ISSN 1598-0170 (Print)
ISSN 2287-1136 (Online)
http://www.jksii.or.kr

사용자의 패스워드 인증 행위 분석 및 피싱 공격시 대응방안 - 사용자 경험 및 HCI의 관점에서

Behavioural Analysis of Password Authentication and Countermeasure to Phishing Attacks - from User Experience and HCI Perspectives

유 홍 렬[1] 홍 모 세[1] 권 태 경[1*]
Hong Ryeol Ryu Moses Hong Taekyoung Kwon

요 약

아이디와 패스워드를 통한 인증은 고전적인 방법이나 여전히 가장 널리 사용되고 있다. 오늘날 사용자들의 패스워드의 인증 수행 과정은 그 단순함과 편리함, 반복적인 수행으로 인해 적응무의식화 되었다. 즉, 의식화된 상태가 아닌 무의식적으로 인증을 수행하고 있다. 인증과정은 그 절차가 단순하고 반복 학습되어 인간의 깊은 사고 없이도 무의식적으로 수행할 수 있도록 학습될 수 있다. 또한 사용자들이 보유한 아이디와 패스워드 개수가 적기 때문에 기억에 의존할 수 있는 것도 적응무의식화의 원인 중 하나이다. 소수의 아이디와 패스워드 개수를 보유한 것과 달리 대개 사용자들은 수많은 웹, 모바일, 인터넷사이트 서비스에 가입되어 있다. 계정의 수는 많은 반면 소수의 아이디, 패스워드 쌍을 보유했을 때, 그리고 그것이 기억에 의존하여 관리될 때, 마지막으로 인증 과정이 무의식적으로 수행될 때 그것은 인간의 취약점이 된다. 과거에는 정보유출을 위한 해킹 공격이 하드웨어나 소프트웨어 등의 취약점을 이용한 것이었다면 최근에는 이와 더불어 인적 요소의 취약점을 이용하는 사회공학적 공격이 많아지고 있다. 특히 피싱 및 파밍 등과 같은 정보유출형 공격이 급증하고 있다. 피싱 및 파밍 공격은 인적 요소의 취약성을 이용한 것이며, 무의적으로 수행하는 인간의 인증 행위에 취약하다. 과거의 피싱 및 파밍에 대한 연구는 기술적인 분석이나 대책이 주를 이루었지만, 본 논문은 피싱 및 파밍 공격시 반응하는 인간의 행위에 관심이 있다. 사용자가 패스워드를 무의식적으로 입력 할 때, 그리고 인증 행위를 반복 수행할 때, 얼마나 많은 패스워드를 노출할 수 있는지 실험을 통해 확인했다.

☞ 주제어 : 피싱, 파밍, 패스워드, 인증, 사회공학

ABSTRACT

User authentication based on ID and PW has been widely used. As the Internet has become a growing part of people' lives, input times of ID/PW have been increased for a variety of services. People have already learned enough to perform the authentication procedure and have entered ID/PW while ones are unconscious. This is referred to as the adaptive unconscious, a set of mental processes incoming information and producing judgements and behaviors without our conscious awareness and within a second.

Most people have joined up for various websites with a small number of IDs/PWs, because they relied on their memory for managing IDs/PWs. Human memory decays with the passing of time and knowledges in human memory tend to interfere with each other. For that reason, there is the potential for people to enter an invalid ID/PW. Therefore, these characteristics above mentioned regarding of user authentication with ID/PW can lead to human vulnerabilities: people use a few PWs for various websites, manage IDs/PWs depending on their memory, and enter ID/PW unconsciously.

Based on the vulnerability of human factors, a variety of information leakage attacks such as phishing and pharming attacks have been increasing exponentially. In the past, information leakage attacks exploited vulnerabilities of hardware, operating system, software

[1] Graduate School of Information, Yonsei University, Seoul, 120-749, Korea.
* Corresponding author (taekyoung@yonsei.ac.kr)
[Received 31 January 2014, Reviewed 18 February 2014, Accepted 9 April 2014]

☆ 본 연구는 미래창조과학부 및 한국산업기술평가관리원의 산업융합원천기술개발사업(정보통신)[10039180, 모바일 환경하에서 모바일 인증과 보안 강화를 위해 직관적이며 사용하기 편하고 안전한 인간-컴퓨터 상호작용(HCI) 기반 Usable Security 원천기술 개발]과 2012년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업(No. NRF-2012R1A1B3000965)의 일환으로 수행하였음.
☆ 본 논문은 2014년도 인터넷정보학회 춘계학술발표대회 우수논문 추천에 따라 확장 및 수정된 논문임.

and so on. However, most of current attacks tend to exploit the vulnerabilities of the human factors. These attacks based on the vulnerability of the human factor are called social-engineering attacks. Recently, malicious social-engineering technique such as phishing and pharming attacks is one of the biggest security problems. Phishing is an attack of attempting to obtain valuable information such as ID/PW and pharming is an attack intended to steal personal data by redirecting a website's traffic to a fraudulent copy of a legitimate website.

Screens of fraudulent copies used for both phishing and pharming attacks are almost identical to those of legitimate websites, and even the pharming can include the deceptive URL address. Therefore, without the supports of prevention and detection techniques such as vaccines and reputation system, it is difficult for users to determine intuitively whether the site is the phishing and pharming sites or legitimate site. The previous researches in terms of phishing and pharming attacks have mainly studied on technical solutions. In this paper, we focus on human behaviour when users are confronted by phishing and pharming attacks without knowing them. We conducted an attack experiment in order to find out how many IDs/PWs are leaked from pharming and phishing attack.

We firstly configured the experimental settings in the same condition of phishing and pharming attacks and build a phishing site for the experiment. We then recruited 64 voluntary participants and asked them to log in our experimental site. For each participant, we conducted a questionnaire survey with regard to the experiment. Through the attack experiment and survey, we observed whether their password are leaked out when logging in the experimental phishing site, and how many different passwords are leaked among the total number of passwords of each participant.

Consequently, we found out that most participants unconsciously logged in the site and the ID/PW management dependent on human memory caused the leakage of multiple passwords. The user should actively utilize repudiation systems and the service provider with online site should support prevention techniques that the user can intuitively determined whether the site is phishing.

☞ keyword : Phishing, Pharming, Password, Authentication, Social Engineering, HCI

1. 서 론

정보의 금전적 가치가 날로 커지고 있다. 이를 반영하듯 개인정보나 산업정보를 막론하고 정보 자체를 탈취하려는 시도가 끊임없이 증가하고 있다. 과거에는 정보유출을 위한 해킹 공격이 하드웨어나 소프트웨어의 취약점 등을 이용한 것이었다면 최근에는 이와 더불어 사회공학(Social Engineering)을 이용한 공격이 많아지고 있다. 사회공학은 사람의 심리를 조정하여 기밀 정보를 누설하도록 하거나 특정행위를 하도록 유도하는 것을 의미한다 [1]. 정보시스템을 구축하거나 운영하는 것은 결국 사람이다. 하지만 그동안 정보시스템을 구축, 운영하거나 보안을 논의할 때 가장 취약한 부분 중 하나인 인적 요소는 간과되었다. 그동안의 보안 논의는 주로 승인되지 않은 사용자가 불법적으로 정보에 접근하는 것을 기술적으로 방지하는 것에 초점이 맞추어졌다. 하지만 이제는 합법적인 사용자에 의해 정보가 탈취되는 것에도 관심을 기울여야 한다.

최근 급증하고 있는 피싱(Phishing) 및 파밍(Pharming) 공격은 대표적인 사회공학적 공격들이다. 피싱 및 파밍은 금융정보나 개인정보를 탈취하기 위해 변조된 웹사이트로 사용자를 유도하는 공격이다 [2]. 공격자는 특정 사이트와 동일한 모양의 웹사이트를 만들어 놓고 사용자로 하여금 특정 정보 입력을 유도한다. 피싱 및 파밍 공격은 피해자가 정보를 직접 제공할 때 성공한다. 따라서 사용자의 인식을 제고하여 스스로 정보를 노출하지 않도록 하는 것은 피싱 및 파밍을 막기 위한 중요한 요소이다.

본 논문은 2013년도 한국인터넷정보학회 춘계학술대회 우수 논문 추천에 따라 확장 및 수정된 논문이다. 기존의 연구는 사용자의 무의식적인 인증 과정이 패스워드 유출에 미치는 영향을 알아보기 위해 공격 실험을 수행하였고 그 결과값를 제시하였다 [3]. 이후 확장된 연구에서는 연구모델을 보완하여 유출요인과 결과와의 관계를 명확하게 하였다 [4]. 본 논문은 기존의 연구 결과들을 확장한 것으로, 실험결과를 사용자 경험과 HCI 관점에서 재해석하였다. 이로써 피싱 및 파밍의 기술적 관점이 아닌 사용자 관점의 패스워드 인증 행태에 대해서 분석하였다.

2. 연구목적

아이디와 패스워드를 사용하는 인증은 고전적인 방법이나 여전히 널리 사용되고 있다. 이러한 인증은 대개 많은 사이트에서 동일한 절차와 방법에 의해 수행되며 단순하고 반복적으로 이루어진다. 수행 절차는 아이디와 패스워드를 입력한 후 엔터를 치거나 로그인 버튼을 클릭하는 것이 전부이다. 따라서 인터넷을 처음 접하는 사람이 아닌 한 인증 과정 수행을 위한 별도의 학습은 필요

하지 않다. 오늘날 많은 인터넷 사용자들은 특정 사이트나 서비스에 접속할 때마다 아이디와 패스워드 인증을 반복 학습하고 있고 충분히 적응된 상태이다.

아이디와 패스워드를 이용한 인증과정은 그 단순함과 간편함, 반복적인 학습 때문에 무의식적으로 수행하게 될 위험이 발생한다. 이러한 현상은 인증 과정의 수행이 적응무의식(Adaptive Unconscious)화 되었기 때문이다. 적응무의식은 깊은 사고 과정 없이 단숨에 결론에 도달하거나 행동에 착수케 하는 뇌의 영역을 의미한다 [5]. 아이디와 패스워드를 입력하는 과정은 이미 적응무의식화 되어 피싱 및 파밍 사이트의 공격에 취약하다. 피싱이나 파밍 사이트에 대한 합리적인 의심 없이 아이디와 패스워드와 같은 민감한 정보들을 무의식적으로 입력할 가능성이 있기 때문이다. 따라서 인증 과정에서 사용자의 인식을 제고할 수 있는 방법이 필요하다.

인터넷 사용자들은 대부분 수많은 인터넷 사이트 계정을 가지고 있으나, 그에 비해 소수의 아이디와 패스워드 쌍을 보유하고 있다. 계정의 수와 아이디 및 패스워드 쌍의 수가 비례하지 않는 것은 그만큼 패스워드 관리가 어렵기 때문이다. 만약 피싱 및 파밍 공격으로 인해 아이디와 패스워드가 유출된다면 하나의 아이디, 패스워드 쌍만으로 피해자가 가입한 다수의 웹사이트 계정이 위협받을 수 있다.

본 논문은 피싱 및 파밍 공격에서 사용자의 부주의가 패스워드를 어떻게 노출할 수 있는지 실험을 통해 확인하였다. 또한 소수의 아이디와 패스워드 쌍이 기억에 의존하여 관리될 때 얼마나 많은 패스워드가 노출될 수 있는지 실험했다. 이로써 피싱 및 파밍 공격에서 다수의 아이디와 패스워드가 유출될 수 있는 요인들을 사용자의 부주의 측면에서 분석해 보았다.

3. 관련연구

과거의 사회공학은 사회과학과 관련 있었지만, 최근에는 정보보안 전문가들 사이에서 다뤄지고 있다 [6]. 사회 공학은 심리를 조작하는 행위이다. 사람의 심리를 조정하여 기밀 정보를 누설하도록 하거나 특정행위를 하도록 유도한다 [1]. 과거의 사회공학 공격 기법은 대부분 기술적 지식이 크게 필요하지 않았다. 그러나 IT기술이 발전함에 따라서 사회공학 공격 기법은 기술을 통해서 발생한다. 즉, 사회공학 공격 기법은 IT기술의 발전 전과 후로 나눠지게 된다. 기술이 발전하기 전에는 쓰레기통 뒤지기(Dumpster Diving), 테일게이팅(Tailgating, Piggybacking), 숄더 서핑(Shoulder Surfing), 프리텍스팅(Pretexting)등이 있다. 기술이 발전하고 난 후에는 기존의 사회공학 공격 기법들이 인터넷, 핸드폰 등의 매체를 통해서 일어나는데 대표적으로 피싱, 파밍, 스미싱(Smishing) 등이 있다 [1][6].

3.1 피싱

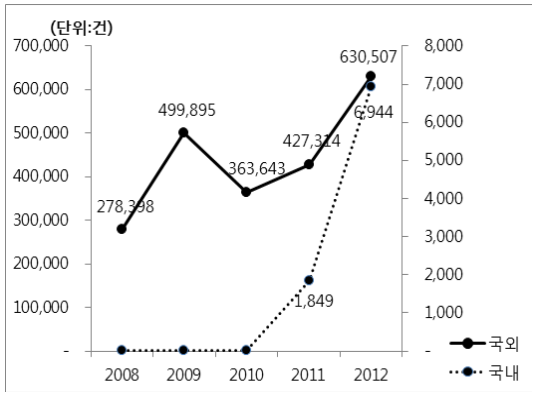
피싱은 개인정보나 금융정보와 같이 금전적인 가치가 있는 정보들을 취득하기 위해서 변조된 웹사이트로 사용자를 유도하는 사회공학 공격 중 하나이다 [2]. 공격자는 인터넷 사용자를 기만할 목적으로 실제 웹사이트와 동일한 화면의 웹사이트를 제작한다. 이후 이메일 또는 게시판에 피싱 사이트의 링크를 배포한다. 이메일, 게시물의 내용이나 그 안에 담긴 링크는 정상적인 링크처럼 보이지만 사실 공격자가 피싱 사이트로 유도하기 위해 만들어진 링크이다. 인터넷 사용자들은 해당 링크를 정상적인 것으로 간주하고 클릭하지만 공격자가 준비된 사이트로 연결되고, 피해자들은 이내 공격자가 유도한 정보들을 입력하게 된다. 사용자가 스스로 입력한 정보는 공격자에게 유출된다 [7].

3.2 파밍

파밍은 피싱 공격이 한단계 진화한 형태이다. 피싱 공격은 링크나 iFrame 태그를 통해 다른 웹서버로 유도하지만 URL을 검증하면 해당 사이트가 피싱인지 아닌지 판단할 수 있다. 그러나 파밍은 DNS 취약점을 이용한다. 사용자가 정상적인 URL을 요청하면 DNS는 공격자가 준비해 둔 IP주소로 안내한다. 따라서 파밍은 피싱에 비해 상대적으로 그 위험을 인지하기 어렵다. 피싱과 파밍은 공격 방식에 있어서는 차이가 있지만, 사용자가 직접 웹사이트에 접근해서 스스로 정보를 내어준다는 점에서는 동일하다 [8][9].

3.3 피싱 피해 현황

실제 개인 인터넷 사용자에게 가장 큰 금전적인 피해를 주는 사회공학 공격 기법은 피싱이다. 2006년부터 2013년 5월까지 경찰청에 41,807건의 신고가 접수 되었으며 집계된 피싱 사기의 피해 규모는 4,380억원 정도의 규모이다. 보이스 피싱, 피싱 웹사이트, 파밍은 사기의 주



(그림 1) 국내, 해외 피싱 사이트 현황 [8][10]
(Figure 1) Increasing phishing sites [8][10]

요경로이다. 2012년 국내 피싱 사이트의 수는 6,944개로 2011년에 1,846개에 비교하여 3배 이상 급증하였다.

피싱은 주로 개인의 금융정보나 개인정보를 입력하도록 유도한다. 금융 정보가 유출되면 금전적인 피해를 일으킬 수 있다. 개인정보가 유출되면 지속적으로 광고성 전화 및 스팸 메일에 시달리거나 명의가 도용되는 등 2차 피해가 발생할 수 있다.

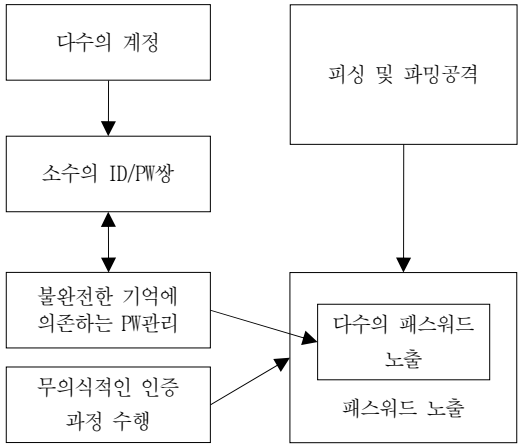
4. 패스워드 노출요인에 관한 실험

사용자들이 패스워드를 노출하는 요인을 실험을 통해 알아보았다. 실제 피싱 및 파밍 사이트와 동일한 환경을 구축하여 피실험자들을 대상으로 공격을 수행하였고, 그 결과를 관찰하였다. 공격 목적은 첫째, 피실험자를 피싱 및 파밍 사이트로 유도하여 패스워드를 입력하도록 요구했을 때 패스워드가 유출되는지의 여부를 알아보기 위한 것이며 둘째, 피실험자에게 패스워드 입력을 반복 요구했을 때 피실험자가 보유한 패스워드 범위 중 얼마나 많은 패스워드가 유출되는지 알아보기 위한 것이다. 이에 본 실험을 '패스워드 입력 재시도 요구 공격'이라 명명하였다.

4.1 연구가설

많은 인터넷 사용자들은 웹사이트를 이용하기 위해 다수의 서비스에 가입하고 있다. 다수의 서비스에 가입했다는 것은 다수의 계정을 가졌다는 것을 의미한다. 하지만 다수의 계정에 비해 소수의 아이디와 패스워드를 가지고 있다. 아이디와 패스워드의 개수가 많아지면 관리가 어렵기 때문이다. 또한 많은 사람들은 아이디와 패스워드 관리를 기억에 의존하고 있다. 이것 역시 적은 수의 아이디, 패스워드를 보유하게 만드는 원인이다. 만약 다수의 아이디와 패스워드를 보유하게 된다면 더 이상 기억에 의존할 수 없다. 별도의 파일 관리가 필요하다.

사용자들은 인증 절차를 깊은 사고 과정 없이 무의식적으로 수행한다. 로그인 입력창과 화면, 절차 등은 거의 모든 사이트에서 동일하며 사용자들은 이러한 인증 절차에 반복 학습되었다. 따라서 이러한 과정은 무의식의 단계로 수행할 수 있게 되었다. 만약 사용자들이 이와 같은 상황에서 피싱 및 파밍 공격에 노출된다면 아이디와 패스워드를 노출할 가능성이 높다. 특히 아이디와 패스워드를 기억에 의존하는 상태에 인증을 실패한다면, 인증 절차를 재시도할 가능성이 높다. 이것은 다수의 패스워드를 노출을 유발한다. 본 논문은 이와 같은 상황을 가정하여 Figure 2와 같은 연구가설을 도출했다.



(그림 2) 연구모형
(Figure 2) Research model

4.1.1 다수의 계정

대개 인터넷 사용자는 SNS, 이메일, 쇼핑몰, 게임, 금융, 클라우드, 음악, 영화 등 수많은 인터넷 사이트를 이용하고 있다. 서비스 제공자들은 사용자 식별을 통해 각 사용자들에게 맞춤형 서비스를 제공하고 있으며, 이를 달성하기 위해 사용자를 인증한다. 사용자들은 다수의 사이트에 가입한다고 가정하며 이것은 다수의 계정을 보유한다는 것을 의미한다.

4.1.2 소수의 아이디, 패스워드쌍

비록 사용자들이 다양한 인터넷 서비스를 이용하기 위해 다수의 계정을 가지고 있지만, 모든 서비스에 저마다 독립적인 아이디와 패스워드를 사용하지는 않는다. 보유한 아이디와 패스워드가 많아질수록 관리상의 문제가 발생하기 때문이다. 이를 해결하기 위해 하나의 아이디로 다수의 사이트를 이용할 수 있는 오픈 아이디(Open ID)와 같은 기술들이 도입되어 있지만 이것 역시 아이디와 패스워드를 이용한 인증임에는 변함이 없다. 따라서 사용자들은 소수의 아이디와 패스워드 쌍을 다양한 서비스에 인증 파라미터로 사용하고 있다고 가정한다.

만약 하나의 아이디와 패스워드 쌍이 공격자에 의해 유출되면 동일한 아이디와 패스워드를 사용하는 또 다른 사이트에서 권한이 탈취되는 등 2차 피해가 발생할 수 있다. 특히 최근에는 특정인이 어느 서비스를 이용하고 있는지 사회공학적 기법을 통해 알아낼 수 있다. 또한 탈취된 계정이 페이스북이나 구글 등 오픈아이디의 기능을 가지고 있다면 더 많은 사이트의 권한이 탈취되거나 도용될 수 있다.

사용자들이 소수의 아이디 패스워드 쌍을 보유한다면 개인의 보안성은 낮아질 수는 있다. 그러나 패스워드를 별도의 기록으로 관리해야 하는 관리적 문제를 해결할 수 있다. 이것은 동일한 아이디와 패스워드 쌍을 다수의 사이트에 적용하여 편리함을 추구하는 사용성 증가, 보안성과의 절충점(Trade-off)과 관련이 있다.

4.1.3 불완전한 기억에 의존하는 패스워드 관리

많은 사용자들은 아이디와 패스워드를 관리하기 위한 체계가 부재하다고 가정한다. 특히 소수의 아이디, 패스워드 쌍을 보유할수록 암기에 의존한다고 가정한다. 암기에 의존하는 관리는 사회공학적 공격에 취약할 수 있다. 가령 사용자가 다수의 계정을 보유하고 있는 상태에서 자주 사용하지 않는 계정에 접근할 때 불완전한 기억으로 인증을 시도할 가능성이 높다. 자주 이용하는 사이트에서 입력하는 아이디와 패스워드 값은 비교적 정확할 수 있다 하지만 1년에 1~2회 이용하는 사이트의 경우 정확한 패스워드를 입력할 가능성이 상대적으로 높다고 볼 수 없다.

4.1.4 무의식적인 인증 과정 수행

사용자는 아이디와 패스워드를 사용한 로그인 인증 절차를 무의식적으로 수행한다고 가정한다. 이것은 피싱 및 파밍 공격시 패스워드가 유출되는 원인이 된다. 많은 인터넷 사이트는 사용자를 식별하고 구분하기 위해서 아이디와 패스워드 인증에 의존하고 있다. 사용자가 아이디와 패스워드를 인증하는 과정은 아이디와 패스워드를 입력하고 엔터, 혹은 로그인 버튼을 누르는 것이 전부이다. 이 단순한 과정은 수많은 반복을 통해 학습되어 사용자들에게 익숙하다. 다수의 계정을 가지고 하루에도 다양한 서비스를 이용하는 인터넷 사용자들에게, 인증 수행 과정에는 깊은 인지적 사고 처리가 필요하지 않다. 따라서 이러한 인증 과정은 적응무의식화 되어 있으므로 무의식적으로 수행할 수 있다고 가정한다.

일반적으로 사용자들은 아이디와 패스워드 인증이 실패했을 때 다시 시도하는 경향이 있다고 가정한다. 이것은 두 가지 요인이 있는데, 하나는 입력한 패스워드가 해당 사이트의 패스워드와 일치하는지 여부에 대한 불확실성이다. 또 다른 요인은 패스워드 값의 입력 오류이다. 사용자가 패스워드를 입력하면 텍스트 박스는 입력값을 애스터리스크(asterisk, *)로 변환 처리하므로 정확한 문자열이 입력되었는지 확인하기 어렵다.

이와 같이 인증을 무의식적으로 수행하고, 이러한 수행을 합리적 의심이나 검증 절차 없이 반복한다면 피싱 및 파밍과 같은 정보 유출형 사회공학적 공격에 치명적이다. 특히 피싱 및 파밍 공격이 인증 실패를 유발하고, 사용자로 하여금 패스워드를 반복 입력하도록 유도했을 때 다수의 패스워드가 유출될 수 있다는 것을 실험을 통해 증명하였다.

4.2 실험설계

Figure 2에서 나타난 연구가설을 증명하기 위해 '패스워드 입력 재시도 요구 공격' 실험을 준비했다. 피실험자가 피싱 및 파밍 공격에서 패스워드를 반복 입력하는 이유, 그리고 반복 입력했을 때 얼마나 많은 패스워드를 노출하는지 알아보기 위해 먼저 측정해야 할 변수들을 선정했다. 이후, 선정된 변수를 측정하기 위한 조작적 정의를 만들었다. 마지막으로 실험을 설계하고 피실험자들을 대상으로 공격을 수행하였다.

4.2.1 측정 변수 및 조작적 정의

연구가설을 통해서 알아보고자 하는 변수들과 가설은 Table 1과 같다. '계정의 개수'는 피실험자가 얼마나 많은

(표 1) 측정 변수 및 가설
(Table 1) Measuring variables and hypothesis

변수	가설
계정의 개수	다수
아이디와 패스워드 개수	소수
패스워드 관리 방법	불완전한 기억에 의존
인증 과정 수행 행태	무의식적인 절차 수행
패스워드 노출량	다수 노출

사이트 혹은 웹/모바일 서비스에 가입되어 있는가를 나타낸다. '아이디와 패스워드 개수'는 보유하고 있는 아이디와 패스워드 개수를 나타낸다. 가령 특정 피실험자가 5개의 웹사이트에서 동일한 아이디 값을 사용한다면 그것은 하나의 아이디 값으로 본다. 여기서 계정의 수가 다수라는 것은 아이디 또는 패스워드 개수에 비해 계정의 수가 상대적으로 많다는 의미이다. 마찬가지로 아이디와 패스워드 개수의 수가 소수라는 것은 계정의 수에 비해 적다는 의미이며 절대적인 기준은 없다. '패스워드 관리 방법'은 피실험자만의 특별한 아이디, 패스워드 관리 방법을 의미한다. 관리 방법은 피실험자에 따라 매우 다를 수 있으므로 '암기', '브라우저 자동저장', '파일저장', '기타 관리도구 이용'으로 나누어 범주를 한정하였다. '인증 과정 수행 행태'는 안전한 인증 과정 수행을 위한 피실험자의 특별한 검증 절차나 방법의 유무를 의미한다. '마지막으로 패스워드 노출량'은 피실험자가 보유한 패스워드의 개수에 비해서 얼마나 많은 패스워드가 노출되었는지를 의미한다.

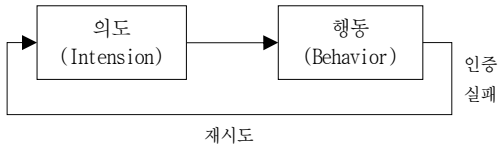
(표 2) 조작적 정의
(Table 2) Operational definitions

변수	조작적 정의	측정방법
계정의 개수	얼마나 많은 사이트에 가입되어 있는가?	인터뷰
아이디 개수	아이디의 개수(종류)는 몇 개인가?	인터뷰
패스워드 개수	패스워드의 개수(종류)는 몇 개인가?	인터뷰
패스워드 관리 방법	{암기, 브라우저 자동저장, 파일저장, 관리도구이용, 기타}	인터뷰
인증 과정 수행 행태	피싱 또는 파밍을 방지하기 위한 검증 절차가 존재했는가?	실험 및 인터뷰
패스워드 노출량	몇 개의 패스워드를 노출했는가?	실험

연구가설을 통해서 측정하고자 하는 변수들과 측정을 위한 조작적 정의, 측정 방법은 Table 2와 같다.

4.2.2 실험 모형

실험은 Figure 3과 같은 모형에 의해 구성하였다.



(그림 3) 실험 모형
(Figure 3) Experimental model

① 의도 : 피실험자가 피싱 및 파밍 사이트에 접속하여 로그인을 시도하려는 '의도'를 의미한다. 실험자는 피실험자에게 일련의 과제를 부여함으로써 피싱 및 파밍 사이트에 접속하고 로그인 과정을 수행하도록 유도한다. 이것으로 피실험자의 로그인 의도를 생성한다. 이때 실험의 의도를 드러내지 않으면서 피실험자의 로그인 수행을 유도해야 한다.
② 행동 : 피실험자가 로그인을 실제로 수행하는 것을 의미한다. 아이디와 패스워드를 입력하고 로그인을 시도함으로써 행동의 목적은 달성된다.
③ 재시도 : 피실험자의 로그인 시도 이후 인증은 실패된다. 성공할 수 없도록 설계하였기 때문이다. 피실험자는 인증이 실패했을 때 다시 시도하려는 의도로 돌아간다.

Figure 3의 사이클이 반복되는 횟수는 피실험자가 인증과정의 수행을 반복하는 횟수가 된다.

4.3 실험수행

실험은 사전설문, 공격실험, 사후인터뷰 순으로 진행하였다. 사전설문을 통해 실험자의 실험 의도가 드러나지 않도록 한 상태에서 공격실험을 진행하였다. 실험이 끝난 후에는 사후인터뷰를 통해 실험 결과 평가하고 피실험자에게 실험의 목적을 설명하였다.

실험을 위해 준비된 피싱 및 파밍 사이트는 포털, 쇼핑몰, SNS 등 총 4개이며 실제 사이트와 동일한 화면으로 제작하였다. 특별히 로그인 기능을 구현하기 위해 Apache Server환경에서 PHP로 제작하였고, 호스트 변조를 통해

파밍 사이트를 구축하였다. 이로써 실제 웹사이트에 대한 URL 요청을 준비된 공격 사이트가 응답하도록 했다.

4.3.1 사전설문

준비된 4개의 피싱 및 파밍 사이트를 대상으로 사전에 이용 빈도를 조사하였다. 설문 결과 중 이용 빈도가 가장 낮은 사이트를 실험 도구로 사용하여 공격 실험을 진행하였다. 이용 빈도가 가장 낮은 사이트를 실험에 사용한 이유는 기억에 의존하는 아이디와 패스워드 관리의 위험성을 증명하기 위함이다.

4.3.2 공격실험

준비된 피싱 및 파밍 사이트에서 피실험자의 패스워드를 자연스럽게 노출시키기 위해 실험 목적과 무관한 수행과제를 부여했다. 수행과제는 반드시 준비된 사이트에 접속하여 로그인을 해야만 가능한 과제였다. 피실험자가 과제수행을 위해 접속한 URL은 실제 웹사이트가 아닌 준비된 파밍 사이트로 연결되었다. 아울러 피실험자의 아이디와 패스워드가 정확하게 입력되더라도 인증을 실패하도록 설계하였다. 재시도를 유도하기 위함이다. 만약 피실험자가 스스로 로그인 수행을 중단하거나 '비밀번호 찾기'버튼을 클릭하거나, 피싱을 의심하는 표현을 했을 경우 실험을 종료했다. 피실험자가 입력한 아이디와 패스워드는 데이터베이스에 저장되었다.

4.3.3 사후인터뷰

실험이 종료된 직후, 저장된 아이디와 패스워드를 피실험자가 직접 열람하도록 했으며 실험자는 열람하지 않았다. 피실험자가 스스로 노출했던 아이디와 패스워드를 데이터베이스에서 직접 열어보도록 한 후 사후인터뷰를 진행하였다. 이 사후인터뷰를 통해서 피실험자가 입력했던 아이디의 개수, 패스워드의 개수, 로그인을 시도한 횟수, 노출된 패스워드의 개수 등을 파악할 수 있었다. 저장된 실험 데이터는 피실험자로 하여금 스스로 파기할 수 있도록 인터페이스를 제공하였다. 사후인터뷰 종료 직후 피실험자는 스스로 자신의 실험 결과를 삭제하였다.

4.4 실험결과

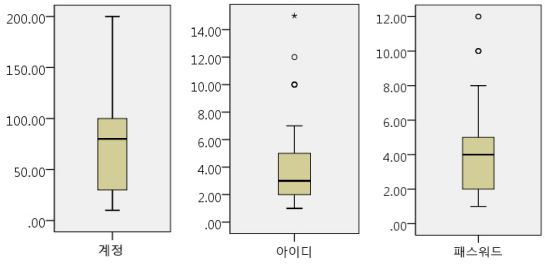
피실험자는 총 65명(남성 37명, 여성 28명)이며 평균 나이는 26.5세이다. 전공과 무관한 대학생이나 대학원생을 대상으로 실험을 진행하였다. 실험결과는 Table 3과 같다.

(표 3) 설문 및 실험결과
(Table 3) Survey and experimental results

항목	결과값
계정의 보유 개수	평균 75.6개 (sd: 45.1)
아이디 보유 개수	평균 4.0개 (sd: 2.9)
패스워드 보유 개수	평균 4.1개 (sd: 2.7)
로그인 시도 횟수	평균 5.8회 (sd: 2.8)
노출된 패스워드 개수	평균 2.2개 (sd: 1.3)
패스워드 관리를 암기에 의존하는 피실험자 비율	92.31%

4.4.1 보유한 계정, 아이디, 패스워드의 수

피실험자들이 보유한 계정은 평균 75.6개(표준편차 45.1)이다. 반면 아이디와 패스워드의 수는 각각 평균 4.9개(표준편차 2.9), 4.1개(표준편차 2.7)이다.



(그림 4) 계정, 아이디, 패스워드의 수
(Figure 4) The number of accounts, ID, passwords

계정과 아이디 두 수에 대한 상관계수는 각각 -0.09, 0.10으로 나타났다. 즉 계정이 많다고 하여 아이디나 패스워드의 수가 많아지는 것은 아니었다. 이러한 원인 중 하나는 관리상의 어려움 때문이다. 만약 75개의 계정에 서로 다른 아이디와 패스워드를 사용할 경우 150개의 컨텍스트를 암기해야 하는 문제가 발생한다. 사후인터뷰에서 아이디와 패스워드를 암기에 의존하는 피실험자의 비율은 92.4%로 나타났다.

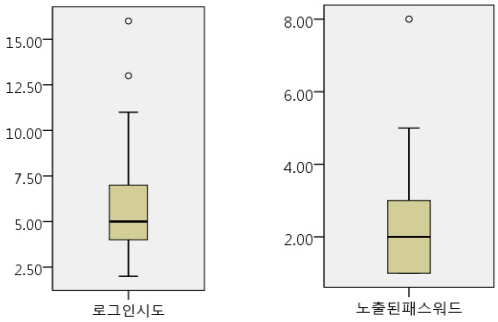
또한 아이디와 패스워드 두 수의 관계에서 Pearson 상관계수는 0.41로 나타났다. 보유한 아이디가 많을수록 패스워드의 개수가 많아지는 경향을 보였다.

(표 4) 아이디-패스워드 개수의 상관계수
(Table 4) Correlation coefficient between ID and password

		아이디	패스워드
아이디	Pearson 상관계수	1	.409**
	유의확률 (양쪽)		.001
	N	65	65
패스워드	Pearson 상관계수	.409**	1
	유의확률 (양쪽)	.001	
	N	65	65

4.4.2 인증 시도 횟수 및 패스워드 노출량

피실험자들은 평균 5.8회(표준편차 2.8) 로그인을 시도했다. 이때 피실험자들이 보유한 패스워드 평균 4.1개 중 평균 2.2개(표준편차 1.3)의 패스워드를 노출했다. 약 54%의 높은 비율로 노출됨을 알 수 있었다.



(그림 5) 로그인 시도 횟수, 노출된 패스워드의 수
(Figure 5) Reattempt times, the number of and leaked passwords

Table 5에서 볼 수 있는 것과 같이 로그인 시도 횟수와 노출된 패스워드 개수간의 상관계수는 0.49로 나타났다. 즉 로그인 시도 횟수가 높을수록 노출된 패스워드의 개수는 많아졌다.

(표 5) 로그인 시도 횟수-노출된 패스워드 개수의 상관계수
(Table 5) Correlation coefficient between reattempt times and leaked passwords

		로그인시도	패스워드
로그인 시도	Pearson 상관계수	1	.496**
	유의확률 (양쪽)		.000
	N	65	65
패스워드	Pearson 상관계수	.496**	1
	유의확률 (양쪽)	.000	
	N	65	65

암기에 의존하는 피실험자의 패스워드 노출량은 평균 2.23개(표준편차 1.3)였지만, 암기에 의존하지 않는 사용자의 평균 노출량은 1.4개(표준편차 0.54)로 나타났다.

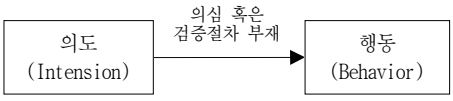
5. 시사점 및 피싱 대응 전략

5.1 검증 절차

(표 6) 실험결과
(Table 6) experimental results

항목	결과값	비율
로그인 행동을 수행한 피실험자 수	65명	100%
인증 실패 후 재시도한 피실험자 수	65명	100%
파밍을 의심한 피실험자 수	0명	0%

Table 6의 실험 결과처럼 실험자가 피실험자를 피싱 사이트로 유도했을 때 모든 피실험자가 로그인을 시도했다. 다시 말해 피실험자에게 실험 의도가 부여되었을 때 그것이 로그인 행위로 나타나지 않은 피실험자는 없었다. 이것은 Figure 6처럼 의도가 로그인 행위로 나타나기 이전에 피싱 및 파밍 사이트에 대한 검증절차가 부재했거나, 피싱 및 파밍 사이트에 대한 판별이 실패했음을 나타낸다. 실험 후 인터뷰에서 모든 사용자는 피싱 및 파밍 사이트임 의심하지 못했다고 응답했다.



(그림 6) 의심 혹은 검증절차의 부재
(Figure 6) Absence of qualification procedures

피싱 및 파밍 공격을 검증하는 것은 매우 어렵다. 피싱 공격은 사용자가 직접 해당 웹페이지의 URL을 검증하는 것으로 확인할 수 있다. 하지만 파밍 공격은 URL을 기만할 수 있으므로 이에 대응하기 매우 어렵다. 오늘날 많은 백신 소프트웨어들은 피싱 공격을 막기 위한 평판 시스템을 운영하고 있다. Figure 7처럼 웹브라우저에 플러그인 형태로 작동하며 피싱이 의심되는 사이트에 대해서 사용자에게 경고한다. 이처럼 사용자가 직접 모든 사이트에 대해서 URL을 검증하는 현실적인 어려움을 평판 시스템이 보조함으로써 피싱 공격에 대한 사용자의 인식을 개선할 수 있다.

(그림 7) 피싱 사이트를 판별하는 Avast의 평판 시스템
(Figure 7) Avast's reputation system

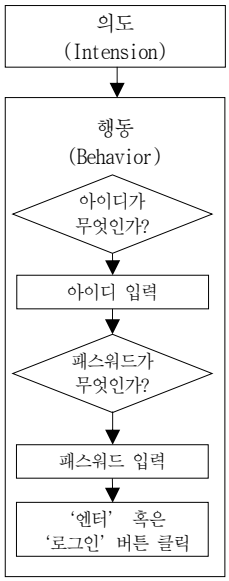
이와 같은 평판 시스템은 파밍 공격을 탐지할 때에도 사용될 수 있다. 평판 데이터베이스에 파밍 사이트의 IP 주소를 블랙리스트로 사용하거나, 실제 웹사이트의 IP주소를 화이트리스트로 사용할 수 있다. 또는 평판 데이터베이스에 URL과 IP주소를 동시에 평가하여 IP주소의 이상치를 판별하는 방식으로도 파밍을 탐지할 수 있다. 기존의 대응 방안에서는 제3의 인증기관을 이용하거나, 주소등록기관 및 WHOIS 데이터베이스를 활용하는 방안이 제시되고 있다 [11].

5.2 인증수행의 적응무의식화

인증 과정을 수행할 때 사용자는 Figure 8과 같은 행동과 사고 과정을 거친다. 사용자는 아이디가 무엇인지 판단한 후 결과 값인 아이디를 텍스트 박스에 입력한다. 이후 패스워드가 무엇인지 판단한 후 그 결과 값을 텍스트 박스에 입력한다. 마지막으로 엔터를 입력하거나 로그인 버튼을 찾아 클릭함으로써 서버로 데이터를 전송한다. 이 과정은 비교적 단순하지만 오래전부터 오늘날까지 많은 사이트에서 널리 적용되고 있는 인증 방식이다.

Figure 8에서 볼 수 있듯이 로그인 과정에서 두 번의 사고 작용이 이루어진다. 하나는 아이디를 판별하는 것이고, 또 다른 하나는 패스워드를 판별하는 것이다. 그러나 아이디와 패스워드를 판별하는 것을 포함하여, Figure 8의 모든 과정은 이미 적응무의식화 되어 무의식적으로 수행된다 된다. 적응무의식이란 인간의 고도의 정교한 사고를 많은 부분 무의식의 영역으로 끌어내림으로써 빠른 판단이 가능하도록 하는 것을 의미한다. 세상을 판단하거나 위험을 인식했을 때 깊은 사고의 과정 없이 빠른 결론에 도달하여 효율성을 높이는 장점이 있다.

적응무의식화의 원인으로는 패턴의 단순함과 반복 수행이 있을 수 있다. 아이디와 패스워드를 이용한 인증은 그 단순함과 반복적인 수행으로 인해 적응무의식의 단계에서 수행될 위험이 크다. 피싱 및 파밍에서 아이디와 패스워드를 탈취하는 것은 이러한 취약점을 이용하는 것이다. 특히 아이디와 패스워드의 보유 개수가 작고, 불완전한 기억에 의존하며, 반복 학습 가능성이 높은 인증 과정의 특성상 적응무의식의 단계로 전이될 가능성이 높다.



(그림 8) 로그인 절차
(Figure 8) Login process

5.3 불완전한 기억에 의존하는 아이디와 패스워드

아이디와 패스워드를 암기에 의존하는 피실험자 비율이 92.31%임을 사후인터뷰 결과를 통해 확인했다. 기억에 의존하는 것은 그만큼 관리의 어려움이 존재한다는 것이며, 이것은 아이디와 패스워드를 적은 개수로 보유하게 되는 원인이기도 하다. 평균 75.6개의 계정에 서로 다른 아이디와 패스워드 쌍을 사용한다면, 사용자는 그것을 모두 기억할 수 없는 현실적인 어려움이 발생한다.

공격 실험에서 실험자는 4개의 준비된 피싱 및 파밍 사이트 중 피실험자가 자주 방문하지 않는 사이트를 실험 도구로 사용했다. 방문 빈도가 낮은 사이트는 자주 방문하는 사이트보다 상대적으로 인증을 수행하는 횟수가 적다. 즉, 해당 사이트에서 사용하는 아이디와 패스워드를 입력하는 경험이 적다. 방문 빈도가 높은 사이트에서 인증을 수행하면 장기기억 속에 존재하는 아이디와 패스워드에 대한 기억이 강화되지만, 그렇지 않은 사이트에 대해서는 퇴화될 가능성이 있다. 이것은 불완전한 기억을 야기하며 잘못된 패스워드를 입력하는 요인이 된다.

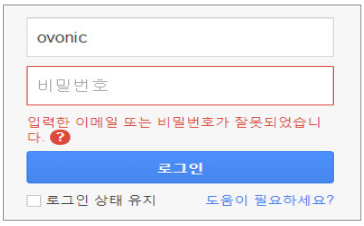
피실험자들은 평균 4.0개의 아이디와 4.1개의 패스워드를 보유하고 있었다. 아이디와 패스워드를 이용한 인증은 두 값의 조합에 의해 이루어진다. 따라서 아이디와 패스워드의 개수를 조합하면 최대 16.1개의 쌍을 암기해

야 하며, 더 나아가 75.6개의 사이트에 대해서 최대 16.1개의 아이디, 패스워드쌍이 기억속에서 매치되어야 한다.

피실험자들은 공격 실험에서 평균 2.2개의 패스워드를 노출하였다. 피실험자가 보유한 패스워드 범위 내에서 또 다른 패스워드를 입력하는 것은 패스워드에 대한 기억이 불확실하고, 입력한 패스워드의 정확성을 확신하지 못하기 때문이다.

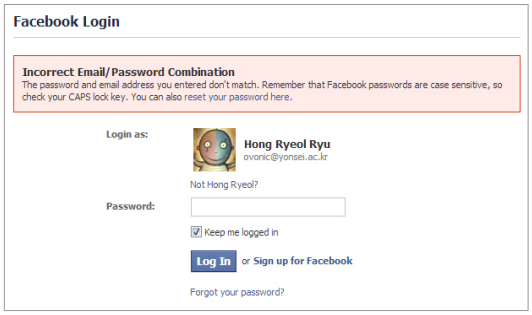
5.4 인증 실패 결과 화면

피실험자는 최초의 인증 수행을 포함하여 평균 5.8회의 로그인을 시도하였다. 반복되는 인증 실패는 재시도를 유발했으며 평균 2.2개의 패스워드를 노출시키는 결과를 낳았다. Figure 9은 아이디와 패스워드 인증이 실패했을 때 보여지는 전형적인 화면이다. 이러한 인증 실패 화면은 재시도의 편의성을 위해 아이디와 패스워드 입력 텍스트박스를 제공하고 있다.

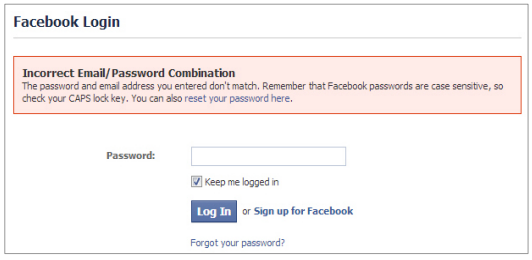


(그림 9) 로그인 실패시 결과화면
(Figure 9) Login failure screen

피싱 및 파밍 공격시 사용자의 재시도를 막고, 다수의 패스워드를 노출을 방지할 수 있는 방법 중 하나는 실제 사이트의 인증 실패 화면을 개선하는 것이다. 실제 사이트의 인증 실패 화면이 피싱이나 파밍에서 구현할 수 없는 방식으로 구현되어 있다면, 그리고 그것이 사용자들에게 충분히 학습되어 있다면, 사용자는 피싱 및 파밍 사이트에서 1회의 로그인 실패만으로도 직관적으로 파밍 사이트임을 확인할 수 있을 것이다. 이를 구현할 수 있는 기법 중 하나는 로그인 실패 화면에 개인화 이미지를 사용하는 것이다. 많은 사이트에 사이트에서 이와 같은 기능들을 제공되어야 한다. 이러한 기능들이 보편화 되어 사용자들에게 충분히 학습되면, 추가로 로그인을 시도하는 일을 막을 수 있을 것이다. 페이스북은 Figure 10에서 보이는 것처럼 최초의 로그인 실패시 개인화 이미지를 제공하고 있다. 하지만 그림 Figure 11에서 보이는 것처럼 실험을 위해 제작된 파밍 사이트는 이와 같은 개인화 이미지를 적용할 수 없었다.



(그림 10) 개인화 이미지가 적용된 인증 실패 화면
(Figure 10) Facebook's login failure screen

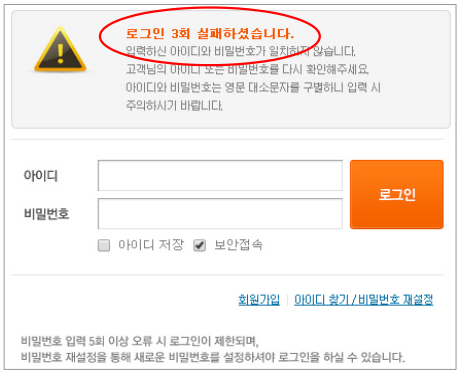


(그림 11) 실험을 위한 피싱 사이트의 인증 실패 화면
(Figure 11) Login failure screen for experiment

2014년 1월 현재, 랭키닷컴의 사이트 점유율 순위 중 상위10개의 사이트(네이버, 다음, 네이트, 싸이월드, 구글, G마켓, 11번가, 옥션, KB국민은행)를 조사한 결과 모든 사이트에서, 2회 이상의 반복되는 인증 실패에도 동일한 실패 결과 화면이 반복되는 것을 확인하였다. 사용자가 입력한 비밀번호는 별표로 표시되어 있으므로 인증실패 시에도 본인이 올바르게 입력했는지 확신하지 못하며, 이것은 재시도를 행위를 유발하는 하나의 요인이 된다. 인증 실패 화면이 동일하게 반복되는 것은 로그인 재시도에 대한 의도를 방어하지 못하고, 로그인 시도 행위를 유발하는 하나의 원인이다.

5.5 재시도 허용 횟수의 제한

인증의 재시도 허용 횟수를 제한하는 사이트들이 많아지고 있다. 그러나 이것은 전사공격을 방지하기 위함일 뿐, 사용자의 부정확한 기억을 보호하거나 패스워드 노출을 방지하기 위한 것이 아니다. 하지만 평소에도 재시도 허용 횟수를 제한하는 것은 사용자의 인식 재고에 효과가 있을 수 있다.



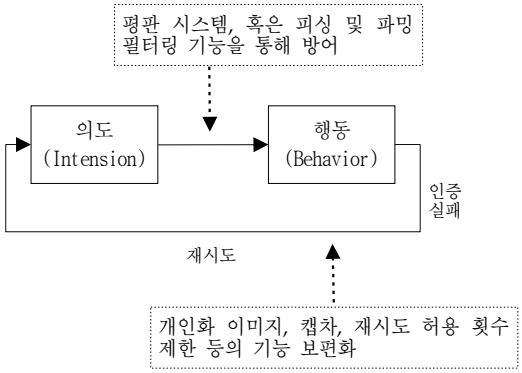
(그림 12) 로그인 횟수를 알려주는 실패 화면
(Figure 12) Text to indicate the number of failed login

국내의 인터넷 뱅킹의 계좌 비밀번호와 카드 비밀번호 인증은 대개 허용횟수가 3회로 제한되어 있고, 사용자에게 충분히 학습되어 있다. 따라서 일반적인 패스워드 입력과는 다르게 신중한 입력이 요구된다. 신중한 입력은 적응무의식화된 인증 수행을 의식적인 과정에서 수행할 수 있도록 돕는다. 이처럼 일반적인 패스워드 인증에도 재시도 허용 횟수를 제한하고 Figure 12에서 보이는 것처럼 실패 한계 횟수와 현재 실패 횟수를 안내한다면 사용자들의 인식 재고에 도움이 될 것이다. 공격 실험에서 피실험자들의 평균 재시도 횟수가 5.8회인 것을 볼 때 5회 보다 적은 숫자로 재시도 허용을 제한하는 것이 바람직하다.

6. 결 론

공격 실험을 통해서 사용자의 인증 수행 과정이 무식적인 행위임을 확인하였다. 전형적인 아이디 및 패스워드의 인증 수행 과정은 많은 인터넷 사용자들에게 적응무의식화 되었고, 이는 피싱 및 파밍 공격의 취약점으로 작용한다. 이와 더불어 기억에 의존하는 아이디, 패스워드 관리는 다수의 패스워드 노출의 원인이 될 수 있음을 확인하였다.

피싱 및 파밍 공격은 사용자가 직관적으로 판단하기 힘든 기술적인 문제가 존재한다. 피싱 사이트의 화면은 실제 웹사이트 화면과 동일하며, 파밍 사이트는 URL 마저 기만할 수 있으므로 백신이나 평판시스템과 같은 기술적인 보조 도구 없이, 사람이 직관적으로 판별하기란 쉽지 않다.



(그림 13) 로그인 의도와 행동 사이에서 피싱과 파밍을 방지할 수 있는 방안들
(Figure 13) Countermeasures to phishing and pharming in model

사용자 경험 및 HCI관점에서 이와 같은 문제를 해결하기 위해서는 Figure 13에서 나타난 것과 같이 사용자의 학습된 경험이 필요하다. 파밍 사이트가 구현할 수 없는 기능들(개인화 이미지, 로그인 횟수 제한 등)이 실제 웹사이트에 구현되어 있어야 한다. 또한 사용자가 실제 웹사이트를 이용할 때 로그인 과정에서 이와 같은 기능들을 충분이 학습될 수 있도록 해야 한다. 많은 사이트에 적용될수록 학습 효과는 커질 것이며 추후 사용자 스스로 파밍을 식별하는데 도움이 될 것이다. 마지막으로 인증의 재허용 횟수를 제한하고 시도 횟수를 표시함으로써 적응무의식화된 인증 수행을 의식적인 과정에서 수행할 수 있도록 도와야 한다.

참 고 문 헌(Reference)

[1] H. Christopher, Social Engineering The Art of Human Hacking, John Wiley & Sons Inc, Dec. 2010.

[2] D. Rachna, J.D. Tygar and M. Hearst, “Why phishing works,” Proceedings of the SIGCHI conference on Human Factors in Computing, pp. 581-590, Apr. 2006.

[3] M. Hong, H. Ryu and T. Kwon, “The Impact of Unconscious User Authentication Process on the Leakage of Passwords - Focussing on Phishing,” Proceedings of the Korean Society for Internet Information Conference, vol. 14, no. 2, pp. 73-74, Nov. 2013.

[4] H. Ryu, M. Hong and T. Kwon, “A Study of Multiple Password Leakage Factors Caused by Phishing and Pharming Attacks,” Journal of the Korea Institute of Information Security and Cryptology, vol. 23, no. 6, pp. 1225-1229, Dec. 2013.
[5] T.D. Wilson, Strangers to Ourselves: Discovering the Adaptive Unconscious. Cambridge, MA: Harvard Univ. Press, 2002.
[6] R.J. Anderson, Security engineering: a guide to building dependable distributed systems 2nd Ed., Wiley, Apr. 2008.
[7] D. Rachna and J.D. Tygar, “The battle against phishing: Dynamic security skin,” Proceedings of the Symposium on Usable Privacy and Security, pp. 77-88, Jul. 2005.
[8] S. Kim, S. Lee and S. Jin, “Active Phishing Attack and its Countermeasures,” Electronics and Telecommunications Trends, vol. 28, no. 3, ETRI, 2013.
[9] S. Gastellier-Prevost and M. Laurent, “Defeating pharming attacks at the client-side,” Network and System Security(NSS), 2011 5th International Conference on. IEEE, pp. 33-40, 2011.
[10] Anti-Phishing Working Group, “Phishing Activity Trends Report 4th Quarter 2012,” Anti-Phishing Working Group, Apr. 2013.
[11] J. Kang, E. Cho, S. Lee, “Analysis of Phishing URL using Internet Registration Authority,” Review of KIISC, vol. 23, no. 6, pp. 13-20, Dec. 2013.
[12] Y. Lee, “An Analysis on the Vulnerability of Secure Keypads for Mobile Devices,” Journal of Korean Society for Internet Information, vol. 14, no. 3, pp. 15-21, June. 2013.
[13] T. Kim, B. Park and T. Park, “An Augmented Memory System using Associated Words and Social Network Service,” Journal of Korean Society for Internet Information, vol. 11, no. 6, pp. 41-50, Dec. 2010.

◐ 저 자 소 개 ◑

유 홍 렬 (Hong Ryeol Ryu)
2013년 서울과학기술대학교 산업공학전공 졸업(공학사)
2013년 연세대학교 정보대학원 재학(석사과정)
관심분야 : HCI, Usable Security, Social Engineering, Human Factors.
E-mail : ryeol@yonsei.ac.kr

홍 모 세 (Moses Hong)
2010년 한국교통대학교 컴퓨터공학과(공학사)
2013년 연세대학교 정보대학원 재학(석사과정)
관심분야 : 사회공학, 보안 정책 기획
E-mail : mose@yonsei.ac.kr

권 태 경 (Taekyoung Kwon)
1992년 연세대학교 컴퓨터과학과(이학사)
1995년 연세대학교 컴퓨터과학과(이학석사)
1999년 연세대학교 컴퓨터과학과(공학박사)
1999년~2000년 U.C. Berkely Post-Doc.
2001년~2013년 8월 세종대학교 컴퓨터공학과 교수
2007년~2008년 Univ. Maryland at College Park 교환교수
2013년 9월~현재 연세대학교 정보대학원 부교수
관심분야 : 암호프로토콜, 네트워크 프로토콜, 센서네트워크 보안, HCI 보안, Usable Security 등
E-mail : taekyoung@yonsei.ac.kr