

번역문서

The Easier Form of Hackig Social Engineering

해당 문서는 연구 목적으로 진행된 번역 프로젝트입니다.

상업적으로 사용을 하거나, 악의적인 목적에 의한 사용을 할 시

발생하는 법적인 책임은 사용자 자신에게 있음을 경고합니다.

원본 : <http://resources.infosecinstitute.com/the-easier-form-of-hacking-social-engineering/>

번역자 : 김연우

편집자 : 조정원



보안프로젝트

kisec

한국정보보호교육센터
Korea Information Security Education Center



내용

1. 상세내역	2
2. 요약	8
2. 끝맺음	9

1. 상세내역

우리가 해킹에 대해 대화를 나눌때면, 보통 미디어에서 해커들이 어떻게 데이터베이스에 들어와 정보를 훔쳐갔다는식의 이야기가 진행된다. 이를테면 이 기사처럼 말이다.

RICHMOND, Va. - 워싱턴 D.C 근처 Fairfax 에 소재한 George Mason University 에서 학생, 스태프 개인정보가 해킹되는일이 발생했다. 관계자에 의하면 유출 정보는 이름, 사회보장번호등이며 이 사건의 피해자수는 3 만명이 넘는다. 대변인 Daniel Walsh 는 지난 1 월 3 명의 침입자가 서버에 보호, 보관중인 정보들을 해킹한 사실을 포착했으며 이 사실을 교내에 공지하고 정보 핫 라인을 개설, 교내 경찰에 사건을 넘겼다고 밝혔다.

“아직 우리는 내부자의 소행인지 외부에서 이루어진 일인지 모릅니다.”

해킹이 일어나기전, 이 대학에서는 작년에 개정된 법에 의해 학생들의 사회보장번호를 내부번호로 바꾸고, 도용가능성이 있는 ID 카드들을 없애는 일을 진행중이었다. 그는 사건 발생후, 당국 서버 일부를 중지하고 보안 지침을 점검중이라고 말했다.

작년에는 Berkeley 에 있는 University of California 에서는 보안 허점을 통해 140 만명의 노인 부양대상자 정보가 유출되었으며 2003 년에는 Georgia Institute of Technology 와 Austin 에 위치한 University of Texas 가 보관하던 정보가 해킹당했다.

전세계적으로 해킹에 대한 소식은 이런식이다. 스텍스넷 Stuxnet 웜이나 플레임 Flame 은 어떤가? 다른 예를 들어 악성코드 공격 시스템이나 정보 탈취, 오작동 유발 등등.. 하지만 사회공학 Social Engineering 이 해킹에 있어 큰 역할을 차지한다는 사실은 아무도 귀를 기울이지 않는다. 이 글에서는 소셜 엔지니어링이 어떻게 해킹을 쉽게 할수있게 해주며 어떻게 방어할수 있는지 짚어볼 것이다.

Stuxnet - 산업시설을 감시하고 파괴하는 최초의 악성 소프트웨어. 코드내에 Stuxnet 키워드가 자주 등장해서 스텍스넷이라 명명되었다. 이란의 핵시설 원심분리기 1000여개의 피해를 입힌것뿐만 아니라 매우 정교하게 만들어진 악성 소프트웨어라는면에서도 화제가 되었다.

자세한 정보는 다음 링크를 참고하자.

<http://ko.wikipedia.org/wiki/%EC%8A%A4%ED%84%B1%EC%8A%A4%EB%84%B7>

좁게는 프로그램 특징부터 넓게는 사이버전쟁까지 여러분들의 시야를 넓혀줄 흥미로운 내용들이 들어있다.

Flame - 이란, 시리아, 사우디아라비아 등 중동국가들의 컴퓨터시스템에 집중적으로 침투, 전자문서를 도용하거나 변경할 수 있는 기능을 갖추고 있는 정보 수집을 목적으로 만들어진 가장 정교

한 형태의 악성 프로그램이다. 일부 모듈이 Stuxnet 과 유사해서 같은 곳에서 개발한게 아니냐는 의혹이 있다. 시만텍에 따르면 이 프로그램을 제작한 해커들이 역추적을 막기위해 최근 수행했던 행위를 모두 삭제하는 '자폭(Self-Destruction)명령'을 수행하고 있다고 한다.

자세한 정보는 다음 링크를 참고하자.

https://www.securelist.com/en/blog/208193522/The_Flame_Questions_and_Answers

최초로 발견한 회사가 카스퍼스키 랩인데, 여기에 근무하는 전문가의 글이다.

- 역자 주

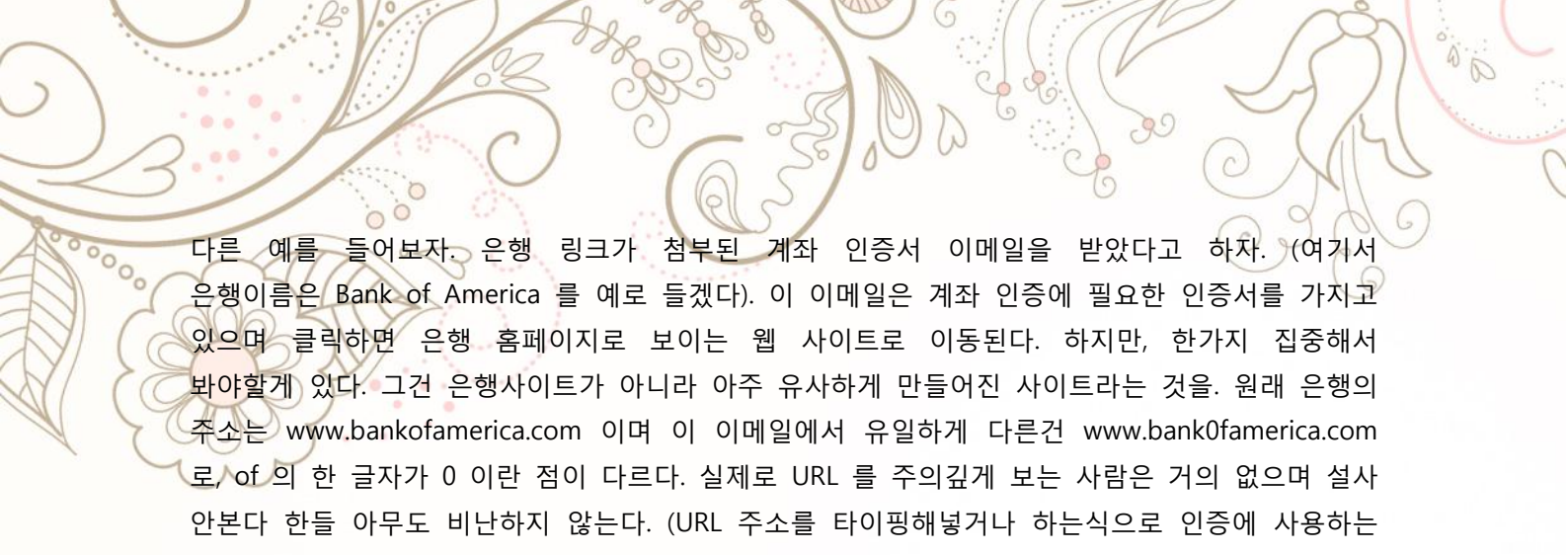
유명한 해커 케빈 미트닉 Kevin Mitnick 의 저서 "Ghost in the Wires" 의 내용을 잠시 보자. 이 책에 나오는 미트닉 Mr.Mitnick 은 사회공학을 유용하게 사용한다. 그는 전화회사에 전화를 걸어 네트워크에 접속하기위해 여러가지 역할을 연기하곤 했다. 그것도 아주 자연스럽게! 아직 미트닉이 어린애일때 버스 운전수에게 천공기 punch 를 어디서 살수있는지 물은적이 있다. 잠시후 그는 방금 구입한 천공기와 쓰레기통안에 다 쓰지 않은 버스환승티켓으로 샌 페르난도 계곡 San Fernando Valley 을 공짜로 돌아다녔다. 이 역시 사회공학인데, 미트닉은 어릴때 이미 뛰어난 사회공학자로서의 면모를 보이고 있었다. 그가 체포되기전까지 얘기지만.

케빈 미트닉의 저서 "Ghost in the Wires" 는 한국에도 "네트워크속의 유령" 이란 제목으로 번역되었다.

- 역자 주

"Ghost in the Wires" 에 따르면 그는 지금 사회공학을 건전하게 회사 침투 테스트에 활용하고 있다고 밝히고 있다. 그런 그가 우리에게 한가지 지적하는게 있다. : 그는 사회 공학이 우리주위에 있는한, 당신은 주변에 대해 살펴보고, 타겟을 주시하며 어떻게 정보를 얻어낼지 궁리할 필요가 있다고 주장한다.

사람들은 그런 일은 나에겐 일어나지 않을것이며 설사 일어난다해도 당하지 않을거라고 자신하는데, 무서운 사실은 우리가 두번 생각할 필요없이 바로 돈을 쓰게 만드는 기술이 점점 정교해지고 있다는 것이다. 예를 들어보자. 한 여성에게서 들은 이야기인데 여기서 셸리라고 부르겠다. 셸리는 손자 랄프라고 하는 사람에게서 전화를 받았는데 지금 브라질의 감옥에 있으며 석방되기 위해 보석금이 필요하다는 전화였다. 셸리는 그 목소리가 마치 랄프 본인 같았다면서 그 계좌번호에 바로 송금하려했다고 했다. 그런데 식료품 가게에서 입금하려하니 담당직원이 아까 두사람이 같은 계좌로 거래하고 갔다며 혹시 그들처럼 사랑하는 사람(가족, 친구등을 말함 - 역자주)을 위해서 거래하려는 거냐고 물어왔다. 셸리는 믿을수 없었다. 그건 마치 랄프의 목소리 그자체였다. 패닉상태가 된 그녀는 아들 벤에게 전화해 혹시 거기에 랄프가 있냐고 물어보았다. "네 어머니, 랄프는 지금 제 옆에 있어요." 그제서야 셸리는 안심했지만 신용사기에 걸릴뻔했다는걸 아직도 믿을 수 없었다.



다른 예를 들어보자. 은행 링크가 첨부된 계좌 인증서 이메일을 받았다고 하자. (여기서 은행이름은 Bank of America 를 예로 들겠다). 이 이메일은 계좌 인증에 필요한 인증서를 가지고 있으며 클릭하면 은행 홈페이지로 보이는 웹 사이트로 이동된다. 하지만, 한가지 집중해서 봐야할게 있다. 그건 은행사이트가 아니라 아주 유사하게 만들어진 사이트라는 것을. 원래 은행의 주소는 www.bankofamerica.com 이며 이 이메일에서 유일하게 다른건 www.bank0famerica.com 로, of 의 한 글자가 0 이란 점이 다르다. 실제로 URL 를 주의깊게 보는 사람은 거의 없으며 설사 안본다 한들 아무도 비난하지 않는다. (URL 주소를 타이핑해넣거나 하는식으로 인증에 사용하는 경우라면 예외겠지만 이런 사례는 없을것이다.)

어떤회사의 직원들은 꼭 사원증을 패용해야한다. 만약 닫힌 문 뒤에 기밀이 있다면 PIN(personal identification number)이 필요할 것이다. 사회공학자는 이런 상황이라면 꼭 누군가 문 너머에 있기 마련인걸 알고있다. 우선 인내심 있게 기다린후, 누군가가 들어가려할때 다가가서는 “안녕하세요, 저는 제인 도 Jane Doe 이고 샘 스미스 Sam Smith 씨와 업무중입니다. 하지만 오늘은 사원증을 안가져왔네요. 이번만 봐주면 안될까요? 한번만입니다.” 나는 대부분의 사람들이 도와주겠다는 생각이 앞서 별생각없이 들여보내주는걸 보아왔다. 심지어 샘 스미스가 제인을 아는지 알아보지도 않는다... 그들은 실수한거다.

물론 현명한 사람이라면 아무리 업무때문이라고 해도 별말 없이 통과시켜주진 않을것이다. 하지만 사원증을 걸은채, “샘 스미스씨를 찾게 해주십시오. 그가 어디에 있는지 압니다. 그와 함께 돌아오도록 하겠습니다.” 이 경우는 제인 도가 두번 생각한 경우다. 단순히 통과하는것뿐만 아니라 샘 스미스가 그녀가 누군지 의아해하며 문쪽으로 왔을때 그곳에 계속 있을 필요도 없다.

또 다른 예로 미트닉이 자신의 저서에서 소개한 사원증 활용 사례가 있다. 그는 침투 테스트를 위해 인터넷의 회사 웹사이트에서 로고를 복사해 사원증과 비슷하게 만들어 착용했다. 이 가짜 사원증을 가지고 뒷문에서 담배피는 사람들이 회사로 돌아갈때 맨 마지막 사람과 같이 자연스럽게 들어갔다. 경비원이 그의 사원증을 유심히 보지않아서 가능했던일인데, 만약 주의깊게 봤다면 들어가지도 못했을것이다.

회사에 들어갈때 사회공학자들에게 좋은 방법중 하나는 USB 메모리를 이용하는 것이다. 나는 한 사람이 회사 출입정보를 얻기 위해 USB 메모리를 주차장 곳곳에 뿌렸다는 이야기를 들었다. 왜일까? 순진한 회사원은 안에 뭐가 들었는지 주인은 누구인지 궁금해 하면서 주워들 것이다. 그리고 그들은 회사 컴퓨터에 꼽고...짜잔.. 악성코드님이 로그인하셨습니다. 만약 HIDS 나 HIPS 등 안티바이러스 탐지시스템 하나 없다면, 컴퓨터 하나로 끝나지 않는다. 아예 사내 네트워크 전체를 가질수 있게 된다! 만약 이런일이 일어난다면, 최소한 보안 담당자에게 장치를 넘기고 무얼 했는지 보고해야한다.

HIDS - Hostbased Intrusion Detection System 침입감지 시스템.

HIPS - Hostbased Intrusion Prevention System 침입방지 시스템.

HIDS는 네트워크 활동 감시에 특화되어있다.

HIPS는 시스템 내의 이벤트를 감시하며 주로 윈도우 OS 에 쓰인다.

자세한 정보는 영문 위키에 정리되어있다.

http://en.wikipedia.org/wiki/Intrusion_prevention_system

http://en.wikipedia.org/wiki/Intrusion_detection_system

- 역자 주

사회공학자들은 페이스북 같은 소셜미디어에서부터 가끔 선물을 받는다. 사람들은 자신의 페이스북이 보다 많은 사람들에게 보여지는걸 좋아한다... "이번주에 엄마에게 갈게요! 오늘 밤에 봐요!" 이렇게 사생활을 쓰기도 하는데 덕분에 그들이 언제 나가거나 어디로 떠나는지 물어볼 필요가 없다. 이미 위에 다 적혀있으니까. 이건 그 집을 몰래 들어가 탐색하기 딱 좋은 기회 된다. 한가지 더 알아둘게 있다면 대부분의 사람들은 페이스북 계정을 잠궜두지 않는다. 그러므로 사회공학자는 친구에, 친구에 친구등등까지 다 보면서 타겟을 고를수 있다. 한 회사의 CEO 같은 사람의 신상정보를 알고 싶다면 구글같은 검색엔진을 사용하자. (대상이 아직 페이스북 프로필이 없을때.) 그들의 취미나 관심사를 찾아라. 그리고 잠재되어있는 그들의 신분을 훔쳐라.

누구도 돈을 얻기위해서 이렇게 긴 과정을 거치지 않을거라 생각하는 사람이 많은데, 이게 얼마나 쉬운일인지 알게 되면 놀랄것이다.

정보를 훔치는 7단계 과정

신분 도용 피해는 뒷정리만 짧게는 몇달, 길게는 몇년에 걸쳐 고생하는 짜증나는 일이다.. 이 이야기는 내가 실제로 들은 이야기이다. 나의 친한 친구가 한순간에 범죄 피해자가 되었고, 더욱 소름끼치는 사실은 그 도둑이 일을 시작하기위해 필요했던것은 이메일 패스워드 리셋뿐이었다는 것이다. 다행히 그 친구는 이메일에 간단한 패스워드를 사용하지않았던 덕분에 아직 신원 도용이 성공하진 못했다. 당신의 암호와 보안질문을 만들때 다른 계정과 똑같이 만들어선 안된다.

보안 질문에는 일부러 오답으로 쓰라. 이 오답 역시 확실하지 않은 정보로 써야한다. 예를 들어 자신의 부모님 이름을 물을때 자신이 몰래 좋아하는 연예인 이름을 거꾸로 뒤집어 쓰거나 하는 식이다. 부모님 정보 같은건 약간 조사하면 누구나 알수있다. 아마 당신은 여러계정에 대한 정보를 메모해야할것이다. - 다 기억하는건 힘들니까 - 하지만 약간의 불편이 신원 도용이라는 끔찍한 악몽을 막아줄 것이다.

헐버트 톰슨은 괴짜로 사는걸 좋아하는 학원 소프트웨어 개발자다. 그는 조금 아는사이인 몇몇의 사람들의 신원을 훔쳤다. 그는 간단한 7단계 과정으로 은행 계좌를 훔쳤다. 아무런 프로그래밍 속임수도 쓰지 않았으며 오직 약간 탐정같은 일을 했을뿐이다. 한번의 실험과 몇몇 사람과는 간신히 아는정도인 상황에서 톰슨은 얼마나 다른사람의 정보와 은행 정보를 아는지 쉽다는 것을 보여주었다.그의 실험은 자유롭게 얻을수 있는 돌아다니는 약간의 개인정보만 필요했었다. 이 과정은 우리가 얼마나 보안결함에 노출되어있는지 보여준다.

피해자 : 톰슨은 그녀의 이름을 김이라고 알고 있으며, 어디서 사는지, 어디에 일하는지 그녀의 나이는 대충 몇인지 알고 있다. 그녀의 은행과 그녀의 유저네임(ID?)도 알고있다. 그가 말하길, 그녀의 유저네임을 추측하는건 아주 쉬웠다고 했다. 그녀의 이니셜과 이름으로 되어있었기 때문에.

정보를 훔치는 7단계 과정

- 1) 구글에서 블로그나 이력서를 검색한다. 그는 그녀의 블로그를 금광이라고 불렀다. 금같이 탐스러운 정보가 많이 있었기 때문이다.
- 2) 그는 그녀의 은행 웹 사이트의 비밀번호 리셋을 활용했다. 하지만 은행은 비밀번호 리셋 링크를 그녀의 이메일로 보냈다. 다음엔 그녀의 지메일 계정에 들어가야 할 차례다.
- 3) 그는 지메일 비밀번호 스워드 리셋을 시도했다. 하지만 지메일 역시 리셋 링크를 그녀의 대학교 이메일 주소로 보냈다. 지메일은 그가 이미 조사해둔 이메일 주소로 메일을 보냈음을 안내했다.
- 4) 톰슨이 대학 이메일 계정페이지에서 패스워드 분실 링크를 클릭하니 몇가지 질문이 나왔다. 집 주소, 우편번호, 국가? 걱정마시라. 그건 모두다 그녀의 이력서에 있었으니까. 다만 그녀의 생일이 뭔지 물어볼때는 벽을 칠수밖에 없었다. 나이는 대충 알고 있었지만 정확한 생일은 모르고 있었으니까.
- 5) 폭력 관련 법정 출두 기록을 살펴보니 그녀의 이름이 있었다. (페이스북 역시 쉽게 정보를 얻을수 있게 해준다. 만약 사람들이 그들의 생일을 적지 않았다면.. 톰슨은 그저 그녀의 나이가 어느정도였는지 대충 알고만 있었다는걸 기억하라.) 톰슨은 모터 차량 부서에서 마무리지었다.
- 6) 도로 그 블로그로 돌아가 birthday로 검색해보았다. 생일은 알아냈는데 출생년도는 알수 없었다.
- 7) 마지막으로 톰슨은 그 대학교에서 비밀번호 리셋을 다시 시도했다. 생일을 써넣고, 년도를 추측해서 써넣었다. 물론 그건 틀렸지만 사이트는 5번의 기회를 주었다. 나이대를 짐작해서 계속 넣은결과, 5번내로 그녀의 대학 이름을 바꿀수 있었다. 이제 gmail 패스워드를 리셋할 차례다. 구글은 약간의 개인정보를 필요로 하는데, 이걸 그녀의 블로그에서 쉽게 얻을수 잇는 것이었다. 아버지의 중간 이름도. 톰슨은 지메일 패스워드를 바꿨고 은행 계정 리셋 패스워드 이메일을 볼수있었다.

다시 개인정보를 물어보긴 했지만 그는 더이상 kim의 블로그에서 가져올게 없었다. 애완동물 이름, 폰 번호 등.. 그는 은행 계정 암호를 리셋한후 즉시 그녀의 기록과 돈을 다 얻었다.

톰슨으로부터 :

이 글에서 이해한대로 Kim은 곤경에 처했다. 그녀의 디지털 신원은 대학 이메일 계정에 불안정하게 방치되어있었다. 한번 액세스 한걸로 보안벽들이 도미노처럼 뚫려나갔다. Kim의 사례는 아주 흔한 일이다. 우리들에게 있어 풍부한 개인정보를 가지고 보통 많이 쓰는 패스워드를 보내 이메일을 리셋하는건 우리의 온라인 보안이 불안하게 방치되어있음을 말해준다.

위 개인정보는 그녀의 블로그에서 얻었다. 하지만 페이스북 페이지나 다른 온라인 커뮤니티 페이지에서도 얻을수 있다.톰슨은 과학적인 미국인들에게 조언하고 있다. 스스로 실험해보라. 당신의 패스워드를 리셋할때 나오는 질문들이 당신의 신원을 확인해주는지 말이다. 몇몇 질문들은 다른거보단 낫지만 당신의 생일을 물어보는건 최악이다. 그건 온라인의 재산 기록에도 있으며 당신이 어디에서 태어났는지까지도 추적할수있다.

계정이 리셋될땐 대부분 당신에게 질문을 선택하게 하거나 방법을 고르게 한다. 잘 알려져있지 않은 것이나 당신이 절대 잊어버리지 않을(또는 작게 유추할수있는), 자주 타는 비행기 번호등. 쉽게 추측이 가능한 질문

은 피해라.

한가지 중요한걸 기억해야할것은 데이터를 한번 온라인에 넣었을때 나중에 그걸 지우기는 거의 불가능하다는 것이다. 블로그에서 자신에 대해 프로필을 쓰거나 더 자세히 소셜네트워킹 프로필에 쓰거나 하면 그 정보들은 즉시 압축되고, 복사되고, 백업되며 분석된다. 먼저 생각하고 나중에 글을 쓰라.

Read story@ smartplane

위 글에서 얻을수 있는 교훈은, 주말에 떠난다는 사실을 누구에게도 말하지 말라는 것이다.(또는 언제든지 간에) 당신의 포스트를 친구들만 볼수있게 계정을 잠궜두고 그 친구들 역시 계정을 잠궜두길 권한다. 다른 방법으로는 특정 컴퓨터에서만 액세스할수있게 지정하는것이다.

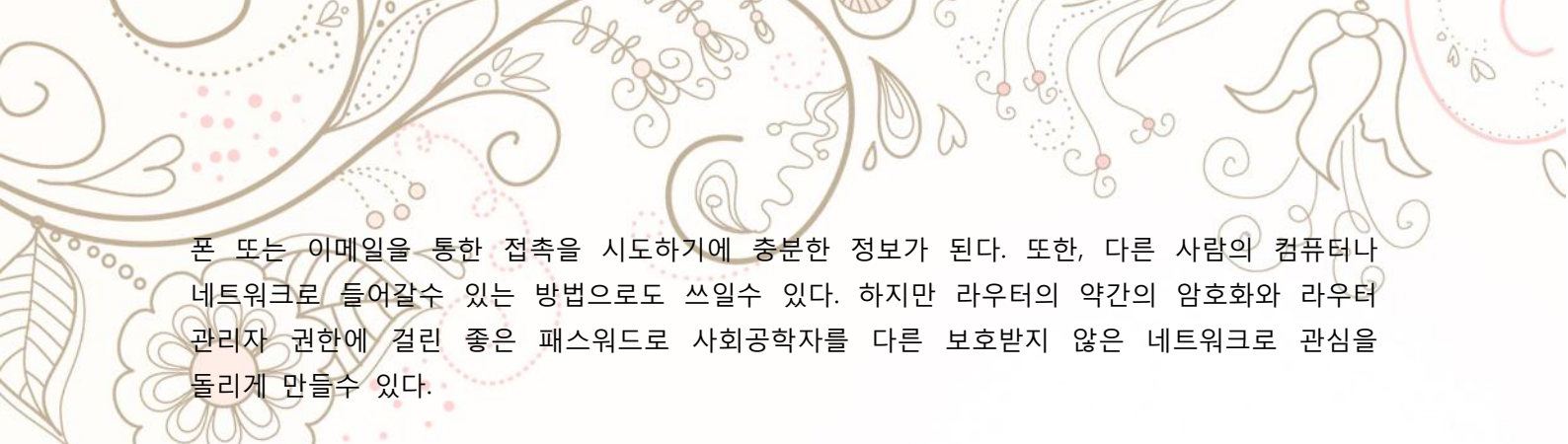
(페이스북 계정 세팅에서 보안부분을 누르면 볼수 있다.) 만약 해커가 당신의 자격을 얻는다면, 그들은 어디서든 언제나 당신의 계정에 로그인할수 있게 된다. 만약 한 유저가 왼쪽의 홈버튼을 클릭하고 help 를 클릭한다면 페이스북은 계정 세팅에 있는 보안과 개인설정에 있어 유용한 정보들을 제공할 것이다.

예전에 나는 실제로 사회공학 사례를 경험한적이 있다. 나는 Craigslist 라는 사이트에서 물건을 팔면서 사진을 같이 올려놓은적이 있는데 사람들이 흥미를 가지고 이메일을 보내주면 전화번호를 보내줄 생각이었다. 물건을 한 2 주간 올려놓았는데 연락 하나 오지 않다가 마침내 내 물건에 흥미를 보이는 한사람이 연락해왔다. 그래서 나는 물건에 대해 이야기해보자며 폰 번호를 알려주었다. 답변은 이러했다. 캘리포니아(아마도) 로 보내는 것에 한정한 거였다며 돈을 보내면 물건을 받는... 그래, 아무일도 일어나지 않았다. 난 답변하지 않았고 우연히 그 물건에 흥미를 가진 다른사람에게도 그래버렸다.(맙소사)

내가 마주친 다른 사회공학 사례로는 조그만 마을에서였다. 나는 호텔에 이틀간 머무르고 있었으며 바로 가서 어른들의 음료를 마셨다. 나는 음료를 현금으로 지불했고 내방으로 돌아갔다. 체크아웃하기전, 여행 바우처를 작성하면서 호텔 영수증을 보니 호텔 바에서 \$20 을 쓴것으로 나와있었다. 황당한 기분에 사람을 불러 이 상황에 대해 설명해보라고 하자 그들은 실수가 있었다며 이 비용은 다른 방에 있는 고객의 것이라고 했다.

같은 호텔에 묵고있던 동료에게 이 일을 설명하니 "오, 이런. 그 바에서는 네 방번호만 말하면 되는데. 그럼 그들이 방에다 계산서를 날릴거야" 그렇다. 만약 내가 사회공학자였다면 나는 누군가가 방에 들어가는것을 확인, 음료수를 마신후에 그 방에다가 계산하게 만들것이다. 바텐더가 뭔가 확인하거나 방번호를 물어보기전에 내가 얼마나 멀리 갈지 누가 알수 있을까?

여러 네트워크를 사회공학적으로 이해한다는 것은 와이어샹크처럼 특화된 어플리케이션으로 누군가의 무선 활동을 모니터링하는것과 같다. 웹사이트에 사람들이 방문하고 그들이 주고받는 암호화되지 않은 정보인 그들의 관심사, 취미들을 지켜본다. 이것은 사회공학자들이 스팸메일이나



폰 또는 이메일을 통한 접촉을 시도하기에 충분한 정보가 된다. 또한, 다른 사람의 컴퓨터나 네트워크로 들어갈수 있는 방법으로도 쓰일수 있다. 하지만 라우터의 약간의 암호화와 라우터 관리자 권한에 걸린 좋은 패스워드로 사회공학자를 다른 보호받지 않은 네트워크로 관심을 돌리게 만들수 있다.

마지막으로 Ira Winkler 의 책 "Spies Among Us"에 있는 사회공학 사례를 알아보자. Mr.Winkler 와 그의 어시스턴스는 핵 발전소 침투 테스트를 위해 고용되었다. Mr.Winkler 와 그의 어시스턴스는 프론트 데스크에서 아무런 인증이나 서류 작성 없이 본사 배지를 얻었다. 그리고 그들은 원자로 시설을 돌아다니면서 그중 한곳에서 네트워크에 접속한후 몇십억의 가치에 달하는 핵 정보와 서버 이름을 약간의 사회공학으로 얻을수 있었다.

2. 요약

사회공학에는 옷을 입거나 회사 직원처럼 이야기하는걸 포함한 많은 기법이 있다. 모든 노동자들은 자산을 입발림, 감정을 자극하는 행동, 또는 액세스 또는 정보 열람시 시간을 엄격히 지켜야할 필요가 없다는 생각등에서 어떻게 회사의 자산을 보호해야하는지 교육받아야한다. 특히 빠르게 돌아가는 세상에 살고있는한 더욱 그렇다. 하지만 주의하면서 누군지 전화를 통해 물어보는 것만으로도 충분하다.

"Mr. Doe 를 뵙길 원하십니까? 누가 찾는지 전해드릴테니 번호를 남겨주겠습니까?" 이런 질문은 사회공학 공격을 막고 다른 곳으로 타겟을 돌리게 할수있다.

관련된 콘텐츠

- [can i go to jail for social engineering](#)
- [social engineer the PIN](#)
- [social engineering bus tickets](#)
- [social engineering database](#)
- [social engineering examples obtaining products free](#)
- [social engineering examples presentation](#)
- [social engineering phone calls example doctor database](#)
- [social engineering stories](#)
- [social engineering telephone operator](#)
- [social hacker networks target women](#)
-

저자에 관하여



Stuart Gentry 는 Infosec 학회 회원이자 컴퓨터 보안의 열정적인 연구자이며 GSEC 및 GCIH 정보보증 석사학위 보유자이다. 1984년에 해킹에 입문, 2011년 9월까지 리버스 엔지니어링과 멀웨어 연구를 하였다. Stuart는 언제나 새로운 코딩 언어 및 익스플로잇 방법을 찾아 연구하고 있다.

연락은 gentry_s1@yahoo.com, www.linkedin.com/in/stuartgentry 를 이용하라.

2. 끝맺음

<http://resources.infosecinstitute.com/> 사이트에서는 다양한 해킹 공격 시연 문서 및 방어들이 정기적으로 배포되고 있습니다. 입문자들 대상으로 설명한 문서들이 많아서 연구 목적으로 번역을 시작하였습니다. 앞으로도 좋은 콘텐츠에 대해서는 정기적으로 번역을 해서 배포하도록 하겠습니다.

또한 꾸준히 활동하는 멤버들에게 번역출판의 기회를 드리고 있습니다. 번역에 참여해주신 멤버들에게 감사합니다.