OUCH! | 2019 년 2 월 호

SANS SECURITY AWARENESS

OUCH!

전 국민대상 월간 정보보호 인식제고 뉴스레터

개인화된 사기

개요

사이버 범죄자들은 사람들을 속이기 위해 새롭고 창조적인 방법을 계속해서 만들어 내고 있습니다. 최근 개인화된 사기인 새로운 유형의 사기가 인기를 얻고 있습니다. 사이버 범죄자는 수백만 명의 사람들에 대한 정보를 찾거나 구매한 다음 이 정보를 사용하여 공격을 개인화합니다. 아래에서는 이러한 사기가 어떻게 동작하는지 보여주고 일반적인 예를 보여줍니다. 이 사기에 대해 더 많이 알수록, 쉽게 찾아 내고 막을 수 있습니다.

동작방법

이메일 사기나 전화사기는 새로운 것이 아니며, 사이버 범죄자들은 오랫동안 사람들을 속이려고 시도해 왔습니다. 예를 들어 "복권 당첨"또는 악명 높은 나이지리아 왕자 사기가 있습니다. 그러나 이러한 전통적인 사기 범죄에서 사이버 범죄자는 누구를 타겟팅하고 있는지 알지 못합니다. 그들은 단순히 일반적인 메시지를 작성하여 수백만 명의 사람들에게 보냅니다. 이 사기는 매우 일반적이어서 탐지가 쉽습니다. 개인화된 사기가 다릅니다. 사이버 범죄자가 먼저 조사하고 각 피해자에 대해 맞춤형 메시지를 만듭니다. 이들은 사람들의 이름, 패스워드, 전화번호 또는 다른 세부 사항이 있는 데이터베이스를 찾거나 구매하여 이를 수행합니다. 이러한 유형의 정보는 해킹된 모든 웹 사이트로 인해 쉽게 사용할 수 있습니다. 또한 소셜 미디어 사이트 및 공개된 정부 기록에서 일반적으로 사용할 수 있습니다. 범죄자들은 자신들이 보유한 정보의 모든 사람을 대상으로 공격합니다.

사이버 범죄자들이 흔히 사용하는 속임수 중 하나는 두려움이나 협박을 이용해서 돈을 지불하도록 하는 것입니다. 공격은 이런 식으로 작동합니다. 이들은 해킹된 웹 사이트에서 얻은 사람들의 로그인 및 패스워드에 대한 정보를 찾거나 구매합니다. 이들은 데이터베이스에 포함된 귀하의 계정 정보를 찾아서 해킹된 웹 사이트에서 사용한 원래 패스워드를 비롯하여 귀하에 관한 개인정보가 담긴 이메일을 보냅니다. 범죄자는 자신의 컴퓨터 또는 기기를 해킹한 사실을 "증명"하기 위해 패스워드를 언급하지만 이는 사실이 아닙니다. 범죄자들은 컴퓨터를 해킹하는 동안 우리가 온라인 포르노를 보았다고 주장합니다. 그 이메일은 귀하가 돈을 지불하지 않으면 귀하의 가족이나 친구 또는 온라인에 난처한 사진이나 동영상을 공유할 것이라고 위협합니다.

하지만 대부분의 상황에서 사이버 범죄자는 시스템을 해킹하지 않았습니다. 그들은 우리가 누구인지 또는 어떤 웹 사이트를 방문했는지조차 알지 못합니다. 사기꾼은 자신의 컴퓨터나 기기를 해킹한 것으로 믿을 수 있는 몇 가지 개인정보를

사용하려고 시도하고 있으며, 돈을 지불하도록 속이는 것입니다. 범죄자들은 전화사기에 대해서도 동일한 기술을 사용할 수 있다는 것을 기억하십시오.

예방방법

이러한 이메일이나 전화는 사기라는 것을 인식해야 합니다. 다른 사람이 귀하에 관한 개인정보를 가지고 있을 때 두려워하는 것은 자연스러운 일입니다. 그러나 발신자가 거짓말하고 있다는 것을 기억하십시오. 이러한 공격은 자동화된 대량 발송 캠페인의 일부이며, 직접적으로 우리를 공격대상으로 삼고 시도하는 것은 아닙니다. 오늘날 사이버 범죄자가 개인정보를 찾거나 구매하는 것이 훨씬 쉬워지고 있으므로 향후 더 많이 더 자주 개인화된 사기를 당할 수 있습니다. 사기라는 것을 알 수 있는 단서는 다음과 같습니다.

- **매우 긴급한 이메일, 메시지 또는 전화를 받는다면, 의심해 보시기 바랍니다. 누군가가 두려움이나 긴박감과 같은 감정을 사용하고 있다면, 당신을 실수로 유도하려고 하는 것입니다.**
- **누군가 비트코인, 기프트 카드 또는 기타 추적할 수 없는 방법으로 지불을 요구할 때**
- **의심스러운 이메일, 전화를 받으면 포털에서 검색하여 다른 사람들이 유사한 공격을 신고했는지 확인하십시오.**

궁극적으로 상식적으로 판단하는 것이 최선의 방어입니다. 그러나 각 온라인 계정에 대해 고유하고 긴 패스워드를 항상 사용하는 것이 좋습니다. 모든 비밀번호를 기억하지 못합니까? 패스워드 관리프로그램 사용하십시오. 또한 가능할 때마다 2 단계 인증을 사용하십시오.

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

레니 젤트서는 사이버보안 베테랑입니다. 미네르바 연구소에서 악성코드 방지 솔루션을 만들고 SANS 연구소의 강사입니다. 레니는 보안 서비스 관리 및 컨설팅 등의 경험이 있습니다. zeltser.com/blog 및 트위터 @lennyzeltser에서 팔로우하십시오.

참고자료

사회공학:	https://www.sans.org/u/MUU
피싱 예방:	https://www.sans.org/u/MUZ
온라인에서 본인 검색하기:	https://www.sans.org/u/MV4
패스워드 관리프로그램:	https://www.sans.org/u/MV9