 위험인식, 사용자의 개인특성, 보안정책에 영향을 받는다. 조직구성원의 개인특성은 조직 수준에서 통제가 어려운 요인이나 정보보안 교육을 통하여 개인의 위험인식 수준을 높이고 조직의 보안정책에 따르려는 의지는 높일 수 있다.

본 연구에서는 실험 상황의 통제 수준을 높이기 위해 기업의 사내 이메일 시스템 사용에 대한 영역으로 연구 범위를 한정하였고, 이와 관련된 보안교육을 진행하고, 기업 차원의 보안정책은 '발신처가 불분명하거나 스팸 또는 바이러스, 악성 이메일로 의심되는 경우는 열람하지 않고 즉시 삭제'하는 것이었다.

과거에 스팸 이메일은 단순히 광고를 위하여 불특정 다수를 대상으로 무작위로 발송하는 형태가 일반적이었다. 그러나 영리목적의 광고성 정보를 전달하지 않더라도 수신자가 원치 않는 모든 유형의 이메일을 스팸 이메일로 봐야한다는 주장도 있다(권영관·염흥열, 2007). 또 과거에는 보안 취약점을 이용해 정보를 빼내기 위한 기술 중심의 해킹이 주를 이루었다면 최근에는 인간 심리를 이용한 사회공학적 기법을 이용한 스팸 이메일이 늘어나고 있다(최양서·서동일, 2006). 즉, 이벤트 당첨 등 수신자가 관심을 가질 법한 콘텐츠로 이메일 열람을 유도하거나 기관의 관리자를 사칭해 안전한 이메일로 착각하게 함으로써 사전 지식이 없는 수신자가 쉽게 공격에 노출될 수 있는 것이다. 예를 들어, 2011년 국내 포털 보안담당자로 위장한 발신자로부터 '북한의 네트워크 바이러스 공격으로 피해를 받을 수 있으니 이메일에 링크된 파일을 내려 받아 설치하여 피해를 예방하라'는 내용의 악성코드를 포함한 이메일이 유포된 적이 있는데, 당시 북한의 대남선전 매체인 '우리 민족끼리' 홈페이지 해킹사건이 발생한 직후였기 때문에 이는 사회적 이슈를 악용한 전형적인 사회공학적 스팸 이메일 공격이었다고 볼 수 있다(AhnLab, 2011).

따라서 사회공학적으로 정교하게 설계된 스팸 이메일은 단순히 이메일 차단이나 백신프로그램 설치 등의 물리적, 기술적 보안만으로 대응하기에는 한계가 있다. 반드시 조직구성원 스스로의 대응이 필요한데 이는 단순히 보안 정책을 수립하는 것만으로 해결되지는 않는다. 조직구성원이 보안 정책의 목적 및 규정 사항에 대해 명확히 이해하고 정책의 방향에 맞게 이를 준수하는 행동을 이행해야지만 진정한 의미의 보안 정책 수립 목적이 달성되는 것이라 할 수 있다. 이러한 노력의 일환으로 대부분의 기업에서는 보안교육을 실시하고, 보완적으로 정책준수를 위한 기술적인 지원서비스를 제공하기도 한다. 이러한 보안서비스는 교육 효과의 지속성을 높일 수 있고 일부 조직구성원이 교육을 통해 일정한 인식 수준에 도달하지 못한다 할지라도 보완적인 기술적 지원을 통해 이들로부터 보안정

책 준수 행동을 유도할 수 있다. 본 연구는 조직에서 자체적으로 사용하는 사내 이메일 시스템 환경을 이용해 스팸 이메일에 대한 실험연구를 진행하였고, 관련 보안정책과 교육 및 서비스에 대하여 아래와 같이 정의하였다.

보안 정책: 발신처가 불분명하거나 스팸 또는 바이러스 등을 포함한 악성 이메일로 의심되는 경우는 열람하지 않고 즉시 삭제

보안 교육: 보안 의식 함양을 위한 교육으로 이메일을 통한 해킹, 바이러스 감염 사례를 공유하고 조직의 보안정책 내용을 교육

보안 서비스: 보안 기술 지원 서비스로 기존에 수신 기록이 없는 발신자로부터 온 이메일에 대하여 열람 시도 시 보안경고 알림 서비스 제공

4. 연구 문제

앞서 기술한 연구 배경 및 선행 연구 결과들을 기반으로 도출한 연구문제들은 다음과 같다. 첫째, 보안교육의 우선 목표는 조직의 정보보안 정책에 대한 내용을 인식하도록 하는 것이고, 정책에 대한 이해가 선행되어야 개별 사례에 대해 정책 준수/미준수 행동의 기준이 명확해질 수 있다(임명성, 2012). 따라서 보안교육이 효과적으로 이뤄지면 보안정책 준수 행동에 긍정적인 영향을 미칠 것이라 예상할 수 있다. 구체적으로 본 연구에서는 조직구성원을 대상으로 스팸 이메일에 대한 대응 교육을 실시하고 교육의 단기적 효과성을 알아보기 위해 교육을 이수한 집단과 미이수한 집단의 스팸 이메일 열람률의 차이를 알아볼 것이다. 보안정책을 준수하는 행동은 스팸을 가장해 발송한 이메일을 열어보지 않는 것, 반대로 보안정책 미준수 행동은 스팸 이메일을 열람하는 것으로 정의할 수 있다. 또한 스팸 이메일을 열어본 후 이메일 안의 링크를 클릭하는지, 첨부된 파일을 열어보는지 여부도 함께 알아볼 것이다.

연구문제 1: 스팸 이메일에 대한 보안교육은 조직구성원의 스팸 이메일에 대한 보안정책 준수 행동에 영향을 미치는가?

둘째, 조직이나 기관에서 교육을 실시할 때 또 다른 이슈는 교육의 효과가 얼마나 지속될 것인가이다. 교육 효과의 지속성에 따라 얼마나 자주 정기적으로 교육을 실시해야 하는지에 대한 구체적인 방침이 결정될 수 있다. 본 연구에서는 일회성 단기 교육 효과의 지속 기간을 확인하기 위해 보안교육 후 3개월이 지난 시점에서 다시 한 번 교육 이수 집단과 미이수 집단을 비교할 것이다. 만약 교육 효과의 지속성이 길지 않다면 3개월 후 스팸 이메일 열람률은 교육 이전과 크게 다르지 않을 것으로 예상된다.

연구문제 2: 스팸 이메일에 대한 보안교육은 조직구성원의 스팸 이메일에 대한 보안정책 준수에 지속적으로 영향을 미치는가?

마지막으로 기술지원 보안서비스가 보안정책 준수 행동에 효과가 있는지 알아보기 위해 과거 수신 기록이 없는 미지의 발신자로부터 이메일이 발송되면 경고 알림창이 뜨는 서비스를 제공하고, 이 서비스를 제공한 집단과 미제공한 집단 간 스팸 이메일 열람률의 차이를 알아본다. 마찬가지로 스팸 이메일을 열어본 후 안의 링크를 클릭하는지, 첨부된 파일을 열어보는지 여부도 함께 알아볼 것이다. 만약 보안서비스 제공이 효과가 있다면 보안정책 준수 행동에 긍정적인 영향을 미쳐 스팸 이메일 열람률이 낮아질 것으로 예상된다.

연구문제 3: 스팸 이메일에 대한 보안서비스는 조직구성원의 스팸 이메일에 대한 보안정책 준수에 영향을 미치는가?

Ⅲ. 연구 설계

1. 보안교육 실험

본 연구를 위해 임직원 수 약 3천명 규모의 국내 대기업 A사를 대상으로 현장실험을 수행하였다. 보안교육의 효과성과 지속성에 관해 알아보는 연구 1을 약 5개월에 걸쳐 진행한 후 시간차를 두고 그 다음 해 보안서비스 효과를 알아보는 연구 2를 약 2개월 동안 진행하였다.

임직원을 대상으로 무작위로 교육(실험)집단과 미교육(통제)집단으로 나누고 보안교육을 실시하기 전에 이들의 스팸 이메일 열람 현황을 조사하였다. 약 1개월 후 실험집단에는 보안교육을 실시하고 통제집단에는 보안교육을 실시하지 않은 상태에서 다시 스팸을 가장한 이메일을 발송한 뒤 열람률을 알아보았다. 마지막으로 약 3개월 뒤에 스팸 이메일을 다시 발송해 보안교육 효과의 지속성을 살펴보았다.

실험집단에 실시한 보안교육은 오프라인에서 1시간 동안 진행되었다. 특히 스팸 이메일을 통한 바이러스 및 악성코드의 감염으로 발생한 보안사고 사례들을 소개하고 이메일을 통한 해킹이 이뤄지는 과정에 대해 교육하였다. 그리고 이러한 사고를 예방하기 위해 조직구성원이 기업의 보안정책을 반드시 준수해야 한다

〈표 1〉 연구 1에 사용된 스팸 이메일 내역

구분	이메일 제목	발신자 주소
1차 이메일 (교육 전)	봄 여행 이벤트 당첨안내	nx@okKTX.com
2차 이메일 (교육 후)	문화상품권 할인안내	10won@10won.com
3차 이메일 (교육 3개월 후)	귀하의 아이디/비밀번호가 변경되었음을 알려드립니다	m@fakebook.all

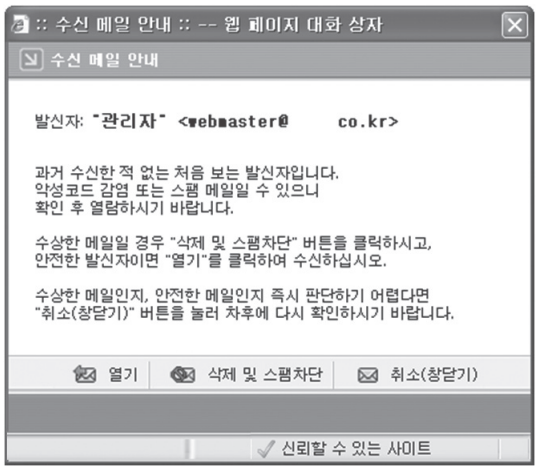
〈그림 1〉 스팸을 가장한 이메일 예시

는 점을 강조하였다. 구체적 행동지침으로 스팸 또는 바이러스나 악성 이메일로 의심되는 경우는 열람하지 않고 즉시 삭제해야 하며, 열람했을 경우에도 바이러스나 악성코드에 감염되지 않도록 첨부된 링크를 클릭하거나 파일을 다운받지 않도록 교육하였다. 보안교육 전, 교육 후, 교육 3개월 후에 발송한 스팸 이메일 내역은 〈표 1〉과 같다.

실험재료는 일반적인 스팸 이메일과 유사해 보이도록 구성했으며, 사회공학적 측면에서 아주 정교한 수준으로 설계하지는 않았고, 보통 수준을 유지하도록 했다. 예를 들어, 발신자 계정은 조직구성원이 어느 정도 주의를 기울이면 스팸 이메일인지 확인할 수 있는 수준으로 설정하였다. 실험에 사용된 스팸 이메일의 예시를 들면 〈그림 1〉과 같다.

2. 보안서비스 실험

보안교육 실험을 실시하고 약 6개월이 지난 후 보안서비스 제공 효과를 검증하는 실험을 진행하였다. 연구 1과 마찬가지로 무작위로 실험집단과 통제집단을 나누고 보안서비스를 제공하기 전에 두 집단의 스팸 이메일 열람 현황을 사전 조사하였다. 약 2개월 후 실험집단에는 해당 기업에서 실제 사용하는 이메일 시스템 내 그룹웨어를 통해 과거 수신 내역이 없는 발신자를 식별하여 해당 이메일 열람을 시도하는 경우 팝업창 형태로 경고 메시지를 보여줌으로써 수신자의 주의를 환기시키는 보안서비스를 제공하였다. 통제집단에는 이런 보안서비스를 제공하지 않았다. 보안서비스는 보안교육과 달리 스팸 이메일 열람을 시도하는 시점에 즉각적으로 제공되는 것이므로 3개월 뒤 효과지



〈그림 2〉 보안서비스 제공 화면 예시

〈표 2〉 연구 2에 사용된 스팸 이메일 내역

구분	이메일 제목	발신자 주소
1차 이메일 (보안서비스 적용 전)	귀하는 올해 암검진 대상이오니 암검진을 받으십시오.	admin@bbungbbung.com
2차 이메일 (보안서비스 적용 후)	회의 참석 안내	disguise@company.com

속성 여부를 확인하는 사후조사는 실시하지 않았다. 연구 2에 사용된 경고 메시지는 〈그림 2〉와 같다.

보안서비스 제공 전과 후에 사용된 스팸 이메일 내역은 〈표 2〉와 같다. 서비스 제공 전 1차 스팸 이메일을 발송한 후 열람률을 조사했고, 2차 이메일을 발송하는 시점에 실험집단에만 보안서비스를 제공하고 통제집단에는 서비스를 제공하지 않았다.

Ⅳ. 연구 결과

1. 보안교육 효과

보안교육 실험에 참여한 참가자는 총 543명(실험집단 256명, 통제집단 287명)이었다. 실험은 약 5개월에 걸쳐 진행되었다. 먼저 1차 스팸 이메일을 발송한 후, 1개월 내에 보안교육을 실시했고, 보안교육 후 1개월 이내에 2차 스팸 이메일을 발송했으며, 마지막으로 2차 이메일 발송으로부터 약 3개월 후 3차 스팸 이메일을 발송했다. 총 3번에 걸쳐 발송된 스팸 이메일의 열람자 수, 링크 클리자 수, 첨부파일 열람자 수는 〈표 3〉과 같다. 보안교육을 이수한 실험집단과 미이수한 통제집단 간 유의한 차이가 있는지 알아보기 위해 SPSS Statistics 24 프로그램을 이용하여 교차분석을 실시하였다. 직급이나 성별 차이는 유의하게 나타나지 않았으므로 분석 결과는 교육 이수집단과 미이수집단을 비교한 결과만을 보고한다.

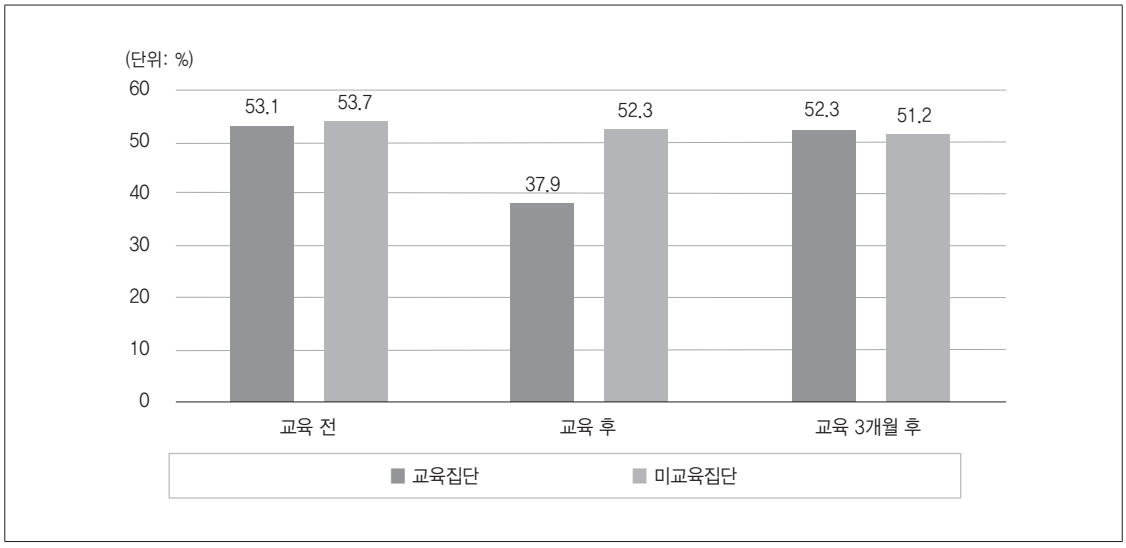
1) 보안교육과 이메일 열람률

보안교육 전 실험집단과 통제집단의 차이를 알아보기 위해 카이제곱 독립성 검정을 실시한 결과 이메일 열람 빈도수에 두 집단 간 차이가 유의하게 나타나지 않았다, χ^2 (1, n = 543) = .015, p = .901.〈표 3〉에도 나와 있듯이 실험집단에서는 256명 중 53.1%인 136명이, 통제집단에서는 287명 중 53.7%인 154명이 이메일을 열람했다. 즉, 두 집단 모두에서 약 절반 이상의 수신자들이 스팸 이메일을 열어본 것이다.

그러나 보안교육을 실시한 후 조사한 스팸 이메일 열람률은 두 집단 간 유의하게 다른 것으로 나타났다, χ^2 (1, n = 543) = 11.275, p = .001. 교육을 이수한 실험집단은 37.9%인 97명이 이메일을 열람했으나 교육을 이수하지 않은 통제집단은 52.3%에 해당하는 150명이 이메일을 열어본 것으로 나타나 이수집단에서는 열람률이 많이 낮아진 한편 미이수집단의 열람률은 교육 전과 크게 다르지 않았다. 따라서 스팸 이메일에 대한 보안교육이 조직구성원의 보안 정책 준수 행동에 긍정적인 영향을 미친 것으로 볼 수 있다.

〈표 3〉 연구 1 실험 결과 빈도표

보안교육		표본크기	교육 전	교육 후	교육 3개월 후
이메일 열람자 수	이수 (집단 중 %)	256 (100%)	136 (53.1%)	97 (37.9%)	134 (52.3%)
	미이수 (집단 중 %)	287 (100%)	154 (53.7%)	150 (52.3%)	147 (51.2%)
링크 클릭자 수	이수 (집단 중 %)	256 (100%)	34 (13.3%)	10 (3.9%)	26 (10.2%)
	미이수 (집단 중 %)	287 (100%)	41 (14.3%)	20 (7.0%)	36 (12.5%)
첨부파일 열람자 수	이수 (집단 중 %)	256 (100%)	8 (3.1%)	3 (1.2%)	16 (6.3%)
	미이수 (집단 중 %)	287 (100%)	11 (3.8%)	9 (3.1%)	14 (4.9%)



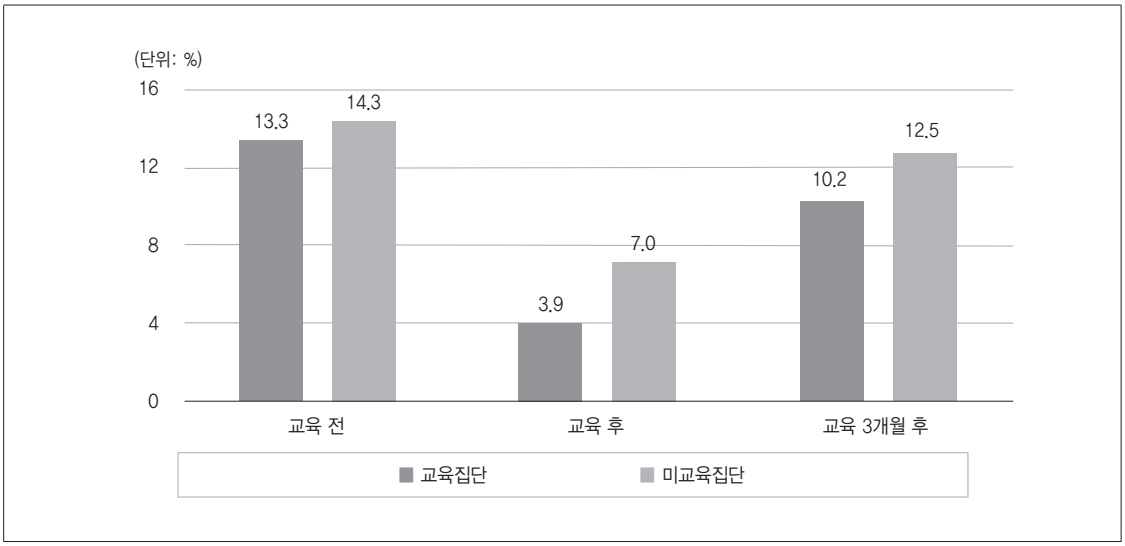
〈그림 3〉 정보보안 교육집단과 미교육집단 이메일 열람률 비교

보안정책 준수 행동이 3개월이 지난 뒤에도 지속되는지 알아보기 위해 3차 스팸 이메일을 발송한 후 두 집단 간 이메일 열람률을 분석한 결과 집단 간 유의한 차이는 사라진 것으로 나타났다, χ^2 (1, n = 543) = .068, p = .794. 교육 미이수집단에서 51.2%(147명)이 이메일을 열어보았고, 이는 1차, 2차 이메일 발송 시기와 크게 다르지 않았다. 그러나 실험집단인 교육 이수집단의 이메일 열람률은 52.3%(134명)으로 교육 이전 수준으로 회귀하는 현상을 보여 보안교육의 효과가 3개월 이상 지속되지 않는다는 문제점이 드러났다. 〈그림 3〉에 제시된 두 집단의 스팸 이메일 열람 퍼센티지를 보면 이러한 변화를 관찰할 수 있다.

2) 보안교육과 링크 클릭률

스팸 이메일을 열람하는 것은 조직의 정보보안정책을 준수하지 않는 행동이다. 여기서 더 나아가 스팸 이메일 안의 링크를 클릭하는 것은 미준수 수준이 더 높은 행동이라고 볼 수 있다. 보안교육 전에 스팸 이메일을 열어본 후 링크를 클릭한 빈도수를 교차분석한 결과, 두 집단 간 차이가 유의하지 않았다, χ^2 (1, n = 543) = .115, p = .735. 전체 수신자 543명 중 13~14% 가량이 이메일 내 링크를 클릭한 것으로 나타났다. 이메일을 열람한 사람 290명을 기준으로 보면, 약 25.9%인 75명이 이메일 내 링크를 클릭한 것이다.

보안교육이 이뤄진 후 스팸 이메일 안의 링크 클릭률에 교육 이수집단과 미이수집단 간 차이 경향성이 나타났으나, 통계적으로 유의한 수준은 아니었다, χ^2 (1, n = 543) = 2.431, p = .119. 유의확률이 .10 수준보다 약간 높은 값을 보여주어 통계적으로 유의하지는 않아도 경향성은 드러났다. 예상한대로 교육 이수집단은 3.9%(10명)가 링크를 클릭했고 교육 미이수집단은 7.0%(20명)가 링크를 클릭해서 보안교육을 받은 집단이 상대적으로 보안정책을 더 잘 준수한 것으로 나왔다. 스팸 이메일을 열어본 사람 247명(이수집단: 97명, 미이수집단: 150명) 기준으로 링크를 클릭한 사람은 이수집단에서 10.3%(10명), 미이수집단에서 13.3%(20명)로 집단 간 차이가 없었다, χ^2 (1, n = 247) = .505, p = .477. 보안교육을 이수했다할지라도 스팸 이메일을 이미 열어본 수신자라면 어차피 보



〈그림 4〉 교육집단과 미교육집단 링크 클릭률 비교

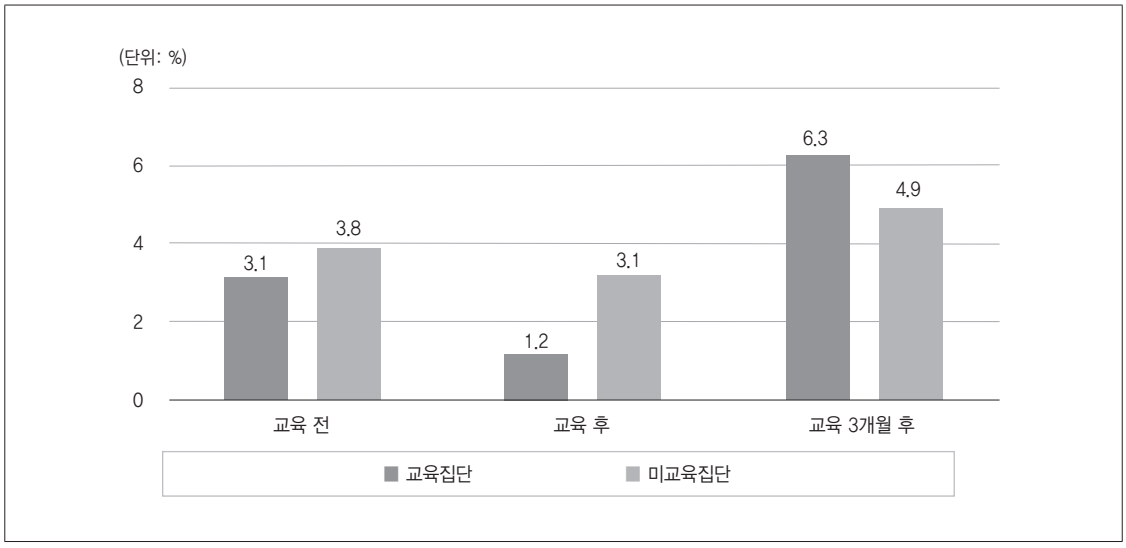
안교육의 효과가 없었다고 봐야하기 때문에 링크 클릭률이 이수집단과 미이수집단 간 다르지 않은 것은 예상 가능한 결과이다.

교육 이수 후 3개월이 지난 시점에서 두 집단 간 링크 클릭 비율은 다시 비슷해지는 것으로 나타났다, χ^2 (1, n = 543) = .762, p = .383. 특히 교육이수 집단의 변화를 보면, 교육 전 13.3%(34명)였던 클릭 퍼센티지가 교육 직후 3.9%(10명)로 낮아졌다가, 교육 3개월 후 다시 10.2%(26명)로 상승한 것으로 나타나 이메일 열람 퍼센티지의 결과와 마찬가지로 교육 이전 상태로 회귀하는 것으로 밝혀져 교육 효과의 지속성이 길지 않다는 문제점이 다시 한 번 확인되었다. 링크 클릭에 관한 전체 실험 결과는 〈그림 4〉에 제시되어 있다.

3) 보안교육과 첨부파일 열람률

본 실험연구에서 측정한 3가지 변수(이메일 열람, 링크 클릭, 첨부파일 열람) 중에서 보안 민감도가 가장 낮은 즉, 보안인식 수준이 가장 낮은 행위는 스팸 이메일 내 첨부파일을 열어본 행동이라고 할 수 있다. 즉, 가장 적극적인 형태의 보안 정책 미준수 행동이기 때문에 발생빈도가 높지는 않았다. 전체 실험 참가자 수가 500명 이상임에도 불구하고 독립성 검증을 위한 교차 분석에서 한 셀에 포함되는 사례수가 5 이하로 떨어지는 경우도 있었다. 보안교육 전에는 스팸 이메일을 열어본 후 첨부파일을 열람한 빈도수에 집단 간 차이가 없었다, χ^2 (1, n = 543) = .201, p = .654. 전체 수신자 중 3.5% 정도만 첨부파일을 열어본 것으로 나타났다. 이메일을 열어본 사람 290명 중 첨부파일을 클릭한 사람의 비율을 보면 6.6%로 소폭 증가하지만 역시 집단 간 차이는 없었다, χ^2 (1, n = 290) = .187, p = .665.

보안교육 후 스팸 이메일 내 첨부파일을 열어본 빈도수를 비교하면 이수집단과 미이수집단 사이에 차이가 있었으나 유의확률이 .10보다 커서 통계적으로 유의한 수준은 아니었다, χ^2 (1, n = 543) = 2.415, p = .120. 이수 집단에서는 1.2%(3명)가 미이수집단에서는 3.1%(9명)가 파일을 열어본 것으로 나타났다. 따라서 보안교육을 받은 집단에서 첨부파일 열람률이 낮은 경향성이 있었다. 이메일을 열어본 수신자 247명을



〈그림 5〉 교육집단과 미교육집단 첨부파일 열람률 비교

기준으로 파일을 열어본 사람은 각각 3.1%(이수집단), 6.0%(미이수집단)로 소폭 증가하면서 역시 약간의 차이 경향성이 나타났으나, 통계적으로 유의한 수준은 아니었다, χ^2 (1, n = 247) = 1.077, p = .299.

교육 이수 후 3개월이 지난 시점에서는 첨부파일 열람 비율에 집단 간 차이가 사라져 앞선 결과들과 마찬가지로 보안교육의 효과 지속성이 길지 않다는 문제점이 드러났다, χ^2 (1, n = 543) = .488, p = .485. 이전 분석결과와 비교해 특이한 점은 이수집단에서 6.3%(16명)가 그리고 미이수집단에서 4.9%(14명)가 첨부파일을 열어본 것으로 나와 교육을 받은 집단에서 보안정책 위반 행동 비율이 더 높았다는 점이다. 물론 이 차이는 통계적으로 유의하지 않기 때문에 우연히 발생한 결과로 볼 수도 있다.

〈그림 5〉에서 볼 수 있듯이, 교육이수 집단의 첨부파일 열람률은 교육 전 3.1%(8명) → 교육 직후 1.2%(3명) → 교육 3개월 후 6.3%(16명)로 변화하였고, 미이수집단은 교육 전 3.8%(11명) → 교육 후 3.1%(9명) → 교육 3개월 후 4.9%(14명)로 변화해 마지막에 발송된 스팸 이메일의 첨부파일 열람이 교육 이전보다 오히려 더 높게 나왔다. 이는 스팸 이메일의 제목이 개인정보(아이디와 비밀번호 변경)와 관련이 있기 때문으로 보인다. 앞서 3차 스팸 이메일의 파일 열람률이 미이수집단보다 이수집단에서 오히려 높았던 이유도 이런 맥락에서 해석해볼 수 있다. 정보보안 교육을 받았기 때문에 개인정보와 관련된 이메일에 더 민감하게 반응한 것으로 해석될 수 있는 것이다. 이런 경우 3차 스팸 이메일은 사회공학적으로 더 잘 설계된 것으로 볼 수 있으며 그래서 역설적으로 정보보안 민감도가 높은 사람들이 오히려 더 위험에 노출될 수도 있음을 시사한다.

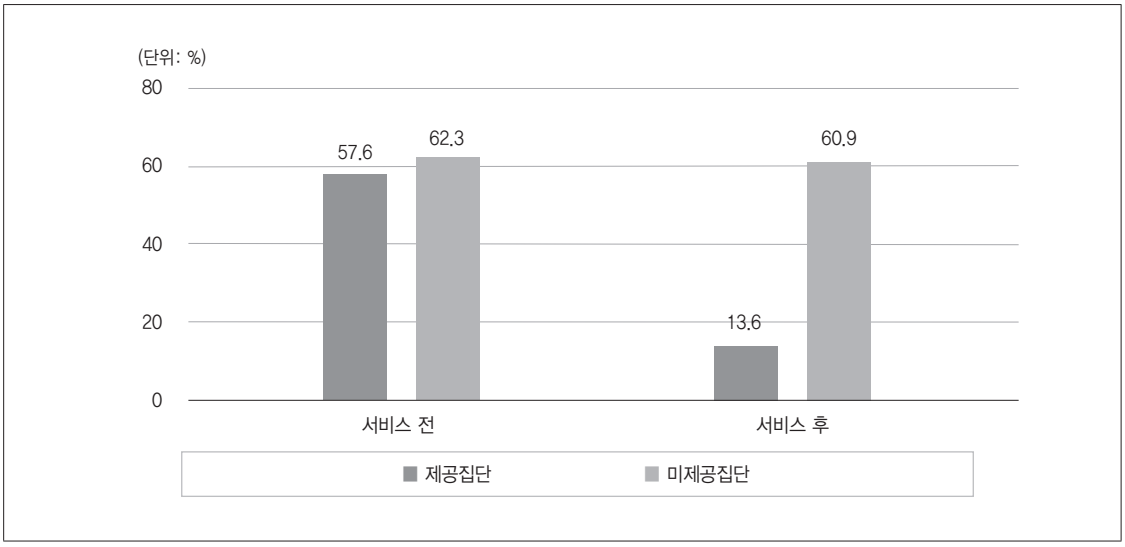
2. 보안서비스 효과

보안서비스 실험은 앞의 보안교육 실험과 별도로 진행하였다. 보안교육 실험의 직접적인 영향을 최소화하고 실험 상황에 대한 통제 수준을 높이기 위하여 두 실험 간에는 약 반 년 정도의 시간차를 두었다. 보안서비스를 제공하기 전 1차 스팸 이메일을 발송했고, 보안서비스를 제공 시기에 맞춰 2차 스팸 이메일을 발

〈표 4〉 연구 2 실험 결과 빈도표

보안서비스		표본크기	서비스 제공 전	서비스 제공 후
이메일 열람자 수	제공 (집단 중 %)	132 (100%)	76 (57.6%)	18 (13.6%)
	미제공 (집단 중 %)	138 (100%)	86 (62.3%)	84 (60.9%)
링크 클릭자 수	제공 (집단 중 %)	132 (100%)	20 (15.2%)	4 (3.0%)
	미제공 (집단 중 %)	138 (100%)	22 (15.9%)	24 (17.4%)
첨부파일 열람자 수	제공 (집단 중 %)	132 (100%)	12 (9.1%)	2 (1.5%)
	미제공 (집단 중 %)	138 (100%)	12 (8.7%)	12 (8.7%)

송했다. 자료는 약 2개월에 걸쳐 수집되었다. 실험에 참여한 참가자는 총 270명(실험집단 132명, 통제집단 138명)이었다. 본 연구에서 보안서비스는 조직구성원의 정보보안 정책 준수 행동을 향상시키기 위해 보완적으로 제공하는 기술적 지원으로 정의하고, 스팸 이메일을 읽으려 시도할 때 잠재적 위험을 알리는 메시지 팝업을 제공하는 것으로 구현되었다. 보안서비스 제공 전과 후 스팸 이메일의 열람, 링크 클릭, 첨부파일 열람 빈도는 〈표 4〉에 제시되어 있다. 서비스를 제공한 집단(실험집단)과 미제공한 집단(통제집단)의 차이를 알아보기 위하여 카이제곱검정 즉, 독립성 검증 교차분석을 실시하였고 결과변인은 연구 1과 마찬가지로 3개의 변수(이메일 열람, 링크 클릭, 첨부파일 열람)에 대한 빈도측정치를 사용했다.



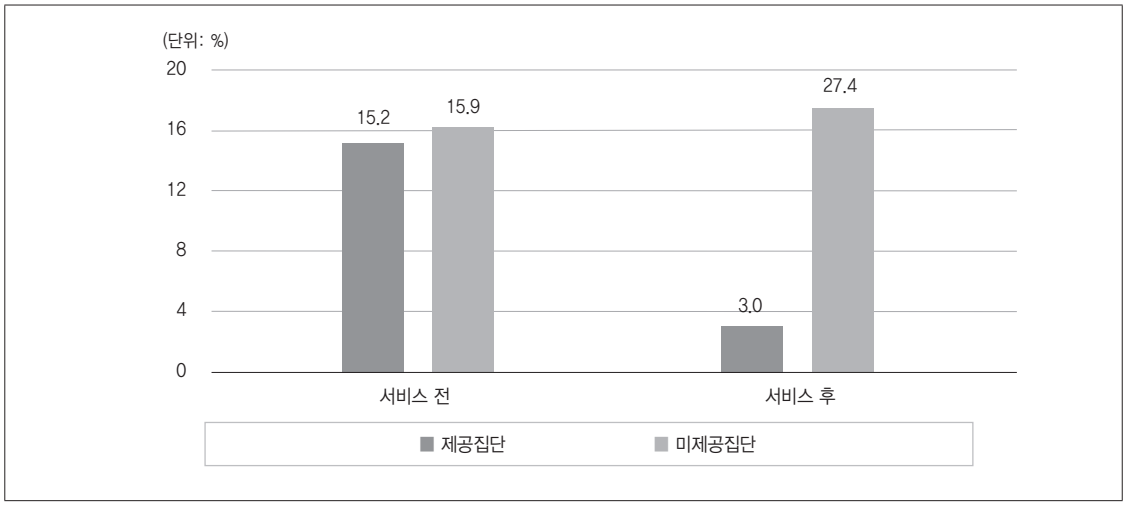
〈그림 6〉 보안서비스 제공집단과 미제공집단 이메일 열람률 비교

1) 보안서비스와 이메일 열람률

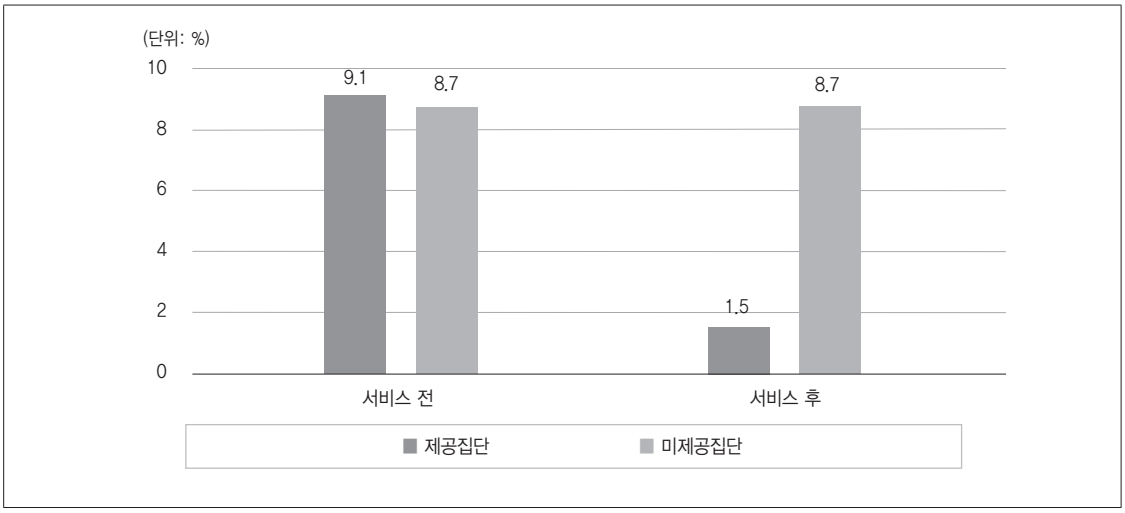
총 270명의 참가자들이 보안서비스 적용 전에 스팸 이메일을 열람한 비율은 실험집단과 통제집단 간 유의하게 다르지 않았다, χ^2 (1, n = 270) = .632, p = .426. 보안서비스 적용 후에는 위험 경고 메시지 창에 노출된 실험집단과 노출되지 않은 통제집단 사이에 이메일 열람 퍼센티지가 유의하게 달라진 것으로 나타났다, χ^2 (1, n = 270) = 64.03, p = .000. 보안서비스 제공 전에는 실험집단에 속한 참가자의 반 이상이 스팸 이메일을 열람했으나 보안서비스 제공 후에는 13.6%(18명)까지 대폭 감소하였다. 보안서비스를 제공하지 않은 집단에서는 이러한 변화가 관찰되지 않았다. 보안서비스의 유의한 효과는 〈그림 6〉에 제시된 두 집단의 스팸 이메일 열람 퍼센티지를 보면 알 수 있다.

2) 보안서비스와 링크 클릭률

보안정책 미준수 행동 혹은 위반 행동의 수준은 스팸 이메일 열람, 링크 클릭, 첨부파일 열람 순으로 높아진다고 볼 수 있다. 이메일의 내부 링크를 클릭한 비율을 비교하면, 보안서비스 적용 전에는 총 270명의 참가자들 중 15.6%(42명)가 링크를 클릭했고, 집단 간 차이는 유의하지 않았다, χ^2 (1, n = 270) =.032, p = .858. 그러나 보안서비스 적용 후에는 서비스를 제공한 실험집단과 미제공한 통제집단 간 링크 클릭 비율의 차이가 유의하게 다른 것으로 나타났다, χ^2 (1, n = 270) = 14.970, p = .000. 보안 경고 알림창에 노출된 집단은 132명 중 3.0%(4명)만 링크를 클릭한 것에 비해, 비노출 집단은 138명 중 17.4%(24명)가 링크를 클릭한 것이다(〈그림 7〉 참조). 알림창에 노출된 후에도 이메일을 열어본 수신자는 132명 중 13.6%인 18명이었고, 이 중 22.2%(4명)가 첨부된 링크까지 클릭했다. 알림창에 노출되지 않은 집단에서 이메일을 열람한 수신자는 138명 중 60.9%인 84명이었고, 이 중 28.6%(24명)이 링크를 클릭했기 때문에 일단 스팸 이메일을 열어봤다면 그 후 링크를 클릭하는 비율에는 집단 간 차이가 존재하지 않았다, χ^2 (1, n = 102) = .300, p = .584. 즉, 보안 경고 메시지를 받은 집단에 속해있다 할지라도 일단 스팸 이메일을 열었다면 해당 수신자에게는 보안서비스 제공이 이미 효과가 없었다고 볼 수 있으며, 따라서 이미 스팸 이메일을 열람한 수신자들만 대상으로 링크를 클릭하는



〈그림 7〉 서비스 제공집단과 미제공집단 링크 클릭률 비교



〈그림 8〉 서비스 제공집단과 미제공집단 첨부파일 열람률 비교

비율을 비교했을 때 실험집단과 통제집단이 서로 유의하게 다르지 않았던 것으로 해석할 수 있다.

3) 보안서비스와 첨부파일 열람률

마지막으로 정보보안 정책에 대한 위반 강도가 가장 높다고 할 수 있는 스팸 이메일 안의 첨부파일 열람 분석결과를 보면, 보안서비스 적용 전에는 집단 간 차이가 없다가(χ^2 (1, n = 270) = .013, p = .909), 보안서비스 적용 후 집단 간 차이가 유의하게 드러났다, χ^2 (1, n = 270) = 7.076, p = .008. 〈그림 8〉에서 볼 수 있듯이 보안 경고 알림창 노출집단에서는 전체 132명의 스팸 이메일 수신자 중 겨우 1.5%에 해당하는 2명만이 첨부파일을 클릭했으나, 비노출집단에서는 전체 138명의 수신자 중 8.7%인 12명이 첨부파일을 클릭하는 단계까지 도달한 것으로 나타났다. 경고 알림창에 노출되었음에도 스팸 이메일을 열어본 수신자 18명 중 11.1%인 2명은 첨부파일을 클릭한 것으로 나타났고, 비노출 집단에서 이메일을 열람한 84명 중 14.3%인 12명이 첨부파일을 클릭한 것으로 나타나 집단 간 차이가 없었다, χ^2 (1, n = 102) =.126, p = .722. 앞선 링크 클릭 결과와 마찬가지로 보안 알림창을 보았음에도 불구하고 스팸 이메일을 열람한 수신자에게는 이미 보안서비스 제공의 효과가 없었다고 보이므로 첨부파일 클릭 비율이 비노출 집단과 다르지 않았다고 볼 수 있다.

Ⅴ. 논의

본 연구는 정보보안 정책준수 의도나 태도가 아닌 정책준수 행동에 대한 보안교육의 효과성과 지속성 그리고 기술적인 보안 지원 서비스 제공의 효과성을 알아보기 위해 실제 기업 현장에서 실험을 진행하였다. 실험의 통제 수준을 높이기 위해 정보보안 실험 대상은 스팸 이메일에 대한 대응으로 한정하였다.

연구 결과 스팸 이메일에 관한 정보보안 교육은 스팸 이메일 열람률을 낮추는데 효과가 있는 것으로 나타났다. 그러나 이 효과가 3개월 이상 지속되지는 않았다. 스팸 이메일 안의 링크 클릭률과 첨부파일 열람률에 대해서도 보안교육의 효과가 있다고 짐작되는 경향성이 나타났다. 그러나 마찬가지로 이러한 보안정책 준수 행동이 3개월 이상 지속되지는 않는 것으로 나타났다. 보안경고 메시지를 제공했던 보안서비스의

효과는 매우 커서 스팸 이메일 열람률, 링크 클릭률, 첨부파일 열람률을 모두 유의하게 낮추는 것으로 드러났다. 그리고 전반적으로 정책 위반의 정도가 심해질수록 즉, 이메일 열람, 링크클릭, 첨부파일 열람 순으로 위반 행동의 빈도는 감소하는 경향이 있었다.

연구 1에서 보안교육이 단기적으로는 효과가 있으나 장기적으로는 시간이 지날수록 효과가 사라지는 것을 확인하였기 때문에 조직 현장에서는 보안교육 기간과 연간 시행 횟수 등을 결정할 때 이 부분을 고려해서 프로그램을 설계할 필요가 있어 보인다. 또한 연구 2에서 보안서비스 제공의 효과가 아주 큰 것으로 드러나 기술적으로 교육을 보완하는 여러 형태의 서비스가 지원된다면 보안교육과 시너지 효과를 낼 수 있을 것으로 기대된다. 본 실험에서는 보안교육의 효과와 보안서비스 효과를 독립적으로 알아보았으나 추후 보안교육과 보안서비스의 상호작용 효과를 검증하는 실험연구를 통해 보안서비스가 교육 효과의 향상과 지속성에 어떤 영향을 미치는지 살펴볼 필요가 있다.

연구1의 결과 중 이벤트 당첨에 관한 1차 스팸 이메일이나 상품권 할인에 관한 2차 스팸 이메일보다 개인정보 변경과 관련된 3차 스팸 이메일에서 첨부파일 열람률이 가장 높았던 점, 그리고 교육 미이수집단보다 이수집단에서 오히려 더 열람률이 높았던 점에 주목할 만하다. 보안교육을 받은 집단이 개인정보와 관련된 이메일에 더 민감하게 반응한 것으로 해석될 수 있기 때문이다. 스팸 이메일뿐 아니라 정부기관을 사칭하며 접근하는 문자 메시지나 보이스 피싱 등 개인정보를 빼내기 위한 범죄는 더욱 다양해지고 있고, 그 방법은 사회공학적으로 더 정교해지고 있다. 따라서 이 연구결과는 정보보안 민감도가 높아진 사용자들이 오히려 더 취약해지는 상황을 피하기 위해서는 더욱 안전한 기술을 개발하는 것만큼이나 보안교육 컨텐츠의 주기적이고 신속한 업데이트 역시 중요함을 시사한다.

본 연구는 설문을 통해 태도나 의도에 대한 응답을 수집한 것이 아니라 참가자들의 실제 행위를 측정하였고, 실험실이 아닌 실제 기업 현장에서 실험을 진행했기 때문에 분석 결과의 신뢰도와 타당도가 높다는 장점이 있다. 그러나 특정 조직 한 곳만을 대상으로 자료를 수집했기 때문에 조직문화 등과 같은 외적, 환경적 요인의 효과를 통제하지 못했다는 한계가 존재한다. 또한 연구에 사용된 스팸을 가장한 이메일들은 제목이 각각 달랐는데, 참가자들이 과거에 발송된 이메일을 기억할지도 모르기 때문에 학습효과를 통제하기 위해서 취한 조치이지만 실험에 이용된 재료들의 '동등성' 수준을 어디까지 볼 것인가라는 부분에서 방법론적 논의가 더 이뤄질 수 있다. 실제로 연구 1에서 사용된 개인정보 변경과 관련된 이메일 열람률에서 이런 설계적 한계가 노출되었다고 볼 수도 있다.

본 연구는 효과적인 정보보안 대책을 고민하는 조직들에 기초적인 도움을 제공하고 조직구성원을 위한 보안교육 및 보안서비스 프로그램 구성에 단초를 제공할 수 있을 것으로 기대된다. 향후 동일한 실험을 다른 여러 조직에서 수행한다면 본 연구결과의 타당도와 일반화가능성을 더욱 높일 수 있을 것이다. 그리고 스팸 이메일 이외의 정보보안과 관련된 주제(예: 기밀문서 취급에 관한 정보보호 정책과 준수)를 대상으로 후속 실험 연구를 진행할 수도 있다. 앞으로 더 다양한 후속연구들을 통해 조직구성원의 보안정책 준수 행동에 결정적인 영향 요인들을 밝히고 보안정책 준수율을 향상시키기 위한 보다 구체적인 방안이 수립되기를 기대한다.

■ 참고문헌

권영관·염흥열 (2007). "스팸 이메일 현황과 대응에 대한 고찰." 「정보보호학회지」, 17(2): 66-79.

김기영·안개일·장종수·이상호 (2001). "실시간 인터넷 보안 서비스 제공을 위한 정책기반 통합 서버 설계 및 시뮬레이션." 「정보처리학회논문지C: 정보통신,정보보안」, 8(5): 565-572.

김상훈·박선영 (2011). "정보보안 정책 준수 의도에 대한 영향요인." 「한국전자거래학회지」, 16(4): 33-51.

김상훈·이갑수 (2015). “정보보안기술 사용의 영향요인에 관한 실증적 연구.” 「한국전자거래학회지」, 22(4): 151-175.

김수홍·김상희·심정신 (2007). “간호 대학생의 심폐소생술 교육 효과 및 교육효과 지속에 대한 연구.” 「대한응급의학회지」, 18(6): 496-502.

김종기·강다연 (2008). “보안정책, 보안의식, 개인적 특성이 패스워드 보안효과에 미치는 영향.” 「정보보호학회논문지」, 18(4): 1-26.

김종기·전진환 (2006). “컴퓨터 바이러스 통제를 위한 보안행위의도 모형.” 「정보화정책」, 13(3): 174-196.

박서기·황경태 (2016). “빅데이터 보안 분야의 연구동향 분석.” 「정보화정책」, 23(1): 3-19.

박수진·박명찬·이새롬·최용락 (2002). “실시간 e-mail 대응 침입시도탐지 관리시스템의 설계 및 구현.” 「정보처리학회논문지C: 정보통신,정보보안」, 9(3): 359-366.

박철주·임명성 (2012). “보안 대책이 지속적 보안 정책 준수에 미치는 영향.” 「디지털정책연구」, 10(4): 23-35.

신희은 (2014). “대기업에 당하고 직원이 빼가고 스파이에 멍든 中企.” 「머니투데이」. 11월 24일.

임명성 (2012). “조직 구성원들의 정보보안 정책 준수행위 의도에 관한 연구.” 「디지털정책연구」, 10(10): 119-128.

임명성 (2014). “정보보안 인식 교육의 효과에 대한 연구.” 「디지털융복합연구」, 12(2): 27-37.

채명정·이진희·송인자·김진일 (2015). “심폐소생술 교육 후 재교육이 간호대학생의 지식, 수행능력 및 자기효능감 지속에 미치는 효과.” 「한국응급구조학회논문지」, 19(1): 51-62.

최양서·서동일 (2006). “사회공학적 공격방법을 통한 개인정보 유출기술 및 대응방안 분석.” 「정보보호학회지」, 16(1): 40-48.

한국인터넷진흥원 (2015). 「2015 국내 정보보호산업 실태조사」. 미래창조과학부, 한국인터넷진흥원, 한국정보보호산업협회.

AhnLab (2011). 「ASEC Report Vol. 13」. 경기: 안철수연구소.

Bulgurcu, B., Cavusoglu, H. & Benbasat, I. (2010). “Information Security Policy Compliance: An Empirical Study of Rationality-based Beliefs and Information Security Awareness.” *MIS Quarterly*, 34(3): 523-548.

Dhillon, G. & Backhouse, J. (2000). “Technical Opinion: Information System Security Management in the New Millennium.” *Communications of the ACM*, 43(7): 125-128.

Fornell, C. & Larcker, D. F. (1981). “Evaluating Structural Equation Models with Unobservable and Measurement Error.” *Journal of Marketing Research*, 18: 39-50.

Trček, D., Trobec, R., Pavešić, N. & Tasič, J. F. (2007). “Information Systems Security and Human Behaviour.” *Behaviour & Information Technology*, 26(2): 113 - 118.

Desman, M. B. (2002). *Building an IS Security Awareness Program*. Boca Raton: Auerbach Publishing.

Mitnick, K. D. & Simon, W. L. (2002). *The Art of Deception: Controlling the Human Element of Security*. Indianapolis: Wiley Publishing, Inc.

Sheeran, P. (2002). “Intention-Behavior Relations: A Conceptual and Empirical Review.” *European Review of Social Psychology*, 12(1): 1-36.

Straub, D. (1990). “Effective IS Security: An Empirical Study.” *Information Systems Research*, 1(3): 255-276.

Straub, D. & Welke, R. (1998). “Coping with Systems Risk: Security Planning Models for Management Decision Making.” *MIS Quarterly*, 22(4): 441-469.

Da Veiga, A. & Eloff, J. H. P. (2007). “An Information Security Governance Framework.” *Information Systems Management*, 24(4): 361-372.

Warkentin, M. & Willison, R. (2009). “Behavioral and Policy Issues in Information Systems Security: The Insider Threat.” *European Journal of Information Systems*, 18(2): 101-105.

Workman, M. & Gathegi, J. (2007). “Punishment and Ethics Deterrents: A Study of Insider Security Contravention.” *Journal of the Association for Information Science and Technology*, 58(2): 212-222.