Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.29, NO.4, Aug. 2019 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2019.29.4.847

스팸메일 모의훈련 현장실험을 통한 기업의 인적 취약요인 연구

이 준 희,† 권 헌 영‡
고려대학교 정보보호대학원

A Study on Human Vulnerability Factors of Companies : Through Spam Mail Simulation Training Experiments

Jun-hee Lee,† Hun-yeong Kwon‡
Graduate School of Information Security, Korea University

요 약

최근 랜섬웨어, 스피어 피싱, APT공격 등 전자메일을 통한 다양한 수법의 사이버 위협이 커지고 있다. 이러한 공격의 특징은 과거 패턴기반탐지 등의 기술적 대책을 우회하기 때문에 개인의 보안인식 개선을 통한 관리적 대응이 중요하다는 점이다. 본 연구는 현장실험을 통해 이러한 스팸메일 공격에 취약한 임직원들의 인적요인을 연구하고 향후 개선방안을 수립하고자 하였다. 한 기업의 임직원을 대상으로 7차례에 걸쳐 훈련용 스팸메일을 발송하고 열람정보를 분석한 결과 훈련의 횟수와 수신자의 성별, 나이, 근무지 등의 인적요인이 열람율과 관계가 있음을 확인하였다. 이러한 분석 결과를 바탕으로 훈련개선 방안을 도출하여, 향후 각 기관의 실효성 있는 모의훈련 수행과 인식개선을 통한 대응능력 향상에 도움이 되고자 한다.

ABSTRACT

Recently, various cyber threats such as Ransomware and APT attack are increasing by e-mail. The characteristic of such an attack is that it is important to take administrative measures by improving personal perception of security because it bypasses technological measures such as past pattern-based detection The purpose of this study is to investigate the human factors of employees who are vulnerable to spam mail attacks through field experiments and to establish future improvement plans. As a result of sending 7times spam mails to employees of a company and analyzing training report, It was confirmed that factors such as the number of training and the recipient 's gender, age, and workplace were related to the reading rate. Based on the results of this analysis, we suggest ways to improve the training and to improve the ability of each organization to carry out effective simulation training and improve the ability to respond to spam mail by awareness improvement.

Keywords: experiment, phishing, training, spam mail, security awareness

I. 서 론

정보통신기술의 발전은 우리 삶의 편의성을 향상시키고 기업의 비약적인 생산성 향상에 이바지 하였다. 하지만 그와 더불어 사이버공격으로 인한 기업의 정보 유출, 개인의 사생활 침해 등 새로운 위험이 발생하였고, 최근 정보시스템에 대한 사이버공격은 우리 삶에 직접적인 위해를 가할 수도 있게 되었다. 더욱이 기반 시설 등에 정보통신 시스템이 도입되면서 악성메일, 랜섬웨어, APT(Advanced Persistent

Received(07. 01. 2019), Modified(07. 30 2019), Accepted(07. 30. 2019)
† 주저자, l22juny@korea.ac.kr
‡ 교신저자, khy0@korea.ac.kr(Corresponding author)

Treat) 공격 등 다양한 사이버 공격으로 인한 인명 및 경제적인 손실을 포함한 대규모 피해 사례를 지속적으로 야기하고 있다[1].

2018년 TrendMicro사의 보고서에 따르면 세계적으로 보안 시스템에서 약 410억 건의 이메일 공격을 탐지했다고 밝혔으며, 이메일을 통한 피싱, 스팸 공격 등은 높은 파급력과 해킹 성공률로 인해 폭발적으로 증가하고 있어 이에 대한 각국의 대비가 필요하다고 주의를 하였다. 한국 인터넷 진흥원과 경찰청 또한 2019년의 7개 주요 사이버 위협 중 하나로 스피어 피싱을 선정했다[2].

이에 따라 국내의 많은 기업 및 기관에서는 스팸 차단 시스템, APT대응 시스템 등 다양한 메일관련 보안설비를 구축하고 운영하고 있다. 하지만 최근의 APT나 피싱 공격은 단순 패턴기반으로는 전부 탐지하기가 사실상 불가능에 가까우며, 이러한 기술적 대응의 한계점은 사용자의 지속적 교육이나 훈련을 통해 임직원의 보안 인식을 높이는 것으로 보완해야 한다.

실제로 2019년 국가정보원에서는 중앙행정기관, 공기업, 준정부기관, 광역지자체 등 155개 기관을 대상으로 '사이버공격 대응훈련'을 실시한다고 밝혔으며, 금융보안원 또한 국내 180개 금융회사를 대상으로 한 침해사고 대응훈련을 상시적으로 진행한다고 발표했다. 다만 이처럼 다양한 기업 및 기관에서 이메일 모의훈련이 중요하다는 것을 인식하고 훈련을 수행하고 있으나, 단순히 훈련을 '수행'하는 것에 목적을 두고 그치는데 있어 아쉬움이 있다. 대부분의 기업은 시간상 훈련 결과를 경영자에게 보고하고 훈련 성공률을 높이는 데만 급급하기 마련이다. 훈련 실패자에 대한 추가 교육이나 확인서 징구로 해당 차수를 마무리 한 뒤 다음 훈련을 대비하는 것에 준비를 쏟을 뿐, 실패원인 파악이나 취약요인에 대한 후속 연구는 부족한 것이 현실이다.

본 논문에서는 한 기업의 스팸메일 모의훈련 현장실험을 통해 1년간 7차수에 걸쳐 실제 피싱 형태의 스팸 훈련메일을 지속적으로 발송하였다. 매번 무작위로 지정된 인원을 대상으로 악성메일 훈련시스템을 활용하여 이러한 메일공격 실행 시 열람에 영향을 미치는 개인의 사회적, 인적 요인에 대해서 분석코자 하였다. 향후 분석된 해당 연구결과를 통해 효과적 훈련 개선방안을 제시하여 기업의 보안 실무자로 하여금 효율적인 훈련 수행을 가능케 하고, 학술적으로는 현장실험을 통한 보안인식 개선에 관한 이론적 연구결과 검증사례에 기여코자 한다.

II. 연구배경 및 선행연구

2.1 연구배경

2.1.1 스팸메일

스팸(spam)이란 정보통신망 이용촉진 및 정보보호 등에 관한 법률에 따르면 "정보통신망을 통하여 전송되는 영리목적의 광고성 정보"를 의미한다. 본 논문에서는 발신자의 금전적 이득 또는 수신자의 피해를 입힐 목적으로 피싱, 스피어피싱, 스미싱 등 다양한 형태로 전송되는 불법적인 전자메일을 통칭하여 스팸메일이라고 개념을 정의 하고자 한다[3].

이러한 스팸메일은 피해자의 PC에 첨부파일을 이용해 실행 시 악성코드를 감염 시키는 전통적인 방법뿐 아니라, 메일 본문에 직접 악성코드를 삽입시키고 피싱 메일과 결합하는 등 복잡한 형태로 진화 및 지능화되고 있어 피해가 지속되고 있다. 또한 최근 유행하는 랜섬웨어의 주요 전파매체로 사용되거나 사회공학적 방법을 이용한 금융사기, 주요자료 탈취 등 점점 이메일 자체가 공격이 아닌 수단으로 사용되는 공격이 확대되고 있다[4].

이런 스팸메일 공격은 국내외에서 큰 이슈가 되고 있는데, 한국인터넷진흥원은 2017년 상반기까지 국내에서 탐지된 스팸메일은 1,535만 건으로 2016 년 하반기 대비 120%나 증가한 것으로 발표하였다. 국외 또한 글로벌 이메일 보안 벤더인 Proofpoint사의 2018년 설문조사결과에 따르면 IT 의사결정권자의 82%는 이메일 공격 위협을 우려하고 있으며, 59%가 이메일을 통한 사기공격을 가장 큰 보안 위협으로 생각하는 것으로 나타냈을 정도로 세계적으로 많은 관심을 가지고 있음을 알 수 있다[5].

2.1.2 피싱과 스피어 피싱

피싱(phishing)공격은 개인 정보(private data)와 낚시(fishing)의 합성어로 개인정보를 낚는다는 의미로 사용되며, 주로 금융기관 또는 공공기관 등을 사칭하여 전화나 이메일로 피싱 사이트 링크 접속을 유도하여 개인의 접속정보(id/pw) 또는 금융정보(보안카드, 공인인증서 정보) 등을 입력하도록 요구해 사용자의 중요한 정보를 몰래 빼가는 수법이

다[1].

일반 피싱 메일은 다수의 상대를 표적으로 하지만 스피어 피싱(spear-pishing)은 의도한 피해자에 맞추어 따로 작성된 이메일을 이용해 구체적인 표적을 노린다. 즉 스피어 피싱이란 피싱의 한 형태로써, '불특정 다수가 아닌 특정인을 표적으로, 신뢰할 만한 발신인이 보낸 것처럼 위장한 메일을 통해 악성웹사이트로 유도 또는 악성 첨부 파일로 악성코드에 감염시키는 일종의 온라인 사기행위'로 정의될 수 있다[6]. 이러한 스피어 피싱의 공격 순서를 살펴보면 먼저, 공격 대상을 선정하고 공격 대상에 대한 정보를 수집한 뒤, 이후 수집된 정보를 바탕으로 공격대상에 악성 링크나 첨부파일이 담긴 이메일을 보내고 메일을 클릭한 대상자의 PC를 감염 시키는 순서로 진행된다. 약 2년 전 유행했던 페트야(Petya) 랜섬웨어 역시 주로 스피어 피싱 메일형태로 전파되었으며, 이는 기존의 수법과는 다르게 사회 공학적 기법이 사용되는 공격 형태로 이후 APT 공격의 시발점이 될 수 있으므로 훨씬 위험하다고 볼 수 있다.

2.1.3 모의훈련

구미가 당기는 제목을 통해 사용자를 현혹 시키고 악성코드를 감염시키는 메일전송은 고전적인 방법이라 할 수 있지만, 이런 방법이 아직도 효과가 있다는 것이 문제가 된다. 이는 '최대의 보안 취약점은 바로 사람'이라는 다수의 보안전문가들의 지적과도 일치하는 현상이다[7]. 이처럼 기계적으로 탐지할 수 없게 지능화된 스팸메일 공격에 대응하는 방안은 기업 내 임직원 개개인의 보안인식을 향상 시켜 감염을 예방하는 수밖에 없다.

따라서 이론적으로 가장 좋은 케이스는 적절한 교육을 통해 임직원 모두가 이메일 공격에 대한 인식을 하고 의심스러운 메일을 열람하지 않는 것이지만, 실제 상황에서 열람했거나 악성코드에 감염된 경우에는 신속하고 정확하게 대응하는 것이 중요하다. 하지만 보안부서가 아닌 일반직원의 경우 긴급상황에서 쉽게 당황할 수 있기 때문에, 현실적인 모의훈련을 시행하여 체득할 수 있도록 해야 한다.

모의훈련의 중요성은 주요 지침에서도 나타나는데 공공기관의 경우, 국가 정보보안 보안지침[8]에 따르면 '각 기관은 자체 정보통신망을 대상으로 매년 정기 또는 수시 사이버위기 대응 모의훈련을 실시하여야 한다.'라고 명시 되어있으며, '사용자는 출처가 불분명하거나 해킹이 의심되는 메일 수신시 해킹메일 신고기능을 통해 정보보안담당자에게 즉시 신고해야 한다.'라고 되어있다.

또한 국가정보원과 정부에서는 매년 산하 공공기관을 대상으로 '정보보안 관리실태 평가' 항목 중 하나로 전산망 침투훈련과 더불어 해킹메일 대응훈련을 수행하며 기관의 관심도를 증대시키고 있지만, 단순히 연간 1회성 평가에 그치며 해당 결과를 통보하는데 한계가 있다.

2.2 선행연구

2.2.1 보안인식

정보보호 인식(보안인식)이란 사람들이 자신의 직무를 수행하는 데 있어, 정보보호의 함축된 상태를 잘 알 수 있도록 하는 프로세스이다. 여기에는 정보보호의 중요성 인식, 보안사고 발생 시 이에 대한 대응 방안과 보고 체제 등이 포함된다[9]. 이에 Bulgurcu[10] 등은 조직원의 정보보호 인식은 보안정책 준수에 대한 태도와 결과에 대한 믿음을 형성하는데 직접적이고 긍정적인 영향을 미치며, 조직 내 보안 인식 문화의 조성을 위해서는 적절한 보안인식 교육 및 프로그램이 중요하다고 하였다. 또한 임채호[11]의 연구에 따르면 정보시스템 사용자의 정보보안을 위한 인식제고가 우선적으로 이루어질 때 비로소 올바른 정보보안 대응조치가 가능하다고 강조하였다. 결국 스팸메일 대응을 위한 임직원의 보안인식 향상을 위해서는 가장 먼저 적절한 관리적 대응 방안이 수립되어야 한다.

2.2.2 지속적 모의훈련의 중요성

보안 인식향상을 위한 방안으로 손유승[12]은 스피어 피싱 이메일의 본문은 사전에 정보를 수집하여 개인에게 특화된 이메일이기 때문에 기존의 자연어 처리 기법과 통계적 기법을 이용한 스팸 메일탐지 솔루션으로는 탐지하는데 한계가 있음을 나타내며, 정기적인 보안 교육을 통한 인식 제고와 직원을 대상으로 한 모의훈련의 중요성을 강조하였다.

또한 윤덕상[13]은 실전형 훈련은 임직원들의 실질적 피싱메일 대응역량 향상에 큰 도움을 주는 교육방법이며, 훈련기간을 단기가 아닌 정기적이고 지속적으로 실시할 때 임직원들로 하여금 적절한 메일공

격에 대한 대응을 이룰 수 있다고 하였다. 이는 단발성이 아닌 여러 번의 정기적 훈련과 교육이 효과적 인식개선을 이끌어 낸다고 볼 수 있다.

2.2.3 스팸메일 실험과 인적요인

인구통계학적 특성 실험으로, 메릴랜드 대학에서는 1,350명의 학생을 대상으로 피싱 공격을 수행하고 스팸메일 열람율 및 인구 통계 조사를 실시하였다[14]. 연구는 여러 인구통계 요인과 학생의 피싱 공격에 대한 취약성 사이의 연관성을 발견했는데, 근무환경(컴퓨터 사용시간, 전공), 성별, 연령, 학년 등의 인적요인과 열람율에 관한 실험 이였다. 연구결과 IT와 관련이 있는 학부이거나 컴퓨터 사용시간이 길고, 활용에 더 친숙한 인원일수록 피싱 공격에 대한 인식이 더 높다는 것을 나타낸다.

Sheng[15]은 카네기 멜론 대학교에서 1,001명의 참가 학생을 대상으로 온라인 설문 조사를 통해 나이, 성별 등 인구 통계와 피싱 취약성 간의 관계를 연구하였으며, 그 결과 참가자들의 성별과 나이가 피싱 피해에 영향을 미치는 것을 나타내며 교육의 중요성을 이야기 하였다. 또한 Zarka[16]는 샤르자 대학(AUS)의 교수와 학생 10,000명을 대상으로 단순 교육에 대한 메일실험을 수행하였는데, 첫 번째 실험에서는 피싱 메일을 발송했고 두 번째는 일괄적으로 피싱에 관한 주의 메일을 보낸 뒤 스팸메일을 발송했다. 두 번의 실험을 통해 나이와 성별 특성을 분석하였으며, 인구적 특성 보다는 교육을 통한 최종 사용자와의 사이버 범죄에 대한 확실한 인식의 중요성을 강조하였다.

결국 본 실험에서는 앞선 선행연구를 정리한 결과, 반복적 훈련의 효과 더불어 사용자의 근무환경, 성별, 나이 등의 인적 요인에 대한 연구를 수행코자 한다.

III. 연구설계

3.1 연구모형

본 연구는 앞선 선행연구 결과 분석을 통해 앞선 사례들이 국내 현실에도 부합한지 재확인 할뿐만 아니라 교육기관으로 한정된 연구 환경 한계성을 극복하고자, 국내 한 공공기관의 협조를 통해 기업 실무자들을 대상으로 훈련을 수행하고 데이터를 수집하여

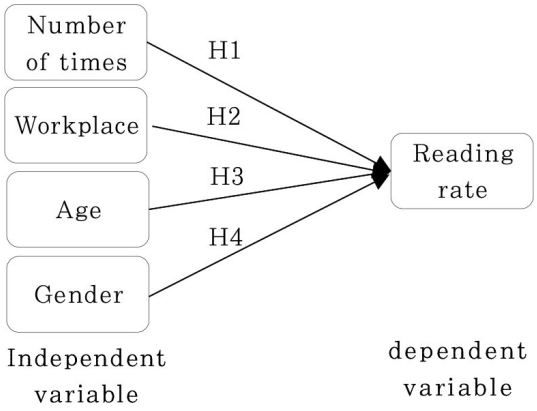

Fig. 1. Research model design

연구를 진행하였다.

연간 7차례 훈련을 통해 스팸열람에 영향을 주는 원인을 실증적으로 분석하고자 선행연구 분석과 실무자와의 인터뷰를 통해 가설을 수립하고, 훈련횟수와 임직원의 근무지, 나이, 성별 등 4가지 요소와 열람율과의 관계를 규명하고자 아래 Fig.1.같이 연구모형을 설정하였다.

3.2 가설수립

3.2.1 훈련횟수와 관계

연구가설1(H1)은 모의훈련의 지속적이고 정기적인 반복 횟수와 임직원의 훈련메일 열람율과의 영향을 알아보기 위한 가설이다. 앞선 선행 연구결과에서 손유승[12]과 윤덕상[13]은 공통적으로 교육을 중요성을 설명함과 동시에 단발성 모의훈련이 아닌 장기간의 지속적인 훈련이 효과적으로 인식을 개선할 수 있다하였다. 따라서 본 실험에서도 훈련의 반복에 따른 열람율의 변화 추이를 살펴보기로 하였다.

○ 가설1(H1) : 모의훈련의 반복 횟수에 따라서 스팸메일 열람율에 차이가 있을 것이다.

3.2.2 근무지와 관계

연구가설2(H2)는 본사와 사업소간에 스팸메일 열람율에 차이가 있을 것이라는 가설이다. 앞서 Diaz[14]는 사용자의 근무환경에 따른 보안 인식이 차이를 나타낸다고 하였으며, Vishwanath[17]는 높은 수준의 이메일로드가 있을 때 미디어 사용습관

패턴은 관련성 높은 이메일에 대한 자동 응답을 시작하는 경향이 있기에 스팸 메일에 취약하고 하였다. 인터뷰 결과, 기관 특성상 지역사무소의 경우 본사에 비해 현저히 업무강도가 낮으며 이메일 사용량이 극히 적다고 들었다. 따라서 근무 환경에 따라 업무량과 이메일 사용시간이 다르기 때문에 열람율에도 차이가 있을 것이라고 가정하였다.

○ **가설2(H2) : 근무지에 따라 스팸메일 열람율에 차이가 있을 것이다.**

3.2.3 나이와 관계

연구가설3(H3)은 임직원의 나이와 열람율과의 관계에 대한 가설이다. 앞선 Sheng[15]의 연구에 따르면, 젊은 실험 참가자가 나이든 사람에 비해 피싱 메일에 더 취약했는데, 그 이유는 젊은 나이의 실험 참가자들의 보안인식 개선을 위한 교육기간이 비교적 짧으며 사이버 공격 위험에 대한 회피성향이 적기 때문이라고 하였다. 또한 실제 기업 내에서도 직급이 낮고 어린직원의 업무량이 관리자보다 훨씬 많으므로, 나이대별 스팸메일 열람율에 차이를 보일 것이라 가정하였다.

○ **가설3(H3) : 나이대에 따라서 스팸메일 열람율에 차이가 있을 것이다.**

3.2.4 성별과 관계

연구가설4(H4)는 성별에 따른 열람율과의 관계이다. 선행 연구를 살펴보면 연구 결과는 약간씩 차이가 있지만, 공통적으로 남성과 여성의 열람율에 약간의 차이가 있음을 알 수 있다. Zarka[16]의 연구에서 여성은 남성에 비해 더 높은 빈도로 피싱메일을 열람하고 피싱 웹사이트에 정보를 제공 했는데, 이러한 차이점은 여성이 IT기술적인 면에서 교육과 지식이 비교적 부족하기 때문이라 밝혔으며, Jagatic[18]의 인디애나 대학 현장실험 연구결과에서도 성별에 따른 피싱 성공률에 차이를 보였다. 따라서 본 실험에서도 성별과 열람율에 상관관계가 있을 것이라 가정하였다.

○ **가설4(H4) : 성별에 따라서 스팸메일 열람율에 차이가 있을 것이다.**

3.3 변수정의

가장 먼저 횟수별 열람율의 관계를 알아보기 위해 모의훈련 차수(NO)를 독립변수로 선정하였으며 차수에 따라 1~7까지 순서화 하였다. 이후 인적요인 통계분석을 위해 임직원들의 민감정보 또는 고유식별정보를 제외한 훈련결과 와 관련된 직급, 근무지, 나이, 성별 등의 인적정보를 제공받은 뒤, 상관분석을 통해 수집한 변수들 간의 상관도가 없거나 낮은 항목들만(피어슨 상관계수가 0.25 이하) 선별하여 변수로 설정하고 위의 Table 1.과 같이 구성하였다.

3.4 훈련방법

3.4.1 훈련인원 및 기간

본 연구에서는 국내 한 기관의 협조를 통해 임직원을 대상으로 실험을 수행하였다. 7차수의 훈련기간 마다 실제와 같은 피싱형태의 스팸 메일을 발송하고 열람시간, 신고여부 등의 훈련결과를 수집하였으며, 실험대상은 같은 인원만 반복 시 보편적 결과를 알 수 없으며 보안인식 변화에 따른 추가적인 요소가

Table 1. Variable definition and measurement method

type	variables	definition	measurement method
independent	NO	Number of times	1~7 (1~7 time)
	WO	Workplace	1 : headquarter 2 : branch office
	AG	Personal age	2: 20's , 3: 30's 4: 40's , 5: 50's
	GE	Gender	1 : male, 2 : female
dependent	RR	Reading rate	0 : Not Read, 1 : Read

개입할 수 있어, 매회 차수별 평균적으로 약 350명을 무작위로 선정하였다.

기존 선행연구는 대부분 1~2회 내지 단발성 훈련을 실험실 환경에서 학생들을 대상으로 분석된 결과이므로 자료의 신뢰성에 의문을 제기할 수 있기에 국내 기업 실정에 적용하기가 어려웠다. 따라서 본 연구에서는 '18년 1사분기부터 '19년 1사분기 까지 약 1년간 총 7번에 걸쳐 주기적으로 훈련을 실시하여 2,500건 이상의 많은 양의 유의미한 훈련 결과 데이터를 수집하였으며 각 훈련 간에 독립성을 유지하였다.

3.4.2 훈련 시나리오

실제 훈련 시, 기본적인 스팸메일 대응훈련 평가 프로세스는 아래의 그림 Fig.2.와 같이 이뤄진다. 훈련 담당자는 정상메일로 위장한 피싱 방식의 스팸메일을 발송하고, 수신자는 해당 메일을 열람하지 않으면 훈련에 성공한 것으로 구분한다. 단, 훈련 메일을 열람했다 하더라도 제한 시간 내에 정보보안 담당자에게 열람 사실을 신고 할 경우 성공으로 간주한다.

모든 훈련이 종료되면, 자체 구축한 스팸메일 대응훈련 시스템을 통해 자동으로 로그를 수집하여 최종 결과를 확인한다. 하지만 본 연구에서는 이러한 모의훈련의 성공여부에 목적을 두지 않았으므로, 중간 과정인 훈련 대상이 스팸메일을 열람했는지의 사실관계만을 가지고 향후 분석을 진행한다.

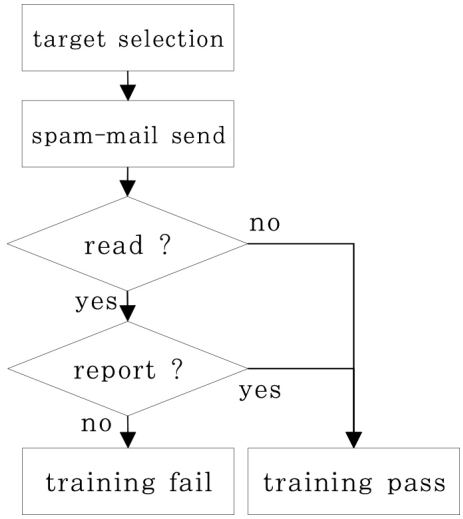

Fig. 2. mail-training process

IV. 분석결과

Table 2. sample status

definition		frequency	percent
Reading rate	Not read	2.408	93.3
	read	174	6.7
gender	male	2.270	87.9
	female	312	12.1
age	20's	349	13.5
	30's	625	24.2
	40's	980	38.0
	50's	628	24.3
workplace	headquater	849	32.9
	branch office	1.733	67.1
number of times	1st	351	13.6
	2nd	409	15.8
	3rd	324	12.5
	4th	370	14.3
	5th	385	14.9
	6th	373	14.4
	7th	371	14.4
sum		2.582	100.0

4.1 훈련결과 분석

4.1.1 표본현황

총 7차에 걸친 훈련결과를 종합 수집한 뒤, 훈련기간 동안 퇴사, 징계 등의 사유로 인사정보가 변경된 인원 등을 제외하고 유효 데이터만을 추려낸 결과, 훈련 대상 총 인원은 2,582명이며 전체 열람결과와 성별, 나이대별, 근무지별, 횟수별 상세내역은 아래의 표 Table 2.와 같다.

4.1.2 횟수별 특성

먼저 별도의 통계프로그램을 사용하지 않아도 추세를 한눈에 알아보기 위하여 훈련 횟수와 열람인원, 열람율의 관계를 아래의 Fig.3.과 같이 그래프를 통해 나타내었다. 그래프를 살펴보면 빨간색 선은 열람한 인원수를, 파란색 선은 열람율을 나타내며 차수가 더해질수록 열람율과 열람인원이 모두 감소하는 추세임을 한눈에 알 수 있다. 이는 주기적이고 반복적인 훈련이 임직원들로 하여금 보안인식 개선에 긍정적으로 영향을 미쳐 스팸메일 열람 감소라는 효과적인 교육결과를 나타낸 것으로 보인다.

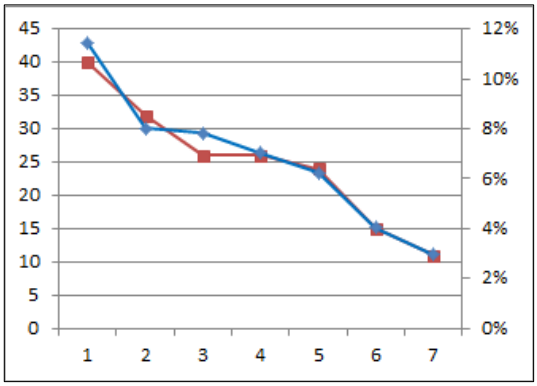

Fig. 3. Reading rate graph

4.1.3 주제별 특성

본 연구는 매 훈련을 진행하면서 많은 임직원들을 속이기 위해서 메일제목과 주제를 각각 다르게 선정하여 시행했다. 메일제목은 크게 나눠서 범죄, 여가, 금융, 사회이슈, 개인생활 등 5가지로 분류하여 매회 같은 비율로 훈련메일을 발송하였다. 하지만 수신자가 미열람하고 완전 삭제한 메일에 관해서는 기관 내 시스템에도 자료를 저장하지 않아 발송된 자료의 정확한 모수를 통계로 나타내기 곤란하여, 아래의 표 Table 3.를 통해 비교하고자 한다. 즉 5가지 주제의 동일한 비율로 발송된 메일의 열람인원을 살펴보면, 범죄에 관련된 부분이 34%로 가장 높은 비율을 차지하고 있으며, 여가와 금융이 뒤를 따른다. 범죄와 관련된 주제인 경우 Wang[19]의 연구결과처럼 대부분 긴급성을 요하기 때문에 수신자로 하여금 스팸메일에 대한 판단력을 흐리게 만들어 쉽게 클릭하게 된다고 여겨진다.

Table 3. reading rate by topic

Topic	Number of reader	Rate
crime	60	34%
leisure	50	29%
finance	30	17%
social issue	25	14%
personal life	9	5%
sum	174	100%

4.2 연구가설 검증

4.2.1 검증방안

표본수집은 1년간 7회의 스팸메일 대응훈련 시행결과로 얻어진 데이터와 기관 인사정보를 기반으로 하였으며, 각 변수간의 관련성을 구하고자 SPSS21 통계프로그램을 이용하여 연구에 활용하였다. 연구가설1(H1)부터 4(H4)를 검증하기 위해 각 독립변수와 종속변수간의 상관관계가 있음을 규명하기 위하여 H1을 제외한 나머지 가설은 단순 교차분석을 실시하였으며, H1은 별도로 선형분석을 실시하였다. 이어 가설을 모두 검증하고, 마지막으로 인과관계 분석을 위해 회귀분석을 수행한 결과도 살펴보고자 한다.

4.2.2 횟수별 관계 분석

횟수별 열람율의 감소는 위의 그래프에서 확인했으나, 선형분석 결과를 통해 재확인 하고자 한다. 아래의 표 Table 4.에 따르면 유의확률이 0으로 유의미한 결과를 나타내었으며, 분석결과 음의 영향을 미친다는 것을 알 수 있다. 즉, 모의훈련 횟수를 반복할수록 스팸메일 열람율은 적게 나타난다는 것을 나

Table 4. Linear analysis result

	coefficient		t	p
	B	Beta		
(constant)	.116		10.570	.000
Number of times	-.012	-.098	-4.979	.000

타낸다.

4.2.3 근무지별 관계 분석

근무지와 열람율의 관계를 나타내기 위해 교차분석(카이제곱 검정)을 시행한 아래의 결과표Table 5.를 보면, 유의확률은 0으로 유의미한 결과를 보이며 이는 근무지와 열람율에 관계가 있음을 시사한다. 또한 본사(10.5%)가 지역 사무소(4.9%)에 비해 2배의 열람율을 보였다.

Table 5. Analysis result by workplace

Workplace		No Read	Read	x^2	p
headquater	N(%)	760 (89.5%)	89 (10.5%)	28.212	.000
branch office	N(%)	1648 (95.1%)	85 (4.9%)		

4.2.4 나이별 관계 분석

나이대와 열람율 간의 관계검증을 위한 분석 결과는 아래의 표Table 6.과 같으며, 유의확률은 0으로 유의미한 결과를 보인다. 나이대와 열람율간에는 관계가 있으며, 나이가 많을수록 열람율이 낮아지는 것을 볼 수 있다. 이는 어린 직원들의 경우 위험회피 성향이 낮기 때문으로 볼 수 있다.

Table 6. Analysis result by age

Age		No Read	Read	x^2	p
20's	N(%)	296 (84.8%)	53 (15.2%)	53.966	.000
30's	N(%)	576 (92.2%)	49 (7.8%)		
40's	N(%)	935 (95.4%)	45 (4.6%)		
50's	N(%)	601 (95.7%)	27 (4.3%)		

4.2.5 성별 관계 분석

성별과 열람율 간의 관계검증을 위한 분석 결과는 아래의 표 Table 7.과 같으며, 유의확률은 0.05미만으로 유의미한 결과를 보인다. 성별과 열람율 간에는 관계가 있으며, 여성이 남성에 비해 스팸메일 열람율이 약간 더 높은 것을 볼 수 있다. 정확한 사회심리적 원인을 파악할순 없으나, 대다수를 차지하는 기술직에 여성의 비율이 극히 적다는 점을 들어 IT 기술지식의 부족에 기반한 것으로 보인다.

Table 7. Analysis result by gender

Gender		No Read	Read	x^2	p
male	N(%)	2127 (93.7%)	143 (6.3%)	5.771	.016
female	N(%)	281 (90.1%)	31 (9.9%)		

4.3 검증결과

4.3.1 가설 검증결과

앞서 수립한 연구가설1(H1)부터 가설4(H4)까지의 전체 상관관계 분석 결과는 아래의 표 Table 8.와 같이 채택되었다. 각 변수들간의 상관계수는 모두 0.25 이하로 낮다고 볼 수 있으며, 따라서 스팸메일 모의훈련 시 훈련횟수, 임직원의 나이, 성별, 근무지는 직원들의 스팸메일 열람률과 상관관계가 있다는 것을 확인 하였다.

Table 8. Result of research hypothesis

Hypothesis	Pearson Co.	P	result
H1	-.098**	.000	Accept
H2	-.105**	.000	Accept
H3	-.128**	.000	Accept
H4	.047*	.016	Accept

4.3.2 영향도 분석

앞선 가설 검증과 상관관계 분석 결과를 바탕으로, 변수간의 인과관계를 규명해보기 위해 다중회귀분석을 실시한 결과는 아래의 표Table 9.과 같다. 표를 살펴보면 성별의 유의확률은 높기 때문에 성별의 인과관계는 무의미하다 볼 수 있으나, 나머지 변

수들은 유의확률과 공선성 진단을 만족해 통계적으로 타당한 인과관계를 가진다고 볼 수 있다. 즉 차수가 높을수록, 나이대가 많을수록, 사업소에 근무할수록 스팸메일 열람율이 낮아졌다고 해석할 수 있다.

Table 9. Regression analysis result

	coefficient		t	p	VIF
	B	Beta			
(constant)	.284		6.510	.000	
NO	**-.013**	-.100	-5.174	**.000**	1.004
GE	.005	.007	.354	.724	1.086
AG	**-.029**	-.111	-4.921	**.000**	1.367
WO	**-.049**	-.092	-4.482	**.000**	1.132

V. 결 론

5.1 연구결과 및 시사점

그동안 스팸메일 공격에 취약한 인적요인에 대한 연구과 임직원의 보안인식 개선을 통한 기업 보안수준 향상에 대한 연구가 다양하게 많이 이루어져 왔지만, 대부분의 국내연구는 이론적 연구에 그쳤으며 국외의 경우 교육기관을 중심으로 단발성 실험에 그쳐 국내 기업의 현실에 맞지 않는다는 문제점이 있었다.

반면 본 연구는 위의 한계점을 극복하고자 실제 국내기업에서 근무하는 임직원들을 대상으로 약 1년에 걸쳐 장기적 모의훈련을 수행하고 결과를 수집하였다. 또한 기존의 선행 연구결과처럼 지속적 훈련을 통한 인식개선이나 취약한 인적요인이라는 각각의 별개 주제들을 융합하여 연구하였으며, 열람에 취약한 주제에 대한 조사결과 분석 등 새로운 연구 분야 제시에 관한 학술적 의의가 있다.

또한, 스팸메일 모의훈련 프로세스 역시 실제 공격방식과 동일한 조건과 방식의 환경을 구성함으로써 현실성 있는 현장실험 결과를 수집하였으며, 반복적 훈련을 통해 임직원들의 보안인식 향상을 꾀하였다. 즉 단순히 훈련 성공율을 높이는 것에 목적을 두지 않고 실제로 기업에 도움이 되는 연구를 수행하며, 훈련결과를 분석하고 취약점을 찾아내 개선방향을 제시하는데 목적을 둠으로써 실무적으로 기여하였다.

본 연구의 가설은 모두 채택되어 횟수, 나이, 근무지, 성별은 열람율과 상관관계를 지녔으며, 이 중 성별을 제외한 나머지 변수는 종속변수와 음(-)의 관계를 나타냈다. 타당성 확보를 위해 총 2,582건의 결과값을 가지고 다양한 통계분석을 실시하였으며(교차분석, 선형분석, 상관분석, 다중회귀분석 등), 연구 결과에 따른 효율적 모의훈련 개선방향을 다음과 같이 제시한다.

첫째, 외부 평가 등에 의한 단발성 훈련보다는 체계적이고 반복적인 모의훈련을 통해 임직원들의 인식을 개선한다. 연간 1~2회에 걸친 휘발성 훈련이 아닌 정기적으로 장기간 훈련을 시행 할 때 더 많은 인원들에게 스팸메일 대응에 대한 인식을 각인 시킬 수 있고 이는 열람율의 감소로 이어질 수 있었다. 단, 지나치게 잦은 훈련은 앞선 연구결과처럼 기업의 임직원들로 하여금 보안스트레스의 상승과 연관되므로, 사전에 취지를 잘 설명하고 전사적 공감을 얻는 것이 무엇보다 중요하다고 할 수 있다.

둘째, 젊은 직원에 대한 보안 교육을 강화해야한다. 기본적으로 젊은 직원들은 인터넷 사용이 익숙한 세대임에도 불구하고, 회사 내에 사이버 공격에 대한 실제 경험이 더 부족하며 위험을 감수하려는 성향으로 스팸메일을 쉽게 클릭하는 경향이 있었다. 따라서 보안 교육 담당자는 해당 결과를 바탕으로 훈련 또는 교육에 반영하여, 입사 시 신입사원 보안교육의 필수화 또는 진급시험 시 보안관련 문제출제 등의 방식으로 적용할 수 있을 것이다.

셋째, 모의훈련 시 훈련 대상을 세부적으로 분류하고 결과에 대해 상세히 분석해야 한다. 연구 결과에 따르면 기존 예상과 반대로 본사에 근무하는 직원이 오히려 사업소에 근무하는 직원보다 스팸메일 열람율이 높은 것으로 나타났는데, 이는 업무특성상 사업소 직원의 메일 접속률 자체가 현저히 낮았기 때문에 생긴 현상 이였다. 즉 열람율 자체가 보안 의식수준을 의미하지 않는다는 것과 기업의 환경적 특수성을 고려해야 하며, 인과관계에는 나타나지 않았으나 성별 역시 상관관계를 나타내므로 보안 실무자는 교육 또는 훈련 계획수립 시 이러한 다양한 인적특성을 고려하는 것이 좋다.

전체 직원에 대한 일괄적인 집체 보안교육을 수행하는 구시대적인 교육방식에서 벗어나, 비단 메일훈련이 아니라도 악성코드 감염, 침해사고 분석 등의 다양한 방법을 통해 기관 내 취약한 인적요인을 분석하고 조치하는 것이, 기반시설을 운영하는 기관의 보안업무 담당자로 향후 지능화된 공격에 선제적 대응을 위해 중요하다.

5.2 한계점 및 향후 연구방안

본 연구는 모의훈련을 통해 수집한 데이터를 사용하여 임직원들의 스팸메일 열람율을 분석하고 그 결과와 시사점을 제시한 연구로써 몇 가지 한계점이 있었다. 가장 먼저 훈련을 수행하고 결과를 수집하는 과정에서 개인정보 보호법 준수와 정보통신기반보호법, 기업비밀 등으로 수집 가능한 자료에 대한 한계가 있었으며, 이는 모든 인적요인과 메일 송수신 내역 분석을 통해 세그먼트별 공격에 취약한 주제를 분석코자 했던 초기 목적을 이루기 어려웠다. 또한 단순 열람에 대한 연구가 아닌 전체 훈련으로 시야를 확장시켜 열람여부와는 별도로 훈련을 성공하고 실패하게 만드는 원인에 대한 분석도 불가능 하였다. 하지만 실제 기업을 대상으로 학술적 목표를 가지고 훈련을 수행하였으며, 임직원의 기본 인적정보를 가지고 가설을 검증함으로써 단순 이론적 연구에 그치지 않았다는 점과, 개선방안 제시를 통해 향후 각 기관의 모의훈련 수행 시 참고할 만한 유의미한 결과를 나타낸 점에서는 의의가 있다고 여겨진다.

또한 향후 보안정책 및 인식 개선분야에서 정기적 교육과 훈련의 실효성을 연구함과 더불어, 스팸메일의 어떠한 주제들이 사용자의 열람행동에 사회심리학적으로 영향을 미치는지에 대한 융합 연구가 진행될 수 있다. 앞으로도 이러한 현장실험 연구가 계속되어 공공기관 뿐만 아니라 많은 기업의 모의훈련의 실효성을 증대시키고, 학술적으로도 보안인식 개선방안에 대한 다양한 연구가 이루어지길 기대한다.

References

[1] NIS, government etc. "National Information security white paper", 2018.

[2] KISA, "Cyber Security Issue Report 1Q", Apr. 2019.

[3] Korea Communications Commission, "Information Networking Guide for Anti-Spam Protection," Sep. 2015.

[4] Lee doyeon, "The Effect of Punishment and Training on Information Security Policy Compliance Behavior: The Empirical Analysis through Field Experiments," master dissertation, yonsei university, Dec. 2017.

[5] proofpoint, "understanding email fraud," https://cdw-prod.adobecqms.net/content/dam/cdw/on-domain-cdw/brands/proofpoint/survey-of-understanding-email-fraud.pdf, Jan. 2018.

[6] Ahnlab, "How to avoid persistent spear phishing!,"https://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?curPage=1&menu_dist=2&seq=21905&dir_group_dist=0,Dec. 2013.

[7] Kim kyoungah, "The beginning of APT attack Knowing Spear Phishing," https://www.boannews.com/media/view.asp?idx=38916, Dec. 2013.

[8] NIS, "National Information Security Basic Guidelines", 2018.

[9] Moon gunwoong, "Relationship between information security activities of enterprise and infringe : the center of effects of information security awareness," master dissertation, korea university, Jun. 2017.

[10] Burcu Bulgurcu, Hasan Cavusoglu, and Izak Benbasat "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness," MIS Quarterly Vol.34 , no. 3, pp. 523-548, Sep. 2010.

[11] Lim chaeho, " Effective information protection awareness plan", Journal of Information Security, 16(2), pp. 30-36, Apr. 2006.

[12] Sohn Yu-Seung, Nam Kil-Hyun, and Goh Sung-Cheol, "On the administrative security approaches against spear phishing attacks", J. Korea Inst. Inf. Commun, Vol.17, No.12, pp. 2753-2762, 2013.

[13] Yoon Duck-sang, Lee Kyung-ho, and Lim Jong-in, "A Study on the Change of Capability and Behavior against

Phishing Attack by Continuous Practical Simulation Training," Vol.27, No.2, pp. 267-279, Apr. 2017.
〔14〕 Alejandra Diaz, Alan T. Sherman, and Anupam Joshi, "Phishing in an Academic Community: A Study of User Susceptibility and Behavior," cornel univ, arXiv:1811.06078, Nov. 2018.
〔15〕 S. Sheng, M. Holbrook, P. Kumaraguru, L.F. Cranor, and J. Downs, "Who Falls for Phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions," Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 373-382, Apr. 2010.
〔16〕 Jamshaid G. Mohebzada, Ahmed El Zarka, Arsalan H. Bhojani, and Ali Darwish, "Phishing in a university community: Two large scale phishing experiments," 2012 International Conference on Innovations in Information Technology (IIT), Mar. 2012.
〔17〕 Arun Vishwanath, Tejaswini Herath, Rui Chen, Jingguo Wang, and H.R. Rao "Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model," Decision Support Systems archive, Vol. 51, no.3, pp. 576-586, June, 2011.
〔18〕 Tom N. Jagatic, Nathaniel A. Johnson, Markus Jakobsson, and Filippo Menczer, "social phishing," Communications of the ACM, Vol. 50, No. 10, pp 94-100, Oct. 2007.
〔19〕 Jingguo Wang, Tejaswini Herath, Rui Chen, Arun Vishwanath, and H.R. Rao, "Phishing Susceptibility: An Investigation Into the Processing of a Targeted Spear Phishing Email," IEEE Transactions on Professional Communication, Vol.55, no.4, pp. 345 - 362, Aug. 2012.

〈저자소개〉

이 준 희 (Jun-Hee Lee) 정회원
2014 2월 : 한국항공대학교 정보통신과 졸업
2018 3월~현재 : 고려대학교 정보보호대학원 석사과정
〈관심분야〉 정보보호 정책, 보안인식, 보안교육

권 헌 영 (Hun-Yeong Kwon) 종신회원
1992년 2월: 연세대학교 법학과 졸업
1998년 2월: 연세대학교 법학과 석사
2005년 2월: 연세대학교 법학과 박사
2015년 9월~현재: 고려대학교 정보보호대학원 교수
〈관심분야〉 정보보호법 및 정책, 정보통신법 및 정책, 사이버법률, 인터넷규제, 전자정부