OUCH! | 2018 년 04 월 호

SANS SECURITY AWARENESS

OUCH!

전 국민대상 월간 정보보호 인식제고 뉴스레터

피싱 예방

개요

이메일 및 메시징 서비스(예: 문자, 페이스북, 트위터, 스냅샷)는 통신을 위한 주요한 수단 중 하나입니다. 우리는 매일 업무에 사용할 뿐 아니라, 친구나 가족 간의 연락을 위해서도 이러한 기술을 이용하고 있습니다. 전 세계 너무도 많은 사람들이 이러한 기술에 의존하고 있기 때문에, 사이버 범죄자들이 다른 사람들을 공격하는 데에도 사용되는 주요한 방법 중 하나입니다. 이러한 공격 방법을 피싱이라고 합니다. 피싱이 무엇인지, 그리고 직장이나 집에서 이러한 공격을 찾아 내고 막을 수 는 방법에 대해서 알아봅니다.

피싱이란?

피싱은 이메일이나 메시징 서비스를 사용하여 악의적인 링크를 클릭하거나 패스워드를 공유하거나 감염된 이메일 첨부 파일을 여는 등 사람을 속여서 하지 말아야 할 일을 하도록 하는 것입니다. 공격자는 이러한 메시지를 설득력 게 만들고, 긴급한 일이나 호기심을 자극합니다. 친구들이나 자주 사용하는 신뢰할 수 있는 회사와 같이 자신이 아는 사람이나 누군가에게서 온 것처럼 보이게 합니다. 아니면 은행이나 공공기관의 로고를 포함하거나 이메일 주소를 위조하여 메시지가 합법적인 것처럼 보일 수도 있습니다. 공격자는 이러한 메시지를 수백만 명의 사람들에게 보냅니다. 그들은 누가 속을 지 모릅니다. 더 많은 사람들에게 보내면 더 많은 사람들이 걸려들게됩니다.

보호 방법

대부분 경우에 이메일이나 메시지를 열고 읽는 것이 괜찮습니다. 피싱 공격이 성공하려면 공격자는 우리를 속여 클릭하거나, 전화를 하거나 등 뭔가를 하도록 해야 합니다. 다행히도 이러한 메시지에는 공격이라는 단서가 있습니다. 가장 일반적인 경우는 다음과 같습니다.

- 계정을 폐쇄하겠다고 위협하거나, 감옥에 보내겠다고 위협하는 것과 같이 엄청 긴박한 것, 즉시 뭔가를 행동하도록 요구하는 것. 공격자는 이를 통해 실수를 유도합니다.
- 직장에서 정책이나 절차를 무시하거나 무시하도록 압력을 가합니다.
- 호기심을 자극하거나, 진짜로 믿기에는 너무 좋은 것 (로또에 당첨될 확률은 거의 없습니다.)

- “친애하는 고객님”과 같은 일반적인 인사말 사용. 대부분의 회사 나 친구가 우리의 이름을 알고 있습니다.
- 신용카드 번호나 패스워드 또는 합법적인 발신자가 이미 알고 있어야 하는 민감한 정보를 요청합니다.
- 메시지에는 공식 조직에서 왔지만 문법이나 철자가 틀리거나 @naver.com, @gmail.com과 같은 개인 이메일 주소가 사용되어 있습니다.
- 메시지에는 회사 상사와 같은 공식 이메일에서 왔지만, 누군가의 개인 이메일 계정으로 가는 Reply-To 주소가 있습니다.
- 아는 사람이 메시지를 보냈는데, 어휘나 표현은 그 사람이 작성한 것 같지 않습니다. 이런 경우에는 발신자에게 전화를 걸어서 확인해 볼 필요가 있습니다. 사이버 공격자가 친구나 동료의 이름으로 메시지를 만드는 것은 쉽습니다.

궁극적으로 상식이 최선의 방어책입니다. 이메일 또는 메시지가 이상하거나 의심스럽거나 사실로 보기에 좋지 않은 경우 피싱 공격 일 수 있습니다.

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.

객원 편집자

토니아 더블리는 2011 년부터 수상경력이 있는 정보보호 인식제고 프로그램을 개발하고 운영해 오고 있습니다. 토니아는 www.linkedin.com/in/toniadudley 에서 찾을 수 있습니다.

참고자료

사회공학:	https://www.sans.org/u/Cb1
지인들에게 보안조치 알리기:	https://www.sans.org/u/Cb6
이메일 사용시 주의사항:	https://www.sans.org/u/Cbg
CEO 사기:	https://www.sans.org/u/Cbl
OUCH! 문서:	https://www.sans.org/u/Cbq

특허

 편집위원회: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley | 번역: 진수희 (ITL Inc.)