악성 이메일에 대한 안전한 대응의 효과성 연구

[1]이태우, [2*]장항배

A Study on the Effectiveness of Secure Responses to Malicious E-mail

[1]Taewoo Lee, [2*]Hangbae Chang

요 약

이메일은 일상생활에서 사람들과 커뮤니케이션하는데 중요한 도구 중 하나이다. COVID-19(코로나바이러스)로 비대면 활동이 증가하면서 스팸메일, 피싱, 랜섬웨어 등과 같은 이메일을 통한 보안사고가 증가하고 있다. 이메일 보안사고는 이메일이 가지고 있는 기술적인 취약점으로 발생하는 것보다는 사람의 심리를 이용한 사회공학적 공격으로 증가하고 있다. 사람의 심리를 이용한 보안 사고는 보안 인식 개선을 통해 예방과 방어가 가능하다.

본 연구는 국내외 기업 임직원을 대상으로 악성 이메일 모의 실험을 통해 보안 인식 개선으로 악성 이메일에 대한 대응 변화 분석을 실증적 연구하였다. 본 연구에서 보안교육, 상향식 보안 관리, 보안 이슈 공유의 요인은 악성 이메일을 안전하게 대응하는데 효과가 있음을 확인하였다.

본 연구는 보안 인식에 대한 이론적 연구 내용을 악성 이메일 대응과 관련하여 실증적 분석을 실시하여 새로운 연구를 제시해 학술적 의의가 있으며, 실무 환경에서 모의 실험으로 얻어진 결과는 보안담당자에게 업무 하는데 실무적으로 도움을 줄 수 있을 것이다.

Abstract

E-mail is one of the important tools for communicating with people in everyday life. With COVID-19 (Coronavirus) increasing non-face-to-face activity, security incidents through e-mail such as spam, phishing, and ransomware are increasing. E-mail security incidents are increasing as social engineering attack using human psychology rather than arising from technological weaknesses that e-mails have. Security incidents using human psychology can be prevented and defended by improving security awareness.

This study empirically studies the analysis of changes in response to malicious e-mail due to improved security awareness through malicious e-mail simulations on executives and employees of domestic and foreign company. In this study, the factors of security training, top-down security management, and security issue sharing are found to be effective in safely responding to malicious e-mail.

This study presents a new study by conducting empirical analysis of theoretical research on security awareness in relation to malicious e-mail responses, and results obtained from simulations in a practical setting may help security work.

Keywords: *Malicious mail, Security awareness, Security education, Training, Social engineering attack*

[1] *중앙대학교 융합보안학과 석사과정 (skasea@cau.ac.kr)*
[2*]*교신저자* *중앙대학교 산업보안학과 교수 (hbchang@cau.ac.kr)*

Received: May. 25, 2021, Revised: Jun. 01, 2021, Accepted: Jun. 24, 2021

I. 연구의 배경 및 필요성

IT 발전으로 인해 인터넷은 일상생활에 일부가 되었다. 인터넷을 이용하는 사람들 60.4%가 이메일을 이용하고, 이중 86.1%는 이메일을 업무적으로 활용하고 있다[1]. 즉, 일상 생활에서 이메일은 사람들과 커뮤니케이션을 하는데 중요한 도구 중 하나이다.

많은 사람들이 이메일의 이용이 늘면서 이메일을 통한 보안 사고가 꾸준히 증가하고 있다. 공공기관, 기업, 직장 상사 등을 사칭한 보안 사고는 매스컴을 통해 확인할 수 있다. 사칭 이메일은 실제 있는 기관이나 사람으로 위장하여 이메일이 발송되기 때문에 피해자의 심리를 이용한 수법을 이용하고 있다. 이러한 보안 사고가 발생되는 이유는 공격자가 보안 시스템의 취약점을 공약하여 어렵게 공격하는 것보다 쉽게 공격이 가능하고, 이메일 주소만 안다면 다양한 사람들에게 공격이 가능한 이점이 있다. 최근 COVID-19(코로나바이러스)로 인해 비대면 활동이 증가하면서 이메일을 통한 보안 사고는 '20 년 1 분기 232 백만 건으로 '19 년 4 분기 대비 36% 증가했다[2]. 이러한 보안 사고를 예방하고자 정부에는 주요 공공기관을 대상으로 연 1 회 악성 이메일 대응 훈련을 시행하고 결과를 통보하고 있다[3]. 기업 역시도 지속적인 모의 훈련을 통해 취약한 부분에 대해서는 보안 정책 준수 실천과 보안 교육 등을 통해 대응하고 있다.

악성 이메일의 위험성은 보안 사고가 이메일 이용자 자신도 모르게 이루어진다는 것이다. 이메일 이용자가 의심없이 이메일 개봉, 첨부파일 열람, 링크 클릭 시 사고가 발생한다. PC 내 악성코드 감염 및 설치로 인해 중요 데이터 및 개인정보 유출, 금전 요구 등 사회적으로 문제가 발생되고 있다.

자산을 보호하고 자산의 손실 방지하는 것을 산업 보안이라 하는데[4], 기업은 기업이 가지고 있는 독창적인 우수한 기술과 고객의 개인정보를 보호하기 위한 노력을 하고 있다. 최근 발생하는 보안 공격의 유형을 보면 사람의 심리를 이용한 사회공학적 공격(Social Engineering Attack)을 포함하여 다양한 위험 요인을 융ㆍ복합적인 방법을 결합하여 활용되고 있다[5]. 점차 사람과 기술에 대한 통제력이 약화되고 있어, 기술적 보안대책 대신 인간 중심 보안 전략 필요하다[6].

중요 자산을 보호하기 위해 기업에서는 많은 노력을 하고 있다. 임직원이 보안 정책 준수 및 보안 위험 요소를 식별할 수 있는 능력을 키우기 위해 보안 인식 활동 수행을 하고 있다. 보안 인식 활동에는 여러 방법이 활용되고 있는데, 이메일에 대한 위험을 예방하고자 보안 교육 및 악성 이메일 모의훈련이 실시된다. 본 연구에서는 악성 이메일로부터 안전하게 대응할 수 있는 효과적인 방법을 모색하고자 한다.

II. 선행 연구 및 연구 주제

2.1 사회공학적 공격 및 악성 이메일

사회공학적 공격은 핵심 정보가 있는 곳을 직접 접근하는 기존 산업기술 유출 방법과 달리, 사람의 심리를 이용하여 공격자에게 직ㆍ간접적으로 정보에 접근하는 방법을 제공하게 하는 기망을 이용한 범죄이다[7]. 이러한 사회공학적 공격의 위험은 기업이 중요 자산을 보호하기 위하여 외부로부터 접근 차단하는 보안 시스템을 구축하더라도 정보에 접근하는 방법을 공격자에게 제공하기 때문에 공격에 대한 방어와 보안관리체계는 소용이 없게 된다. 공격자는 IT 시스템 취약점을 이용한 공격보다 쉽게 대량의 정보를 접근 가능하다. 대표적인 예가 이메일 피싱, 전화 사기, SNS 및 메신저를 통한 피싱, 우편물 절취 등이 있을 것이다[8].

사회공학적 공격은 4 단계를 걸쳐서 공격이 이루어진다. 공격자는 원하는 정보가 있는 공격 대상자를 선정하여 필요한 정보를 수집한다. 심리를 이용한 공격이다 보니 공격 대상자가 평소에 관심 사항이나 신분, 주변 환경 등을 분석하고 공격에 필요한 도구의 특징을 확인한다. 이후 공격자는 공격 대상자와 긴밀한 관계(Rapport)를 형성하기 위해 공격 대상이 관심 있는 사항의 콘텐츠를 이용하거나 주변 인물을 사칭하여 접근을 한다. 충분히 관계 형성을 통해 공격 대상의 의심이 없어진다면 공격자는 공격 대상에게 요구사항을 전달하여 원하는 정보를 얻거나

이행하게 만든다. 공격 대상자는 피해 사실을 인지하지 못하고 정보 유출 및 파괴 등으로 이어지는 경우가 많다. 공격자는 목적이 달성 후 정보 및 흔적을 지우고 다른 공격을 계획하여 진행하거나 공격 대상자와 관계를 끊고 새로운 공격 대상자를 찾아 새로운 공격을 진행한다.

악성 이메일은 사회공학적 공격을 이용한 경우가 많다. 이메일에 악성코드를 첨부하여 이메일 이용자가 관심이 있는 콘텐츠의 이메일을 보냈을 때 해당 이메일을 개봉한다면 보안 사고가 발생할 가능성이 높다. 즉, 사회공학적 공격은 지능화 되고, 기술적인 보안 대책을 우회하기 때문에 모든 보안 공격을 막는 데는 한계가 있다[9]. 이메일 주소만 안다면 쉽게 공격이 가능하고 많은 수의 공격 대상을 설정할 수 있어 공격자에는 매력 있는 공격방법이다. 주요 악성 이메일의 특징을 알아보고자 한다.

스팸(Spam)메일은 이메일 이용자에게 일방적으로 영리적인 목적의 광고를 보내는 것을 의미한다[10]. 일방적으로 보내지기 때문에 이메일 수신자는 직 · 간접적으로 피해가 발생하고 있다. 최근 COVID-19 로 인해 불법 대출 및 주식 등의 금융 광고 이메일이 증가하고 있어[11], 사람들이 관심있는 내용으로 대량으로 발송하고 있다. 피싱(Phishing)은 공격자가 공공기관이나 금융기관 등으로 사칭하여 공격 대상자가 개인정보 및 금융정보 등의 입력 또는 알려주어 관련 정보를 탈취하는 기법이다. 스피어 피싱(Spear-Phishing)은 피싱과 같은 원리로 공격하지만 구체적인 공격 대상을 지정한다는 특징이 있다. 그렇기 때문에 공격 대상자가 PC 에서 자주 사용하는 문서 파일이나 압축 파일에 악성코드를 포함하여 보내거나 파일을 다운로드 받을 수 있게 링크를 발송한다[12]. 이메일 수신자가 신뢰할 수 있는 인물, 기관, 내용으로 보내 지다 보니 이메일 개봉만으로도 위험에 노출되기 쉽다. 이는 일시적인 보안사고가 아닌 APT 공격(Advanced Persistent Threats Attack)과 같은 지속적인 공격으로도 이어질 수 있어 위험성은 높다. 랜섬웨어(Ransomware)는 PC 를 잠그거나 파일을 암호화하여 자료를 이용 못하게 하여 금전을 요구하는 공격이다. 공격자는 금전적인 이익이 발생하기 때문에 랜섬웨어는 개인뿐만 아니라 기업, 공공기관에서의 보안사고가 지속적으로 발생하고 있다. 랜섬웨어 역시도 이메일에 포함된 첨부파일 및 링크 클릭으로 발생하고 있어, 이메일 이용자는 무방비 된 상태에서 공격을 받고 있다.

2.2 보안 인식

보안 인식은 보안을 이해하고 중요성에 대한 인식이며, 보안 정책 준수 등에 긍정적인 영향이 있다는 것을 확인할 수 있다[13]. 이처럼 보안 인식 향상을 위해 많은 연구가 되고 있으며, 조직의 보안에 중요한 영향을 미치기 때문에 보안 인식을 강조하고 있다[14]. 보안 인식 향상은 보안 정책 준수 및 행동의 변화를 보고 있다. 이러한 변화를 위해 보안 교육이 중요한 도구로 활용되고 있다.

보안 교육은 보안 수준 향상에 있어서 중요한 요소이며[15], 조직에서는 지속적인 노력이 필요하다[16]. 보안 교육을 통해 조직원들이 업무를 수행하는 동안 보안 절차 및 접근 통제 등의 준수를 통하여 보안 사고 방지할 수 있다[17]. 이처럼 보안 관리에 있어 취약한 인적 보안을 개선하는데 보안 교육은 활용하고 있고, 조직은 보안 정책 준수와 내부정보 유출 예방을 위해 다양한 방법으로 보안 교육을 수행하고 있다.

교육은 학습자의 관심도와 경험에 따라 습득하는 수준의 차이가 발생한다[18]. 즉, 보안 교육 역시도 학습자의 관심과 경험을 바탕으로 이루어져야 한다는 것이다. 조직에서는 다양한 직무가 있고 직무에 따라 업무 수행 방법이 다르다. 업무 수행하는 방법을 모색하고 그들이 관심이 있는 부분이 무엇인지 파악하여 맞춤식 교육을 해야한다. 직무에 따라 발생하는 보안 취약점이 무엇인지 분석하고 이를 개선할 수 있는 방법을 보안교육을 통해 이뤄져야 한다. 보안 교육을 통해 보안 정책 준수로 이어지는지 지속적인 점검이 필요하다[14].

보안 부서는 조직에서 정보자산을 보호를 위해 보안정책 수립 및 관리, 사고 예방 및 대처, 보안 인식 활동 등 다양한 활동을 수행하고 있다. 즉, 보안 부서는 보안 정책이 수립되면 조직원이 정책 준수를 할 수 있도록 다양한 활동을 수행하게 된다. 보안 사고 발생 시에도 보안 책임자를 중심으로 보안 사고 원인과 대처 방안 모색을 위해 컨트롤타워 역할을 수행한다. 사고 대응 과정에서 유관 부서와 협력이 필요하고 관련 내용은 관련 인물에게 보고 및 공유해야 추가적인 피해를 예방 할 수 있다. 이처럼 보안 책임자는 전반적인 조직의 현황을 이해하고

조직원들과 소통을 잘하는 인물이어야 한다. 이처럼 보안 책임자는 조직원이 보안 정책 준수를 할 수 있도록 전략적인 보안 활동 방향을 세우고 이행하고 있으며, 조직의 보안 보호자로서 역할을 하고 있다[19].

III. 연구 모형과 설계

3.1 연구 모형

본 연구는 앞서 선행 연구 분석을 통해 보안 인식 향상을 주는 원인을 실증적 분석을 통해 검증하고자 한다. 선행 연구 분석 결과 내용이 기업 환경에서도 부합한지 확인하고, 실무적인 검증을 하고자 한다.

보안 인식과 관련하여 선행 연구에서 확인된 원인을 통해 가설을 수립하였다. 보안 교육, 상향식 보안 관리, 보안 이슈 공유 등 3 가지 요소와 안전한 이메일 이용과의 관계를 확인해보고자 한다. [그림 1]과 같이 연구 모형을 설정하였다.

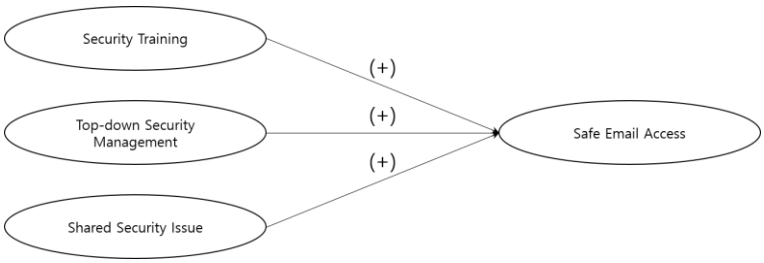

Figure 1. **Research Model Design**

보안 인식 향상을 위한 활동인 보안교육, 상향식 보안 관리, 보안 이슈 공유를 변수로 삼았고, 이 독립변수들이 안전한 이메일 이용에 어떻게 영향을 미치는지 연구를 하고자 한다. 보안 인식 향상은 보안 정책 준수로 이어진다[13]는 선행 연구를 바탕으로, 대부분의 조직에서 '이메일을 업무적으로 사용하고 안전하게 사용해야 한다'는 규정이 있기 때문에 이메일을 안전하게 이용하는 것을 보안 정책 준수로 간주할 것이다.

3.2 연구가설

3.2.1 보안 교육과 관계

연구가설 1 은 보안 교육과 안전한 이메일 이용과의 관계를 알아보는 가설이다. 앞서 선행 연구를 통해 보안 인식 향상을 위해서는 보안 교육이 중요한 요소라 확인하였다[15]. 또한 피싱 이메일 대응에 있어서도 교육과 실전형 훈련이 지속적으로 되어야만 도움이 된다고 하였다[20]. 이처럼 보안 교육이 보안 인식 향상으로 이어져 안전한 이메일 이용을 하게 될 것이라고 가정하였다.

보안 교육은 이메일 이용 취약자를 대상으로 단순 보안 지식 전달이 아닌, 일반적 보안 내용과 이메일 이용 시 주의사항 및 보안 사고 내용을 전달하여 위험성 등을 안내할 것이다. 이메일 이용 취약자는 단순 이메일 개봉이 아닌, '메일 개봉 + 링크 클릭' 또는 '메일 개봉 + 첨부파일 개봉'을 수행한 인원을 대상으로 집계한다.

(가설 1) 보안 교육은 안전한 이메일 이용에 정(+)의 영향을 미칠 것이다.

3.2.2 상향식 보안 관리와 관계

연구가설 2 는 상향식 보안 관리와 안전한 이메일 이용과의 관계를 알아보는 가설이다. 보안 책임자는 조직의 자산을 보호하기 위하여 보안관리체계 수립 및 운영, 외부로부터 보호하기

위한 자산의 위험 분석 및 보완 활동을 수행하는 역할을 가진다. 보안 책임자는 조직의 경영진 관심으로 보안 활동을 수행한다면 보안 정책 준수의 긍정적인 효과가 있다고 본다[21, 22]. 상향식(Top-down) 방식은업무를 추진하는 빠른 의사 결정과 복잡한 이해 관계를 최소화할 수 있다는 장점이 있다[23].

이처럼 보안 책임자가 빠른 시일 내 보안 인식 강화를 위하여 상향식 관리와 경영진의 관점에서 보안 관리를 운영하게 될 때 조직원의 인식 변화를 알아보고자 한다. 상향식 관리를 위해 보안 책임자는 각 부서장들과 긴밀히 소통하고 보안 위험성 및 이메일 이용 취약 인원의 관리 요청을 한다. 더불어 경영진의 관점에서 보안 사고 등으로 인해 발생할 수 있는 문제점을 충분히 설명할 것이다. 이를 바탕으로 이메일 취약 인원이 소속되어 있는 부서의 취약 인원 추이를 확인하고자 한다.

(가설 2) 상향식 보안 관리는 안전한 이메일 이용에 정(+)의 영향을 미칠 것이다.

3.2.3 보안 이슈 공유와 관계

연구가설 3 은 보안 이슈 공유에 따른 안전한 이메일 이용의 차이를 확인하는 가설이다. 안전은 적절한 시간에 위험을 감지하고 적기 대응이 필요하다. 중요한 시기에 빠른 대응을 통해 생명 및 피해 등의 확산을 막기 위한 시간을 골든 타임(Golden Time)이라 한다[24]. 보안 역시도 보안 사고 발생 시 더 큰 피해를 예방하고 적절한 조치가 있을 때 추가적인 피해가 없을 것이다. 하지만 현실은 그 시간을 놓치는 경우가 많다. 외국계 보안회사 Verizon 에 따르면 84%가 보안 사고 발생 후 1 시간 내 기업의 피해가 발생하지만 1 시간 내 사고를 인지하는 기업은 9% 밖에 없다[25]. 이처럼 보안 이슈 시 즉각 감지하고 조치가 필요하다.

보안 부서의 역할 중 보안 사고 대응이 있다. 사고에 대한 원인 분석도 중요하겠지만 2 차적인 피해가 발생하지 않도록 관련 내용을 관련 인물들에게 빠르게 공유할 필요가 있다. 사고에 대한 범위 및 영향에 따라 조금씩 공유해야 하는 사람은 달라지겠지만, 알아야 하는 사람에게는 빨리 공유를 해야 한다. 악성 이메일의 경우도 다르지 않다. 악성 이메일이 조직 내 유입되고 이를 보안 부서에서 인지하고 이메일 이용자에게 공유한다면 실제 경험을 통한 보안 인식 향상으로 이어질 수 있을 것이다. 보안 이슈 공유로 이메일 취약 인원의 변화를 확인하고자 한다.

(가설 3) 보안 이슈 공유는 안전한 이메일 이용에 정(+)의 영향을 미칠 것이다.

위 가설은 악성 이메일 모의훈련을 통해 실증적 연구를 통하여 결과 값에 대한 데이터를 분석하고 안전한 이메일 이용과 관련하여 시사점을 도출하고자 한다.

3.3 변수 정의

보안 교육에 따른 안전한 이메일 이용과의 관계를 알아보기 위해 보안 교육 참석(TR)를 독립변수로 선정하였다. 상향식 보안 관리를 통해 이메일을 안전하게 이용하는지 확인을 위해 상향식 보안 관리 수행(TS)를 독립변수로 정하였다. 보안 이슈 공유(SH) 역시도 독립 변수로 정하였다. 더불어 보안 인식 변화를 안전한 이메일 이용으로 판단하여 이메일 이용 취약 여부로 판단하였다. 선정된 변수는 [표 1]과 같이 변수를 정의하였다.

Table 1. Variable definition and measurement method

Variables	Definition	Measurement Method
TR	Security Training	1 : Participated, 2 : Not participated
TS	Top-down Security Management	1 : Management, 2 : Not Management
SH	Shared Security Issue	1 : Shared, 2: Unshared
SM	Safe Mail Access	1 : Unvulnerable, 2: Vulnerable

3.4 훈련 방법

A 기업의 임직원, 협력사 인력, 해외 법인 인력 대상으로 악성 이메일 모의훈련을 실시하였다. '20 년 2 분기부터 분기별로 총 4 차례 악성 이메일 모의훈련을 실시하였으며, 이메일은 실제 악성 이메일로 유입된 내용, 이메일 이용자가 관심이 있거나 사회적으로 이슈가 있는 내용, 업무적으로 이메일로 주고받은 내용을 각색하여 실제 이메일과 유사하게 첨부 파일과 링크를 포함하여 발송하였다. 이메일 내용을 충분히 이해 할 수 있도록 이메일을 받는 임직원이 사용하는 언어 또는 영어로 제작하여 발송하였다. 훈련 마다 약 4,900 여 명에게 악성 이메일을 발송하여 실험하였다. 휴직 및 퇴직으로 인해 근무하지 않은 인원은 제외하여 실제 근무하는 인원을 대상으로 분석하였다. 훈련 마다 조금의 차이는 있으나, 실제 분석했던 인력은 약 4,400 ~ 4,600 여 명을 분석하였다.

훈련은 모든 임직원에게 이메일 이용자가 이해할 수 있도록 악성 이메일을 제작하여 발송하였다. 이메일 이용자의 행동에 따라 이메일 개봉, 링크 클릭, 첨부파일 개봉 여부를 이메일 발송 시스템에 행위 여부와 시간을 자동으로 기록하게 하였다. 훈련 종료 후 기록 내용을 가지고 분석하였다. 단순히 이메일 개봉만 가지고 분석한 것이 아니라 이메일 이용 취약자는 '메일 개봉 + 링크 클릭' 또는 '메일 개봉 + 첨부파일 개봉'을 수행한 인원을 대상으로 분석하였다.

IV. 연구 결과

본 연구의 결과는 연구 모형 및 연구 가설을 기반으로 악성 이메일 모의훈련을 통해 나온 결과 값을 분석하였다. 유의미한 결과 값만 가지고 분석하였으며, 직급, 연령 등 인구통계학적으로 유의하게 나타나지 않아 별도 분석은 하지 않았다.

연구한 결과는 SPSS 프로그램을 이용하여 독립변수와 종속변수 간의 상관관계를 확인하기 위하여 교차분석을 실시하였다.

Table 2. Status of participation in experiments

Experiment	Number of malicious mails sent	Number of Effective Cases (Effective Ratio)
Q2-2020	4,907	4,450 (90.7%)
Q3-2020	4,903	4,497 (91.7%)
Q4-2020	4,926	4,450 (92.4%)
Q1-2021	4,961	4,631 (93.3%)

4.1 보안 교육과 관계 분석

본 연구는 국내 인력 '20 년 2 분기의 이메일 이용 취약 인원을 대상으로 매 분기 훈련 시 이메일 이용 취약 현황을 분석하였다. '20 년 2 분기 취약 인원은 3 분기 전에 보안 교육에 참여하도록 하였다. 이후 4 분기에서도 취약 인원으로 선정되면 또 보안 교육에 참여하게 하였다.

보안 교육을 통해 이메일 이용 취약 인원은 낮아지는 추이를 확인할 수 있어, 악성 이메일에 대한 안전한 대응의 효과가 있다. '20 년 2 분기(100%), '20 년 3 분기(24.9%), '20 년 4 분기(33.3%), '20 년 4 분기(8.7%) 변화된 추이를 보면 보안 교육 수행했을 때 크게 낮아지는 효과를 얻고 있다.

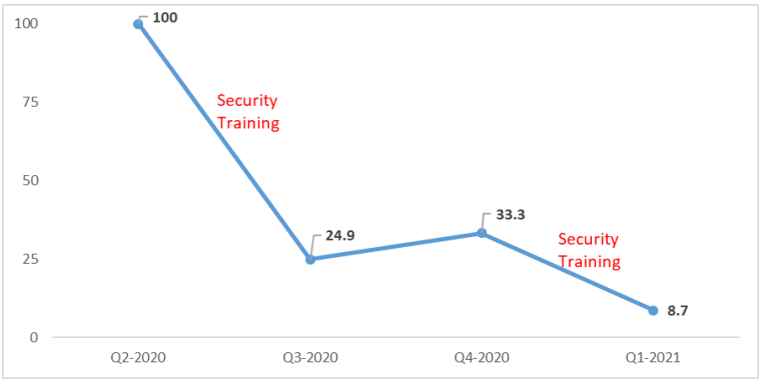

Figure 2. Trends in changes in the number of vulnerable people using mail

'20 년 4 분기 결과를 보면 3 분기 대비 취약율이 상승한 결과를 확인할 수 있다. 이는 보안 교육이 일회성으로 끝나면 일정 시간 지나면 보안 인식이 낮아진다고 볼 수 있다. 반대로 지속적으로 보안 교육을 했을 경우, '21 년 1 분기 결과와 같이 취약율이 낮아지거나 유지할 수 있다.

보안 교육과 안전한 이메일 이용에 대한 상관관계를 분석하기 위하여 교차분석을 실시하였다. 교차분석 결과는 [표 3]와 같이 $\chi^2(1, n = 7,671) = 36.387$, $p = .001$ 로 0.05 미만이므로 유의미하게 나타났다. 즉, 보안 교육과 안전한 대응은 상관관계가 있다는 것을 의미한다.

Table 3. Cross-analysis results based on security training

Participation in training	Not vulnerable	Vulnerable	$\chi 2$	Significant Probability
Participated in Q2-2020	296 (95.8%)	13 (4.2%)	36.387	.001
Not participating in Q2-2020	3,448 (97.6%)	86 (2.4%)		
Participated in Q4-2020	869 (99.3%)	6 (0.7%)		
Not participating in Q4-2020	3,058 (99.0%)	31 (1.0%)		

4.2 상향식 보안 관리와 관계 분석

본 연구는 상향식 보안 관리가 보안 인식 변화를 확인하기 위한 실험이다. 국내 '20 년 4 분기 이메일 이용 취약 인원 중 이전 훈련에서도 이메일 이용 취약으로 분류된 인원이 있는 부서를 대상으로 하였다. 보안 부서장은 취약 인원이 소속되어 있는 부서장에게 취약 인원을 공유하고 안전한 이메일 이용을 할 수 있도록 관리 요청하였다. 또한 취약 인원과 함께 소속 부서장도 '21 년 1 분기 전까지 보안 교육을 함께 참석하도록 하였다. 단, 부서장이 취약 인원으로 포함되어 있을 경우, 취약 인원 당사자에게 안내하는 것이므로 본 연구에서는 제외하였다.

'21 년 1 분기의 모의 훈련 결과는 전체 인원 4,632 명 중 254 명(5.5%)가 이메일 이용 취약 인원으로 나타났다. 상향식 보안 관리를 받는 조직은 1,323 명 중 68 명(5.1%)로 전체 취약율보다 낮은 수치를 나타냈지만, 인원이 적은 부서의 경우 효과성을 확인하기 어려워 부서원이 40 명 이상의 부서만 [표 4]과 같이 결과를 나타내었다.

[그림 3]를 확인하면 대부분의 부서에서는 '20 년 4 분기보다 취약율이 낮아졌다. 이는 앞에서 연구했던 보안 교육의 효과와 상향식 보안 관리가 함께 유의미하게 적용되었다. 하지만 인원이 많은 부서에서는 전체 취약율 평균보다 높게 나타나고 있다. 이는 부서원이 많은 조직에서는 부서장이 모든 부서원을 통제할 수 없기 때문에 인적 보안 관리의 한계가 있다는 것이다. 이를 극복하기 위해서는 앞에서 언급하였듯이 보안 교육을 지속으로 수행하고 임직원이 참여할 수 있는 보안 관리 방법이 필요하다. 취약율이 높거나 부서장이 통제할 수 있는 부서에서는 효과가 있다. 하지만 너무 큰 조직에서는 한계점이 있고, 관리가 용이하지 않다. 전체 취약율과 상향식 보안 관리 부서의 취약율이 비슷한 수치를 나타내고 있어 통계 분석은 생략하도록 하겠다.

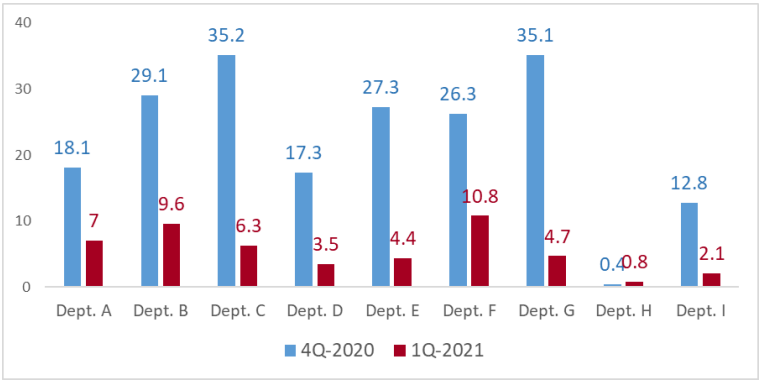

Figure 3. Comparison of changes in the number of vulnerable people using mail by department

Table 4. Study 4.2 Experimental Results

Department	4Q-2020		1Q-2021	
	Training people	Vulnerable people (Rate)	Training people	Vulnerable people (Rate)
A	94	17 (18.1%)	100	7 (7.0%)
B	55	16 (29.1%)	52	5 (9.6%)
C	54	19 (35.2%)	48	3 (6.3%)
D	52	9 (17.3%)	57	2 (3.5%)
E	44	12 (27.3%)	45	2 (4.4%)
F	190	50 (26.3%)	195	21 (10.8%)
G	37	13 (35.1%)	43	2 (4.7%)
H	244	1 (0.4%)	245	2 (0.8%)
I	47	6 (12.8%)	48	1 (2.1%)

4.3 보안 이슈 공유와 관계 분석

본 연구는 보안 부서의 역할에 따른 보안 인식 변화를 확인하는실험이다. 보안 사고 시 보안 부서에서 관련 내용을 공유했을 때 이메일 이용자의 행동 변화를 확인할 수 있었다. 악성 이메일 모의훈련 시 해외 법인 인력에게는 훈련 사실을 공유하지 않고 진행하였다. 해외 법인 보안 부서는 악성 이메일 모의훈련이라고 할지어도 악성 이메일로 간주하여 보안 사고 대응 매뉴얼따라 움직였다. 보안 사고 대응 매뉴얼에 따라 관련 내용을 최초 수집하여 사고 내용을 분석하고 비상 연락망을 활용하여 관련 인물에게 보고 및 공유를 한다. 국내는 훈련 주체이기 때문에 사고 접수만 받고 관련 내용을 임직원들에게 공유하지 않았다.

보안 이슈 공유를 통해 B 국가는 '20 년 2 분기부터 4 분기까지 총 3 차례 공유하였고, C 국가는 '20 년 2 분기부터 3 분기까지 총 2 차례 공유하였다. [그림 4]와 같이 보안 이슈 공유 시 이메일 이용 취약율은 전반적으로 낮게 확인되었다. 하지만 B, C 국가 모두 공유하지 않을 때는 상대적으로 이메일 취약 인원이 높게 나타났다.

취약율이 낮게 나타났을 때는 빠른 시간 내에 보안 부서가 보안 이슈사항을 대응했을 경우만 나타났을 것으로 추정된다. 만약 악성 이메일 유입된지 오랜 시간이 지났다면 자연스럽게 이메일 이용자는 이메일 개봉 등을 할 것이다. 즉, 보안 이슈 사항을 적절한 시간에 공유하지 않는다면 공유를 하지 않는 것과 다르지 않을 것이다. 보안에서도 골든타임이 존재한다는 것을 의미하고 적절한 시기를 놓쳤을 때 보안 사고는 확산되거나 2 차 피해가 발생할 수 있을 것이다.

보안 사고 시 보안 부서의 역할의 중요성이 강조된다. 쉽게 보안 신고를 하고 이를 많은 사람들이 확인할 수 있는 창구가 있다면 보안 인식에 대한 효과는 높아질 것으로 예상된다.

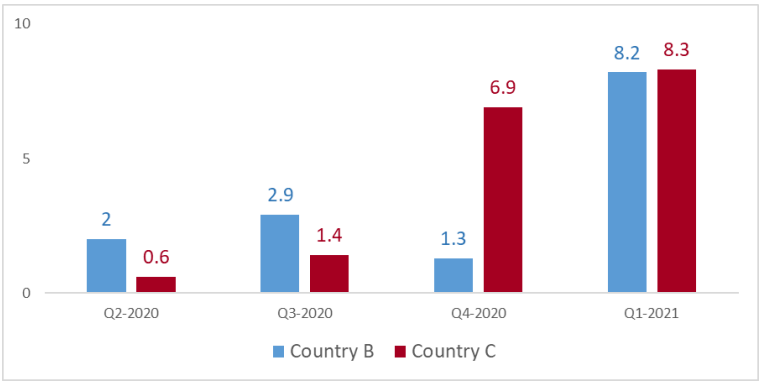

Figure 4. Status of mail vulnerabilities by country

보안 이슈 공유와 안전한 이메일 이용에 대한 상관관계를 분석하기 위하여 교차분석을 실시하였다. 교차분석 결과는 $\chi^2(1, n = 3,245) = 15.879, p = .003$ 로 0.05 미만이므로 유의미하게 [표 5]와 같이 나타났다. 즉, 상황 공유와 안전한 대응은 상관관계가 있다는 것을 의미한다.

Table 5. Cross-analysis results based on situation sharing

Situation Sharing	Not vulnerable	Vulnerable	$\chi 2$	Significant Probability
Country B Shared	1,192 (99.4%)	7 (0.6%)	15.879	.003
Country B Unshared	298 (98.0%)	6 (2.0%)		
Country C Shared	682 (99.4%)	4 (0.6%)		
Country C Late Shared	325 (98.8%)	4 (1.2%)		
Country C Unshared	710 (97.7%)	17 (2.3%)		

V. 결론

이메일은 일상생활에서 커뮤니케이션하는데 도움을 주는 중요한 도구이다. 일상 생활에서도 사용하고 있겠지만 기업 임직원에게는 업무 수행에 있어서 꼭 필요한 도구이다. 최근 COVID-19(코로나바이러스)로 인해 비대면 활동이 증가하면서 이메일 보안 사고는 증가되고 있다. 생활 속에서 많은 사람들과 자료 공유 및 소통하는데 도움을 주지만 보안 위험에 쉽게 노출되어 있는 도구 중 하나이다. 이메일 보안 사고는 기술적인 공격도 있지만 최근 발생하는 내용들은 사람의 심리를 이용한 사회공학적 공격이 많다. 사회공학적 공격은 기술적으로 대응하기 어렵기 때문에 보안 인식에 의존 할 수 밖에 없다.

보안 인식에 대한 연구는 다양하게 이루어지고 있다. 하지만 연구가 이론적으로만 이루어지고 있고, 해외 단발적인 실증적 연구가 이루어지고 있다. 보안 인식에 대해 이론적인 사항을 기업 임직원을 대상으로 1 년동안 악성 이메일 모의훈련을 통해 검증하였다. 지속적인 연구를 통해 보안 인식의 변화에 따른 안전한 이메일 이용의 변화 분석은 새로운 연구 제시에 관해 학술적 의의가 있다. 또한 실무환경에서 보안 부서의 담당자가 안전한 이메일 이용에 대한 제시 방법 등을 할 수 있고, 이를 이용하여 보안 교육 등 보안 인식 활동하는데 도움이 될 수 있을 것이라 실무적으로 활용 가치가 높다고 판단된다.

본 연구는 산업 현장에서 다양한 연령, 직급, 성별을 포함한 4,000 여 명을 대상으로 1 년동안 수행하여 객관성을 확보하였다. 훈련 결과를 통계 프로그램을 이용하여 분석(교차분석)을 하였다. 분석 결과, 3 가지 가설 모두 채택되었으며, 보안 교육 참여, 상향식 보안 관리, 보안 이슈 공유 유무는 안전한 이메일 이용에 도움이 되었다.

연구 결과를 바탕으로 효과적인 보안 인식 활동에 대해 다음과 같이 제시하고자 한다.

첫째, 보안 교육은 일회성이 아닌 반복적으로 수행을 해야한다. 특히 보안 취약 인원에 대해서는 반복적인 교육을 통해 보안 인식에 대한 변화를 목적으로 두어야 한다. 너무 어렵거나

보안 지식 전달보다는 피교육자의 눈높이에서 교육을 수행해야 한다. 근무 환경, 보안에 대한 지식 및 인식, 보안 위험의 노출 정도 등의 차이가 있기 때문에 실질적으로 도움이 될 수 있는 교육을 제공하고 이를 활용할 수 있도록 지속적으로 보안 교육을 수행해야 한다.

둘째, 보안 취약 인력에 대해 관리가 필요하다. 본 연구는 이메일을 이용하여 모의훈련을 실시하여 분석을 하였지만, 일상 생활에 있어 다양한 보안 취약 인력이 있을 것이다. 보안 취약 인력을 대상으로 지속적인 보안 교육을 수행하고 보안 부서에서는 근무지를 방문하여 근무 환경의 문제점 발견과 지원을 해줘야 한다. 보안 취약 인력 대부분 본인이 어떤 이유에서 취약한 이유를 모르는 경우가 많을 것이다. 정확히 알지못해 발생하는 경우이기 때문에 그들에게 실제 도움이 될 수 있는 방법을 모색할 필요가 있다. 더불어 보안 부서가 옆에 있다는 점을 인식시켜줄 필요가 있다. 또한 보안 취약 인력이 소속되어 있는 부서장도 보안 부서와 함께 옆에서 지속적으로 관리를 한다면 보안 인식 향상의 효과는 높아질 것이다.

셋째, 모의 훈련은 지속적으로 수행하며 다양한 관점에서 점검이 필요하다. 모의 훈련을 통해 다양한 취약점이 발굴될 것이다. 이러한 취약점을 발굴하기 위해서는 지속적인 모의 훈련을 실시하고 전 임직원이 참여하도록 유도해야 할 것이다. 취약점이 발견이 되면 세부적인 확인을 위해 추가 훈련이나 대응 방법을 모색해야 한다. 연간 모의 훈련 계획을 수립하여 훈련을 실시하고 임직원들이 훈련하고 있다는 것을 인지시켜줄 필요가 있다.

하지만 연구의 한계점도 있다. 매 연구마다 같은 콘텐츠를 이용하지 않아 취약 인원이 일정하게 나타나지 않았다. 또한 훈련 대상의 보안 인식 및 지식 수준을 고려하지 않은 상태에서 훈련이 실시되었다.

향후 악성 이메일에 대해 개인화 서비스를 적용했을 때 보안 인식에 대한 연구를 진행한다면 피싱 이메일이나 랜섬웨어 등 대응에 도움이 될 것으로 생각된다. 사회공학적 공격은 사람의 관심있는 내용을 가지고 접근하기 때문에 중요한 연구 내용이 될 것이라 생각된다. 앞으로 이론적 연구를 통해 발전된 보안 인식 개선에 대해 다양한 기관에서 실증적 연구를 수행되기를 기대한다.

VI. Acknowledgment

본 논문은 제 1 저자(이태우) 석사과정 학위논문을 학회 논문지 목적에 맞게 분석정리하여 발표한 내용입니다.

VII. 참고문헌

[1] Ministry of Science and ICT, National Information Society Agency, "2020 Yearbook of Internet Usage Survey Report", 2020
[2] Jiransecurity, "Q1 Spam Mail Trend Analysis Report", 2020
[3] Jun-hee Lee, Hun-yeong Kwon, "A Study on Human Vulnerability Factors of Companies : Through Spam Mail Simulation Training Experiments", Korea Institute Of Information Security And Cryptology, Vol.29, No.4, pp.847-857, 2019
[4] Chang-Moo Lee, "A Critical Review of Industrial Security Concepts", Korean Security Journal, Vol.50, pp.285-303, 2017
[5] PriceWaterhouseCoopers, "Convergence of security risks : Addressing the security dilemma in today’s age of blended threats", 2010
[6] Kunwoo Kim, Jungduk Kim, "The Values and Strategies of Industrial Security in Digital Economy", Korean Journal of Industry Security, Vol.8, No.1, pp.61-74, 2018
[7] Jin A Heo, Seong Bhin Joo, Jung Min Lee, Chan Hyuk Park, "Countermeasures for Industrial Technology Protection in Social Engineering attack", The Journal of Social Science, Vol.23, No.1, pp.279-306, 2016
[8] June Sung Choi, Kwang Ho Kook, "Social Engineering Attack Trends on the Korean Defense

Industry and the Countermeasures", Journal of the Korean Association of Defense Industry Studies, Vol.19, No.1, 22-37, 2012
[9] Young-Mook Kang, Sang-Jin Lee, "A Study On Malicious Mail Training Model", Journal of the Korea Institute of Information Security & Cryptology, Vol.30, No. 2, pp.197-212, 2020
[10] Korea Communications Commission, Korea Internet & Security Agency, "Information and Communication Network Act Guide to Prevent Illegal Spam", 2020
[11] Korea Communications Commission, Korea Internet & Security Agency, "Spam distribution status in the second half of 2020", 2021
[12] Trendmicro, "Spear-Phishing Email: Most Favored APT Attack Bait", Trend Micro Incorporated Research Paper, 2020
[13] Eun-Hee Shin, Chang-Moo Lee, Hang-Bae Chang, "An Empirical Study on the Impact of Industrial Security Awareness and Knowledge of Corporate Employees on the Will to Comply with Security Policy", Korean Journal of Industry Security, Vol.10, No.2, 59-78, 2020
[14] Michael J. Wolf, "Measuring an information security awareness program", University of Nebraska, 2010
[15] National Intelligence Service, Ministry of Science and ICT, Ministry of the Interior and Safety, Korea Communications Commission, Financial Services Commission, Ministry of Foreign Affairs, 2020 Yearbook National Information Protection White Paper, 2020
[16] D'Arcy, J., Hovav, A., "Deterring Internal Information Systems Misuse. Communications of the ACM", Vol.50, No.10, pp.113-117, 2007
[17] In Hwan Cha, "A study on the Development of Personnel Security Management for Protection against Insider threat", The Journal of The Korea Institute of Electronic Communication Sciences, Vol.3, No.4, pp.210-220, 2008
[18] Woosung Jung, " A Design for the Personalized Difficulty Level Metric based on Learning State", Journal of the Korea Convergence Society, Vol.11, No.3, pp.67-75, 2020
[19] Taryn Aguas, Khalid Kark, Monique François, " The new CISO: Leading the strategic security organization", Deloitte, 2019, https://www2.deloitte.com/global/en/insights/deloitte-review/issue-19/ciso-next-generation-strategic-security-organization.html
[20] Duck-sang Yoon, Kyung-ho Lee, Jong-in Lim, "A Study on the Change of Capability and Behavior against Phishing Attack by Continuous Practical Simulation Training", Journal of the Korea Institute of Information Security & Cryptology, Vol.27, No.2, pp.267-279, 2017
[21] Jun Heo, Seongjin Ahn, "A Study on the Influence of Biased Thinking on Compliance with Security Policy Based on the Mediation of Factors of Protection Motivation and Role of Management", The Journal of Korean Association of Computer Education, Vol.23, No.6, pp.35-49, 2020
[22] Myungseong Yim, "A Study on the Level of Perception about Information Security Countermeasures : Differences between Managers and Non-Managers", Korean Management Consulting Review, Vol.16, No.4, pp.33-41, 2016
[23] Jong One Cheong, "The Effects of Organizational Politics and Conflicts on Job Satisfaction and Organizational Performance : Analyzing the Moderating Effects of the Top-down Way of Working", Korean Local Government Review, Vol.20, No.4, pp.47-70, 2019
[24] Sloan, H., "The Annals of Thoracic Surgery", R. Adams Cowley, MD: 1917–1991, Vol.53, No.6, 954, 1992
[25] Verizon, "The 2013 Data Breach Investigations Report", 2013

저자 소개

이태우(*Taewoo Lee*)

2019 년 9 월 중앙대학교 융합보안학과 석사과정

관심분야 : 보안인식, 산업보안, 개인정보

장항배(*Hangbae Jang*)

2006 년 연세대학교 대학원 정보시스템관리 박사
2014 년 ~ 현재 중앙대학교 산업보안학과 교수

관심분야 : 산업보안, 기업보안, 인수합병, 정보유출