Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.23, NO.6, Dec. 2013 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2013.23.6.1037

피싱 대응 솔루션 연구 및 개발 현황 그리고 앞으로의 방향*

신 지 선†‡
세종대학교

Study on Anti-Phishing Solutions, Related Researches and Future Directions*

Ji Sun Shin†‡
Sejong University

요 약

피싱(phishing) 공격의 피해가 증가함에 따라 그에 대한 대응책 및 관련 연구가 활발히 진행되어 왔다. 피싱 공격을 막는 솔루션(anti-phishing solutions)들은 웹브라우져(web-browser)의 보안 기능으로 혹은 보안 툴바(toolbar)의 형태로 다양하게 개발되었고, 그밖에도 이메일 필터링(email-filtering), 비밀 이미지 공유를 통한 서버 인증 강화 등의 방식으로 솔루션들이 개발되었다. 피싱 관련 연구로는 피싱 공격이 성공하는 이유에 대한 분석 연구, 피싱 공격을 막는 솔루션들이 효과적인지에 대해 사용자 입장에서 분석한 연구들이 발표되었다.

이 논문에서는 피싱 공격을 막는 다양한 종류의 솔루션들을 소개하고, 대표적인 솔루션들의 기술적 원리를 이해한다. 또한, 피싱 관련 연구 결과들을 함께 짚어봄으로써 피싱 공격을 막는 솔루션들이 개선되어야할 점들을 강조하여 살펴보고, 앞으로 피싱을 막기 위한 대책 연구가 진행되어야할 방향을 제시한다.

ABSTRACT

As damages from phishing have been increased, many anti-phishing solutions and related researches have been studied. Anti-phishing solutions are often built in web-browsers or provided as security toolbars. Other types of solutions are also developed such as email-filtering and solutions strengthening server authentication via secret image sharing. At the same time, researchers have tried to see the reasons why phishing works and how effective anti-phishing solutions are.

In this paper, we review relevant anti-phishing solutions, their techniques and other phishing-related researches. Based on these, we summarize recommended ways to improve anti-phishing solutions and suggest the future directions to study to protect users from phishing attacks.

Keywords: Phishing, Anti-Phising Solutions, Security, Usability, User Protection

I. 서 론

피싱(phishing) 공격은 사용자들에게 친숙한 웹 페이지로 가장하여 사용자의 로그인 정보 등을 얻어내고 그 정보를 이용하여 사용자에게 금전적 피해나 사생활 침해 등을 주는 공격을 말한다. 피싱 공격은 일반적으로 공격 이메일(spoofed email)과 가짜 서버(fraudulent server)로 구성되어있다. 공격자는 사용자가 가짜 서버에 연결을 하도록 유도하는 공격 이메일을 작성하여 사용자에게 보낸다. 이때 이메일 대신에 스마트폰을 대상으로 문자 메시지가 사용되기도

접수일(2013년 10월 1일), 수정일(2013년 10월 17일), 게재확정일(2013년 10월 21일)
* 이 논문은 2012년도 세종대학교 교내연구비 지원에 의한 논문입니다.
† 주저자, jsshin@sejong.ac.kr
‡ 교신저자, jsshin@sejong.ac.kr(Corresponding author)

Table 1. General Steps of Successful Phishing Attacks

단계	내용
1	사용자가 서버 연결을 유도하는 피싱 공격 이메일을 받는다 (예, 서버 연결 링크 포함 이메일).
2	사용자가 웹브라우져를 통해 가짜 서버의 주소로 연결한다.
3	가짜 서버는 진짜 서버의 웹페이지를 모방한 웹페이지를 보내고 사용자는 이를 웹브라우져를 통해 본다.
4	사용자가 진짜 서버에서 사용하는 개인 비밀정보(예, 로그인 정보)를 입력하면 그 정보가 가짜 서버로 전달된다.

Table 2. Classifications of Anti-Phishing Solutions

	단계별 솔루션의 종류	솔루션의 형태 및 내용
1	연결단계(2, 3 단계)에서 제공되는 솔루션	웹브라우져나 웹브라우져의 확장판인 툴바 형태의 솔루션으로 사용자에게 연결 서버에 대한 보안 정보를 제공하여 사용자가 피싱 서버에 개인 정보를 입력하는 것을 피하도록 도와준다[4, 17, 10, 2, 23, 15, 19, 3].
2	이메일 수신 단계(1 단계)에서 제공되는 솔루션	이메일 필터링 형식으로 제공되어 사용자에게 이메일이 피싱 공격 이메일로 분류됨을 알려주어 사용자가 공격 이메일에서 유도하는 서버연결을 피할 수 있도록 한다[7].
3	사용자 정보가 서버로 전달되는 단계(4단계)에서 제공되는 솔루션	사용자의 비밀정보가 서버에게 그대로 전달되는 것을 막아준다[18, 8, 9].

한다. 사용자는 이메일 혹은 문자 메시지에 포함된 링크 등을 통해 가짜 서버에 연결하게 되고, 가짜 서버에서 보여주는 페이지를 진짜 서버로 오인하여 자신의 개인정보를 입력하면, 그 정보는 가짜 서버를 관리하는 공격자에게 전달되게 된다. Table 1.에서 이러한 피싱의 공격과정을 단계 별로 정리하여 보여준다. Table 1.의 첫 번째 단계는 그 방법이 이메일로만 제시되어있으나, 실제 피싱의 공격 방법과 경로는 전화(보이스), 문자 메시지 등으로 다양하다. 본 논문은 피싱 공격 방법보다는 피싱 대응 솔루션 연구와 개발에 더 초점을 맞추므로, 가짜 서버로 연결을 유도하는 (Table 2.의 두 번째 단계에 이르는) 다른 다양한 공격 방법에 대해서는 자세히 다루지 않는다. 하지만, 그들에 대해서도 Table 2.의 2, 3, 4 단계를 따르는 피싱 공격의 경우에 본 논문에서 다루는 대응책이 공통으로 적용될 수 있다.

II. 피싱 공격을 막는 솔루션 (Anti-Phishing Solutions)

피싱 공격을 막는 솔루션(anti-phishing solution 이하 '안티 피싱 솔루션')들은 Table 1.에 정리된 단계 중에서 어떠한 단계에서 공격 진행을 막느냐에 따라 세 가지 종류로 나뉠 수 있다. 가장 많은 솔루션들이 연결 단계(2, 3 단계)에서 제공된다. 다른 두 종류의 솔루션들은 각각 첫 번째 단계(이메일 수신 단계)와 네 번째 단계(사용자 정보가 서버로 전달되는 단계)에서 제공된다. Table 2.에 이러한 세 가지 분류를 간단히 소개하고 있다, 대부분의 솔루션이 연결 단계에서 제공되기 때문에 이 분류를 첫 번째로 두고, Table 2.에 분류된 순서대로 각각에 대해서 살펴본다.

2.1 연결 단계에서 제공되는 솔루션

이 단계의 솔루션들은 사용자에게 연결 서버에 대한 보안 정보를 제공하여 피싱 서버에 연결한 사용자가 다음 단계(4단계: 사용자가 자신의 비밀정보를 입력하는 단계)로 진행하는 것을 막는다.

이러한 솔루션들은 다시 두 가지 종류로 세분화 될 수 있다. 첫 번째는 피싱 공격 서버를 판별하는데 집중하는 솔루션들이고 두 번째는 진짜 서버를 밝히는데 집중하는 솔루션들이다(Table 3. 참조). 많은 솔루션이 첫 번째에 속한다. 이들은 웹브라우져 혹은 웹브라우져의 확장형태로 툴바(toolbar)에서 제공되는

Table 3. Two Classifications of Anti-Phishing Solutions that are invoked at the Server-Connection Step

구체적 작업에 따른 솔루션의 종류	작업
피싱 공격 서버 판별 (phishing server detection)	사용자에게 사이트에 대한 보안 정보(예, 피싱 사이트의 가능성)를 제공[4, 17, 10, 2, 23].
합법적 서버 인증(legitimate server authentication)	사용자들이 좀 더 쉽게 진짜 서버인지를 확인할 수 있도록 도와줌으로써 서버 인증을 강화[15, 19, 3].

솔루션으로 웹브라우져에 주어진 서버주소를 분석하여 서버가 피싱 공격서버인지 판별하거나 서버에 관련된 보안 정보를 제공한다. 이러한 솔루션들에 대해 아래에서 좀 더 살펴본다.

2.1.1 피싱 공격 서버를 판별해 내는 솔루션들

이들 솔루션에 대표적으로 사용되는 방법으로 블랙리스트(blacklist)와 휴리스틱(heuristics)이 있다. 블랙리스트는 피싱 공격 사이트로 알려진 서버들의 주소를 블랙리스트에 등록하고 배포하여 이 리스트에 속한 경우에는 피싱 공격 서버임을 인지하는 방법이다. 휴리스틱(heuristics)은 과거 경험의 특징들을 바탕으로 한 방법이다. 일반적으로 사용되는 휴리스틱 방법은 피싱 공격 사이트의 특징을 파악할 만한 지표(feature)들을 선택하여 이러한 지표들을 기계학습(machine-learning) 기법에 도입하여 알고리즘을 학습하고 그 결과를 바탕으로 대상 서버가 피싱 공격 서버인지 밝혀내는 것이다.

구현이 간단하기 때문에 많은 솔루션들이 블랙리스트 방법을 사용한다. 하지만 블랙리스트 방법은 업데이트 정도에 따라 그 성능에 안전성이 떨어질 수 있다[23, 24]. 휴리스틱 방법은 업데이트에 의존할 필요가 없는 장점이 있는 대신, 공격자들이 휴리스틱 방법에 사용된 기술을 분석하여 탐지(detection)를 피해갈 수 있다[23]. 또한, 탐지 성능이 높은 휴리스틱 방법은 거짓 양성 오류(false-positive: 합법적 서버인데 피싱 공격 서버로 잘못 판단되는 것)가 높은 성향이 있다. 거짓 양성 오류를 극복하기 위하여 진짜 서버를 탐지하는 휴리스틱이 함께 사용되거나[23] 화이트리스트 방법을 도입한다[24]. 화이트리스트(white-list)는 합법적인 진짜 서버들의 주소를 모아둔 리스트이며, 주어진 서버가 피싱 공격 서버가 아님을 알려주는 데 이용된다.

대부분의 솔루션들이 블랙리스트 방법 사용하고, 필요에 따라 휴리스틱 방법을 함께 사용하기도 한다. 이러한 솔루션들로는 구글의 파이어폭스와 크롬을 위한 Safe Browsing, 마이크로소프트의 Internet Explore 7에서 제공되는 피싱 필터, eBay Toolbar, Spoofstick, Trustbar 등이 있다[1] [28, 29, 30, 4, 17, 10]. 또한, 휴리스틱 방법을 위주로 사용한 대표적인 솔루션으로는 SpoofGuard[2]와 CANTINA[23]가 있다.

원리가 비교적 간단한 블랙리스트 방법에 비해 휴리스틱 방법에서는 앞에서 설명된 일반적인 휴리스틱 방법(특징되는 지표들을 가지고 가짜 서버 판별)외에 다양한 기술적 기법이 사용될 수 있다. SpoofGuard는 전자(일반적인 휴리스틱 방법 사용)의 예가 될 수 있고, 후자의 예로 CANTINA의 기술적 방법에 대해 좀 더 살펴본다.

2.1.1.1 휴리스틱 솔루션의 예: CANTINA[23]

CANTINA는 용어의 빈도(term frequency)와 로버스트 하이퍼링크(robust hyperlinks)의 두 가지 중요한 기법을 이용한다:

- 용어의 빈도(term frequency): TF-IDF는 정보 분석 및 문서 마이닝에 자주 사용되는 알고리즘으로 주어진 문서에서 특정 단어(a word)가 얼마나 중요한지를 나타내주는 지표이다. 단어가 주어진 문서에서 얼마나 중요한지는 그 단어가 일반적으로 문서들에서 나타나는 빈도에 비해 주어진 문서에서 얼마나 자주 나타나느냐에 따라 증가하게 된다. TF는 term frequency의 약자로 주어진 문서에서의 중요성을 나태내는 지표이고, IDF는 inverse document frequency의 약자로 특정 단어(a word)가 일반적으로 (총체적인 문서들에 대해서) 얼마나 자주 사용되는지를 나타내는 지표이다.
- Phelps와 Wilensky의 로버스트 하이퍼링크(robust hyperlinks[16]): 기존에 있던 웹사이트의 링크가 바뀌는 등으로 인해 생기는 링크 깨짐 문제(broken links problem)을 해결하기 위해 제안된 방법이다. 기본적으로 이 방법은 '어휘 서명(lexical signature)'라고 정한 중요 단어들(well-chosen terms)을 이용하여 웹사이트를 찾는다. 예를 들어, abc.com을 찾고 싶은 경우 우선 abc.com으로 웹사이트를 연결해보고 실패할 경우에는, 관련된 중요단어들을 어휘 서명(lexical signature)으로 선택하여 그 단어들과 함께 기존의 웹사이트를 검색 엔진에 검색하고 가장 가깝게 매칭되는 링크를 찾는다. 이 방법에서 중요한 것은 좋은 어휘 서명(lexical signatures)를 찾는 것인데 이를 위해서 CANTINA에서는 TF-IDF를 사용한다.

1) 이들 안티 피싱 솔루션들에 대한 좀 더 자세한 소개와 설명은 [21, 24, 26]를 참조.

Table 4. PILPER's Important Features Characterizing Phishing Emails[7]

지표	내용
주소 URL이 IP 주소로 구성되어 있는가(IP-based URLs)	합법적인 회사의 사이트들은 IP주소를 바탕으로 페이지를 표현하는 일이 드물다. 공격당한 PC (compromised PC)등을 이용한 웹사이트의 경우에 적절한 DNS 없이 IP 주소로만 사이트를 표현하는 경우도 있다. 따라서 이런 경우에 이메일 안에 IP-based URL이 있는 지는 피싱 공격을 발견하는데 유용한 지표가 될 수 있다.
이메일 안에 링크들의 도메인 네임의 나이(Age of linked-to-domain names)	피싱 공격에 사용되는 도메인은 대체로 짧게 사용되고 사라지기 때문에 이메일에 포함된 링크의 도메인이 얼마나 되었는지가 중요한 지표가 될 수 있다.
하이퍼링크와 맞지 않는 URL (Nonmatching URLs)	하이퍼링크에 표시된 URL과 실제로 연결되는 URL이 다른 경우도 (예: 〈a href="badsite.com"〉 paypal.com〈/a〉) 피싱 공격 이메일을 판별하는데 중요한 지표가 된다.
HTML이 사용된 이메일인가 텍스트로만 이루어진(text-only) 이메일인가	텍스트로만 이루어진(text-only) 이메일에 올바르지 않게 가장된(disguised) 주소를 넣기 어렵기 때문에 HTML 이 사용되지 않은 이메일인 경우에는 피싱 공격이 아니라고 판별하는데 도움이 된다.

위에 소개된 두 기법을 이용하여 CANTINA는 다음과 같은 절차로 피싱 공격을 판별해낸다:

(1) 주어진 웹페이지에 나타나는 각각의 용어(term)에 대해서 TF-IDF 점수를 산출한다.
(2) TF-IDF 점수가 가장 높은 5개의 용어를 어휘 서명(lexical signature)으로 택한다.
(3) 위에서 채택한 어휘 서명(lexical signature)를 검색 엔진에(CANTINA의 경우에는 구글 사용) 넣어 검색한다.
(4) 검색 결과로 나온 N[2] 개의 최상의 결과 중에서 현재의 웹페이지와 도메인 이름이 같은 것이 있는지 확인한다. 같은 것이 있으면 합법적인 사이트로 판별하고 그렇지 않으면 피싱 사이트로 판별한다.

CANTINA는 위에 기본 원리를 따라 작동하면서, 몇 가지 실제적인 문제(예, 거짓 양성 오류)에 맞추어 보완하는 방법으로 다음과 같은 방법들을 사용한다:

- 검색 결과가 없으면 피싱이다: 검색 결과가 아무것도 나오지 않을 경우에는 경험(heuristic)에 따라 "무(無)결과는 피싱을 의미한다"라는 원칙을 따른다. 이를 ZMP(Zero results Means Phishing heuristic)라고 부른다.
- 추가적 휴리스틱(heuristic) 지표를 사용: SpoofGuard[2]나 PILFER[7]에서 사용하듯이 피싱 공격과 관련된 지표(feature)들(도메인의 생성기간, IP로 구성된 주소 사용 등)을 추가적인 정보로 사용한다.

2) N에 대해서는 1에서 50까지 다양하게 선택할 수 있지만 실험결과에 따르면 30이상은 결과에 크게 의미가 없다[23].

2.1.2 합법적 서버 인증을 강화하는 솔루션들

두 번째로 분류되는, 합법적인 서버를 인증하는 데 집중한 솔루션들은 서버인증의 사용성을 높이는데 그 초점이 맞추어져있다. 이미 SSL 등을 통하여 서버를 인증하는 방법은 있으나 관련개념에 익숙하지 않은 사용자가 올바르게 서버인증 결과를 확인하는 데 있어서 어려움이 따를 수 있고, 실제로 알려지지 않은 CA로부터 서버인증서를 받아서 마치 올바른 SSL 연결처럼 가장하는 것도 가능하다[31]. 따라서 일반 사용자들이 좀 더 쉽게 진짜 서버인지를 인지할 수 있도록 도와줌으로써 서버인증을 강화시키는 솔루션들이 제공되고 있다. 대표적인 예로 PassMark[15]는 사용자와 서버가 비밀번호 이외에 비밀 이미지를 공유하도록 하여 사용자가 비밀번호 입력 전에 서버가 공유된 비밀 이미지를 보여주는 지 확인하는 절차를 갖도록 한다. 이를 통하여 올바른 서버에 비밀정보를 보내도록 도와준다. Verified by Visa[19]와 Dynamic Security Skins[3]도 이미지를 이용하여 서버 인증을 강화시키는 솔루션들이다.

2.2 이메일 수신 단계에서 제공되는 솔루션

이 종류에 속한 대표적인 솔루션은 이메일 필터링으로 사용자에게 이메일이 피싱 공격 이메일로 분류됨을 알려줌으로써 사용자가 잘못된 서버에 연결하는 것을 막아준다. 대표적인 예로는 PILFER가 있다[7].

PILFER는 웹브라우져나 툴바가 가질 수 있는 내용적 한계(서버의 주소 정보만을 이용하여 분석)를 극복하고 좀 더 구체적인 정보를 바탕으로 정확하게 피싱 공격을 가려내기 위해서 이메일 필터링을 이용한다. 이메일 필터링은 사용자가 받은 이메일 자체를 분석하여 피싱 공격 이메일을 가려내는 방법이다. PILFER는 스팸 메일 필터링에서 종종 사용되는 기계학습(machine learning) 기법을 이용하여 피싱 공격 이메일을 골라내는데, 이 솔루션이 기존의 스팸 필터링과 다른 점은 피싱 공격을 판별하는데 유용한 10개의 특징요소 즉 지표(feature)를 사용하여 피싱 이메일을 분류해 낸다는 점이다. 피싱 메일은 합법적인 이메일과 가능한 유사하게 보여야한 다는 점에서 스팸메일과는 다르기 때문에 피싱 메일을 분류하기 위한 특징을 잘 선택하는 것이 핵심이 될 수 있다. 이 솔루션에서 제시된 지표들을 통해서 피싱 공격의 특징을 이해하는데 도움이 되므로 이 논문에서 이들 대표적인 지표 몇 가지를 Table 4.에 소개 한다.

Table 4.에 소개된 지표 이외에도, 링크의 수, 도메인의 수, URL 표시에 사용되는 점(dot, ".")의 수, 자바스크립트를 사용했는지 여부, 연동하는 스팸 필터링의 결과 등을 지표로 사용한다.

추가적으로 PILFER는 웹브라우져와 연계하여 (사용자의 이메일 환경이 웹브라우져와 연계될 수 있는 환경에서) 더 좋은 서비스를 제공하는 방법도 제시한다. 이때에는 추가적으로 웹페이지 분류에서 사용될 수 있는 지표(feature)들을 함께 사용하는 것을 제시한다. 브라우져 히스토리에 있는 웹사이트인가(site in browser history)와 리다이렉트 된 사이트인가(redirected site) 등이 그러한 지표가 된다.

2.3 사용자 정보 전달 단계에서 제공되는 솔루션

네 번째 단계에서 제공되는 솔루션은 사용자가 입력한 비밀정보가 서버에게 그대로 전달되는 것을 막아준다. 대표적인 솔루션인 PwdHash[18]는 사용자의 비밀번호를 도메인에 따라 바꾸어주어, 해당 서버에 보내준다. 이렇게 하여 공격 서버로부터 사용자의 비밀번호를 보호한다. 비슷한 방법을 사용하는 솔루션으로 Lucent Personal Web Assistant[8]와 Password Multiplier[9]가 있다.

III. 피싱 관련 연구

피싱 공격은 사람의 능동적인 행동(예, 링크를 클릭하여 서버에 연결, 자신의 비밀정보 입력 등)을 포함하는 공격이기 때문에, 단순히 사용자의 컴퓨터를 공격하는 형태의 공격들(예, DDos)과 달리 기술적인 솔루션에 대한 연구 이외에도 사용자와 연관된 연구가 많이 진행되었다. 이 장에서는 이러한 연구들에 대해서 살펴본다.

3.1 사용자들이 피싱 공격에 빠지는 이유

2006년 Dhamija 등의 "왜 피싱 공격이 성공하는가 (Why Phishing Works)"에 대한 연구가 발표되었다[31]. 그들은 실험을 통해서 많은 사용자들에게 있어서 보안 경고 및 표시(security indicators)가 피싱 공격을 막는데 효과적이지 못하다는 것을 보였다. 그들이 실험을 통해 분석한 사용자들이 피싱 공격에 빠지는 이유들은 다음과 같다:

- 지식의 부족: 컴퓨터 시스템 지식의 부족이나 보안 및 보안 지표들에 대한 지식이 부족한 경우에 사용자들은 피싱 공격에 빠질 수 있다. 예를 들어, 도메인 네임의 의미나 도메인 네임 문법에 대한 지식이 없는 많은 사용자들은 "www.ebay-members.com"처럼 URL 어딘가에 ebay라는 이름이 들어있으면 "www.ebay.com"에 속하는 페이지라고 생각할 수 있다. 또한, 웹브라우져의 보안 지표가 되는 좌물쇠와 같은 SSL 연결 표시(Fig. 1.의 네모 참조)에 대해 이해하지 못하거나, 서버의 인증서를 제공한 CA를 믿을 만한 곳인지 인지하거나 확인하는 방법에 대해서 모르는 사용자들이 있다.
- 보여지는 모습에 잘 속을 수 있다: 도메인 이름에 대한 typejacking 공격에서와 같이 레터(letter)를 눈에 띄지 않게 바꾸는 공격이 가능하다 (예를 들어, 알파벳 'l'대신 숫자 '1'을 사용하여 URL을 표현함). 또한 하이퍼링크의 연결 링크를 이미지 아래 숨겨두어서 가짜 URL에 눈에 띄지 않게 하는 방법 등이 있다.
- 주의력의 부족: 보안 표시에 대해 주의 깊게 인지하지 못한다. Fig. 1.에서처럼 SSL을 이용한 HTTPS 연결의 경우에 크롬 등의 웹브라우져에서 안전한 연결의 표시로 좌물쇠 잠금 아이

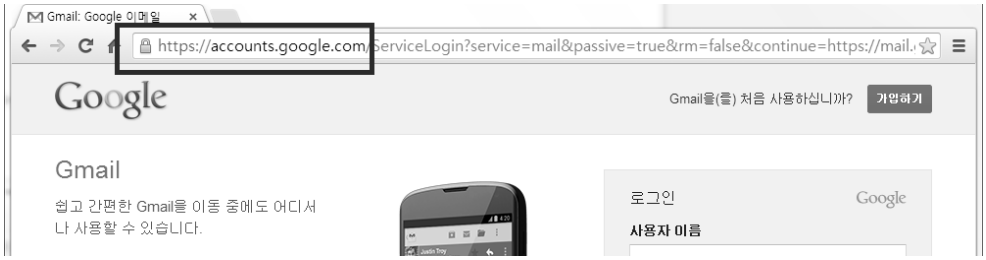

Fig.1. Appearance of the Address-bar showing a Legitimate Gmail Log-in Page. The HTTPS' Green Font and lock icon show that the connection is an HTTPS connection.

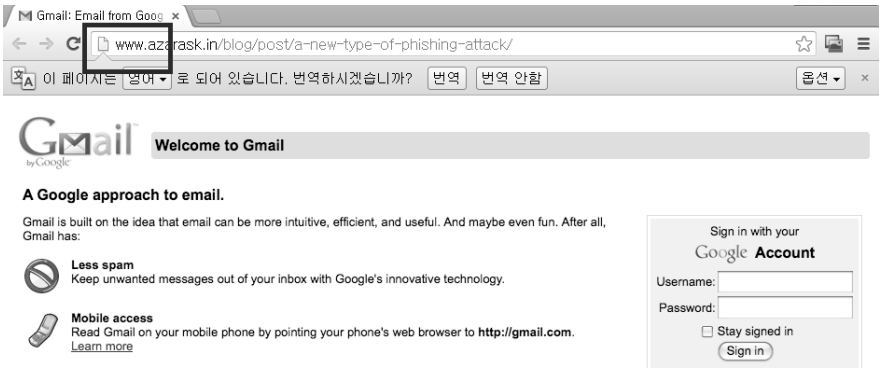

Fig.2. Appearance of the Address-bar showing a fake Gmail Log-in Page connected by tabnabbing attack[1]. The address-bar has neither a HTTPS connection indicator nor a lock icon.

콘을 보여준다. 하지만 사용자들이 이러한 잠금 아이콘 표시를 놓치는 경우가 많아 잠금 아이콘 표시가 있는 경우(Fig. 1.의 경우)와 없는 경우(Fig. 2의 경우)를 다르게 인지하지 못한다.

위의 연구 내용은 사용자가 피싱 공격을 당하는 이유를 기술적인 면에서 분석하였다. 한편, 사회적인 이유에서도 피싱 공격의 가능성이 높아진다는 것을 보여준 연구결과도 있다. Jagatic 등의 "Social Phishing"이라는 연구 논문에 따르면 동일한 내용의 피싱 공격 이메일(spoofed email)을 받는 경우에, 모르는 사용자들에게 이메일을 받은 경우에는 16% 정도의 공격 성공률을 보인 반면 송신자가 지인으로 조작된 이메일을 받은 경우에는 72%의 공격 성공률을 보였다. 이 논문에서는 피싱 공격이 기술적 취약성(technical vulnerabilities)만 이용하는 것이 아니라 사회적 취약성(social vulnerabilities)을 함께 이용한다는 것을 보여주고 있다[12].

3.2 안티 피싱 솔루션들(anti-phishing solutions)이 얼마나 효과적인가.

Wu 등은 보안 툴바(security toolbar)의 효과성에 대한 연구[21]에서, 툴바가 대체로 사용자들이 피싱 공격을 판별하는 데 도움이 되는 정보를 제공하지만 그것이 정말 효과적인지를 알기위해서는 사용성을 평가 해보아야 한다고 주장하였고, 사용자를 대상으로 보안 툴바가 피싱 공격을 피하는데 실질적으로 도움이 되는지 실험하였다. 그들이 실험을 통해서 얻은 것은

Table 5. Reasons why tool-bars are not effective to users[21]

사용자들은 주어진 보안 경고보다 보여 지는 웹페이지에 더 의존한다. 웹페이지에 결함이 없어 보이고 실제와 매우 비슷해 보이는 경우에 사용자는 웹페이지를 진짜라고 간주한다.
사용자들은 경고를 인지했음에도 불구하고, 주어진 작업을 끝까지 마치고 싶기 때문에 계속 진행한다.
사용자들은 경고 박스와 익숙하지 않기 때문에 그 경고를 믿지 않는다.

보안 툴바나 브라우져에서 제공하는 보안 표시등이 실제로 크게 효과적이지 못하다는 결과였다. 많은 경우 사용자들은 툴바를 보지 못하거나, 제공되는 정보를 무시해버리거나 아니면 관심을 갖더라도 그 내용을 잘 이해하지 못하였다. 그들이 분석한 사용자들에게 보안 툴바가 효과적이지 못한 이유는 Table 5.에 정리되어 있다. Table 5.에 정리된 첫 번째와 세 번째의 이유들은 3.1장에 소개된 Dhamija 등의 분석결과[31]와 그 내용이 유사함을 발견할 수 있다.

Wu 등은 이 논문에서는 보안 솔루션들이 좀 더 효과적이기 위해서 보안되어야할 방안들을 제시하였고, 추천 방안들을 정리하면 다음과 같다[21]:

- 수동적 경고보다는 적극적으로 인터럽트를 주는 것이 더 효과적이다. 하지만 이러한 방법은 너무 자주 사용되지는 않아야 한다. 너무 잦은 경고는 쉽게 무시되기 때문에 자주 등장 할수록 효과가 줄어든다.
- 경고는 적절한 시기에 적절한 경고 메시지와 함께 사용되어야 한다. 포괄적인(generic) 내용의 메시지보다는 매우 구체적인 내용의 메시지를 보여주어야 한다.
- 사용자들은 시작한 작업을 끝내고 싶어 한다. 이러한 점을 존중하여 경고 뒤에 그냥 진행을 멈추도록 하는 것보다는 다른 대안을 제시하여 사용자들이 안전하게 주어진 작업을 마칠 수 있도록 안내해주는 것이 바람직하다.
- 인터넷 회사들은 몇 가지 표준 실행을 따르도록 하여 그들의 사이트가 악성 피싱 공격과 구별될 수 있도록 할 필요가 있다. 회사들은 서버에 대해 가능한 하나의 도메인 이름을 사용하고, 도메인 이름이 그들의 브랜드 이름과 일치하도록 하는 것이 좋다(IP 주소나 여러 도메인 이름으로 구성된 것을 피하는 것이 좋다). SSL 연결을 사용하여 웹페이지 통신을 암호화하고, 널리 알려지고 사용되는 CA로부터 공인된 SSL 인증서를 사용하도록 해야 한다.

또 다른 관련 연구로는 Egelman 등의 '피싱 경고가 얼마나 효과적인가'에 대한 연구가 있다[5]. 이들은 웹브라우저에서 제공하는 피싱 경고의 형태에 따라서 그 효과가 어떻게 달라지는 지를 분석하였다. 그들의 연구 결과에 따르면 수동적으로 주어지는 (passive) 피싱 경고를 제공받은 97% 사용자들이 최소한 하나의 피싱 공격에 빠지게 되었고, 피싱 공격의 형태를 적극적(active)으로 바꾼 경우에는(예, 작업의 진행을 방해하는 형태) 79%의 사용자들이 피싱 공격에 조심하여 피싱 공격을 피하는 결과를 얻었다. 결론적으로, 적극적인 보안 경고, 특히 사용자의 중요한 작업(primary task)을 인터럽트하는 형태의 경고가 효과적임을 강조하였다.

또한, Zhang 등은 대표적인 피싱 공격을 막는 솔루션들(anti-phishing tools)의 성능을 실험을 통해 평가하고 그 결과를 분석하였다. 그들은 솔루션들이 블랙리스트 방법에 의존하는 경우에는 실험 테스트베드가 무엇이냐에 따라서 그 결과가 많이 달라짐을 발견하였다. 그 이유는 2장에서 이미 설명하였듯이 블랙리스트의 방법에서는 블랙리스트 업데이트 결과가 솔루션의 성능에 큰 영향을 끼치기 때문이다. 휴리스틱을 사용하는 방법은 이러한 문제를 극복하는데 도움이 되었지만 거짓 양성 오류가 높은 단점이 있었고, 이러한 거짓 양성 오류는 화이트리스트 방법을 함께 사용함으로써 보완할 수 있음을 제시하였다[24].

아래 두 연구[5, 24]에서도 보안 솔루션들을 향상시키기 위한 추천방안들이 제시되었고, 그 핵심내용은 앞에 정리된 내용[21]과 유사하다.

IV. 국내의 대응과 관련 연구

국내에서는 국가와 금융기관(은행, 신용카드 회사 등)을 중심으로 피싱에 대응해가고 있다. 국가가 여러 매체를 통해 피싱 공격에 대해서 홍보하고, 금융기관에서는 홈페이지나 고객에게 이메일 전송 등을 통하여 피싱의 내용과 피싱을 피하는 방법을 알리고 있다. 또한, 웹브라우져에서 제공하는 보안 기능을 이용하여 홈페이지 주소 창에 로고를 표시하거나 HTTPS의 안전한 연결을 이용하여 서버 인증을 강화하고 있다 (Fig. 3. 참조).

피싱 대응에 관한 국내의 연구로는 사준호 등의 "피싱사이트 실시간 탐지 기법"이 있다. 이 연구에서는 피싱 사이트가 사칭하고자 하는 대상 사이트(이하 '원시사이트')에 유입되는 HTTP 트래픽을 수집 분석하여, 원시사이트를 참조한 웹사이트의 URL을 휴리스틱 방법으로 분석하고, 그를 통해서 피싱 사이트를 탐지하는 방법을 설계하고 제안하였다[25]. 그 밖에 피싱 대응에 관해 더 제시된 국내 연구가 있고[20, 22, 27, 32-34], 이들에 사용된 기술들은 2장에 소개된 안티피싱 솔루션들의 기술들과 크게 다르지 않다. 한편, 솔루션의 사용성 혹은 사용자 입장에서 효과적으로 피싱을 막는 대응방안에 대한 국내연구는 아직 많지 않다.

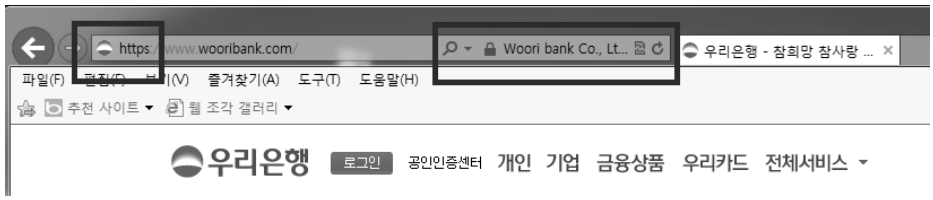

Fig.3. Appearance of the Address-bar when IE connects to the Woori Bank Homepage. The bank logo appears on the left side of the address-bar and lock-icon on the right side shows the HTTPS connection.

사준호는 "국내 피싱사이트 주요특징 및 대응방안" 제목의 보고서에서 피싱에 대한 대응을 요약하고 국내의 대응에 대해서도 정리하였다[26]. 이 보고서에서 지적하였듯이 아직 솔루션 제시에 있어서 국내의 대응은 부족한 편이고, 피싱 공격에 대해서 사회적 관심과 정부 및 관련기관들의 주도적 대응 및 연구가 필요한 상황이다. 또한 이 논문에서 피싱 문제를 대응하는 데 있어서 다양한 대응방안들의 장점들을 수용하여 다각적인 측면에서 대응하는 것을 권장하고 있다.

V. 앞으로 나아갈 방향

앞에 소개된 안티 피싱 솔루션들과 피싱 관련 연구들의 내용을 바탕으로 이 논문에서는 피싱을 막기 위한 앞으로의 대응으로 다음과 같은 방향을 제시한다.

5.1 기술 도입 및 국내 사용자에 맞는 사용성 증진

2장에 소개하였듯이 다양한 안티 피싱 솔루션들이 많이 제안되었다. 이미 휴리스틱과 블랙리스트 기술을 조합하면 피싱 공격 사이트를 97%이상으로 판별해 낼 수 있고, 이때 발생할 수 있는 거짓 양성 오류(false-positive)도 화이트리스트 방법을 이용하여 크게 줄일 수 있다[24]. 따라서, 앞으로 좀 더 관심을 기울여야하는 점은 이러한 솔루션들의 성능보다는 솔루션들의 사용성 향상이다. 앞에 소개된 안티 피싱 솔루션들에 대한 연구들에서 발표하였듯이 100% 올바르게 피싱 공격을 판별할 수 있는 툴이 주어진 상황에서도 그 사용성(usability)에 따라 실제로 사용자들이 피싱 공격을 피하는데 이용될 수 있는 효과는 매우 적을 수 있다[5, 21, 24].

특히 많은 솔루션들이 해외 기업 혹은 해외 기업 및 연구진을 중심으로 제시되어, 그 기업 혹은 그 나라의 고객들의 편의에 맞추어져있기(customized) 때문에, 국내 기업과 기관에서 국내 고객이 친근하고 편하게 사용할 수 있도록 재조정(customizing)하고 이에 대해 사용성을 분석하는 것이 요구된다. 여기서 강조하고 싶은 사용성은 앞에 3장에 소개된 솔루션 개발의 추천방안들에 주목하여 제공될 필요가 있다. 특히, 다음의 몇 가지는 더욱 강조될 필요가 있다:

- 단순히 위험 경고로 사용자의 작업진행을 중단시키기 보다는 다른 안전한 방법 (예, 사용자가 피싱 공격 대상자를 재확인해볼 수 있는 방법) 등을 제시하여 사용자가 주어진 작업을 끝까지 마치고 싶어 하는 욕구에 응해준다.
- 경고는 적절한 시기에 적절한 경고 메시지와 함께 사용되어야 한다. 포괄적인(generic) 내용의 메시지보다는 매우 구체적인 내용의 메시지를 보여주어야 한다.
- 기업과 기관은 그들의 사이트가 악성 피싱 공격과 구별될 수 있도록 도와주는 표준 실행을 따라서 사용자들이 이들에 익숙해지도록 할 필요가 있다. 브랜드 이름과 일치하는 서버 이름을 사용하고, SSL 연결을 사용하여 안전한 연결을 제공하고 널리 알려진 CA로부터 공인된 인증서를 사용하여 그렇지 않은 경우와 구별되게 하는 것이 필요하다.

5.2 상호작용(interaction)을 통한 사용자 교육

두 번째로 제시할 방향은 사용자와 상호작용(interaction)을 하는 교육방법 개발 및 이를 이용한 사용자 교육이다. 좋은 성능을 가진 안티 피싱 솔루션을 갖추는 것보다도, 이러한 사용자 교육이 더 효과적으로 그리고 궁극적으로 피싱 공격을 막는데 도움 될 수 있다.

국내외적으로 이미 정부, 기업, 그리고 기관들이 피싱 공격의 위험성을 홍보하고 피싱 공격을 피하는 방법들을 온라인 자료를 홈페이지에 게시하거나 이메일을 전송하여 알리고 있다. 하지만 수동적으로 주어지

는 온라인 자료들을 사용자들이 흥미를 가지고 적극적으로 읽어 교육의 효과를 얻기를 기대하기는 어렵다. 이는 3장에 소개된 Egelamn등의 연구에서 수동적인 보안 지표가 능동적인 보안 지표에 비해 쉽게 사용자에게 무시될 수 있는 이유와 비슷하다[5].

실례로 수동적으로 주어지는 온라인 자료 외에 좀 더 효과적으로 사용자들에게 피싱 공격을 경험하고 학습하도록 도와주는 대표적인 사례들을 소개 한다:

- Mailfrontier 피싱 IQ 테스트는 실제로 피싱에 사용되었던 이메일들을 가지고 만들어진 10개의 테스트로 구성되어있다. 각각의 문제에 대해서 링크를 클릭하면 이메일 내용이 나오고 그 이메일 내용을 검토하여 합법적인 (legitimate) 이메일인지 가짜(fraud) 이메일인지 답을 선택하면 된다. 10문제에 대해서 각각 답을 선택하면 나중에 몇 개를 맞았는지 점수를 얻을 수 있다[13].
- 사용자들에게 피싱 이메일을 보내서 사용자가 이러한 공격에 취약한지를 테스트한다. 그러한 뒤에는 사용자들에게 피싱 공격에 대해 알려주는 자료가 주어진다. 이러한 학습방법을 체험을 통한 학습(situated learning)이라고 하고[23], 여러 기관에서 사용되었다: Indiana 대학에서 학생들을 교육하기 위해서 사용되었고[12], 웨스트 포인트에서 사관후보생들을 지도하기 위해서 사용되었고[6, 11], 뉴욕 주에서 직원들을 교육하기 위해서 사용되었다[14]. 실제로 뉴욕 주 교육을 통해서 얻은 결과에 의하면 이러한 방법으로 학습한 사람들이 단순히 팜플렛 자료만 주어진 사람들보다 피싱 공격에 대한 분별력이 향상됨이 드러났다.

위에 예와 더불어, 앞에서 소개된 "Social Phishing" 논문의 연구 결과[12]에서 알 수 있듯이, 피싱 공격에 있어서 공격의 기술적인 부분만이 공격의 가능성을 결정하는 것이 아니라, 사회적인 면이 중요하기 때문에, 사용자의 모의 경험과 교육이 피싱 공격을 궁극적으로 막는데 더 큰 효과를 줄 수 있다. 예를 들어, 모의 피싱을 통해 지인으로 꾸며진 피싱 공격 이메일을 경험하고 모의 피싱 후에 대응책을 교육받은 사람은 추후에 지인으로부터 비슷한 종류의 피싱 공격 이메일을 받았을 때, 지인에게 통화를 통해 재확인하거나 교육받은 대응책을 이용하여 피싱 공격을 피할 수 있을 것으로 기대된다.

이처럼 좀 더 사용자와 상호작용하며 사용자의 관심을 끌고, 이로서 사용자를 효과적으로 교육할 수 있는 방법들을 개발하고 도입하는 것이 필요하다.

VI. 결 론

이 논문에서는 대표적인 안티 피싱 솔루션들을 소개하고 종류에 따라 분류하여 살펴보았다. 또한, 피싱 관련 연구들을 바탕으로 피싱을 막는데 있어서 솔루션의 기술적 부분뿐만 아니라 솔루션의 사용성 부분이 어떻게 작용하는지 살펴보았다. 이러한 연구 결과들을 바탕으로 현재까지의 피싱 연구 현황을 알아보고, 앞으로 피싱 연구가 나아가야할 방향을 제시하였다. 특히 솔루션을 국내 사용자에게 맞추어 적용하고, 사용자와의 상호작용을 통해서 사용자를 효과적으로 교육하는 것이 필요함을 강조하였다.

References

[1] Aza Raskin, "Aza Raskin's original tab-nabbing disclosure", http://Azaras k.in, 2010-05-25. Visited 2013-09-18.

[2] N. Chou, R. Ledesma, Y. Teraguchi and J. C. Mitchell, "Client-Side Defense Against Web-Based Identity Theft," Network and Distributed System Security Symposium, 2004.

[3] R. Dhamija, and J.D. Tygar. "The battle against phishing: Dynamic Security Skins," In Proceedings of the First Symposium on Usable Privacy and Security, pp. 77-88, 2005.

[4] eBay Toolbar and Account Guard. http://pages.ebay.com/help/confidence/account-guard.html

[5] S. Egelamn, L.F. Cranor, and J. Hong, "You've Been Warned: An Empirical Study of the Effectiveness of Web Browser Phishing Warnings," CHI, 2008.

[6] A.J. Ferguson, Fostering E-Mail Security Awareness: The West Point Carronade, EDUCASE Quarterly, 2005. http://www.educause.edu/ir/library/pdf/eqm0517.pdf

[7] L. Fette, N. Sadeh, A. Tomasic, "Lea-

rning to Detect Phishing Emails," WWW, 2007.
[8] E. Gabber, P.B. Gibbons, Y. Matias, and A.J. Mayer, "How to make personalized web browsing simple, se- cure, and anonymous," In Proceedings of Financial Cryptography. pp. 17-32, 1997.
[9] J.A. Halderman, B. Waters, and E.W. Felten. "A Covenient Method for Securely Managing Passwords," In Proceedings of 14th International World Wide Web Conference, 2005.
[10] A. Herzberg, A. Gbara, "TrustBar: Protecting Web Users from Spoofing and Phishing Attacks" 2004. http://www.cs.biu.ac.il/~herzbea/Papers/ecommerce/spoofing.htm
[11] J.W. Jackson, A.J. Ferguson, and M.J. Cobb. "Building a University- wide Automated Information Assur- ance Awareness Exercise: The West Point Carronade," In Proceedings of 35th ASEE/IEEE Frontiers in Education Conference 2005.
[12] T. Jagatic, N. Johnson, M. Jakobsson, and F. Menczer, "Social Phishing," School of Informatics and Dept. of Computer Science, Indiana University. 2006, http://www.indiana. edu/~phishing/social-network-experience/phishing-preprint.pdf
[13] Mail Frontier, Phishing IQ. Visited: Sep 20, 2013, http://survey.mailfron tier.com /survey/quiztest.cgi?themailfrontierphishingiqtest
[14] New York State Office of Cyber Secu- rity & Critical Infrastructure Coordi- nation 2005. Gone Phishing… A Briefing on the Anti-Phishing Exer- cise Initiative for New York State Go- vernment. Aggregate Exercise Results for public release.
[15] PassMark Security, Protecting Your Customers from Phishing Attacks - An Introduction to PassMarks, http://www.passmarksecurity.com/
[16] T.A. Phelps and R. Wilensky, Robust Hyperlinks and Locations, D-Lib Magazine, vol. 6 (7/8), 2000.
[17] SpoofStick. 2004. http://www.spoofstick.com/
[18] Stanford Applied Crypto Group, "Pwd-Hash," Visited: Sep 09 2013. http://crypto.stanford.edu/PwdHash
[19] Visa, Verified by Visa, http://www.visa.com/
[20] Iksu Kim and Jongmyung Choi, "De-signinig Authentication Protocol that protects user information from Phishi- ng and Pharming Attacks," Journal of the Korea Society of Digital Industry and Information management, 5(1), pp.63-70, Mar. 2009
[21] M. Wu, R.C. Miller, and S.L. Garfinkel. "Do Security Toolbars Actually Prevent Phishing Attacks?" CHI 2006.
[22] Daeyu Kim and Jung-Tae Kim, "Implementation of Web Searching Robot for Detecting of Phishing and Pharming in Homepage," Journal of the Korea Institute of Maritime Information & Communication Scien -ces, 12(11), pp.1993-1998, Nov. 2008
[23] Y. Zhang, J. Hong, L. Cranor, "CANTINA: A Content-Based Approa- ch to Detecting Phishing Web Sites," WWW, 2007.
[24] Y. Zhang, S. Egelman, L. Cranor, and J. Hong, "Phinding Phish: Evaluating Anti-Phishing Tools," Human Com- puter Interaction Institute, Paper 76, http://repository.cmu.edu/hcii/76, 2006.
[25] Joon ho Sa, Sangjin Lee, "Real-time Phishing Site Detection Method," Journal of The Korea Institute of information Security & Cryptology, 22(4), pp.819-825, Aug. 2012
[26] Joon ho Sa, "Study on Characteristics of Phishing Sites in Korea and related Solutions," Financial Security Agency

Issue Report, 2011(20), pp 6, Nov. 2011
〔27〕 Webcheck System, Korea Internet Security Agency, Visited: Sep 27, 2013, http://webcheck.kisa.or. kr/
〔28〕 Google, Inc. Google Safe Browsing for Chrome. Visited: Sep 27, 2013, https://www.google.com/intl/en/chrome/browser/features.html#security
〔29〕 Mozilla Firefox, Safe Web Browsing, Visited: Sep 27, 2013, http://www. mozilla.org/en-US/firefox/security/
〔30〕 Microsoft Corporation, Internet Explo- re r 7, Phishing Filter, Visited: Sept 27, 2013, http://windows.microsoft.com/en- us/windows-vista/phishing-filter-frequently-asked-questions
〔31〕 R. Dhamija, J.D. Tygar, M. Hearst, "Why Phishing Works," CHI, 2006.
〔32〕 JuHyun Kim, YoungJae Maeng, DaeHun Nyang, KyungHee Lee, "Cog- nitive Approach to Anti-Phishing and Anti-Pharming," Journal of The Korea Institute of information Security & Cryptology, 19(1), pp.113-124, Feb. 2009
〔33〕 Minsu Lee, Hyungku Lee, Hyunsu Yoon, "An Anti-Phishing Approach bas -ed on Search Engine," In Proceedings of Korea Computer Congress, 2010
〔34〕 Daeyu Kim and Jung-Tae Kim, "Analyses of Detection Techniques of Phishing in the Web Site," Conference on Korean Institute of Maritime Information and Communication Sci -ences, 2007

〈저자소개〉

사 진

신 지 선 (Ji Sun Shin) 정회원
2001년 2월: 서울대학교 컴퓨터공학과 졸업
2009년 5월: 메릴랜드 주립대학(University of Maryland at College Park) 컴퓨터 과학과 박사
2009년 9월~2012년 2월: 삼성 SDS 책임연구원
2012년 3월~현재: 세종대학교 조교수
〈관심분야〉 정보보호, 암호학, 컴퓨터 보안