# 1 SNS 보안 위협

## 1 이블 트윈 어택(Evil twin attack)

- 사용자를 속이는 소셜 엔지니어링 공격 기법(사회 공학)
- 와이파이 무선 네트워크에서 공격자가 Rogue AP (가짜 액세스 포인터)로 사용자 정보를 중간에서 가로채어 사용자인 것처럼 행동하는 공격에서 나온 것(Rogue AP)
- 이블 트윈 공격을 통해 공격자는 소셜 네트워크에서 다른 사람의 이름으로 활동할 수 있음(가짜 페이스북 ID)

## 1 이블 트윈 어택(Evil twin attack)

[페이스북 가입화면]


※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

## 1 이블 트윈 어택(Evil twin attack)

[다른 이메일 주소로 같은 정보를 가진
두 개의 페이스북 계정으로 만든 경우]


※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

## 1 이블 트윈 어택(Evil twin attack)

- 단순히 재미로 그치는 경우가 대부분이지만
  금전적인 목적이나 명예 훼손, 주가 훼손, 사이버 폭력
  등의 악의적인 목적을 가지고 행하는 경우도 있음

- 현재 시스템적으로 막을 수 있는 방법은 없음
  (수업 시간에 활용)

## 1 이블 트윈 어택(Evil twin attack)

[유명인의 이름으로 만들어진 가짜 페이스북]


※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

## 2 이블 트윈

- 이블 트윈(Evil Twin→악의적 쌍둥이)은
  로그인 한 사람들을 속이고 비밀번호나
  신용카드 번호를 훔치기 위해 합법적인
  네트워크인 것처럼 가장한 무선 네트워크를 가리킴

- 이블 트윈은 피싱 사기의 무선 버전임

  공격자는 합법적인 제공자처럼 행세하며
  노트북이나 휴대 전화로 핫스팟에 연결한
  무선 사용자들을 갖고 놈(인터넷 - 가짜 AP - 사용자)

## 2 이블 트윈

- 무선 장치들은 근처에 연결할 수 있는 핫스팟을 통해 인터넷에 연결 함, 하지만 이런 핫스팟들은 해커들에게는 먹잇감이 될 수 있음, 충분한 장비를 갖춘 사람은 핫스팟을 찾아 그것 대신에 자신의 '이블 트윈'을 대체시킬 수 있음

- 이러한 종류의 이블 트윈 공격은 해커에 의해 통신 링크를 스누핑(스니핑)하거나 사람들을 선동하여 사기성 웹사이트로 들어가도록 피싱을 함으로써 의심하지 않고 사용하는 사용자들의 암호를 훔치는데 사용될 수 있음(인터넷 - 가짜 AP - 사용자)

## 2 이블 트윈

- 공격자는 누군가가 Wi-Fi 무선 기술을 사용하여 연결한 가짜 베이스 스테이션을 사용함(가짜 AP)
- 또, 합법적인 무선 서비스 공급자의 이름을 모방함으로써, 그들이 제공하는 인터넷 서비스를 사람들이 신뢰하도록 속일 수 있음
- 사용자들이 은행이나 전자 메일 계정에 로그인 할 때, 그 정보들은 공격자의 장비를 통해 전송되기 때문에 공격자는 모든 트랜잭션에 접근할 수 있음(트랜잭션)

## 2 이블 트윈

- 실제로는 공인되지 않은 무선 접속 장치(Access Point)이면서도 공인된 무선 접속 장치인 것처럼 가장하여 접속한 사용자들의 신상 정보를 가로채는 인터넷 해킹 수법 임(가짜 AP)

- 미국에서 진짜 와이파이(Wi-Fi)망을 복사한 가짜 망을 만들어, 접속한 사용자들의 신상 정보를 빼내 가는 해커 수법이 발견된 이후 붙여진 이름 임

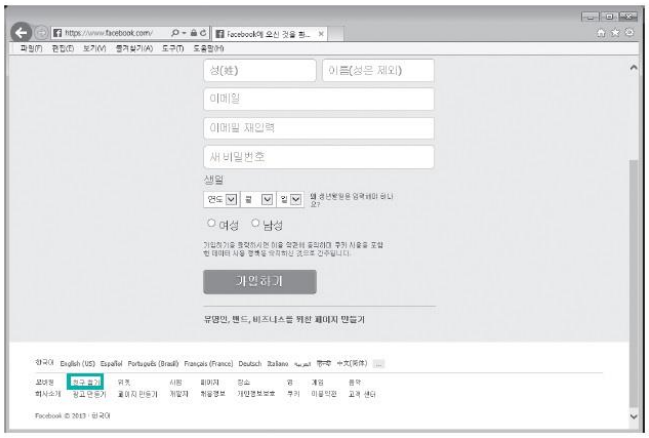
## 2 이블 트윈

- 대응책으로는 와이파이망 이용 시 망의 진위 여부를 확인하고, 접속 후에도 자신의 사용자 보안 설정 및 장치의 보안 설정이 알맞게 맞추어졌는지를 확인하며, 개인 방화벽을 설정하여 인증 받은 이용자만이 데이터에 액세스할 수 있도록 해야 함 (암호화, 개인 방화벽)

## 3 소셜 네트워크 사이트에서 위장 계정 확인하기

### 1 친구찾기

- 페이스북 사이트에 접속하여 [친구 찾기] 클릭



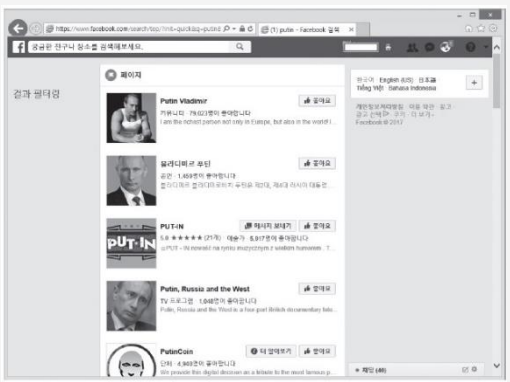

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

## 3 소셜 네트워크 사이트에서 위장 계정 확인하기

### 2 유명인 검색

- 친구 찾기에서 유명인의 이름 검색
- 최근 페이스북은 페이스북에서 인증한 페이지라는 표시를 해주기도 함

[푸틴의 페이스북 리스트]




※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

## 3 소셜 네트워크 사이트에서 위장 계정 확인하기

### 2 유명인 검색

- 친구 찾기에서 유명인의 이름 검색
- 최근 페이스북은 페이스북에서 인증한 페이지라는 표시를 해주기도 함

**[푸틴의 페이스북 화면]**


※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

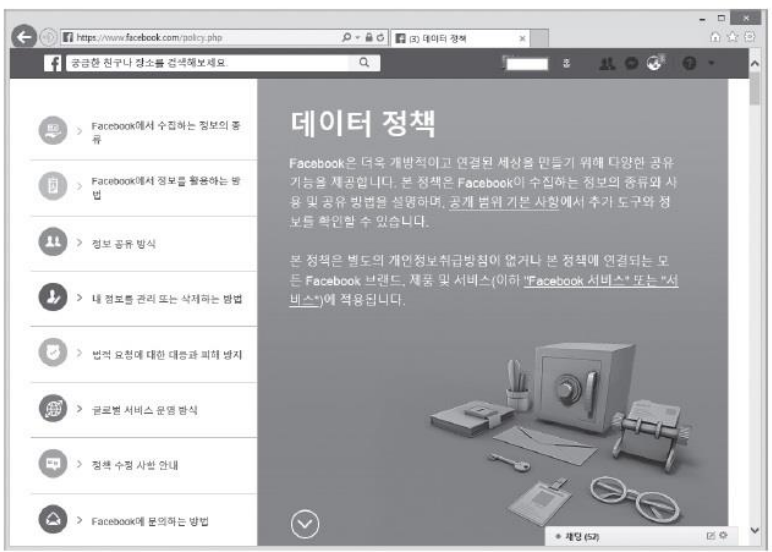
## 4 대응 방안

- 사용 중인 SNS의 정책 살펴보기
  - 페이스북의 개인 정보 취급 방침 정보
  - http://www.facebook.com/policy.php
  - 게시물을 올릴 때 잠금 아이콘을 활용해 게시물을 볼 수 있는 범위를 지정하도록 권고
  - 프로필이나 계정에서 삭제한 정보도 개인 정보 설정에 따라 배포되었거나 다른 사용자가 복사 또는 저장했다면 내용이 그대로 남음

## 4 대응 방안

- 사용 중인 SNS의 정책 살펴보기(공개 범위 기본 사항)

[페이스북의 개인 정보 취급 정책 중 정보 공유 부분]

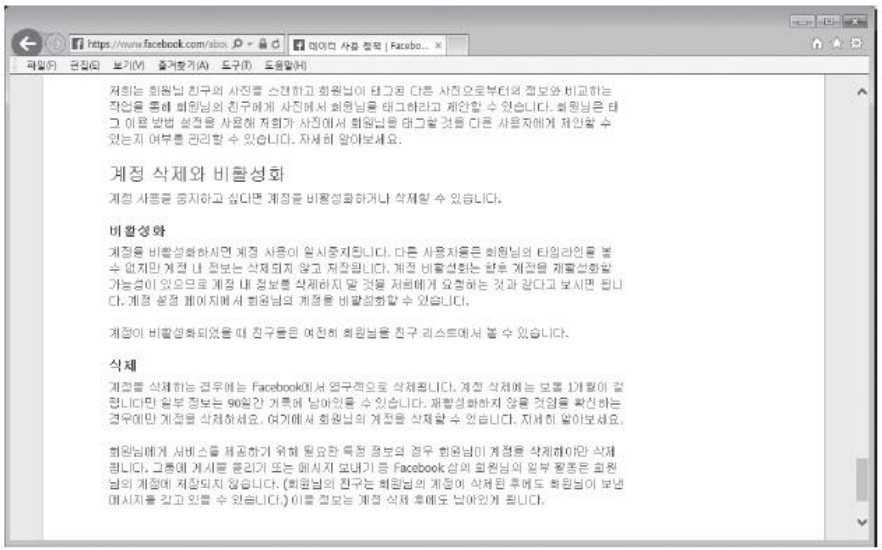



※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

## 4 대응 방안

- 사용 중인 SNS의 정책 살펴보기(계정 삭제와 비활성화)

[페이스북의 데이터 정책 중 계정 부분(2013년 기준)]



저희는 회원님 친구의 사진을 스캔하고 회원님이 태그된 다른 사진으로부터의 정보와 비교하는 작업을 통해 회원님의 친구에게 사진에서 회원님을 태그하라고 제안할 수 있습니다. 회원님은 태그 이용 방법 설정을 사용해 저희가 사진에서 회원님을 태그할 것을 다른 사용자에게 제안할 수 있는지 여부를 관리할 수 있습니다. 자세히 알아보세요.

### 계정 삭제와 비활성화

계정 사용을 중지하고 싶다면 계정을 비활성화하거나 삭제할 수 있습니다.

**비활성화**

계정을 비활성화하시면 계정 사용이 일시중지됩니다. 다른 사용자들은 회원님의 타임라인을 볼 수 없지만 계정 내 정보는 삭제되지 않고 저장됩니다. 계정 비활성화는 향후 계정을 재활성화할 가능성이 있으므로 계정 내 정보를 삭제하지 말 것을 저희에게 요청하는 것과 같다고 보시면 됩니다. 계정 설정 페이지에서 회원님의 계정을 비활성화할 수 있습니다.

계정이 비활성화되었을 때 친구들은 여전히 회원님을 친구 리스트에서 볼 수 있습니다.

**삭제**

계정을 삭제하는 경우에는 Facebook에서 영구적으로 삭제됩니다. 계정 삭제에는 보통 1개월이 걸립니다만 일부 정보는 90일간 기록에 남아있을 수 있습니다. 재활성화하지 않을 것임을 확신하는 경우에만 계정을 삭제하세요. 여기에서 회원님의 계정을 삭제할 수 있습니다. 자세히 알아보세요.

회원님에게 서비스를 제공하기 위해 필요한 특정 정보의 경우 회원님이 계정을 삭제해야만 삭제됩니다. 그룹에 게시물 올리기 또는 메시지 보내기 등 Facebook 상의 회원님의 일부 활동은 회원님의 계정에 저장되지 않습니다. (회원님의 친구는 회원님의 계정이 삭제된 후에도 회원님이 보낸 메시지를 갖고 있을 수 있습니다.) 이로 인해 계정 삭제 후에도 남아있게 됩니다.

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

## 4 대응 방안

- 기본 설정에서 개인 정보 유출 위험 확인하기
  - 2011년에는 페이스북을 이용하는 사람들의 개인 정보 중 일부가 '모든 사람'에게 공개

[2011년 페이스북 개인 정보 설정 관리 부분 (페이스북 권장 설정)]


※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

## 4 대응 방안

- 기본 설정에서 개인 정보 유출 위험 확인하기
  - 2013년부터 타임라인의 콘텐츠를 볼 수 있는 사람을 '친구의 친구'로 한 단계 낮춤
  - 2017년에는 게시물, 게시물 삭제, 프로필, 친구 리스트, 타임라인 등 세부적으로 공개 범위를 설정할 수 있게 변경(공개의 위험성 - 실제 사례?)

## 4 대응 방안

- 기본 설정에서 개인 정보 유출 위험 확인하기

[2013년의 페이스북 개인 정보 설정 관리 부분 (페이스북 권장 설정)]


※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

## 4 대응 방안

- 기본 설정에서 개인 정보 유출 위험 확인하기

[2017년의 페이스북 개인 정보 공개 범위 설정 관리 부분]


※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

## 4 대응 방안

- SNS로 공유되는 정보 파악하기
  - 글을 쓸 때는 개인 정보 노출 위험이나 악용될 여지가 없는지 항상 주의를 기울임 (취업에도 영향을 미침)

## 4 대응 방안

- 기업의 이블 트윈 어택 방지 방법
  - 업무에 필요한 것이 아니라면
    회사에서는 가급적 SNS를 사용하지 않도록 함
  - 임직원을 대상으로 이블 트윈 어택의 위험과
    그로 인한 피해, 예방 방법 등에 대한 교육을 실시
  - 기업이나 직원을 사칭한 이블 트윈 계정이 있는지
    수시로 검색함, 특히 경영진의 이블 트윈 계정이
    있는지 찾아보는 것이 중요(사회 공학)

# 2 신원 도용 및 사이버 폭력

# 2 | 신원 도용 및 사이버 폭력

## 1 신원 도용(Identify theft)

- 미국 연방거래위원회(FTC)
  : '허가 없이 타인의 신원 정보를 이용하여
  이미 이루어졌거나 시도된 사기 행위'로 정의

- SNS의 비약적인 확산에 따라
  공격자가 공격 대상의 '알고 있는 것'을
  획득하는 과정이 전보다 훨씬 쉬워짐
  (공개된 정보를 이용)

## 1 신원 도용(Identify theft)

- 신분 위장 절도(Identity theft)는 다른 누군가로 가장하려고 그 사람의 주민번호, 운전면허증번호, 신용 카드번호 등 개인 핵심정보를 빼내는 범죄를 말함(중요 정보의 암호화)

- 이러한 정보는 피해자의 이름으로 신용 구매를 하거나 제품을 구매하거나 서비스를 받는데 사용될 수 있고, 범죄자가 위조 신분증명서를 만드는 데 사용되는 등 여러 범죄를 일으키는데 사용될 수 있음

# 2 | 신원 도용 및 사이버 폭력

## 1 신원 도용(Identify theft)

- 인터넷이 발달하면서 인터넷 상에서
  신분 위장 절도의 발생이 매우 잦아짐

- 대표적인 신분 위장 절도의 기법으로 피싱이 있음,
  2005년 900만의 미국인이 신분 위장 절도 때문에
  피해를 입었고, 손실액은 566억 달러에 이름
  (피싱, 파밍, 스미싱)

## 2 신원 도용 - 대응 방안

- 보안에 대한 확고한 인식을 갖는 것이
  가장 기본적이고 중요함
- 안티피싱 툴이나 안티바이러스 프로그램을
  항상 최신 버전으로 유지(가장 기본)
- 자신의 신원이 도용되었다면
  해당 사이트의 개인 정보 보안 담당자에게 연락
- 개인정보침해신고센터(국번 없이 118)
  또는 경찰청 사이버안전국(국번 없이 182)에 신고

## 3 주요 개인 정보 유출 사고

| 유출 시기 | 유출 기관 | 피해 규모 |
|---|---|---|
| 2008년 2월 | 옥션 | 1,863만 명(중국 해커로 추정, CSRF 공격) |
| 2008년 4월 | 하나로텔레콤 | 600만 명 |
| 2008년 9월 | GS칼텍스 | 1,125만 명 |
| 2010년 3월 | 신세계몰 | 820만 명 |
| 2011년 4월 | 현대캐피탈 | 174만 명(퇴직 직원의 아이디와 비밀번호 이용) |
| 2011년 7월 | SK커뮤니케이션즈 | 3,500만 명(중국 해커로 추정, 내부 개발자 PC 해킹) |
| 2012년 5월 | EBS | 400만 명 |
| 2012년 7월 | KT | 870만 명 |
| 2013년 6월 | 새누리당, 군장병, 청와대, 주한미군 | 294만 명(6.25 사이버 테러) |
| 2014년 1월 | KB국민카드, 롯데카드, NH농협은행 | 2,000만 명(중복 포함 1억 400만 건, 파견 직원에 의한 유출) |
| 2014년 3월 | KT | 1,200만 명 |
| 2014년 3월 | SKT, LG U+ 등 | 1,230만 명 |
| 2014년 3월 | 국토교통부 | 2,000만 명(자동차민원관리사업자 포털 사이트) |
| 2016년 7월 | 인터파크 | 1,030만 건 |
| 2017년 3월 | 여기어때 | 341만 건(2017년 6월에 26세의 중국 해커 검거) |

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

## 3 주요 개인 정보 유출 사고

| | | | |
|---|---|---|---|
| 2017년 4월 | 야피존 | 가상화폐유출 | 55억원 |
| 2017년 6월 | 빗썸 | 개인정보유출 | 3만 6천명[10] |
| 2017년 7월 | 유진투자선물, 디비피아 등 20개 업체 | 개인정보유출 | 3,300만 건[11] |
| 2017년 9월 | 이스트소프트 | 개인정보유출 | 13만 건[12] |
| 2017년 9월 | 하나투어 | 개인정보유출 | 100만 건[13] |
| 2017년 12월 | 유빗(구 야피존) | 가상화폐유출 | 172억원 |
| 2018년 6월 | 코인레일 | 가상화폐유출 | 400억원 |
| 2018년 6월 | 빗썸 | 가상화폐유출 | 350억원[14] |

※ 출처 : https://ko.wikipedia.org/wiki/대한민국의_정보_보안_사고_목록

## 4 사이버 폭력(Cyberbullying)

- 온라인상에서 특정인을 지속적으로 음해하고 괴롭히는 것으로 주로 아동이나 청소년 사이에서 일어남(가해자가 보호 받는 세상)

- 카카오톡, 페이스북과 같은 SNS와 메신저, 이메일, 휴대전화 문자, 사진 편집 툴, 블로그 등을 통해 더욱 확산되고 있는 추세

- 사이버 폭력은 사이버공간에서 다양한 형태로 타인에게 가해지는 괴롭힘을 의미하며, 신체적 폭력을 수반하는 전통적인 폭력과는 달리 그 형태가 다양함

## 4 사이버 폭력(Cyberbullying)

- 문자로 상대방을 직접 험담하는 것뿐만 아니라 특정인을 비하하는 글·이미지·동영상 혹은 개인 신상 정보를 유포하는 행위, 단체 채팅방에 계속 초대하거나 초대 후 집단적으로 나가버리는 행위 등 다양한 형태로 이루어짐(죽음의 서클)

- 또한 사이버 공간이라는 특성으로 인해 일반 폭력과는 다른 양상을 가지므로 이에 대한 이해가 필요함

## 4 사이버 폭력(Cyberbullying)

- 따라서 사이버 폭력 예방을 위해서는 사이버 공간의 특성에 대한 이해가 선행되어야 하며 다양한 형태 별로 차별화된 대응 노력이 필요하다고 할 수 있음(준비되어 있는가?)

- 사이버 폭력은 비 대면성 · 익명성 · 영구성과 확산성 · 기술의 사용과 물리적 힘의 불필요를 특징으로 함,
  따라서 가해자는 피해자의 고통을 직접 눈으로 확인할 수 없기 때문에 죄책감이나 자신이 가해행위를 한다는 생각을 못할 수도 있음(더 위험)

## 4 사이버 폭력(Cyberbullying)

- 또한 익명성은 자신의 가해행위가 드러나지 않을 것이라는 믿음을 줌, 하지만 유포된 글이나 이미지나 동영상은 쉽게 유포되고 쉽게 지울 수 없어 피해자의 고통은 가중됨, 물리적 힘이 요구되는 전통적 폭력에서는 가해자와 피해자간 구분이 있었으나 사이버 공간에서는 피해자와 가해자가 중첩될 수 있으며 물리적 힘이 부족하더라도 기술 사용 능력이 뛰어난 사람은 사이버 공간에서 가해자가 될 수도 있음(불필요한 카카오톡을 하지 않음)

## 4 사이버 폭력(Cyberbullying)

- 이런 특성 때문에 사이버 폭력이 전통적 폭력보다 더 피해가 크며 일상화 될 수 있음,

  사이버폭력과 전통적 폭력을 비교한 연구에 의하면 사이버폭력이 더 일상화되어 있으며, 피해 후 자살 등 극단적인 생각을 하는 비율도 사이버 폭력에서 더 높음

## 4 사이버 폭력 - 대응 방안

- SNS에서 받은 음해와 험담 메시지는
  마음에 담아두지 말고 무시하는 것이 좋음
  (SNS는 되도록 안 하는 것이 최선)

- 사이버 폭력에 해당하는 메시지는
  나중에 증거 자료로 사용될 수 있으므로
  삭제하지 말고 저장

## 4 사이버 폭력 - 대응 방안

- 아동들에게 사이버 폭력의 위협에 대해 알려주고, 음해나 험담 메시지를 받았을 때 즉시 부모님이나 주위 어른에게 이야기하도록 당부 (아이들의 시그널 파악)

- 가정과 학교에서 적절한 사이버 예절을 가르침
  - 정부는 사이버 폭력 예방 교육 프로그램을 마련해 학생, 교사, 학부모에게 제공(효용성? 없는 것 보단 낫다)