https://doi.org/10.33778/kcsa.2024.24.4.011

악성메일 사고예방 프레임워크 연구: 사용자 행동 지원 중심

최 영 국*, 권 익 현**

요 약

악성 이메일 공격은 피싱(phishing), 스캠(scam), BEC(business email compromise), 사회공학(social engineering), 랜섬웨어(ransomware) 등 다양한 사이버 위협과 연관되어 꾸준히 증가하고 있다. 기존의 악성메일 차단 기술은 진화하는 공격을 완벽하게 방어하지 못하고 있으며, 사용자들은 여전히 취약한 환경에 노출되어 있다. 이러한 상황에서 사용자의 보안 인식 부족과 실수는 사고 발생 가능성을 더욱 높이는 요인으로 작용하고 있다. 이는 단순한 피해를 넘어 조직의 지속가능성(sustainability)에도 중대한 영향을 미칠 수 있다. 본 연구는 이메일 보안에서 사용자가 마지막 방어선으로서 중요한 역할을 수행한다는 인식 아래, 악성메일을 보다 효과적으로 식별할 수 있는 전략을 제안한다. 특히 이메일 확인 과정에서 확장된 검사 정보와 가시성을 제공함으로써 사용자의 악성메일 식별 능력을 향상시키는 방법을 탐구하였다. 이 과정에서 제로 트러스트(zero trust) 보안 모델을 도입하여, 모든 이메일을 잠재적 위협으로 간주하고 심층적인 검토 과정을 통해 악성메일 사고를 예방하는 체계를 구현하고자 하였다. 아울러, 이러한 방법의 성공적인 도입과 보편화를 위해 이메일 검사 정보의 국제 표준화와 소프트웨어 안전 기준의 법제화를 제안하였다. 또한 사용자가 제로 트러스트 보안 개념을 내재화하고 일상적으로 보안 의식을 유지할 수 있도록 교육 및 훈련 프로그램을 구성하여 '악성메일 사고예방 프레임워크'를 정의하고 체계화하였다. 향후 본 프레임워크의 완성을 위해 실질적이고 구체적인 후속 연구를 진행할 계획이다. 이를 통해 사용자의 보안 인식을 제고하고, 보안을 하나의 문화로 정착시킴으로써 더욱 안전한 인터넷 환경 조성에 기여할 수 있을 것으로 기대한다.

A Study on Malicious Email Incident Prevention Framework: Focusing on User Behavior Support

Youngkug Choi*, Ick-Hyun Kwon**

ABSTRACT

Malicious email attacks, including phishing, scams, BEC, social engineering, and ransomware, are increasing and pose significant risks to organizations. Existing email filtering technologies cannot fully defend against these evolving threats, and human errors combined with low security awareness increase the chances of incidents. This study proposes a strategy to enhance users' ability to identify malicious emails by providing extended inspection data and visibility when interacting with emails. It incorporates a Zero Trust security model, treating all emails as potential threats to prevent incidents. We also advocate for the international standardization of email inspection information and the legal establishment of software safety standards. We refer to this approach as the 'Malicious Email Incident Prevention Framework,' which includes user education and training to internalize Zero Trust principles. Future research will focus on refining this framework to improve security awareness and foster a safer internet environment.

Key words : Malicious Emails, Zero Trust, Security Awareness, Phishing Simulation Training, Security as a Culture

접수일(2024년 09월 19일), 게재확정일(2024년 09월 30일)

* 인제대학교 일반대학원 산업융합보안학 협동과정(주저자)
** 인제대학교 스마트물류학과(교신저자)

1. 서 론

이메일은 오늘날 인터넷이 고도로 발달한 사회에서도 개인과 기업이 정보를 유통하는 중요한 수단으로 자리잡고 있다. 그러나 동시에 이메일은 정보를 탈취하고, 시스템을 파괴하며, 재정적 피해를 유발하는 보편화된 사이버 공격 수단으로 작용하고 있다. 지금까지 다양한 방법을 통해 악성메일을 근절하려는 노력이 이루어졌으나 여전히 완전한 해결책은 마련되지 않았으며, 오히려 총체적인 피해 규모는 증가하는 추세에 있다. 이러한 피해는 경제적 손실뿐만 아니라 법적, 사회적, 평판적 손해로 이어지며, 그 결과 조직의 지속가능성(sustainability)과 신뢰성에 심각한 타격을 줄 수 있다.

비록 보안시스템은 점차 고도화되고 있으나, 악성이메일 사고의 주요 원인은 여전히 사용자 측면에 있다. 사용자들은 보안에 대한 인식 부족, 정보 및 지식의 결여, 그리고 경직된 보안정책에 대한 저항감으로 인해 악성메일 공격에 취약한 상태이다. 이러한 이유로 악성메일 사고는 근절되지 않고 있으며, 지속적으로 심각한 피해를 야기하고 있다.

이에 본 연구는 이러한 문제를 해결하기 위한 전략을 제안하고자 한다. 본 연구에서 제안하는 전략은 오랜 현장 경험을 바탕으로 형성된 것으로, 사용자에게 보안 역할의 중요성을 인식시키고, IT 시스템은 사용자가 이러한 보안 역할을 원활하게 수행할 수 있도록 지원하는 인터페이스를 제공해야 한다는 것이다. 이를 통해 본 연구는 제안된 전략을 개념적으로 정의하고 구체화하며, 향후 현실적인 구현 방안을 모색하는 것을 목적으로 한다.

2. 이론적 배경 및 관련 연구

2.1 악성메일의 정의 및 공격 유형

본 연구에서 다루는 악성메일은 '개인 및 조직에 피해를 유발하는 공격의 매개체로 사용되는 이메일'을 의미한다. 악성메일에는 여러 가지 유형이 존재하는데 주로 아래와 같은 공격 방법이 활용된다.

2.1.1 피싱메일(phishing email)

피싱(phishing)은 신뢰할 수 있는 기관이나 신분을 가장하여 정보 탈취, 악성코드 전파, 금전 사기를 하기 위한 행위의 통칭이다. 피싱메일은 APT(advanced persistent threat) 공격자들이 가장 선호하는 침투수단으로 알려져 있다[1].

2.1.2 계정 탈취(account takeover, ATO) 공격

이 공격은 피싱메일을 보내고 가짜 로그인 페이지 등을 통해 계정정보 입력을 유도하여 자격증명을 수집하는 방법으로 이루어진다. 대부분 자격증명 정보를 입력할 당시에는 아무 일도 일어나지 않기 때문에 사용자는 방심하지만 이후 심각한 공격으로 이어질 수 있다.

2.1.3 비즈니스 이메일 침해

비즈니스 이메일 침해(business email compromise, BEC) 공격은 공격자가 이메일을 사용하여 상대를 속여 돈을 보내게 하거나 회사 기밀 정보를 누설하게 하는 사이버 범죄의 한 유형이다[2]. 흔히, 피싱메일이나 ATO 공격과 결합된다.

2.1.4 악성 소프트웨어(malicious software) 설치

이메일에 첨부된 파일이나 링크를 통해 시스템에 악성 소프트웨어를 설치하는 공격이다. 웹페이지에 접속하는 것만으로도 악성코드를 유포하는 공격기법을 'drive-by download 공격'이라고 하며, 이는 주로 웹 브라우저의 보안 취약점을 악용한다. 이러한 공격 방식은 이메일 본문에 포함된 링크를 단순히 클릭하는 것만으로도 악성 소프트웨어가 시스템에 설치될 수 있음을 의미한다. 이선호·한민수(2015)는 미국 국가안보국(National Security Agency, NSA)이 APT 공격을 통해 스틱스넷(Stuxnet)이라는 악성코드를 이란 핵발전소에 침투시켜 시설을 마비시킨 사례를 분석하였다. 이 연구에서는 복잡한 공격 과정 속에서 초기 침투경로로 이메일이 자주 활용된다는 점을 강조하고 있다[3].

2.1.5 사회공학(social engineering) 공격

앞서 언급한 공격들은 대부분 사회공학 기법과 결합된다. 기술적 보호 조치는 일반적으로 이러한 종류의 공격에 대해 별로 효과적이지 못하다. 그뿐만 아니라 사람들은 보편적으로 이런 공격을 탐지하는 데 스스로 능숙하다고 생각한다[4]. ISACA(Information Systems Audit and Control Association, 이하 ISACA)의 보고서에 의하면 기업에 대한 전체 사이버 공격의 25%가 사회공학적 기법과 APT 형태의 공격으로 조사되었다[5]. 그만큼 사람들이 사회공학 공격에 취약하다는 의미이다.

2.2 피해 사례 및 통계적 특성

2013년부터 2015년까지 리투아니아의 사이버 범죄 집단이 하드웨어 공급업체를 사칭하여 페이스북과 구글에 가짜 송장을 발송하는 방법으로 약 1억 달러 이상의 손실을 초래한 사건이 발생하였다. 이 공격은 이메일 확인 절차의 취약점을 악용하여 직원들이 송금을 승인하게 만드는 방식으로 이루어졌다[6]. 국내에서도 유사한 사건이 있었는데, 2016년 L사는 거래회사를 사칭한 피싱메일을 받고 공격자의 계좌에 240억 원을 송금하는 사고가 발생했다[7]. 이 사고로 해당 기업은 재무적인 손실뿐만 아니라 국제적 신뢰도에도 큰 타격을 입었다. 만약 대기업이 아니었다면, 이와 같은 재정적 손실로 인해 기업이 파산에 이를 가능성도 배제할 수 없었을 것이다.

2021년 미국 콜로니얼 파이프라인(Colonial Pipeline)사가 랜섬웨어에 감염되는 사건이 발생하였다. 이로 인해 미국 남동부 일대 석유의 45% 이상을 점유하는 파이프라인 시스템이 일주일 가까이 가동 중단되며 일부 지역에 연료를 공급하는데 차질이 생겼고, 7년 만에 유가가 최고치를 기록하며 주유 대란이 벌어지기도 했다. 공격자들은 75비트코인을 요구했으며 회사는 이를 지불한 것으로 알려져 있다[8]. 2024년 한국의 G사는 221만 명의 고객 개인정보 유출로 인해 개인정보보호위원회로부터 75억 원의 과징금을 부과받았는데 이는 국내 기업 중 역대 최대 규모이다. 이 공격은 직원 계정을 탈취하여 내부망에 접속함으로써 이루어졌는데 계정의 탈취수단으로 피싱메일의 이용을 추정할 수 있다[9].

악성메일로부터 발생한 사고와 이로 인한 피해사례는 일일이 열거하기도 어려울 정도이다. 악성메일의 피해는 국경을 초월하고 전 산업 범위에서 매우 다양한 형태로 발생하고 있다. 위의 사례에서도 볼 수 있듯 악성메일 공격이 데이터의 유출이나 금전적 피해를 유발하는 것도 심각하지만 나아가 기업이나 국가기관의 지속성에 중대한 위협을 가하고 사회적인 혼란을 초래할 수 있을 정도에 이를 수 있다. 결코, 간과해서는 안 되는 악성메일 문제의 최근 동향은 아래와 같다.

2.2.1 일반화된 공격 방법으로써의 이메일

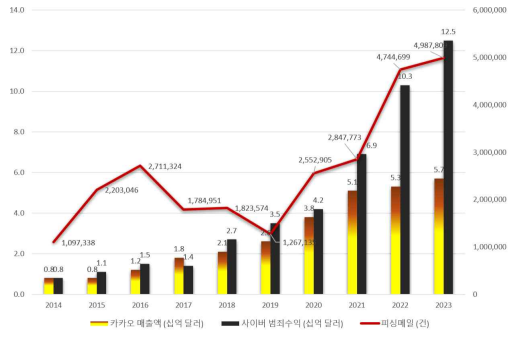
Trellix(2021)의 보고서에서는 스피어피싱(spear phishing)이 공격 대상 시스템에 접근하기 위해 사용되는 가장 일반적인 방법이라고 설명하고 있다[10]. 또한, Barracuda(2023)의 '2023 Email Security Trends'는 전체 공격의 75%가 이메일을 통한 것으로 피싱, 랜섬웨어, BEC 등 다양한 공격 벡터(vector)로 활용되고 있음을 보여주고 있다[11]. 이메일이 시간과 장소를 극복하여 인터넷에서 사용할 수 있는 가장 보편적인 커뮤니케이션 방법이면서 범죄의 수단으로도 광범위하게 이용되고 있음을 알 수 있다.

2.2.2 줄어들지 않는 악성메일 공격

2003년 설립되어 피싱공격에 대한 추적을 해오고 있는 APWG(Anti-Phishing Working Group, 이하 APWG)의 'Phishing Activity Trends Report'와 FBI의 'Internet Crime Report' 등으로부터 지난 10년간의 피싱공격 건수와 사이버범죄 피해액의 증감 자료를 취합하고 이것을 카카오의 연간 매출액과 비교하여 (그림 1)로 나타내었다.

2023년, 카카오 전체 매출의 두 배를 초과하는 125억 달러에 달하는 피해가 발생한 사실은 충격적이다. 그러나 이 수치는 미국 FBI가 발표한 공식 자료에 불과하며, 실제로 집계되지 않은 피해까지 고려할 경우 그 규모는 더욱 커질 것으로 예상된다. 특히 피싱공격의 빈도가 증가할수록 피해 규모도 확대되는 경향이 나타나고 있으며, 이러한 사실은 피싱이 범죄집단의 주요 공격 수단으로 자리 잡았음을 명확히 보여준다.

범죄수익이 발생하는 한, 악성메일을 이용한 공격은 지속적으로 증가할 가능성이 높다.



(그림 1) 2023년까지 10년간의 피싱메일 공격[1], 사이버범죄 수익[2], 카카오 매출액[3] 추이

2.3 선행연구 검토

악성메일로 인한 개인과 기업의 피해사례가 다양하고 사회적인 문제가 되기도 한다. 심지어 기관의 존속에도 영향을 줄 수 있을 만큼 심각한 경우도 있다. 당연하게도 이런 악성메일에 대해 이해하고 탐지방법을 개발하여 피해를 예방하기 위한 연구가 다수 수행되었다.

2.3.1 이메일 스캠, BEC, 사회공학 기법 공격

이은경·조용현(2016)은 무역산업에서의 비즈니스 스캠(scam) 대응의 문제점을 지적하였고[15], 김경철(2022)은 명의 도용된 이메일을 통한 무역사기의 사례와 예방체계에 대해 제안하였다[16]. 김도우·이규범(2019)은 '사회공학적 공격기법의 유형분류' 연구를 통해 사회공학 기법이 오랫동안 활용되어 온 것임을 밝히며 유형별로 대응책을 구성할 수 있는 기초자료를 제공하고자 하였다[17]. Al-Musib et al.(2023)은 BEC 공격에 대해 분석하고 예방 방안 등을 제시하는 것과 함께 해당 위험이 조직에 미치는 영향을 연구하였다[18].

2.3.2 인공지능 등을 적용한 악성메일 차단 연구

인공지능(AI)과 머신러닝(ML) 기술이 발전함에 따라 악성메일의 탐지 및 차단에도 해당 기술을 적용하고자 하는 연구가 다수 진행되었다. 이도경 등(2020)은 BEC 사고 유형과 방법들을 분석하고, 인공지능을 통한 효과적인 BEC 공격 대응방안을 제안하였다[19]. 손한기 등(2021)과 유지현(2021)은 Rule 기반과 순환신경망인 LSTM(long short-term memory) 딥러닝 학습 알고리즘을 사용하여 스팸 분류의 정확도를 높이고 문서 파일의 악성 여부를 판단하는 방법을 제시하였다[20,21].

2.3.3 보호 계층으로서 사용자 역할에 대한 연구

Abroshan et al.(2018)은 공격자들이 사용하는 심리적, 사회적 요인을 파악하는 것이 피싱 공격의 근본 원인을 파악하는 것으로 생각하고 피싱 공격에 대한 원인-결과도(fishbone diagram)를 도출하고자 하였다[22]. Heijden and Allodi(2019)는 피싱메일의 인지적 특징을 기반으로 한 분류 메커니즘을 구축함으로써 사용자의 교육 및 인식개선에 도움을 주고자 하였다[23]. 이준희·권헌영(2019)은 기업 내에서 현장실험을 통해 악성메일에 취약한 인적요인을 연구하여 이에 기반한 사용자 인식개선 및 모의훈련을 통한 대응력 향상을 기대하였다[24].

기존 연구에 따르면, 국가와 산업을 불문하고 발생하는 악성메일 공격에 효과적으로 대응하기 위해서는 적절한 보안체계 구축과 더불어, 직원들의 교육 및 훈련에 대한 지속적인 투자가 필요하다. 또한, 악성메일 문제는 단순한 기술적 대응을 넘어, 기업의 연속성 및 회복성 관점에서 다루어져야 한다는 점이 강조되고 있다. 이러한 연구들은 주로 악성메일의 특성을 분석하여 사전에 탐지 및 차단할 수 있는 기술을 개발하는 것과 사용자 교육 및 훈련의 중요성에 초점을 맞추고 있다. 그러나, 이와 같은 노력에도 불구하고 악성메일 공격은 여전히 증가하고 있으며, 그로 인한 피해 규모도 확산되고 있다. 이러한 현상이 발생하는 원인은 무엇인가? 본 연구는 기업 현장에서의 경험을

1) 2014년~2023년 'APWG Phishing Activity Trends Report' 매 분기별 피싱공격 데이터 취합[12]
2) 2014년~2023년 'FBI Internet Crime Report' 피해액 취합[13]
3) 2014년~2023년 카카오 재무제표(K-IFRS) 매출액(하나은행 고시 매년 말일자 원달러 환율 기준)[14]

바탕으로, 기존 접근 방식의 한계를 분석하고 이를 극복할 수 있는 방안을 제시하고자 한다.

3. 현행 사고예방 접근방식의 한계

3.1 기술적 차단 및 통제 정책의 효용성 저하

대부분의 악성메일은 사용자에게 도달하기 전에 이메일 보안장비에 의해 차단된다. 이것은 전통적인 경계기반 보안모델(perimeter security model)에 기반하여 외곽에 방어선을 구축하고 악성인 이메일은 통과시키지 않는다는 개념적 접근에 의한 것이다. 하지만, 제로데이 공격이나 사회공학 기법 사용 또는 오탐(false positive)을 줄이기 위한 절충적(trade-off) 설정으로 인한 것 등 다양한 이유로 얼마간의 악성메일이 사용자의 수신함으로 유입된다. 앞에서 예시한 피해사례들이 이렇게 차단되지 못한 소수의 이메일로부터 발생한 것이라는 점에서 그 치명성을 다시 한번 깨닫게 된다.

수년 전부터 인공지능과 머신러닝을 활용하여 악성메일을 식별하고 차단하려는 연구가 성과를 거두었으며, 이를 기반으로 한 보안제품도 개발되어 실무에 적용되고 있다. 그러나 공격자들 또한 AI 기술을 활용하여 더욱 정교한 공격 수법을 개발하고 있으며, 이를 통해 보안시스템을 우회하고 사용자를 속이는 사례가 늘어나고 있다. SK쉴더스의 '2024년 보안 위협 전망 보고서'에 따르면, 대형 언어 모델(large language model, LLM) 기반의 생성형 AI인 WormGPT가 개발되어 사용자 맞춤형 BEC 공격을 수행할 수 있다고 언급되었다[25]. 실제로, BEC 공격 건수는 일본(전년 동기 대비 35% 증가), 한국(31% 증가), UAE(29% 증가) 등에서 증가세를 보였다. 이들 국가는 이전까지 문화적 및 언어적 장벽으로 인해 BEC 공격 빈도가 낮았던 지역이었으나, 생성형 AI의 발전으로 인해 공격자들이 다양한 언어로 더욱 정교한 맞춤형 이메일을 발송할 수 있게 된 것이 주된 원인으로 분석된다[26]. 이러한 현상은 보안시스템의 발전에 따라 공격 수단 또한 고도화된다는 사실을 시사한다.

방어체계가 고도화되어도 악성메일은 사용자에게 전달된다. 그리고, 그 악성메일로부터 발생하는 대부분의 피해 또한 사용자가 책임져야만 할 것이다. 하지만, 전통적으로 보안의 관점은 시스템 강화에 초점을 맞춰왔다. Verizon(2023)에 의하면 보안 침해사고의 74%는 인간요인과 관련이 되어있다[27]. 그럼에도 불구하고 기업들은 직원들에 대한 인식개선과 교육에 투자하기 보다는 보안 위협 탐지와 대응에 우선적으로 투자하고자 한다고 밝혔다[28].

HP Wolf Security(2021)의 사무직 근로자 8,443명을 대상으로 한 설문조사에서 직원들의 일부는 보안 시스템이 업무에 방해가 된다고 여기며 회사의 보안 정책을 우회하려는 시도를 하고 있다고 하였다[29]. Proofpoint(2024)의 '2024 State of the Phish' 보고서에서 설문에 응한 직원들 중 71%가 위반행위를 한다고 응답했다. 이 중 96%는 위반임을 알았다고 하였는데 그 이유는 편리함(44%), 시간절약(39%), 긴급함(24%) 등의 순이었다. 이에, 보안 전문가들은 보안교육 강화(83%)와 보안통제 강화(81%)를 방안으로 꼽았지만, 직원 대부분(94%)은 보안통제가 간소화되고 사용자 친화적으로 개선된다면 보안을 우선시하겠다고 답했다[26].

보안통제와 시스템 강화의 방향으로만 맹목적으로 질주해 온 지금까지의 정책은 사용자들을 소외시키고 저항감을 갖도록 하며 함께 참여하는 보안 거버넌스의 정착을 방해할 뿐 아니라 오히려 인간이 보안의 저해 요소로 치부되는 부작용을 낳고 있다. 지금의 악성메일 사고 증가는 시스템 강화 위주의 정책과 그것에 무관심하고 저항하는 사용자 사이에서 일어나는 갈등의 결과일지도 모른다. 악성메일 사고예방은 강한 보안통제와 시스템에만 의존해서는 한계가 있다. 사용자들을 물 건너 불구경만 하는 존재로 만들어서는 안된다. 악성메일과의 전쟁에 사용자가 동참하도록 해야 한다.

3.2 사용자 교육·훈련의 실효성 부족 문제

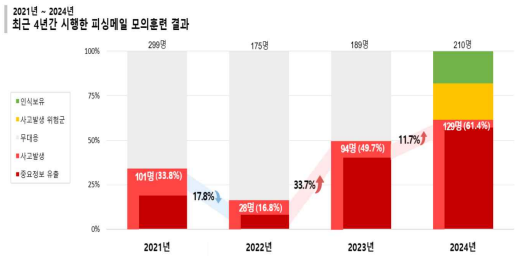
많은 연구에서 악성메일 대응 방안으로 사용자 교육 및 훈련을 강조하고 있다. 요약하자면, 사용자에 대한 교육과 훈련은 보안 인식을 강화하고 피싱메일로 인한 사고를 예방하는 데 효과적이라는 것이 공통된 결론이다. 특히 일회성 교육보다는 체계적인 정책과 계획을 수립하고, 정기적인 교육을 통해 지속적인

학습을 제공하는 것이 중요하다[24,30-32].

그러나, 이러한 이상적인 접근이 현실에서 구현되기에는 여러 도전 과제가 존재한다. 우선, 이러한 교육을 체계적으로 실행하기 위해서는 이를 담당할 운영조직이 필요하며, 지속적인 예산 투입이 요구된다. 그러나 많은 기업에서 이는 쉽지 않은 일이다. 실제 기업 현장에서 악성 이메일로 인한 피해가 발생한 경우에도, 새로운 시스템 도입 등의 기술적 조치는 추진되었으나 사용자 교육은 지속적으로 이루어지지 않는 경우가 많았다. 이는 조직의 구조적 문제나 예산 부족 외에도, 교육의 효과를 장기적으로 유지하는 것이 어렵기 때문이다. 또한, 업무 시간을 할애해 교육을 실시하는 것은 기업과 직원 모두에게 생산성 저하에 대한 우려를 불러일으키며, 이러한 부담은 교육의 지속성을 저해하는 요인으로 작용할 수 있다.

다음은 K사, S사 그리고 F사에서 2024년 상반기에 실시한 피싱메일 모의훈련 결과를 정리한 것이다. 각각 210명, 221명, 125명을 임의로 선정하고 팀장급 이상은 모두 포함하였다. 훈련 시나리오는 은행에서 발송한 '임직원 퇴직연금 조회 안내'인 것처럼 꾸며 첨부파일을 열거나 피싱 사이트에 접속하여 개인정보 입력 여부를 시험하는 것으로 하였다. 첨부파일 실행, 링크 접속, 개인정보를 입력한 경우는 '사고발생'으로 하였고, '무대응'한 직원을 대상으로 추가 설문을 실시하여 훈련 또는 피싱메일 여부를 인지한 경우는 '인식보유'로 그렇지 않은 경우는 '위험군'으로 분류하였다.

훈련 결과, K사는 사고발생(61.4%) + 위험군(20.5%)에 인식보유(18.1%)로 이전 훈련에 비해 최소 11.7% 이상 더 나빠진 결과를 보였다. S사의 경우 사고발생(37.1%) + 위험군(12.2%)에 인식보유(50.7%)로 이전 훈련에 비해 10.5% 개선된 것으로, F사의 경우 사고발생(36%) + 위험군(17.6%)에 인식보유(46.4%)로 이전 훈련에 비해 11.8% 개선된 것으로 집계되었다. 훈련 시나리오의 수준에 영향을 많이 받겠지만 세 기업 모두 전반적으로 직원들의 피싱메일에 대한 식별 능력이 부족한 것으로 보인다. 특히, K사의 경우 (그림 2)에서 볼 수 있듯이 훈련이 반복됨에도 불구하고 이전보다 나쁜 결과를 보임으로써 직원들의 보안 인식의 상태가 심각한 것으로 판단하고 있다.



(그림 2) K사의 연도별 피싱메일 모의훈련 결과

또한, 훈련을 받은 횟수, 직급의 고하, 신입·경력 여부 등으로 구분하여 피싱메일 대응 능력에 차이가 있는지를 통계적으로 분석하였다. 아래의 <표 1>은 그 중 하나인 직급의 구분을 중심으로 카이제곱 검정(교차분석)을 실시한 결과이다. S사의 경우 $p=0.002 < 0.05(\alpha)$로써 직급별로 보안 인식의 보유에 유의미한 차이가 있는 것으로 보이나 다른 두 기업의 경우 직급별로 차이가 두드러지지 않은 것으로 나타났다. 즉, 개인적인 특성과는 무관하게 악성메일에 대해 전반적으로 취약함을 드러냈다.

<표 1> 2024년 모의훈련, 직급 구분 별 훈련결과에 대한 카이제곱 독립성 검정 결과

χ^2 검증

회사		값	자유도	p
S기업	χ^2	17.37	4	0.002
	χ^2 continuity correction	17.37	4	0.002
	사례수	221		
K기업	χ^2	7.13	4	0.129
	χ^2 continuity correction	7.13	4	0.129
	사례수	211		
F기업	χ^2	5.41	4	0.248
	χ^2 continuity correction	5.41	4	0.248
	사례수	125		
전체	χ^2	21.45	4	< .001
	χ^2 continuity correction	21.45	4	< .001
	사례수	557		

수년간 매년 5회 이상의 보안 캠페인을 실시하고, 연 1회의 모의훈련을 진행했음에도 불구하고, 악성메일에 대한 식별 능력에서 뚜렷한 향상을 보이지 않았다. 더불어, 훈련의 빈도, IT 친숙도, 직급 및 수행업무와 같은 변수들 또한 의미 있는 상관관계를 보이지 않았다. 본 연구는 이러한 결과에 대해 다음과 같이 해석한다.

“직원들에 대한 교육·훈련의 효과는 각자의 관심사가 주는 자극에 비해 상대적으로 크지 않을 수 있다.”

즉, 직원들이 악성메일에 속는 이유는 악성메일에 대한 대응법을 알지 못해서가 아니라, 해당 이메일을 악성이라고 믿지 않기 때문이다. 따라서 단순히 훈련의 빈도를 늘리는 것만으로는 이 문제를 해결할 수 없다고 볼 수 있다. 직원들은 반복적인 훈련에 익숙해질 뿐, 악성메일에 대한 경계심이나 주의력은 실제로 향상되지 않을 가능성이 크다. 이러한 결과를 바탕으로, 단순하고 정형화된 훈련의 반복만으로는 악성메일에 대한 대응력을 향상시키는 데 한계가 있다는 가설에 도달하게 되었고, 이에 따라 교육 및 훈련의 목표를 재설정할 필요성이 제기되었다.

4. 성공적인 악성메일 방어를 위한 전략

COVID-19 사태 초기에는 바이러스가 매우 높은 치사율을 보였으나, 몇 년이 지난 현재는 독감처럼 우리 일상 속에서 함께 공존하는 단계에 이르렀다. 이제는 주변에서 COVID-19에 대해 크게 걱정하는 사람도 드물고, 그로 인한 피해도 크지 않게 보인다. 그렇다면 악성메일 문제도 이와 같은 방식으로 치부할 수 있을까?

COVID-19 팬데믹 당시, 대부분의 사람들은 마스크를 착용하고 손소독제를 사용하며, 백신이 없던 상황에서도 눈에 보이지 않는 바이러스와 싸우기 위해 자발적으로 방역 수칙을 따랐다. 이러한 집단적 대응은 바이러스의 높은 치사율에도 불구하고 피해를 줄이는 데 기여하였다. 반면, 심각성을 다르게 판단하여 ‘집단 면역’ 정책을 시행했던 스웨덴의 실패 사례는 우리에게 중요한 교훈을 제공한다. 이 교훈은 악성메일 방어 전략에도 적용될 수 있다.

악성메일로부터 방어하기 위한 “마스크”와 “손소독제”는 과연 무엇일까? 이것은 단순히 기술적 대응만으로는 충분하지 않으며, 조직적이고 체계적인 방어 전략과 함께 사용자들의 자발적인 참여가 필요하다는 점을 시사한다.

4.1 사용자 인식의 변화 필요: 문화로서의 보안

앞서 지적한 바와 같이, 사용자에 대한 교육과 훈련은 반드시 필요한 요소이다. 그러나 그 효과에 대해서는 의문을 제기하지 않을 수 없다. 비용 문제를 떠나, 다층방어체계에서 최종 방어선으로서 사용자의 역할을 인식하고 그들의 능동적인 참여를 이끌어내지 않는다면, 수동적인 교육만으로는 충분한 효과를 기대하기 어렵다. 더 나아가, 교육의 효과 여부를 논하기에 앞서, 실제로 조직 내에서 사용자 보안교육에 대한 정책과 예산, 그리고 체계가 얼마나 존재하는지 의문을 가질 수밖에 없다.

단순히 보안시스템을 확충하고 사용자 교육을 강화해야 한다는 주장만으로는 문제를 해결할 수 없다. 보안은 단순한 기술적 문제를 넘어서, 하나의 문화로 자리 잡아야 한다는 인식이 필요하다. 즉, ‘문화로서의 보안(security as a culture)’은 시민의식, 사회적 규범, 공동체 의식 및 책임감과 같은 사회적 가치와 결부되어야 한다. 보안이 하나의 문화로 정착되기 위해서는, 사람들 사이에서 보안에 대한 인식이 충분히 내면화되는 과정이 필수적이다.

이제 더 이상 사람들은 자신을 단순한 서비스 이용자로만 인식해서는 안 된다. 정보가 지식을 넘어 중요한 자산이 되는 디지털 사회에서, 개인은 사용자로서의 권리뿐만 아니라 보호자로서의 책임 또한 인식해야 한다. 이를 통해 사용자들은 정보보호의 주체로서 적극적으로 참여하게 될 것이며, 이는 장기적으로 조직과 사회의 보안 수준을 한층 더 강화하는 데 기여할 것이다.

4.2 훈련 목표의 변경: 제로 트러스트의 내면화

본 연구에서는 보안 인식의 내면화 방안으로 제로 트러스트(zero trust) 보안모델의 원칙을 기반으로 사용자 교육 및 훈련의 목표를 수정하는 전략을 제안하고자 한다. 제로 트러스트 보안모델은 기존의 경계기반 보안모델의 한계를 극복하기 위해 제시된 개념으로, 조직 내 방화벽 뒤에 있는 모든 것이 안전하다는 전통적 가정을 배제하고 위반을 전제로 모든 요청이 개방된 네트워크에서 시작된 것으로 간주하며 검증하는 방식을 채택한다. 요청이 시작된 위치나 접근할 대

상과 관계없이 “신뢰하지 말고 항상 확인하라”는 원칙을 요구한다[33].

이를 이메일 보안에 적용하면, 모든 이메일이 악성일 가능성을 전제로 “발송자나 내용과 관계없이 모든 이메일을 의심하고 반드시 확인하라”로 바꾸어 표현할 수 있을 것이다. 악성 이메일로 인한 사고는 수신자가 해당 이메일을 의심하지 못했을 때 발생한다. 공격에 성공하는 악성메일은 매우 정교하게 설계되어, 수신자로 하여금 진정성 있는 메시지로 인식하게끔 만든다. 수신자가 의심하지 않는 상황에서 어떠한 보안 조치를 기대하기는 어렵다. 따라서 사용자 교육 및 훈련의 목표는 다음과 같은 방향으로 수정되어야 한다.

“악성메일을 식별하고 차단한다.”

▼ ▼ ▼

“모든 이메일을 의심하고 확인한다.”

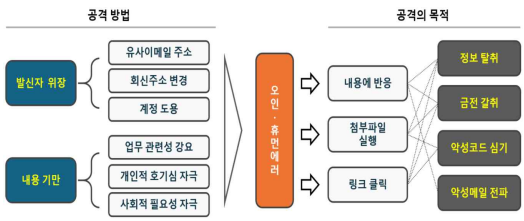
사용자에게 직관적 판단(intuition)을 요구하기보다는 기계적이고 객관적인 대응(objective response)을 유도하는 방안이 필요하다. 즉, 발신자의 신원이나 이메일의 내용에 관계없이 모든 이메일을 의심하고 확인하는 절차를 습관화해야만 사고 발생을 줄이고 피해를 예방할 수 있다.

그러나 이러한 방식의 구현은 쉽지 않다. 사용자에게 모든 이메일을 의심하고 확인하도록 강요하는 것은 과도한 요구일 수 있다. 더불어, 사용자가 이메일을 확인할 수단이 무엇인가라는 문제가 제기된다. 현재의 이메일 클라이언트는 발신자, 수신자, 참조자, 제목, 내용, 첨부파일 등의 정보를 제공한다. 필요시에는 메일의 헤더를 볼 수 있는 기능도 제공한다. 그러나, 대부분의 사용자는 의심을 하지도 않지만 메일 헤더 정보를 해석할 능력도 가지고 있지 않다. 실제로 이를 사용자에게 요구하는 것은 비현실적이다.

따라서 사용자에게 의심과 확인의 책임을 부과하는 대신, 보안을 고려한 사용자 친화적 환경을 제공하는 것이 필요하다. 이는 사용자가 보다 쉽게 보안 역할을 수행할 수 있도록 지원하는 시스템과 인터페이스가 필요함을 의미한다. 궁극적으로, 이러한 개선된 사용자 환경이 제공될 때, 사용자의 보안 대응 능력이 향상되어 악성메일로 인한 사고를 효과적으로 줄일 수 있을 것이다.

4.3 확장된 이메일 정보 제공

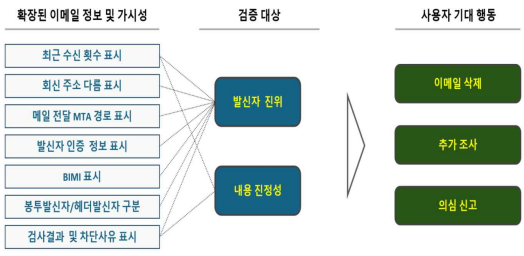
다음 (그림 3)은 악성메일 공격의 목적과 전개 방법을 도식화한 것이다. 그림에서 알 수 있듯이, 이러한 공격의 핵심은 발신자를 위장하고 이메일 내용을 조작하여 수신자의 신뢰를 얻는 데 있다. 이를 통해 공격자는 수신자로 하여금 자신이 의도한 행동을 유도하여, 궁극적으로 공격의 목적을 달성하게 된다.



(그림 3) 악성메일 공격 목적 및 전개 방법

악성메일은 앞서 언급한 바와 같이 기존 보안시스템을 회피하여 사용자 수신함에 도달한다. 그렇다면, 수신자가 겉보기에 평범한 이메일의 악성 여부를 어떻게 판별할 수 있을까? 이 과정에서 가장 중요한 것은 발신자의 신원을 정확히 인증하는 것이다. 발신자가 실제로 신뢰할 수 있는 인물인지 확인하는 것만으로도 대다수의 악성메일을 걸러낼 수 있다.

아래 (그림 4)는 발신자의 진정성을 검증하기 위해 활용할 수 있는 확장된 정보를 설명하고 있다. 이러한 확장된 정보는 수신자가 이메일의 신뢰성을 보다 명확하게 판단할 수 있도록 지원하며, 악성메일로 인한 사고를 예방하는 데 중요한 역할을 한다.



(그림 4) 사용자 기대 행동을 유도하는 확장된 정보

4.3.1 최근 수신 횟수 표시

많은 악성메일 공격이 유사 이메일 주소를 사용한다. 수신자는 발신자의 표시 이름이나 미세하게 변형된 철자에 속는 경우가 많다. 따라서, 해당 이메일 주소로부터 수신자가 최근 일정 기간 수신한 이메일의 수를 사용자가 볼 수 있도록 표시하면 검증의 효과를 얻을 수 있다.

4.3.2 회신 주소 표시

이메일 헤더에는 Reply-to: 필드(RFC 5322)가 있다[34]. 이것은 발신자의 이메일 주소와 다른 이메일 주소로 회신을 받고자 할 때를 지원하기 위해서이다. 주로 대량으로 발송하는 홍보메일에서 사용된다. 하지만, 양자간 교신을 공격자가 삼자간 교신으로 만들 때도 흔히 이용된다. 발신자 주소와 회신 주소가 다르다는 것을 인지함으로써 검증의 효과를 얻을 수 있다.

4.3.3 BIMI 표시

BIMI[4](RFC draft stage)는 이메일 클라이언트 소프트웨어에서 브랜드 로고를 표시할 수 있도록 한다[35]. BIMI를 사용하면 사용자는 이메일의 발신자가 신뢰할 수 있는 기관인지 쉽게 식별할 수 있다. 이것은 시각적인 정보를 통해서 수신자가 발신자의 진정성 여부를 알 수 있도록 지원한다.

4.3.4 이메일 전달 경로 표시

이메일의 헤더에는 어떤 경로를 거쳐서 수신되었는지 MTA[5](message transfer agent)들의 정보를 포함하고 있다. 각 MTA의 공인 IP 주소를 확인하여 해당 메일이 어떤 국가들을 거쳐서 수신되었는지를 시각적으로 표시할 수 있다. 국가정보를 시각적으로 인식함으로써 발신자의 진정성을 검증하는데 도움이 될 수 있다.

4.3.5 발신자 인증 정보 표시

SPF[6](RFC 7208)[36], DKIM[7](RFC 6376)[37], DMARC[8](RFC 7489)[38], ARC[9](RFC 8617)[39]는 모두 발신자의 진정성을 검증하기 위한 이메일 인터넷 표준들이다. 하지만, 이 정보들은 수신 서버에서 검사가 이루어졌다 하더라도 이메일 헤더에 기록될 뿐 사용자에게 노출되지 않는다. 설령 이메일 헤더 조회를 통해 해당 정보에 접근하더라도 전문적인 지식이 없으면 해석하기 어렵다. 이런 정보들을 사용자가 이해하기 쉽게 보여줌으로써 검증의 효과를 얻을 수 있다.

4.3.6 봉투발신자/헤더발신자 구분

이메일 수·발신 과정에서 이메일 인터넷 표준은 봉투발신자(envelope sender)와 헤더발신자(From: 필드)를 구분하고 있다. 봉투발신자는 주로 MTA간 이메일 전송을 위해 사용되며 'MAIL FROM' 명령을 통해 지정된다(RFC 5321, 5322)[40]. 만약, SPF 정보에 문제가 있거나 봉투발신자와 헤더발신자가 서로 다르다면 의심해 볼 여지가 생긴다. 그러나, 봉투발신자는 MTA간의 통신에만 이용될 뿐 이메일 헤더에 기록되지 않는다. 공격자들은 이런 점을 이용한다. 따라서, 이메일을 수신하는 서버는 봉투발신자 정보와 SPF 검사정보를 이메일 헤더에 기록하도록 해야 한다. 그

4) BIMI(brand indicators for message identification): 이메일 발송자가 자신들의 브랜드 로고를 수신자의 이메일 클라이언트에서 표시할 수 있도록 하는 인증 기술이다.

5) MTA(mail transfer agent): 이메일을 송수신하는 소프트웨어로, SMTP를 사용하여 이메일 서버 간에 메시지를 전송한다. 이메일 전달 과정에서 중개 역할을 하며, 수신자 메일서버로 메시지를 배달한다.

6) SPF(sender policy framework): 도메인 소유자가 이메일 발송을 허용한 IP 주소 목록을 정의하는 DNS 레코드이다. 이 목록을 참조하여 발송된 이메일의 출처를 검증하고, 스팸 및 피싱을 방지한다.

7) DKIM(domainkeys identified mail): 도메인 소유자가 전송하는 이메일에 디지털 서명을 추가하여, 수신자가 해당 이메일의 출처를 검증하고 내용이 변경되지 않았음을 확인할 수 있도록 한다.

8) DMARC(domain-based message authentication, reporting & conformance): SPF와 DKIM을 기반으로 이메일 인증을 강화하고, 인증 실패 시의 처리 정책을 정의하며, 인증 결과를 도메인 소유자에게 보고하는 메커니즘이다.

9) ARC(authenticated received chain): 이메일이 여러 중개자를 거칠 때도 초기 인증 결과를 보존하고 전달할 수 있도록 하는 체계이다. 이메일이 중간에 변경되어도 원래의 인증 정보를 유지할 수 있다.

리고 이메일 클라이언트는 봉투발신자와 헤더발신자가 서로 다를 경우 사용자에게 보여주고 경고를 한다면 검증의 효과를 얻을 수 있다.

4.3.7 검사 결과 및 차단 사유 표시

이메일 서버를 사내에 구축하는 경우든 외부 구독 서비스를 이용하는 경우든 메일서버가 단독으로 운영되는 경우는 드물 것이다. 대부분의 경우 스팸필터 또는 추가적인 이메일 보안솔루션이 배치되어 악성메일을 차단하고 있다. 이와 관련하여 두 가지의 개선점을 지적할 수 있다.

첫째, 악성메일로 판단되어 차단된 경우에도 그 이유나 관련 정보가 이메일 헤더에 기록되지 않는다. 차단된 이메일은 사용자에 의해 복구될 수 있는 서비스가 제공되기도 하는데, 이때 사용자는 차단에 대한 별다른 이유를 설명받지 못한 상태에서 자신이 스스로 오탐이라고 판단하면 복구하는 경향이 있기 때문에 매우 위험하게 된다. 따라서, 사용자에 의해 차단된 이메일이 복구되는 경우를 위해서라도 검사정보를 이메일 헤더에 기록해 두어야 한다.

둘째, 관리자가 설정을 조정하여 오탐을 줄이기 위해 기준을 완화하거나 허용필터에 등록한 경우, 악성이메일이 차단되지 않고 사용자에게 전달될 수 있다. 이때에도 사용자는 정상적인 이메일로 인식하고 처리할 가능성이 높다. 따라서, 이메일 보안시스템은 모든 검사정보를 헤더에 기록해야 하며, 강한 보안 설정이 적용된 경우에는 차단 가능성에 대한 정보 등도 함께 제공해야 한다. 이를 통해 사용자는 이 정보를 활용하여 검증 효과를 얻을 수 있도록 해야 한다.

사용자는 중간 단계의 보안장비와 직접적으로 상호작용하는 것이 아니라 이메일 클라이언트만을 사용하므로, 동일한 인터페이스를 통해 검사 정보가 제공되어야 효과적이다. 이러한 방식으로 사용자에게 필요한 정보를 전달함으로써, 악성메일 공격에 대한 대응력을 강화할 수 있을 것이다.

4.4 사용자 보안 인터페이스

아래 (그림 5)는 이메일 클라이언트에서 확장된 정보를 제공하는 사용자 인터페이스의 예시 구현을 보여준다. 본 연구에서 제시하는 개념에 의하면, 이러한 기능은 윈도우 기반 응용프로그램뿐 아니라 웹기반 응용프로그램에서도 동일하게 구현될 수 있다.

사용자는 자신의 관심사-익숙한 발신자, 처리해야 할 업무, 개인적 호기심 또는 사회적 필요 등-에 의해 확인 편향(confirmation bias)[10]을 가질 수 있다. 이와 함께 비주의적 시각정보(inattentional blindness)[11] 문제도 발생할 수 있다. 그러나 이러한 문제는 사용자의 의지에서 비롯된 것이 아니라, 오인이나 착각에 의한 결과라고 볼 수 있다. 즉, 이는 휴먼에러(human error)로 인식해야 한다. 따라서, 이메일 클라이언트는 이러한 문제의 발생 가능성을 고려하여 특정 조건에 따라 자동으로 화면을 제공하거나 경고 메시지를 생성하는 등 사용자의 보안을 지원하는 사용자 인터페이스(human interface for security)에 대한 개선이 필요하다.

(그림 5) 이메일 클라이언트(Outlook)의 확장된 이메일 정보 제공 구현 예시

10) 확인 편향(confirmation bias): 자신의 기존 신념이나 가정을 확인하고 강화하는 정보만을 선택적으로 찾고 해석하는 경향으로, 이는 이미 믿고 있는 것에 맞는 정보를 더 신뢰하고, 반대되는 정보는 무시하도록 한다.

11) 비주의적 시각정보(inattentional blindness): 사람들이 특정한 것에 주의를 집중할 때 그 외의 명백히 보이는 시각적 정보나 물체를 인식하지 못하는 현상으로, 이는 주의가 한정된 자원임을 보여준다.

자동차 분야에서는 운전자 및 보행자를 보호하기 위한 다양한 안전 기준이 국가별로 존재하며, 자동차 제조업체는 이를 준수하여 해당 국가에서 판매할 수 있도록 한다. 예를 들어, 후방 카메라 의무 장착, 자동 긴급 제동 시스템(AEB) 의무, 타이어 공기압 경보장치(TPMS) 의무 등 여러 가지 안전 요구사항이 마련되어 있다.

하지만, 이메일 클라이언트 소프트웨어에 대해서는 서비스 제공이나 개인정보 보호 등과 관련된 기준은 존재하지만, 사용자 인터페이스와 관련된 기준은 여전히 부족해 보인다. 이에 본 연구에서는 이메일 클라이언트가 악성메일 사고의 예방을 위해 사용자에게 반드시 제공해야 하는 기능들을 아래 <표 2>와 같이 제안하고자 한다.

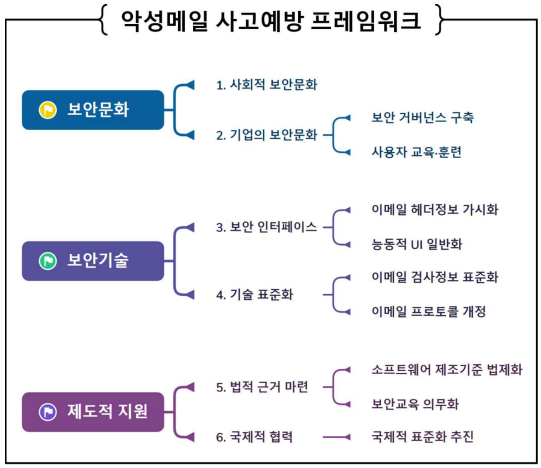
<표 2> 이메일 사용자 안전 인터페이스 요구사항

구분	이메일 클라이언트 기능 요구 사항
정보 제공	① 발신자 식별을 위한 정보 제공 ② 동일 발신자 최근 수신 횟수 표시 ③ 별도 회신주소 사용여부 표시 ④ 확장된 이메일 검사정보 제공 ⑤ 메일발송 국가정보 제공
알림/경고	⑥ 필요 시 확장 정보 자동 노출 ⑦ 필요 시 첨부파일, 본문 링크 접근 전 경고 ⑧ 봉투발신자와 헤더발신자가 다를 시 경고 ⑨ 발신자로부터 최근 수신횟수=0인 경우 경고 ⑩ 회신메일 작성 시 헤더발신자와 회신주소가 다른 경우 경고

5. 결 론

본 연구에서는 악성메일의 공격유형, 피해사례 등으로부터 기존 접근 방식의 한계 및 개선 필요성을 분석하고, 피해를 줄이기 위한 방안으로써 사용자 주도의 보안 인식 전환, 사용자 훈련 목표의 변경, 확장된 이메일 정보 제공, 사용자 보안 인터페이스 등을 제시하였다. 이는 오랜 현장 경험을 바탕으로 하고 제로 트러스트 보안모델의 원칙(fundamental principle)으로부터 착안한 것으로, 인식을 갖춘 사용자에게 확장된 이메일 정보를 제공함으로써 악성메일에 대한 식별력을 높여 피해를 줄이는 전략이다.

이러한 접근에서 무엇보다 중요한 것은 사용자가 단순히 보안시스템에 의존하는 것이 아니라, 스스로 보안의 주체로서 역할을 수행할 수 있도록 하는 것이다. 향후 본 연구에서 제시한 개념을 (그림 6)의 '악성메일 사고예방 프레임워크'로 정의하고, 관련 연구를 지속적으로 진행할 계획이다. 이를 통해 악성메일 공격의 예방 및 대응 체계를 더욱 정교화하고, 사용자 주도의 보안 강화를 통해 전반적인 사이버 보안 환경 개선에 기여하고자 한다.



(그림 6) 악성메일 사고예방 프레임워크

'악성메일 사고예방 프레임워크'는 보안문화, 보안기술, 제도적 지원의 3개 범주에 6개의 하위 목표와 세부 항목들로 구성되어 있다. 그리하여, 향후의 연구는 1) 제로 트러스트 보안 인식 내면화를 위한 교육·훈련 프로그램 개발 2) 이메일 검사정보 표준화 3) 이메일 클라이언트 안전 필수 기능 법제화 추진 등의 하위 주제로 세분화하여 추진하고자 한다.

이 중 '사용자 교육·훈련'의 경우 기업에서 실제로 피싱메일 대응훈련을 실시하며, 제로 트러스트를 사용자에게 내면화할 수 있는 방안을 통해 달성할 수 있을 것으로 본다. 또한, '보안 인터페이스'의 일반화를 위한 '기술 표준화'는 기존 프로토콜을 확장하고 IETF(Internet Engineering Task Force)를 통한 RFC(request for comments) 표준화 시도를 통해 진행할 수 있다. 그다음으로 법제화를 추진하는 단계를 밟아 나가면 '악성메일 사고예방 프레임워크'의 기술적, 제도적 범주의 핵심적인 요소들은 구현 가능할 것

이다.

본 연구는 악성메일로 인한 피해를 줄이기 위한 전략으로 '악성메일 사고예방 프레임워크'를 제안하였다. 그러나 이를 완성하기 위해서는 해결해야 할 몇 가지 한계가 존재한다. 첫째, 기존의 방식과 차별될 뿐만 아니라 다양한 환경에서 보편적으로 적용할 수 있는 사용자 교육·훈련 프로그램에 대한 연구가 이루어져야 한다. 둘째, 이메일 보안솔루션 및 클라이언트 개발업체가 적극적으로 참여해야만 사용자들을 지원할 수 있게 되는데 이를 실현하기 위해서는 검사정보 체계의 국제적 표준화가 필수적이다. 하지만, 이 과정은 최소 수년이 소요될 수 있기 때문에 후속 연구에 대한 지속적인 지원이 반드시 필요하다. 셋째, 소프트웨어 안전 요건의 법제화도 중요한 과제로, 이를 추진하기 위해서는 행정부와 국회의 협력을 이끌어내야 한다. 따라서 행정 및 법률 분야에 대한 추가적인 연구가 필요하며, 해당 분야 전문가들과의 협력이 필수적이다. 이러한 다각적인 노력이 결합되어야만 '악성메일 사고예방 프레임워크'의 성공적인 구현이 가능할 것이다.

위와 같은 한계에도 불구하고, 본 연구는 사용자 중심의 보안 전략을 제시하고 이를 실현하기 위한 구체적인 방법을 제시함으로써 중요한 학문적 기여를 했다고 평가할 수 있을 것이다. '악성메일 사고예방 프레임워크'는 사용자 보안 인식을 하나의 문화로 정착시키고, 기술을 표준화하여 악성메일 위협을 극복하려는 목표를 가지고 있다. 이를 통해 보안 투자 여력이 부족한 사용자들도 안전한 이메일 환경을 구축할 수 있으며, 궁극적으로 누구나 보안 위협으로부터 보호받을 수 있는 인터넷 환경을 조성하는 데 기여할 것으로 기대된다.

참고문헌

[1] I. Ghafir and V. Přenosil, "Advanced Persistent Threat and Spear Phishing Emails", International Conference on Distance Learning, Simulation and Communication, pp. 34-41, 2015.

[2] NCSC(National Cyber Security Centre), 'Business Email Compromise: Dealing with Targeted Phishing Emails', 2020.

[3] 이선호, 한민수, "산업망에서의 APT (지능형 지속 위협) 침투경로 분석 및 대응방안 고찰: 스턱스넷 사례를 중심으로", 한국산업보안연구, 제5권, 제1호, pp. 221-253, 2015.

[4] K. Krombholz, H. Hobel, M. Huber, and E. Weippl, "Advanced Social Engineering Attacks", Journal of Information Security and Applications, Vol. 22, pp. 113-122, 2015.

[5] ISACA(Information Systems Audit and Control Association), 'The State of Cybersecurity 2022 Report', 2022.

[6] SecurityWeek, 'Man Pleads Guilty Over $100M BEC Scheme Targeting Google, Facebook', https://www.securityweek.com/man-pleads-guilty-over-100m-bec-scheme-targeting-google-facebook/ (검색일: 2024.09.10.).

[7] 조선비즈, 'LG화학, 가짜 이메일 믿고 240억 날려… 경영진 문책론 나와', https://biz.chosun.com/site/data/html_dir/2016/04/29/2016042900679.html (검색일: 2024.09.10.).

[8] Kaspersky, 'DarkChronicles: The Consequences of the Colonial Pipeline Attack', 2021.

[9] 보안뉴스, '개인정보 유출된 골프존, 과징금 75억원·과태료 540만원 부과받아', https://www.boannews.com/media/view.asp?idx=129668&page=1&kind=2 (검색일: 2024.09.10.).

[10] C. Beek, D. McKee, J. Fokker, R. Samani and S. Povolny, 'Trellix Advanced Threat Research Report: October 2021', 2021.

[11] Barracuda, '2023 Email Security Trends', 2023.

[12] APWG(Anti-Phishing Working Group), 'Phishing

Activity Trends Report', 2023.
[13] FBI(Federal Bureau of Investigation), 'Internet Crime Report', 2023.
[14] 카카오, 실적보고서, https://www.kakaocorp.com/ir/referenceRoom/earningsAnnouncement (검색일: 2024.09.10.).
[15] 이은경, 조용현, "무역 산업에서의 비즈니스 스캠(Business Scam) 대응 문제점과 대책 방안", 한국컴퓨터정보학회 동계학술대회 논문집, 제24권, 제1호, pp. 307-310, 2016.
[16] 김경철, "명의도용 및 이메일 해킹 무역사기 예방에 관한 연구, 무역금융보험연구, 제23권, 제1호, pp. 137-150, 2022.
[17] 김도우, 이규범, "사회공학적 공격기법의 유형분류", 한국산업보안연구, 제9권, 제2호, pp. 9-21, 2019.
[18] N. S. Al-Musib, F. M. Al-Serhani, M. Humayun and N. Z. Jhanjhi, "Business Email Compromise (BEC) Attacks", Materials Today: Proceedings, Vol. 81, No. 2, pp. 497-503, 2023.
[19] 이도경, 장건수, 이경호, "AI를 통한 BEC (Business Email Compromise) 공격의 효과적인 대응방안 연구", 정보보호학회논문지, 제30권, 제5호, pp. 835-846, 2020.
[20] 손한기, 최성준, 문철한, 민준기, "Rule 기반의 필터링 및 딥러닝 LSTM을 결합한 이메일 스팸 분류", 2021년 한국컴퓨터종합학술대회 논문집, pp. 105-107, 2021.
[21] 유지현, "악성 이메일 공격의 사전 탐지 및 차단을 통한 이메일 보안에 관한 연구", 전기전자학회논문지, 제25권, 제4호, pp. 672-678, 2021.
[22] H. Abroshan, J. Devos, G. Poels and E. Laermans, "Phishing Attacks Root Causes", Lecture Notes in Computer Science, Vol. 10694, pp. 187-202, 2018.
[23] A. Heijden and L. Allodi, "Cognitive Triaging of Phishing Attacks", 28th USENIX Security Symposium, pp. 1309-1326, 2019.
[24] 이준희, 권헌영, "스팸메일 모의훈련 현장실험을 통한 기업의 인적 취약요인 연구", 정보보호학회논문지, 제29권, 제4호, pp. 847-857, 2019.
[25] SK쉴더스, '2024 보안 위협 전망 보고서', 2024.
[26] Proofpoint, '2024 State of the Phish: Today's Cyber Threats and Phishing Protection', 2024.
[27] Verizon, '2023 Data Breach Investigations Report', 2023.
[28] Insight, 'Prioritizing Cybersecurity: What Matters Most to Leaders in 2023', https://au.insight.com/en_AU/content-and-resources/2023/prioritizing-cybersecurity－what-matters-most-to-leaders-in-2023.html (검색일: 2024.09.10.).
[29] HP, 'HP Wolf Security: 'Rebellions and Rejections Report', 2021.
[30] 김보라, 이종원, 김범수, "보안교육 및 보안서비스가 조직구성원의 정보보안정책 준수에 미치는 영향", 정보화정책, 제25권, 제1호, pp. 99-114, 2018.
[31] 윤덕상, 이경호, 임종인, "지속적 실전형 모의훈련을 통한 피싱공격 대응역량 및 행동변화에 관한 연구", 정보보호학회논문지, 제27권, 제2호, pp. 267-279, 2017.
[32] S. Das, C. Nippert-Eng and L. J. Camp, "Evaluating User Susceptibility to Phishing Attacks", Information and Computer Security, Vol. 30, No. 1, pp. 1-18, 2022.
[33] 과학기술정보통신부, 한국인터넷진흥원, 한국제로트러스트포럼, '제로트러스트 가이드라인 1.0', 2023.
[34] P. Resnick, 'RFC 5322 - Internet Message Format', IETF (Internet Engineering Task Force) [On-line] https://datatracker.ietf.org/doc/html/rfc5322, 2008. (검색일: 2024.09.10.).
[35] S. Blank, P. Goldstein, T. Loder, T. Zink, M. Bradshaw and A. Brotman, 'Brand Indicators for Message Identification (BIMI)' [On-line] https://datatracker.ietf.org/doc/draft-brand-indicators-for-message-identification, 2024. (검색일: 2024.09.10.).
[36] S. Kitterman, 'RFC 7208 - Sender Policy Framework (SPF) for Authorizing Use of Domains in Email', IETF (Internet Engineering Task Force) [On-line] https://datatracker.ietf.org/doc/ht

ml/rfc7208, 2014. (검색일: 2024.09.10.).

[37] D. Crocker, T. Hansen and M. Kucherawy, 'RFC 6376 - DomainKeys Identified Mail (DKIM) Signatures', IETF (Internet Engineering Task Force) [On-line] https://datatracker.ietf.org/doc/html/rfc6376, 2011. (검색일: 2024.09.10.).

[38] M. Kucherawy and E. Zwicky, 'RFC 7489 - Domain-based Message Authentication, Reporting, and Conformance (DMARC)', IETF (Internet Engineering Task Force) [On-line] https://datatracker.ietf.org/doc/html/rfc7489, 2015. (검색일: 2024.09.10.).

[39] K. Andersen and M. Kucherawy, 'RFC 8617 - The Authenticated Received Chain (ARC) Protocol', IETF (Internet Engineering Task Force) [On-line] https://datatracker.ietf.org/doc/html/rfc8617, 2019. (검색일: 2024.09.10.).

[40] J. Klensin, 'RFC 5321 - Simple Mail Transfer Protocol', IETF (Internet Engineering Task Force) [On-line] https://datatracker.ietf.org/doc/html/rfc5321, 2008. (검색일: 2024.09.10.).

〔저자소개〕

최 영 국 (Youngkug Choi)
1996년 2월 인제대학교 이학사
현재 인제대학교 일반대학원 산업융합보안학 협동과정 석사과정
포스텍 기업부설연구소 소장
email : kugii2000@naver.com

권 익 현 (Ick-Hyun Kwon)
1998년 2월 고려대학교 공학사
2000년 2월 고려대학교 공학석사
2006년 2월 고려대학교 공학박사
현재 인제대학교 일반대학원 산업융합보안학 협동과정 주임교수
email : ikwon@inje.ac.kr