1.

사회공학(Social Engineering)의 사전적 정의는 '컴퓨터 보안에서 인간 상호 작용의 깊은 신뢰를 바탕으로 사람들을 속여, 정상 보안 절차를 깨뜨리고 비기술적인 수단으로 정보를 얻는 행위'이다.

사회공학은 조직의 특성에 따라 보안에 큰 문제를 야기하기도 하는데 주변을 살펴보면 조직의 구성원에 의해 정보가 상당히 쉽게 유출되는 모습을 볼 수 있다. 일례로 정보를 얻기 위해 "혹시 OO 에 아는 사람 있어?"라고 묻는 것도 사회공학을 이용한 사례에 해당한다.

2.

사회공학해킹은 개인 및 심리 상태 등의 정보를 빼내는 것을 말한다. 1990년대 미국 국방부에 침투하며 유명해진 해커인 케빈 미트닉이 이런 행위를 '사회공학'이라고 부르면서 특정 해킹 기법을 가리키는 용어로 자리잡았다. 사회공학적 해킹의 예로는 공공기관 또는 지인을 사칭해 개인 정보를 요구하는 '피싱(phishing)'을 들 수 있다. 배송 내역이나 입사지원서, 논문 등으로 악성파일을 위장하는 것도 비슷한 범주에 넣을 수 있다.

3.

■ 정보의 가치를 잘 모르는 사람

응접계원이나 청소부처럼 업무와 직접적인 관련이 없는 사람들은 친절하게 물어보면 순순히 정보를 알려줄 수 있다.

■ 특별한 권한을 가진 사람

IT 헬프 데스크 직원처럼 업무용 그룹웨어에서 직원들의 패스워드를 변경하거나 업무에 관련된 정보에 접근하기 쉬운 경우이다. IT 헬프 데스크에 전화를 걸어 자신의 패스워드로 로그인이 안 된다고 하면, 신상정보만으로도 패스워드를 재설정할 수 있다. 이렇게 공격 대상의 패스워드를 바꾸면 그 사람의 아이디로 그룹웨어 등에 로그인할 수 있다.

■ 제조사, 벤더

공격할 회사에 시스템 등을 제공하거나 유지·보수를 해주는 업체이다. 이런 업체는 회사에 대한 정보를 많이 알고 있고, 해당 시스템에 대한 접근 권한과 유지·보수용 계정을 확보하고 있는 경우가 많아 클라이언트로 가장하여 정보를 획득할 수 있다.

■ 해당 조직에 새로 들어온 사람

일반적으로 조직에 처음 발을 들여놓으면 새로운 사람들과 규칙에 낯설어 새로운 환경에 적응하려고 경계심을 푼다. 이런 사람들에게 회사 내부의 지원자(즉 인사과 직원이나 IT 헬프 데스크 직원)로 가장하면 신상 정보나 시스템에 대한 접근 정보를 얻을 수 있다.