Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.27, NO.2, Apr. 2017 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2017.27.2.267

지속적 실전형 모의훈련을 통한 피싱공격 대응역량 및 행동변화에 관한 연구

윤 덕 상,† 이 경 호, 임 종 인‡
고려대학교 정보보호대학원

A Study on the Change of Capability and Behavior against Phishing Attack by Continuous Practical Simulation Training

Duck-sang Yoon,† Kyung-ho Lee, Jong-in Lim‡
Graduate School of Information Security, Korea University

요 약

본 연구는 한 회사에서 실제 업무 중에 있는 임직원들을 대상으로 장기간 여러 차수에 걸쳐 외부 해커들이 공격하는 동일한 경로와 방식으로 피싱(phishing)메일을 발송하고, 차수가 경과됨에 따라 메일 수신자들의 피싱 메일에 대한 식별능력과 대응행동을 측정하였으며, 훈련 간 부가적으로 외부통제 조건을 변화시켜 수신자들의 대응행동이 추가적으로 어떻게 변화되는지를 분석하였다. 분석결과 단발적 훈련보다는 지속적인 훈련이 임직원들의 피싱메일 식별능력과 감염율 감소에 정(+)의 영향을 주고 있음을 확인하였으며, 사회적 이슈나 시기적 이벤트와 연계한 피싱공격에 더 많은 임직원들이 감염이 되며, 감염자에 대한 인사조치와 같은 내부통제정책 강화가 임직원들의 피싱공격 대응행동에 정(+)의 영향을 주고 있음을 확인할 수 있었다. 이러한 결과에 따라 각 기관이 임직원들의 피싱공격 대응역량 강화를 위한 올바른 훈련방향을 제시하고자 한다.

ABSTRACT

This study emulated unscheduled phishing e-mails over a long period of time by imitating the manner in which external hackers attacked a group of employees in a company. We then measured and analyzed the recipient's ability to identify and respond to phishing e-mails as training progressed. In addition, we analyzed the changes in participants' response behavior when changing the external control condition between the training. As a result of the analysis, it was confirmed that the training duration had a positive (+) relationship with the employees' ability to identify phishing e-mails and the infection rate, and more employees read emails and infected with phishing attacks using social issues and seasonal events. It was also confirmed that reinforcement of internal control policy on infected persons affects positively (+) on the phishing attack response behavior of employees. Based on these results, we would like to suggest the right training method for each organization to enhance the ability of employees to cope with phishing attacks.

Keywords: phishing, email, social engineering, APT, advanced persistent threat, security awareness training

I. 서 론

몇 년 전까지만 해도 정보보안에 대한 사회적인 인식이 낮고 대응 기술수준도 높지 않아 사이버 공격 대상의 대부분이 취약한 시스템이나 네트워크였으나, 대응 및 탐지 솔루션들이 고도화되고 정보보안에 대한 투자가 적극적으로 이루어지고 있는 지금은 공격대상이 시스템이나 네트워크가 아닌 사람으로 바뀌

Received(02. 28. 2017), Modified(1st: 03. 29. 2017, 2nd: 04. 06. 2017), Accepted(04. 06. 2017)

† 주저자, yoondark@naver.com
‡ 교신저자, jilim@korea.ac.kr(Corresponding author)

어 가고 있다. 모두가 인정하듯이 사람은 사이버 방어 체인 중에서 가장 취약한 연결고리이기 때문이며 이러한 내용을 증명이라도 하듯 최근 보안침해사고의 대부분이 사람인 내부 직원들로 기인하고 있다[1][2][3].

Nikolakopoulos[4]는 "누군가가 기술적으로 완벽하게 시스템을 디자인 한다고 해도 여전히 사용자는 그 시스템의 취약한 포인트가 될 것이다."라고 했을 정도로 사람은 당분간 사이버 상에서 가장 취약한 존재로 남아 있을 것이다.

이러한 사람의 취약점을 이용하여 공격을 하는 방법 중에 가장 많이 활용되는 방법이 피싱이며, 주로 메일이 이러한 피싱의 도구로 사용되고 있다. 2014년 12월 익명의 해커가 한국수력원자력(이하 한수원)의 임직원 개인정보와 원자로 도면 등을 해킹한 후 웹사이트에 공개하며 원전가동 중단과 돈을 요구했던 사건도 사전에 메일을 이용하여 한수원과 국방분야 전문가들에게 악성코드가 담긴 한글워드 파일을 보내 감염시킨 후 내부정보를 해킹하였으며, 2016년 5월 국내 쇼핑몰 사이트인 인터파크도 동생을 사칭한 피싱메일에 속은 내부 직원 PC를 통해 1천만 명이 넘는 고객정보가 빠져나가는 사건이 발생하기도 하였다[5][6].

상황이 이렇다 보니, 정보보안을 위한 시스템에 대한 투자도 중요하지만 조직내부의 직원들이 스스로 피싱공격을 식별하고 대응할 수 있도록 교육시키고 훈련시키는 것이 성공적인 사이버 방어체계에서 가장 중요한 요소가 되었다. 훈련의 효과를 높이는 방법을 연구하기 위해 몇몇 연구기관에서 이에 대한 연구가 이루어졌지만 대부분 실험실 환경에서 사전에 선발된 실험자들을 대상으로 이루어지다 보니 현실 환경에서의 적용성에 많은 문제가 제기되었다[7].

본 연구는 한 회사에서 실제 업무 중에 있는 임직원들을 대상으로 장기간 여러 차수에 걸쳐 외부 해커들이 공격하는 방식과 동일한 경로와 방식으로 피싱(phishing)메일을 발송하고, 차수가 경과됨에 따라 메일 수신자들의 피싱 메일에 대한 식별능력과 대응행동을 측정하였으며, 훈련 간 부가적으로 외부통제 조건을 변화시켜 수신자들의 대응행동이 추가적으로 어떻게 변화되는지를 분석하였다. 이러한 결과를 통해 본 연구에서는 각 기관이 임직원들의 피싱공격 대응역량 강화를 위해 진행하는 훈련에 대한 올바른 방향을 제시하고 피싱공격 피해를 최소화하는데 기여하고자 한다.

II. 연구의 배경 및 선행연구 분석

2.1 연구의 배경

2.1.1 피싱 공격의 위협

국제피싱대응협의기구 APWG(Anti-Phishing Working Group)가 발표한 2016년 3분기 피싱활동동향보고서(phishing activity trends report)에 따르면 피싱사이트로 탐지된 건수가 월 평균 10만~15만건에 이르고 있으며 월 단위로 신고되는 피싱사고도 7만~9만건이나 되고 있다[8].

국내 바이러스 전문회사인 안랩(AhnLab)의 2016년 11월의 악성코드발생동향 보고서에서도 국내에서 월간 탐지되는 악성코드가 900만건~1000만건에 이르는 것으로 보고되고 있다. 새롭게 등장하는 악성코드의 유형 또한 APWG와 AhnLab 모두 피싱공격에 이용되는 Trojan이 대부분 차지하고 있어 전 세계적으로 피싱공격이 대세적으로 만연하고 있음을 증명하고 있다.

2.1.2 피싱 대응훈련의 필요성 및 기대효과

앞서 개요에서 언급한대로 피싱공격은 사람을 대상으로 이루어지는 공격이기에 이처럼 계속되는 피싱공격의 위협에 대응하는 가장 좋은 방법은 목표가 되는 사람이 피싱공격의 위험을 명확히 인식하고 대응할 수 있는 역량을 갖추도록 훈련시키는 것이다.

이러한 훈련에 대해 ENISA[9]는 임직원들의 정보보안 인식을 강화시키는 훈련은 조직내부의 보안을 강화시키는 효과뿐만 아니라 잠재적으로는 보안 사고와 이로 인해 발생하는 비용까지도 없애주기 때문에 정보보안에 들어가는 투자를 줄여주는 역할을 할 것이라고 했으며, Carlson[10]은 이러한 정보보안 훈련은 기업의 정보자산을 안전하게 보호하게 되어 궁극적으로 비즈니스 위험을 최소화 하고 업무연속성을 증가시켜 기업의 이익을 극대화 시키는 역할을 한다고 말하고 있다.

2.2 선행연구 분석

사용자에 대한 정보보안 인식강화 및 대응 훈련이 기업에 IT정보자산 보호에 가장 중요한 조건임이 인식되면서 이에 대한 연구와 논의가 활발히 진행되고 있다. 일반적으로는 정보보안 인식강화 훈련의 방법

및 효과증진 방안에 대한 연구가 주를 이루고 있으며, 특별히 큰 위협으로 부상하고 있는 피싱 공격에 대한 효과적인 대응훈련에 대한 연구가 다양하게 진행되고 있다.

2.2.1 효과적인 정보보안 훈련 방법

SANS Institute[1]는 효과적인 정보보안훈련 방안으로 3단계 교육훈련을 제시하고 있다. 임채호[11]는 정보보안 관리체계별로 정보보안인식제고 구현모델과 인식제고 4가지 원칙, 인식제고 프로그램 설계방법, 자기교육시스템 등을 제안하였고, 엄정호[12]는 대부분의 사이버보안 교육이 간단한 실습이나 교수중심의 일방향 교육, 훈련 시나리오 예고제 방식으로 진행되기 때문에 교육효과가 없다고 진단하고 사이버보안 역량 강화를 위해서는 이론이나 사전에 알려진 시나리오식 훈련으로 교육이 이루어져서는 안 되며, 실제적 사이버 훈련 과정을 통해 역량을 강화해야 한다며 사이버 훈련체계의 개선방안으로 교육생 훈련역량 평가방법, 훈련생 주도의 창의적 문제해결 방식의 사이버 훈련장 환경조성, 사이버 훈련 성과평가 방법, 지식 전달자에서 학습 촉진자로의 전문교수 역량변화 등의 방안을 제시하였다.

이홍재, 차용진[13]은 효과적인 정보보안교육의 선행요인 분석을 위해 CIPP모형을 토대로 투입-과정-효과로 구성된 연구모형과 가설을 설정하고 관계분석을 통해 정보보안교육은 투입된 인적, 물적 자원이 많고 교육과정과 내용이 적절할수록 훈련효과가 높음을 증명하였으며, 특히 기관장의 관심이 교육훈련효과 증진에 정의 영향이 있음을 확인시켜 주었다.

2.2.2 피싱메일 모의훈련

일반적인 정보보안에 대한 인식강화 방법으로 다양한 교육방법이 연구되었지만 정작 피싱공격은 인간의 습관이나 속성, 심리적인 약점을 이용한 다양한 사회 공학적 기법이 활용되고 있으며, 그 중에서 이메일을 이용한 공격방법을 해커들이 가장 많이 사용하고 있다[14, 15]. 따라서 일반적인 인식강화 훈련과 더불어 어떻게 하면 피싱공격을 회피할 수 있는지에 대한 실전형 훈련을 통해 사람이 직접 경험하고 체득할 수 있는 교육이 이루어진다면 가장 효과적일 것이다.

초기 실전형 훈련 방법으로는 자신이 가지고 있는 피싱공격에 대한 지식을 테스트 할 수 있는 웹페이지를 만들어 사용자가 자신을 평가할 수 있도록 하는 방식으로 이 메일 스크린 샷을 여러 개 올려 그중에 정상적인 메일을 찾아내게 하는 방법이 사용되거나, 학습 환경을 오프라인 교실 내에 만들어 수시로 체득할 수 있도록 하는 방법이 사용되었다[16].

이후 위조된 훈련 이메일을 사용자에게 보내어 대응훈련을 하는 방법이 인디에나 대학의 학생들[17]과 웨스트포인트 육군사관학교 생도들[18]을 대상으로 시도되었다. 웨스트포인트 사관학교 경우 1차적으로 훈련 전 아무런 사전 교육도 실시하지 않은 상태에서 위조메일을 보내 결과를 관찰하고, 두 번째 메일 발송전 사전교육을 실시한 후 다시 한 번 위조메일을 보내 학습효과를 측정하는 방법으로 훈련효과를 평가하였다.

더 나아가 카네기멜론대학교의 Pnnurangam Kumaraguru등은 현실과 유사한 모의훈련 환경을 구성하여 모의훈련을 시도하였으며, 두 번에 걸쳐서 연구결과를 공개하였다. 첫 번째 연구에서는 실험실 환경을 만들어 실험환경 내에서 훈련을 실시하였으며, 실험대상자에게 피싱메일을 보내 피싱에 속은 사람들을 두 그룹으로 나누어 한 그룹에는 텍스트로 된 훈련용 문서를 보내고, 다른 한 그룹에는 만화로 쉽게 만들어진 훈련문서를 보내 학습효과를 비교하여 사람들이 직관적이고 재미있게 구성된 훈련용 자료에 더 반응을 하고 효과가 있음을 증명하였다[19].

두 번째 연구에서 실험실 환경이 아닌 실제 운영중인 포르투갈 회사의 임직원들을 대상으로 타겟형 피싱공격(spear phishing attack)방식으로 가짜 메일을 보내고 해당 메일에 속아 개인정보를 가짜 웹사이트에 입력한 사용자들 한 그룹에는 일반 피싱 위협 대응방법 교육 자료를 보내 대응방법을 교육 시키고 다른 한 그룹에는 스피어피싱 위협 대응방법이 담긴 교육 자료를 보내 교육을 시킨 후 1주일 뒤 다시 한번 훈련을 통해 훈련효과를 비교 하였는데 두 그룹간의 큰 차이가 발견되지 않았지만 전혀 교육을 받지 않은 임직원들 보다는 훈련효과가 높다는 연구결과를 발표하였다[7].

2.2.3 피싱 교육훈련의 제한사항 및 문제점

이러한 교육과 훈련은 보안의식 향상과 피싱공격 방어대책의 일환으로 자주 권장되고 널리 사용되는 접근 방식이지만[20][21][22] 대부분 위험성이나

대응방법을 알려주는 이론형 교육이고 모의훈련을 하더라도 단기간에 한 두 번에 걸친 짧은 훈련을 실험실 환경에서 수행한 연구들일 뿐 실제 환경에서 장기적이고 지속적인 훈련을 통해 효과를 평가 한 연구는 드물다. 실험실 연구는 주어진 실험환경에서 사용자들이 어떻게 행동을 하는지 이해하는 데에는 아주 유용하지만 실제 생활환경을 완전히 반영할 수 없기 때문에 타당성이 부족하고 결과의 유효성 또한 데이터에 영향을 미칠 수 있는 외부 상황들을 충분히 반영하지 못한 상태에서 일반화된 추론을 근거로 하고 있기 때문에 신빙성이 낮다[23].

하지만 실제 환경 하에서 훈련을 실시하는 것은 결코 쉬운 일이 아니다. 해커와 동일한 수준의 효과적인 수단을 만들어 내야하며, 워낙 다양한 외부 변수가 존재하기 때문에 많은 데이터를 얻을 수 있다 하더라도 신뢰할 수 있는 데이터를 추출하는 환경을 만들기가 매우 힘들다. 또한 연구 방법이 완벽히 준비된다 하더라도 실제 근무를 하고 있는 기업에 협조를 얻어 내기는 하늘에 별 따기 만큼이나 어렵고 간신히 협조를 얻는다 하더라도 나타난 결과에 대해 공개적으로 활용하는 것에 동의를 얻어내기가 쉽지 않다. 더불어 훈련 전에 훈련참여자들의 개인적인 동의를 얻지 못하고 훈련을 실시해야 하는 훈련방식의 근본적인 문제로 인해 도덕적 비난 또한 감수해야만 할 것이다[7].

III. 연구모형 및 가설

3.1 연구모형

본 연구는 선행연구들이 가지고 있는 이러한 문제와 한계를 극복하고자 국내 한 통신전문회사의 IT전문계열회사 임직원들을 대상으로 임직원들의 피싱메일 대응 역량강화 목적의 실전형 모의훈련을 실시하였으며, 훈련에 따른 임직원들의 대응역량 변화와 훈련효과를 실증적으로 분석하고자, Fig.1.과 같은 연구모형을 설정하고 장기간에 걸쳐 지속적으로 거듭 실시한 훈련의 횟수와 훈련자들의 직책, 고용유형 그리고 훈련 간 적용된 인사규정, 피싱 시나리오의 사회적 이슈 연관성 등이 임직원들의 대응행동에 미치는 영향을 분석하였다.

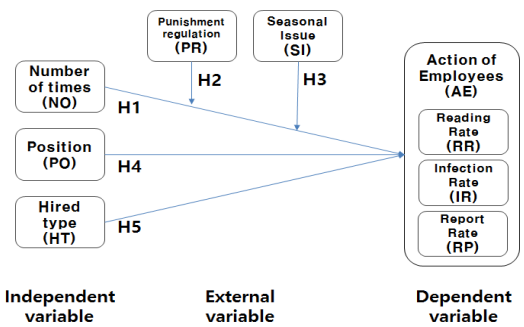

Fig. 1. Research model design

3.2 연구가설

3.2.1 훈련의 횟수와 피싱 대응역량

연구가설1(H1)은 모의훈련의 횟수가 임직원들의 피싱메일 대응역량에 미치는 인과관계에 대한 가설이다. 실전형 모의훈련을 한번으로 그치는 것이 아니라 정해진 기간간격에 주기적으로 여러 번에 걸쳐 지속적으로 실시하면 임직원들의 훈련에 이해와 관심이 높아지고 독일의 심리학자 Hermann Ebbinghaus의 망각곡선이론[24] 시간 내에 재학습이 이루어짐에 따라 잊혀진 기억을 되살려 학습효과 증진 및 대응역량 강화에 긍정적인 영향을 미칠 것이라는 가설을 도출하였다.

3.2.2 인사규정 강화와 피싱 대응역량

연구가설2(H2)는 모의훈련간 외부 변수로 적용한 인사규정변화가 임직원들의 피싱메일 대응행동에 미치는 인과관계에 대한 가설이다.

3.2.3 시즌연계이슈와 피싱 대응역량

연구가설3(H3)은 모의훈련간 사용한 훈련상황 시나리오가 임직원들의 피싱메일 대응행동에 미치는 인과관계에 대한 가설이다.

3.2.4 임직원들의 직책과 피싱 대응역량

연구가설4(H4)는 임직원들의 직책과 피싱 대응역량간 인과관계에 대한 가설이다.

3.2.5 고용유형과 피싱 대응역량

연구가설5(H5)는 기업에 고용형태와 피싱 대응역

량간 인과관계에 대한 가설이다.

3.3 변수의 정의와 측정항목

피싱메일 훈련을 통해 임직원들의 대응역량을 검증하기 위해 Table 1.과 같이 사용되는 연구 개념들의 타입과 변수의 정의 그리고 측정항목 등을 정리하였다.

이번 연구에 가장 중심이 되는 독립변수는 지속적으로 진행된 모의훈련 차수(NO)이며 연구기간동안 수행한 훈련의 횟수로 정의하였다. 훈련차수의 측정은 최초 시행을 1차수로 하여 이후 분기별로 수행된 차수를 순서화하여 차수 증가에 따른 종속변수의 영향을 분석하고자 한다. 임직원들의 직책(PO)은 훈련참가자들이 부여받은 직책으로 정의하였으며, 측정변수로는 임원(1), 팀장(2), 직원(3)를 사용하였다. 고용형태(HT)는 훈련 대상자들의 고용형태로 협력사(0), 정규직(1)을 측정변수로 정의하였다.

임직원들의 피싱대응능력의 실질적인 척도로 사용될 종속변수로는 가공된 메일을 받은 임직원들의 대응 행동(AE)을 변수로 선정하였다. 메일 수신자의 행동을 좀 더 세부적으로 파악하기 위해 피싱메일 수신자 대비 메일열람비율(RR), 열람 후 의도된 악성행위를 실행한 감염비율(IR), 메일수신 또는 열람 후 의심 피싱메일 수신을 신고한 신고율(RP) 등 3가지 반응을 측정항목으로 사용하였다. 이 연구에서는 훈련대상인력을 매번 랜덤하게 선택하여 훈련차수마다 표본의 수가 다르기 때문에 결과의 산술적 비교를 위해 비율척도를 사용하였다.

독립변수 이외에 훈련결과에 영향을 주는 외부변수도 정의하였는데 훈련결과에 따른 패널티 정책(PR)을 중간에 적용시키므로 정책 적용 전(0)과 정책 적용 후(1)의 훈련결과의 차이를 측정하였다. 또한 피싱메일 내용의 계절적 이슈연관성(SI)을 변수로 선택하여 피싱메일 공격 시나리오에 임직원들의 관심의 대상이 되는 시즌적 이슈를 연계(1)하여 보낸 메일과 이슈 미연계(0) 메일로 구분하여 임직원들의 피싱대응행동을 측정하였다.

3.4 훈련방법 및 특징

3.4.1 훈련대상 및 환경

본 연구에서는 실험환경이 가지고 있는 문제점을 극복하고 신뢰성 있는 훈련효과를 측정하고자 현재 다량의 개인정보나 중요정보를 가지고 실제 업무에 임하고 있는 국내 한 통신전문회사의 IT전문계열회사 임직원들을 대상으로 자신들이 업무를 하는 환경과 자원을 이용하여 실전형 모의훈련을 실시하였다. 연구자가 보안총괄책임자(CISO)로 근무하고 있는 회사이기에 별도의 협조가 불필요한 상황이며 실제적으로 임직원들의 훈련과 연구를 병행하여 실시하였다.

Table 1. Variable definition and measurement method

Types	Variables	Definition	Measurement method	Etc
Independent	Number of times (NO)	Number of times of simulated training	Execution Number(6 Quarter) 1 ~ 6	
	Positions (PO)	Responsibilities of the training participants	Title of training participants 1: Officer 2: Team leader 3: Employee	
	Hired types (HT)	Types of employment	0: Partner employees 1: Regular employees	
Dependent	Action of employees (AE)	Employee actions on phishing emails	Percent rate per actions RR: Reading rate IR: Infection rate RP: rePort rate	
External	Punishment regulation (PR)	Penalties for the training Result	0: No regulation 1: Applied regulation	
	Seasonal Issue (SI)	Issue relevance of mail content	0: No relation with issues 1: Related to issues	

3.4.2 훈련기간

기존의 연구가 대부분 1회 또는 2회 정도의 훈련만을 실험실 환경에서 수행 후 분석된 결과이므로 실제적인 자료의 신뢰성에 대해 의문을 갖게 한다. 본 연구에서는 2015년 2사분기부터 2016년 3사분기까지 총 6번에 걸쳐서 분기1회 모의훈련을 주기적으로 실시하여 방대한 양의 결과를 수집하였으며, 훈련간 결과를 상호 비교하여 선행훈련이 후행훈련에 어떠한 영향을 미치는지를 연구하였다.

3.4.3 훈련참가 인원

실험 대상 회사는 임직원 1,500명인 회사로 직급별로 임원 1.6%, 팀장 4.7%, 직원 94.4%로 구성되어 있으며, 협력사 직원 500명을 포함하여 총 2,000명이 근무하는 회사이다. 실전 환경에서 피싱공격이 특정 조건에 있는 임직원들을 대상으로 이루어지기 때문에 훈련 대상 인원 선정은 훈련 시나리오에 따라 사번, 이름, 사외메일 사용건수 등의 조건을 통해 차수별 400명~1000명을 선정하였으며 6회 평균 600명의 인력이 참가하였다. 대상자를 직급과 상관없이 랜덤하게 선정하였지만, 상대적으로 인원이 적은 임원, 팀장들은 평가 모수 확보와 직책자들의 책임감 고취를 위해 모든 훈련차수에 전원 포함시켰다. 이러한 인력선정 방법이 단기적으로는 직급별 훈련평가결과에 어느 정도 영향을 미치겠지만 장기적으로는 오히려 적정모수 확보에 의해 정밀도를 증가시켜 줄 것으로 판단하였다. 또한 정규직 직원과 협력사 직원이 함께 업무를 수행하기 때문에 협력사 인력들도 포함시켜 훈련을 진행하였다.

3.4.4 사용자 대응행동 정의

본 연구에서는 훈련결과를 좀더 명확하게 파악하기 위해 메일 수신후 임직원의 행동을 Fig.2.와 같이 정의하였다. 수신자 행동을 구분한 이유는 임직원들의 피싱메일 식별 시점을 파악하기 위해서이다. 메일열람은 실제로 피싱에 감염된 상태는 아니지만 제목 등에 의해 호기심이 자극되어 메일의 내용을 확인하는 행위로 피싱 피해를 받을 가능성이 높아진 단계이다. 감염은 메일본문이나 첨부로 전달된 유도된 행동(URL 링크를 클릭 또는 첨부파일 실행)을 하는 단계로 실제 피해를 받은 상태를 의미한다. 신고는

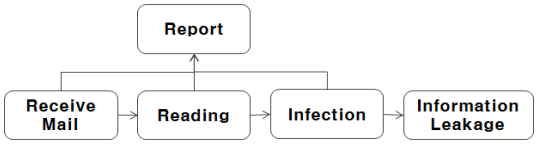

Fig. 2. User behavior process

메일을 수신한 사람이 열람전·후 또는 감염 후에 피싱메일임을 인지하고 신고하는 행위로 피해사실 사내 공유를 통해 추가적인 피해자 발생을 예방하기 위한 자발적 행동을 의미하며 수신자의 열람 및 감염 행동들은 메일 로그를 통해 자동 수집하였다.

3.4.5 기타 훈련환경의 특징

실전환경에서 발생할 수 있는 다양한 외부 변수를 고려하여 처음에는 아무런 규제나 공지 없이 훈련을 진행하다가 어느 정도 훈련횟수가 경과된 뒤부터는 피싱에 감염된 사용자에 대한 인사적 패널티를 부여하는 정책을 전사적으로 적용하여 참가자들의 긴장감을 고조시켜 훈련에 미치는 영향도를 분석 하였으며, 사용자의 메일에 대한 호기심을 유발시키기 위해 각 훈련마다 사용하는 훈련 시나리오를 훈련당시의 계절적 이슈(seasonal issue)들과 연계하여 수행하였다. 다만, 계절적 이슈 적용 시와 그렇지 못한 상황을 분석하기 위해 몇몇 시험 시에는 계절적 이슈와 연계되지 않은 일반적인 시나리오를 사용하였다.

본 연구에 참가하는 회사는 보안서약서와 사내 내부 업무규정에 임직원의 정보보안 준수 의무가 명문화되어 있고 일부 보안위반활동에 대해 인사규제 정책이 정의되어 있기에 임의적, 불시적 정보보안 훈련이나 추가적인 인사정책 변화에 대해 임직원들이 도덕적으로 크게 문제 삼지 않는 기업문화가 이미 구축되어 있는 상태이다. 또한 업무 중 피싱메일이나 악성 바이러스가 포함된 의심 메일을 발견하였을 경우 신속히 주변에 전파를 하고 사내 악성코드 감염통제센터(security119)로 신고토록 하는 제도도 정착이 되어 있기에 장기간에 걸친 실전적 모의훈련을 할 수 있는 토대가 사전에 마련되어 있는 상태이다.

Table 2. Training results by type of employment

Action		15Q2	15Q3	15Q4	16Q1	16Q2	16Q7
Regular Employee	Reading (RR)	34.48%	34.63%	20.46%	23.75%	21.95%	15.59%
	Infection (IR)	22.17%	18.54%	5.19%	1.50%	5.15%	0.89%
	Report (RP)	9.36%	39.02%	24.21%	50.00%	26.47%	36.97%
Partner	Reading (RR)	78.77%	82.44%	71.70%	70.31%	68.97%	62.00%
	Infection (IR)	60.38%	59.51%	3.77%	4.69%	3.45%	4.00%
	Report (RP)	0.47%	19.02%	5.66%	20.31%	12.07%	10.00%

IV. 분석결과

4.1 훈련결과

4.1.1 임직원, 협력사 훈련결과 분석

약 2년 동안 총 6회에 걸쳐 실시한 실전형 피싱메일 대응모의훈련에 대한 정규직 임직원 및 협력사 직원들의 훈련결과는 Table 2.과 같다. 우선 정규직 임직원들의 결과를 살펴보면 훈련결과의 바로미터가 되는 사용자 행동 지수가 감염률(IR)인데 모의훈련의 횟수가 증가함에 따라 메일에 의한 피싱감염율이 최초 22.17%에서 제일 마지막에는 0.89%까지 줄어들어 감염이 거의 발생하지 않고 있음을 알 수 있다. 피싱메일을 수신한 이후 열람율도 완만하게 줄어들어 가고 있는 상황이며, 다소 변화가 심하기는 하지만 신고율 또한 초기보다는 크게 향상되어 있는 상태이다.

협력사 파견인력들도 감염율이 최초에는 모두를 깜짝 놀라게 할 정도로 60.38%를 기록했다가 마지막 훈련시에는 4%대를 유지하고 있는 상황이다. 하지만 악성메일을 열어보는 확률이 매우 높은 상태에 있기 때문에 의심스런 사외메일에 대해 피싱여부를 감지하고 대응하는 방법[25][26]에 대한 교육을 더 많이 실시할 필요가 있어 보인다.

4.1.2 직급별 훈련결과 분석

조직 내에서 책임감이 훈련시 대응행동에 어떠한 영향이 미치는 지를 확인하기 위해 직급별로 대응행동 결과를 정리하였다. 데이터 분석결과 전반적으로는 전사적 결과와 유사하게 훈련과정이 반복됨에 따라 각 직책내 임직원들의 대응 수준이 많이 좋아졌지만 특별히 임원(officer) 직책자들이 다른 팀장(team leader)나 일반직원(employee)보다는 감염율에 있어서 좋은 결과를 보여주고 있다.

하지만 열람율에서 보았을 때 임원들이 다른 직책자에 비해 열람율이 높은 경우가 많이 있으며, 신고율 또한 다른 직책자들과 유사한 상태를 보여주고 있다. 아마도 높은 직급의 임직원일수록 부하직원들이

Table 3. Training result by position

Action	Position	15Q2	15Q3	15Q4	16Q1	16Q2	16Q7
Reading (RR)	Officer(1)	17.24%	31.03%	27.59%	28.57%	5.26%	23.53%
	Team Leader(2)	42.03%	30.14%	21.05%	27.94%	23.53%	14.29%
	Employee(3)	34.29%	38.83%	19.42%	22.51%	22.16%	15.53%
Infection (IR)	Officer(1)	3.45%	6.90%	3.45%	0.00%	0.00%	0.00%
	Team Leader(2)	26.09%	19.18%	3.95%	1.47%	5.88%	1.59%
	Employee(3)	24.76%	21.36%	5.79%	1.61%	5.20%	0.86%
Report (RP)	Officer(1)	10.34%	44.83%	37.93%	47.62%	31.58%	58.82%
	Team Leader(2)	7.25%	38.36%	27.63%	61.76%	33.82%	49.21%
	Employee(3)	10.48%	37.86%	21.49%	47.59%	25.88%	35.57%
External	Punishment Reg.(PR)	0	0	1	1	1	1
	Seasonal Issue (SI)	1	1	1	0	1	0

먼저 피싱 메일을 발견하게 되면 보고를 통해 상급자에게 정보가 전달되기 때문에 다른 직원들보다는 빠른 시간 내에 피싱 공격을 인식할 수 있을 것이다. 따라서 열람율이 유사함에도 불구하고 감염율이 낮아질 수 있는 이유로 판단된다.

4.1.3 외부변수에 의한 행동변화 영향도

이번 연구에서는 두 가지 외부변수를 이용하여 훈련간에 적용함으로 임직원들의 대응행동에 어떤 영향이 있는지를 조사하였다. 두 가지 변수 중 사용자 대응활동에 커다란 영향을 준 변수는 훈련결과에 따라 인사적으로 패널티를 부여하겠다는 정책을 적용한 것이다. 이 정책은 두 번째 훈련이 종료된 후 공표되었으며, 훈련간 감염자로 적발이 되면 감염자에게 경고메일이 발송되고 해당 결과를 부서장에게 통보한다는 정책으로 3번 연속으로 동일한 상황이 발생하면 인사처벌까지 받도록 규정화 되어있다. 특히 현장 파견근무를 하고 있는 협력사 임직원들의 경우 관련결과가 본사에 있는 관리부서에 통보됨으로 임직원들의 경각심을 높여 커다란 관심을 갖게 된 것 같다. 이에 대한 영향으로 감염율이 2차보다 3차 시에 드라마틱하게 감소하였음을 확인할 수 있었다. 하지만 열람율이나 신고율에 대해서는 처벌 규정과 연계되어 있지 않기 때문에 정책변화에 따른 행동변화가 크게 나타나지 않았다.

또 하나의 변수인 피싱메일 내용(시나리오)이 훈련시점에 발생한 사회적, 계절적 이슈와 연관성을 가지고 있을 때와 그렇지 않을 경우의 결과를 확인한 결과 이슈와 연관도가 높을수록 훈련참여자들의 메일 열람율이 증가하고 그렇지 않을 경우 급격히 감소함을 확인할 수 있다. 즉, 이슈연관도가 낮은 메일의 경우 훈련자들이 쉽게 스팸메일임을 인식하게 되어 열람율 뿐만 아니라 감염율, 신고율이 상대적으로 높아지게 된 이유이다. 따라서 피싱메일 본문의 내용과 시나리오는 피싱메일 모의훈련 성과에 가장 큰 영향을 주는 요소이며 이러한 이유로 인해 최근의 피싱 공격이 점점 지능화되고 특정인을 직접 타겟으로 공격하는 스피어피싱으로 발전하는 배경이 되는 것 같다.

4.1.4 피싱메일 신고율 분석

최초 훈련모형 수립시 열람, 감염 이외에 사용자 대응행동으로 피싱메일에 대한 신고율을 정의하였으며 임직원들의 피싱메일 인지수준과 얼마나 적극적으로 피싱메일 출현을 공유하여 다른 동료들의 추가적인 피해를 예방하는데 기여하느냐를 평가하였다. 훈련분석결과 신고는 사내 악성코드 확산방지를 위한 목적으로 이미 훈련 전에 제도로 정착이 되어 있는 행위였기에 첫 번째 차수를 제외하고 전 차수에 걸쳐서 전반적으로 안정적인 수준의 신고율을 보였으며 개인 스스로 인지하여 신고하였다기보다는 먼저 인지한 동료들의 전파에 의해 인지하는 사례가 다수 있고, 미 신고시 패널티와 연계되어 있는 개인별 의무신고규정이 아니기 때문에 부서단위 최초 인지자 몇 명만 신고하는 경우가 많아 차수별 평가결과에 특별한 의미를 부여하는 것은 적절치 않아 보인다. 다만, 이슈 미연계 피싱메일 시나리오에 신고율이 높은 것으로 보아 신고율이 높은 것은 임직원 개개인의 피싱메일 인지율이 높았다는 것을 의미하고 정규직 임직원들에 비해 협력사 임직원들의 신고에 대한 의식이 매우 낮음을 확인할 수 있었다.

4.2 연구가설 검증 및 분석

4.2.1 상관관계 분석

연구가설1(H1) ~ 연구가설5(H5)을 검증하기 위해 각 변수간의 상관분석을 실시하였다. 본 연구의 중심이 되는 독립변수인 훈련차수와 종속변수가 모두 비율척도로 연속적 속성을 가지고 있고, 변수간 선형적 상관관계 분석을 목적으로 하기 때문에 상관계수 분석방법이 가장 적당한 검증방법이라 판단된다.

표본은 2여년에 걸쳐 총 6회의 실전 피싱메일 대응모의 훈련 결과 얻어진 직급별 결과를 기반으로 하였으며, 각 변수간 관련성을 구하기 위해 SPSS24(Statistical Packages for Social System) 통계분석을 활용하였다. 상관분석시 사용된 계수는 Pearson 상관계수이다. 피싱메일에 대해 임직원들은 열람, 감염, 신고의 3가지 대응행동을 할 것이며, 상관분석은 각 변수가 임직원의 이 3가지 대응행동에 어떠한 영향을 주는지를 분석하고, 특히 피싱 감염율과의 관계를 대응역량의 수준으로 판단하였다. Table 4.는 각 연구변수와 임직원 대응행동간의 상관관계 분석결과이다.

일반적으로 $-1 < r < -0.7$ 은 강한 음의 선형관계, $-0.7 < r < -0.3$ 은 뚜렷한 음의 선형관계, $-0.3 < r < -0.1$ 은 약한 음의 선형관계, $-0.1 < r$

Table 4. Correlation analysis between the variables

Variables		Reading(RR)	Infection(IR)	Report(RP)
Number of times (NO)	Pearson Correlation	-.609**	-.705**	.616**
	Sig. (2-tailed)	0.007	0.001	0.007
Punishment regulation (PR)	Pearson Correlation	-.610**	-.789**	0.462
	Sig. (2-tailed)	0.007	0.000	0.053
Seasonal issue (SI)	Pearson Correlation	0.215	.522*	-.700**
	Sig. (2-tailed)	0.392	0.026	0.001
Positoin (PO)	Pearson Correlation	0.152	0.360	-0.232
	Sig. (2-tailed)	0.548	0.142	0.355
Hired types (HT)	Pearson Correlation	-.928**	-0.401	.597**
	Sig. (2-tailed)	0.000	0.052	0.002

**. Sig.〈 0.01, *. Sig.〈 0.05

〈 0.1 은 거의 무시될 수 있는 선형관계, 0.1〈 r〈 0.3 은 약한 양의 선형관계, 0.3〈 r〈 0.7 은 뚜렷한 양의 선형관계, 0.7〈 r〈 1은 강한 양의 선형관계를 나타낸다. 본 연구에서는 모델 검증을 위해 피어슨계수 0.3 이상의 뚜렷한 선형관계에 대해 선정하였다.

4.2.1.1 훈련횟수와 피싱 대응역량간 상관관계

훈련횟수와 임직원들의 열람행동간의 상관계수는 -0.609이고 유의확율이 0.007, 감염행동과의 상관계수는 -0.705, 유의확율 0.001이며, 신고행동과 상관계수는 0.616, 유의확율 0.007로 세 가지 행동 모두 유의수준 0.05에서 통계적으로 유의하며, 열람과 감염에는 음(-)의 영향을, 신고에는 양(+)의 영향을 미침을 확인하고 귀무가설을 기각하고 대립가설을 채택한다.

4.2.1.2 인사규정강화와 피싱 대응역량간 상관관계

인사규정강화와 임직원들의 열람행동간의 상관계수는 -0.610이고 유의확율이 0.007, 감염행동과의 상관계수는 -0.789, 유의확율 0.000이며, 신고행동과 상관계수는 0.462, 유의확율 0.053으로 세 가지 행동 모두 유의수준 0.05에서 통계적으로 유의하며, 열람과 감염에는 음(-)의 영향을, 신고에는 양(+)의 영향을 미침을 확인하고 귀무가설을 기각하고 대립가설을 채택한다.

4.2.1.3 시즌연계이슈와 피싱 대응역량간 상관관계

훈련 시즌에 있는 이슈와 연계된 훈련메일 내용과 임직원들의 열람행동간의 상관계수는 0.215이고 유의확율이 0.392로 통계적으로 무의미 하여 시즌연계이슈와 열람율과는 상관관계가 없음을 확인하였다. 하지만 감염행동과의 상관계수는 0.522, 유의확율 0.026이며, 신고행동과 상관계수는 -0.700, 유의확율 0.001로 두 가지 행동 모두 유의수준 0.05에서 통계적으로 유의하며, 다른 변수와 다르게 시즌 연계성이 높을수록 대응역량을 약화시켜 감염에는 양(+)의 영향을, 신고에는 음(-)의 영향을 미침을 확인하고 귀무가설을 기각하고 대립가설을 채택한다.

4.2.1.4 임직원직책과 피싱 대응역량간 상관관계

임직원직책과 열람행동간의 상관계수는 0.152이고 유의확율이 0.548, 감염행동과의 상관계수는 0.360, 유의확율 0.142이며, 신고행동과 상관계수는 -0.232, 유의확율 0.355로 세 가지 행동 모두 유의수준 0.05에서 통계적으로 유의하지 않았다. 따라서 임직원 직책은 피싱대응역량에는 영향을 미치지 않기에 대립가설을 기각한다.

4.2.1.5 고용유형과 피싱 대응역량간 상관관계

고용유형과 임직원들의 열람행동간의 상관계수는 -0.928이고 유의확율이 0.000으로 어느 변수보다도 대응역량과 강한 선형관계가 있음을 확인하였으

며, 감염행동과의 상관계수는 -0.401, 유의확율 0.052이며, 신고행동과 상관계수는 0.597, 유의확율 0.002로 세 가지 행동 모두 유의수준 0.05에서 통계적으로 유의하며, 열람과는 강한 음(-)의 영향을, 감염에는 약한 음(-)의 영향을, 신고에는 양(+)의 영향을 미침을 확인하고 귀무가설을 기각하고 대립가설을 채택한다.

4.2.1.6 연구가설 검증결과

연구가설 검증결과는 Table 5.와 같다. 연구가설 1(H1) ~ 연구가설3(H3), 연구가설5(H5)는 채택되었으며, 연구가설4(H4)는 대응행동 모두가 통계적으로 유의하지 않아 기각되었다. 따라서 모의훈련의 횟수, 인사규정 강화, 시즌연계이슈, 고용유형은 임직원들의 대응행동과 피싱 대응역량에 영향을 미친다는 것을 확인하였다. 반면, 임직원들의 직책은 임직원들 대응행동에 영향을 주지 않으며, 피싱메일 대응역량에도 커다란 영향이 없음을 확인 하였다.

Table 5. Results of research hypothesis

Hypothesis	Correlation			H-test result
	Reading	Infection	Report	
H1	-.609**	-.705**	.616**	Accept
H2	-.610**	-.789**	.462	Accept
H3	-	.522*	-.700**	Accept
H4	-	-	-	Drop
H5	-.928**	-0.401	.597**	Accept

4.2.2 훈련 효과 영향도 분석 모델

세 가지 항목 각각이 훈련효과에 미치는 영향도에 분석모델을 도출하기 위해 각 항목을 독립변수로 하고 훈련의 결과를 잘 반영해 주는 감염율을 종속변수로 하여 회귀분석을 실시하였다.

Table 6.은 회귀분석결과이며 결정계수 R^2값이 각각 0.497, 0.622, 0.517로 통계분석에 이용된 각 모형들은 훈련효과와 50%이상의 관계임을 설명하고 있으며, 분산분석결과 유의확률이 0.000 ~ 0.008 으로 유의수준 0.05보다 작아 통계적으로 타당한 모형임이 입증되었다. 분석결과에 따른 회귀식은 Table 7.과 같다.

Table 7. The formulas for model

$$Y = -4.332E-07X_1 + 5930782$$
$$Y = -14.473X_2 + 16.955$$
$$Y = 3.123X_3 + 0.920$$

Y: *Injection rate*
X_1: *Number of time*
X_2: *Punishment regulation*
X_3: *Seasonal issue*

V. 결 론

5.1 연구결과 요약 및 시사점

그동안 피싱 대응력 향상을 위한 임직원들의 보안의식 향상과 대응방안에 대해 여러 형태의 연구와 논의가 이루어져 왔지만 대부분이 이론적 교육이나 실험실 환경에서의 단기간의 실습훈련을 통한 연구만 이루어왔다. 반면 본 연구는 실제업무환경에서 근무를 하는 회사의 직원을 대상으로 2년에 걸친 장기적이며 실증형 모의훈련을 실시하여 현실성 있고 타당성 있는 훈련결과를 수집하고 분석하였다. 또한 현실세계에서 실제 사용되는 전파경로와 피싱기법, 그리고 계절적 이슈와 연계된 호기심 유발 방법을 함께 적용하여 실질공격과 동일한 조건의 환경을 구성하였으며 임직원들의 내부 동요나 도덕적 비난을 최소화하기 위해 보안서약서, 업무규정, 교육 등 사전 분위기 조성을 통해 개인의 보안준수 의무를 각인시키고 불시에 점검이 이루어짐을 고지하였다. 이러한 노력

Table 6. Regression analysis among the infection rate and variables

Model		Coefficiants				ANOVA		R2
		B	Beta	t	Sig.	F	Sig.	
1	(Constant)	5930.782		3.980	0.001	15.805	0.001	0.497
	Number of times	-4.332E-07	-0.705	-3.976	0.001			
2	(Constant)	16.955		7.364	0.000	26.344	0.000	0.622
	Punishment regulation	-14.473	-0.789	-5.133	0.000			
3	(Constant)	0.920		1.362	0.203	10.688	0.008	0.517
	Seasonal issue	3.123	0.719	3.269	0.008			

으로 기존 연구의 제한을 극복할 수 있었으며 훈련의 지속성과 훈련간 부가적 통제가 피싱대응역량에 미치는 영향을 실증적으로 분석하여 다음과 같이 효과를 검증하였다.

첫째, 실전형 훈련은 임직원들의 실질적 피싱메일 대응역량 향상에 큰 도움을 주는 교육방법이며 훈련기간을 단기가 아닌 정기적이고 지속적으로 실시할 때 임직원들을 피싱 공격에 대해 항상 긴장상태를 유지시킬 수 있게 만들고 나날이 정교해지는 최신의 공격기법을 식별해 내어 언제 어느 때 공격이 이루어지더라도 적절한 대응이 이루어지게 할 수 있다. 다만 실증결과에서 나타나듯이 효과가 높은 초기 3~4회 정도는 짧은 주기로 훈련을 실시하여 위험에 대한 경각심과 대응방법을 인지시키고 이후 어느 정도 목표수준에 도달한 이후에는 주기를 다소 길게 조정하여 훈련에 소요되는 비용을 절감하는 방안을 찾는 것도 좋을 듯 하다.

둘째, 단순한 모의훈련보다는 훈련결과에 대한 패널티를 주는 인사정책을 함께 병행하므로 임직원들의 훈련에 대한 관심을 높여 훈련의 효과를 배가 시킬 수 있다. 다만, 예고 없는 불시 훈련과 결과에 따른 패널티를 주는 정책을 동시에 적용했을 때 내부적 불만이 더 높아질 수 있으므로 사전에 보안서약서, 내부규정 등을 통해 보안준수의무와 점검방법 안내 등을 통해 사전에 충분히 인지토록 해야 한다. 또한 패널티 정책 적용 전 먼저 1~2회 모의훈련을 실시하여 임직원들이 불시 훈련에 대해 경험을 하도록 한 후 다음번 훈련 결과부터 추가적인 인사 조치가 적용됨을 알리고 시행하는 것이 좋다. 패널티의 수준도 적발 횟수에 따라 경고, 교육, 징계 순으로 강화시켜 나가는 것이 임직원들에게 합리적 제재로 인식될 것이다.

셋째, 훈련 시나리오를 임직원들의 관심을 유발시킬 수 있는 이슈나 관심사항을 연계시켜 구성할수록 훈련효과를 높일 수 있다. 이 방법은 공격자들이 실제적으로 감염확률을 높이기 위해 사용하는 기법으로 날이 갈수록 정교해 지고 있는 추세이다. 실제 피싱공격이 자신들의 관심과 호기심등 심리적 약점을 이용하여 이루어짐을 경험시킴으로 메일 제목이나 내용 등에 대해 신뢰해서는 안 된다는 경각심을 갖도록 만들기 때문에 결과적으로 더 높은 훈련 효과를 얻을 수 있다.

마지막으로 임직원들의 직책의 높고 낮음은 훈련효과에 영향을 미지치 않으며, 다만 고용유형에 따라 계약직, 파견직 근무자들이 정규직 근로자들에 비해 관심이 낮기 때문에 정보를 구분해서 취급토록 하거나 추가적인 통제를 강화해야할 필요가 있다.

5.2 향후 연구 방향

본 연구가 실전형 모의훈련을 통해 임직원들의 피싱대응 행동을 분석하여 실증형 훈련모델을 제시하였지만 모의훈련기간 동안 피싱메일에 대한 대응행동을 한 임직원들을 대상으로만 분석을 실시한 결과이므로 메일을 수신 후 아무런 반응을 보이지 않은 임직원들에 대한 추가적인 분석이 필요하다. 또한 훈련결과에 대한 채찍형 정책이외에 당근형 정책이나 게임모형등을 도입한다면 좀더 효과적인 훈련이 이루어질 것이라 판단하며, 감염에 대한 통제이외에 신고등에 대한 통제를 통해 강제적으로 신속한 내부 정보공유가 이루어지도록 하여 간접적으로 훈련효과를 높이는 방안에 대한 추가적인 연구가 이루어지길 기대한다.

References

[1] S. Ashraf, "Organization need and everyone's responsibility: Information security awareness," Global Information Assurance Certification Paper, SANS Institute, Feb, 2005.

[2] M. Al-Awadi and K. Renaud, "Success factors in information security implementation in organizations," IADIS International Conference e-Society, 2007.

[3] S. Al Awawdeh and A. Tubaishat, "An information security awareness program to address common security concerns in IT unit," International Conference on Information Technology, pp. 273-278, Apr. 2014.

[4] T. Nikolakopoulos, "Evaluating the human factor in information security," Master thesis, Oslo University College, Apr. 2009.

[5] Kyu-sik Kim, Jong-won Choi and Dong-hun Chu, "Nuclear power hacking is spear phishing," http://news.mk.co.kr/newsR

ead.php?year=2014&no=1564190, Maeil Business News, Dec. 2014.
〔6〕 Tae-kyun Kim, "Interpark was robbing 10 million personal information by one phishing e-mails impersonating his brother." http://www.yonhapnews.co.kr/bulletin/2016/08/31/0200000000AKR20160831043451017.HTML?from=search, Yonhap News, Aug. 2016.
〔7〕 P. Kumaraguru, S. Sheng, A. Acquisti, L. F. Cranor and J. Hong, "Lessons from a real world evaluation of anti-phishing training," eCrime Researchers Summit, 2008, pp. 1-12, Oct. 2008.
〔8〕 W. G. Anti-Phishing, "Phishing activity trends report 3rd quarter 2016," Anti-Phishing Working Group, Dec. 2016.
〔9〕 A. ENISA, "Users' guide: How to raise information security awareness," Jun. 2006.
〔10〕 T. Carlson, "Information security management: understanding ISO 17799," Lucent Technologies, Oct. 2001.
〔11〕 Cha-ho Lim, "Effective information security awareness plan," Journal of The Korea Institute of Information Security & Cryptology, 16(2), pp. 30-36, Apr. 2006.
〔12〕 Jung-ho Eom, "The Improvement plan of a customized cyber-training structure for enhancing the capability of cyber security," Journal of Security Engineering, 12(6), pp. 567-580, Dec. 2015.
〔13〕 Hong-jae Lee and Yong-jin Cha, "A study on the effectiveness of privacy education using the CIPP model : focusing on the perceptions of local government officials," The Korean Journal of Local Government Studies, 19(1), pp. 95-119, 2015.
〔14〕 L. James, Phishing exposed, Syngress 2005.
〔15〕 R. Richmond, "Hackers set up attacks on home PCs, financial firms: study," http://www.marketwatch.com/News/Story/Story.aspx?dist=newsfinder&siteid=google&guid=%7B92615073-95B6-452EA3B9, Sep. 2006.
〔16〕 S. A. Robila and J. W. Ragucci, "Don't be a phish: steps in user education, ", vol. 38, no. 3, pp. 237-241, Jun. 2006.
〔17〕 T. Jagatic, N. Johnson, M. Jakobsson and F. Menczer, "Social phishing," Communications of the ACM, vol. 50, no. 10, pp. 94-100, Oct. 2006.
〔18〕 A. J. Ferguson, "Fostering e-mail security awareness: The West Point carronade," Educase Quarterly, vol. 28, no. 1, pp. 54-57 2005.
〔19〕 P. Kumaraguru, Y. Rhee, A. Acquisti, L. F. Cranor, J. Hong and E. Nunge, "Protecting people from phishing: the design and evaluation of an embedded training email system,", pp. 905-914, Apr. 2007.
〔20〕 M. Allen, "Social engineering: A means to violate a computer system," SANS Institute, Jun. 2006.
〔21〕 J. Hiner, "Change your company's culture to combat social engineering attacks," May, 2002.
〔22〕 D. Timko, "The social engineering threat," Information Systems Security Association Journal, Jan. 2008.
〔23〕 M. B. Brewer, "Research design and issues of validity," Handbook of research methods in social and personality psychology, pp. 3-16, 2000.
〔24〕 H. Ebbinghaus, Memory: A contribution to experimental psychology, University Microfilms, no. 3, 1913.
〔25〕 P. Brien, "10 tips for spotting a phishing email," http://www.techrepublic.com/blog/10-things/10-tips-for-spotting-a-phishing-email/, Oct. 2015.
〔26〕 D. Estelle, "10 tips on how to identify a phishing or spoofing email, https://blog.returnpath.com/10-tips-o

n-how-to-identify-a-phishing-or-spoof-
ing-email-v2/ ", Dec. 2015.

〈저자소개〉

윤 덕 상 (Duck-sang Yoon) 종신회원
1989년 2월: 고려대학교 자연과학대 수학과 졸업
2005년 2월: 고려대학교 정보경영공학대학원 정보보호학과 석사
2005년 9월~현재: 고려대학교 정보보호대학원 정보보호학과 박사과정
〈관심분야〉 정보보호 관리체계, 위험관리, 네트워크 보안, 개인정보보호

이 경 호 (Kyung-ho Lee) 종신회원
1989년 8월: 서강대학교 수학학사
1997년 8월: 서강대학교 정보통신대학원 네트워크공학석사
2009년 7월: 고려대학교 정보경영대학원 박사
2011년 8월:~현재: 고려대학교 정보보호대학원 부교수
〈관심분야〉 위험평가·관리, 정보보호 관리체계, 개인정보보호, 개인정보영향평가

임 종 인 (Jong-in Lim) 종신회원
1980년 2월: 고려대학교 수학과 졸업
1982년 2월: 고려대학교 수학과 석사
1986년 2월: 고려대학교 수학과 박사
현재: 고려대학교 정보보호대학원 교수, 고려대학교 사이버국방학과 교수, 대검찰청 디지털수사자문위원회 위원장, 금융보안 연구원 보안전문기술위원회 위원장, 행정자치부 정책자문위원회 위원, 국방부 정보화책임관 자문위원, 한국저작권위원회 위원 등
〈관심분야〉 사이버국방, 정보법학, 디지털포렌식, 개인정보보호, 융합기술보안 등