OUCH! | 2015 년 12 월호

컴퓨터 사용자를 위한 월간 정보보호 인식 뉴스레터

OUCH!

이달 호 주제..

- 개요
- 피싱
- 대응책

피싱

개요

이메일은 통신을 위한 주요한 수단 중 하나입니다. 우리는 매일 업무에 사용할 뿐 아니라, 친구나 가족간의 연락을 위해서도 이메일을 사용하고 있습니다. 또한 이메일은 회사의 제품이나 서비스를 소개할 때나 온라인 구매에 대한 확인 및 온라인 은행 명세서에서도 사용됩니다. 전 세계 너무도 많은 사람들이 이메일에 의존하고 있기 때문에, 이메일은 사이버 범죄자들이 다른 사람들을 공격하는 데에도 사용되는 주요한 방법 중 하나입니다. 이번 뉴스레터에서는 일반적인 이메일 공격 방법인 피싱과, 이메일을 안전하게 사용하는데 필요한 단계를 설명합니다.

객원 편집자

랜스 헤이든 박사는 버컬리 연구그룹의 상무이사이다. 보안 문화 및 행동분야 전문가로서 "사람중심의 보안: 기업의 보안 문화로 전환하기" 의 저자이다. www.linkedin.com/in/drhayden에서 헤이든의 자세한 사항을 알 수 있다.

피싱

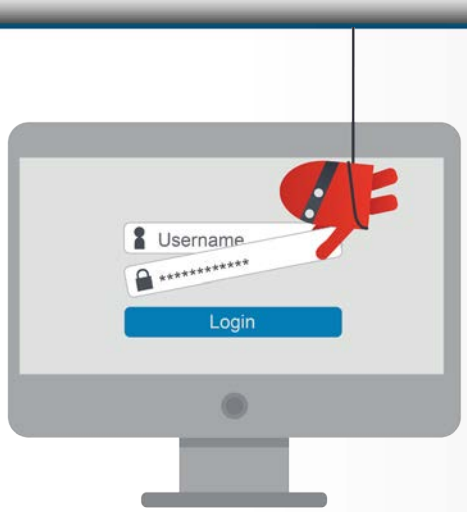
피싱은 소셜 미디어에서 이메일이나 메시징 서비스를 이용하여 링크를 클릭하거나, 첨부 문서를 열어보는 것과 같이 사람을 속이는 공격을 말합니다. 이러한 공격으로 피해자를 만들어 굉장히 민감한 정보가 도난되거나, 컴퓨터가 감염됩니다. 공격자들은 피싱 이메일이 진짜 믿을 수 있도록 열심히 연구합니다. 예를 들어 공격자들은 이메일이 친구나 자주 이용하는 회사에서 온 것처럼 보이게 합니다. 공격자들은 은행의 로고를 포함하거나, 이메일 주소를 조작하여 메시지가 진짜인 것처럼 보이게 합니다. 공격자들은 이러한 이메일을 전세계 수백만 사람들에게 전송합니다. 범죄자들은 누가 피해자가 될지도 정확이 모릅니다. 범죄자들은 단지 더 많은 이메일을 보낼수록 성공가능이 높다는 것을 알고 있습니다. 피싱은 물고기를 잡기 위해 그물을 이용하는 것과 유사합니다. 무엇을 잡을 지는 모르지만, 그물이 클 수록 더 많은 물고기를 잡습니다. 공격자들은 자신들이 원하는 것을 얻기 위해 피싱을 이용하는 여러 가지 방법이 있습니다.

- **정보수집**: 공격자들의 목적은 패스워드, 신용카드 번호 및 은행 상세정보와 같은 개인정보를 수집하는 것입니다. 이를 위해 합법적인 것처럼 보이는 웹사이트로 가도록 하는 링크를 이메일로 보냅니다. 이러한 웹사이트는 계좌정보나 개인정보를 제출하도록 요청합니다. 하지만 이러한 사이트는 가짜이며, 입력한 모든 정보를 공격자에게 바로 갑니다.
- **악성링크**: 공격자의 목적은 기기를 제어하는 것입니다. 이를 위해 링크가 있는 이메일을 보냅니다. 링크를

피싱

클릭하면, 우리의 기기를 대상으로 공격하는 웹사이트로 가도록 하고, 성공하면 기기를 감염시킵니다.

- **악성문서 첨부**: 공격자의 목적은 기기를 감염시키고 제어하는 것입니다. 하지만 링크를 보내는 대신, 공격자들은 워드, 아래아 한글 문서 등의 감염된 파일을 이메일로 보냅니다. 첨부문서를 열면 공격을 시작하여, 공격자들은 시스템을 제어하게 됩니다.
- **사기**: 일부 피싱이메일은 디지털 세계로 온 사기꾼들입니다. 공격자들은 우리를 속여서 복권에 당첨되었다고 말하거나, 자선단체라고 하고 기부하라고 하거나, 큰 돈을 송금해달라고 요청합니다. 만약에 이러한 것에 대응을 하게 되면, 공격자들은 먼저 돈을 내라고 하거나 은행 계좌에 접속해야 한다고 하여, 돈을 빼갑니다.



가장 좋은 방어책은 상식입니다. 이메일이나 메시지가 이상하거나, 의심스럽거나, 믿기 어려울 정도로 좋은 것이라면, 피싱 공격일 수 있습니다.

대응책

대부분의 경우, 단순히 이메일이나 메시지를 열거나 읽는 것은 안전합니다. 실행되는 공격의 대부분은 우리를 속여서 다른 것을 하도록 하는 것입니다. 하지만 다행히 어떤 메시지가 공격인지 알 수 있는 단서가 있으며, 다음은 가장 일반적인 것입니다.

- 이메일에 나쁜일이 발생하거나, 계좌를 폐쇄하기 전에 “긴급 조치”을 요구하거나 긴박감을 조장하는 이메일. 공격자들은 사람들을 서두르게 해서, 생각 없이 실수하도록 만듭니다.
- 기대하지 않은 첨부문서가 있는 이메일을 받거나, 첨부를 열어보도록 만드는 이메일. 예를 들어 해고, 급여정보 또는 기소되었다고 하는 검찰청 문서 등과 관련된 첨무문서가 있다는 이메일이 있습니다.
- 실명을 사용하지 않고, 이메일에 “고객님께”와 같은 일반적인 호칭을 이용. 대부분의 회사나 친구는 우리 이름을 알고 있습니다.
- 신용카드정보나 패스워드와 같이 굉장히 민감한 정보를 요청하는 이메일.
- 공식 기관에서 보낸 이메일인데, 문법이나 철자에 오류가 있고, @gmail.com, @naver.com 또는 @hotmail.com 와 같은 개인 이메일 주소를 사용.
- 오래되어 보이거나, 공식적이 아닌 것 같은 링크가 있는 이메일. 이 경우 링크위에 마우스를갖다 대 보시기

피싱

바랍니다. 이렇게 하면 클릭했을 때 이동하게 될 목적지가 나타납니다. 이메일에 있는 링크가 팝업된 목적지와 다른 경우에는 클릭하면 안됩니다. 모바일 기기에서는 링크에 손가락을 누르고 있으면 동일한 팝업이 나옵니다. 좀 더 안전한 방법은 이메일에서 URL을 복사해서 브라우저로 복사하거나 정확한 링크를 타이핑해봐도 됩니다.

- 지인으로부터 메시지를 받았으나, 문장이나 어투가 실제의 지인같이 보이지 않습니다. 만약에 의심스러우면, 발신자에게 전화를 해서 확인해야 합니다. 사이버 공격자들이 친구나 회사동료처럼 보이는 이메일을 만드는 것은 쉽습니다.

만약에 피싱 공격과 같은 이메일이나 메시지를 받는다면, 바로 삭제하시기 바랍니다. 상식이 가장 좋은 방어책입니다.

자세히 알아 보기

http://www.securingthehuman.org를 방문해서 OUCH! 뉴스레터를 읽어 보시고, 월간 OUCH! 정보보호지식 뉴스레터를 구독하십시오. 그리고 SANS 정보보호지식 솔루션에 대해서 좀 더 알아보시기 바랍니다.

한글판

본 문서는 한국의 ITL(http://www.itlkorea.kr)에서 번역하였습니다. ITL 은 미국 SANS 연구소의 한국 파트너로서 IT 거버넌스 및 IT 보안 분야의 최신의 지식과, 양질의 교육과 세미나를 진행하는 교육기관입니다. 추가적인 사항은 itl@itlkorea.kr 로 문의해주시기 바랍니다.

참고자료

사회공학:	https://www.securingthehuman.org/ouch/2014#november2014
핵심보안 5단계:	https://www.securingthehuman.org/ouch/2014#october2014
해킹당한 후 대응지침:	https://www.securingthehuman.org/ouch/2014#may2014
온가드 온라인:	https://www.onguardonline.gov/phishing
SANS 일일보안팀:	https://www.sans.org/tip_of_the_day.php

편집위원회 : Bill Wyman, Walt Scrivens, Phil Hoffman, Lance Spitzner, 번역: 진수희(ITL Inc.)