
해킹시나리오

CONTENTS

개 요

시나리오

SNS가 발달하면서 수많은 이용자들이 생겨났다. 이용자들이 많아지면서 현재 SNS의 파급력은 굉장히 크다. 그로 인해 범죄에 SNS를 이용하는 방법도 많아질 것으로 보인다. 먼저 우리가 구성한 시나리오는 “FaceBook” 이라는 소셜 네트워크 서비스를 이용하여 이루어지는 해킹이다. “FaceBook” 에는 좋아요, 공유하기라는 서비스를 통하여 여러 사용자가 게시글을 볼 수 있게 하는 서비스가 존재하는데 좋아요와 공유하기가 많은 게시글 일수록 파급력과 큰 신뢰를 얻게 된다. 이점을 이용하여 해킹을 시작하는 것이다.

시나리오

- 먼저 내 게시물에 신뢰를 얻어야 하므로 좋아요와 공유하기를 수집해야한다.

- 첫 번째로 페이지를 개설하여 영화, 만화 등을 무료로 볼 수 있는 링크를 게시글에 포함시킨다.
  이 때 이용자가 링크를 타고 들어오면 영화나 만화를 보기 위해선 사용자 정보를 수집하는
  것에 동의를 해달라는 문구를 보여주어서 이용자가 동의버튼을 누르게 만든다.

- 사용자가 동의 버튼을 누르게 되면 '토큰' 이라는 것을 얻을 수 있게 되는데 토큰은 특정
  페이스북 계정에 접근할 수 있는 임시 보안권한으로, 암호문 형태의 문자열을 말한다.
  이 정보는 페이스북 계정에서 타임라인 글 작성, 좋아요 추가, 팔로워·친구 신청, 이름, 나이,
  친구, 연락처 조회 등 대부분의 주요 기능을 로그인 없이 실행할 수 있는 권한이 포함돼 있다.

시나리오

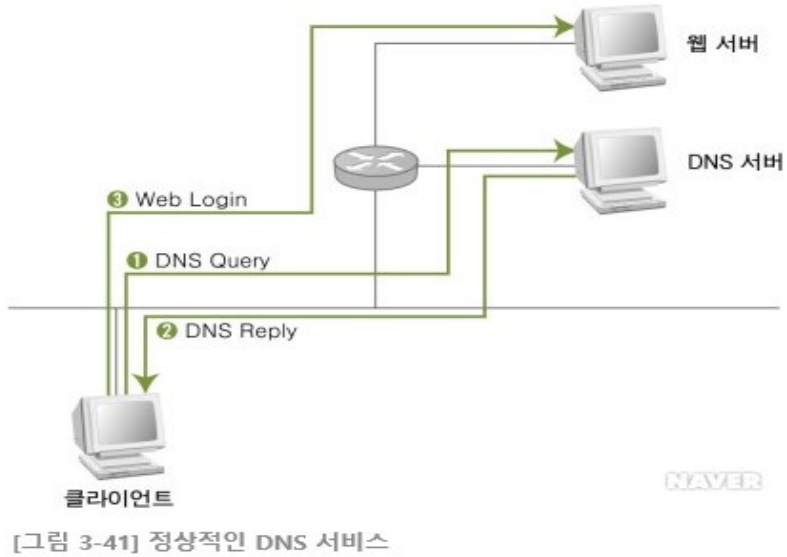
- 이러한 방법으로 토큰을 수집 후 다음으로는 상품판매나 좋은 커뮤니티사이트를 소개하는 게시글을 링크와 함께 업로드 한 후 수집한 토큰으로 게시글 좋아요, 공유하기 기능을 사용해 다른 이용자들의 신뢰를 얻는다. 사용자들은 자신의 페이스북 친구, 또는 많은 좋아요와 공유된 숫자를 통해 이 게시글에 신뢰성을 얻게 되고 신뢰를 얻게 된 게시글에 있는 링크를 타고 들어오게 된다. 이 링크에 기입된 주소는 피싱 사이트이며 이 사이트의 서비스를 이용하기 위해선 모바일 환경 접속이 필요하다는 메시지를 보여준 뒤 자동으로 어플 설치를 위한 사이트로 연결시킨다.

- 연결된 사이트를 통해 사용자가 자신의 모바일기기에 어플을 설치하게 되면 스푸핑을 할 수 있는 악성코드와 함께 다운로드 되며, 어플을 통해 들어온 사용자가 사이트 이용을 위한 회원가입을 할 때 스푸핑을 통해 주민번호, 휴대폰 번호 등 개인정보를 탈취한다.

- 탈취한 개인정보를 이용하여 해커는 소액결제를 시도하게 되고 어플과 함께 다운로드 된 악성코드를 이용 결제사이트에서 사용자에게 전송된 코드를 훔쳐본 뒤 소액결제를 진행한다.

해킹 기법

DNS 스푸핑

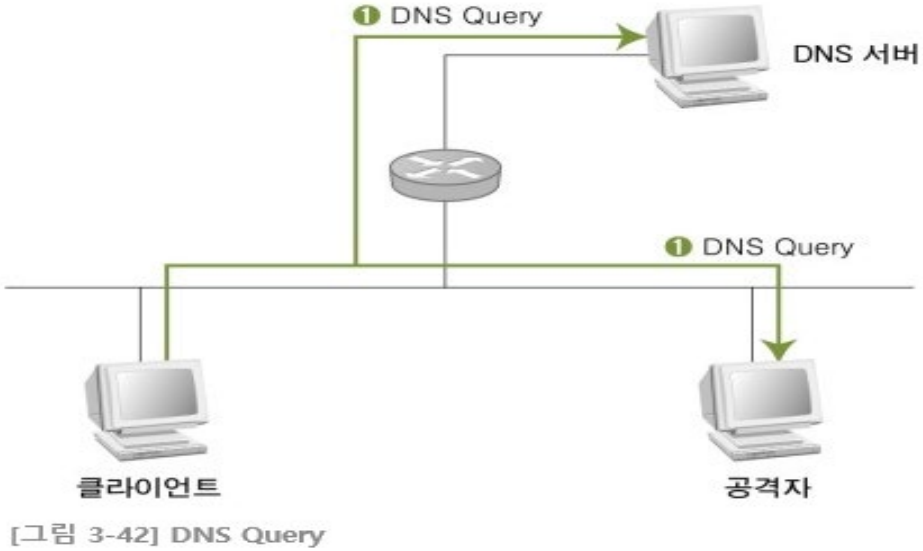


[그림 3-41] 정상적인 DNS 서비스

DNS(Domain Name System) 스푸핑은 실제 DNS 서버보다 빨리 공격 대상에게 DNS Response 패킷을 보내, 공격 대상이 잘못된 IP 주소로 웹 접속을 하도록 유도하는 공격이다. DNS 스푸핑 공격은 때로는 웹 스푸핑과 비슷한 의미로 해석된다.

해킹 기법

DNS 스푸핑



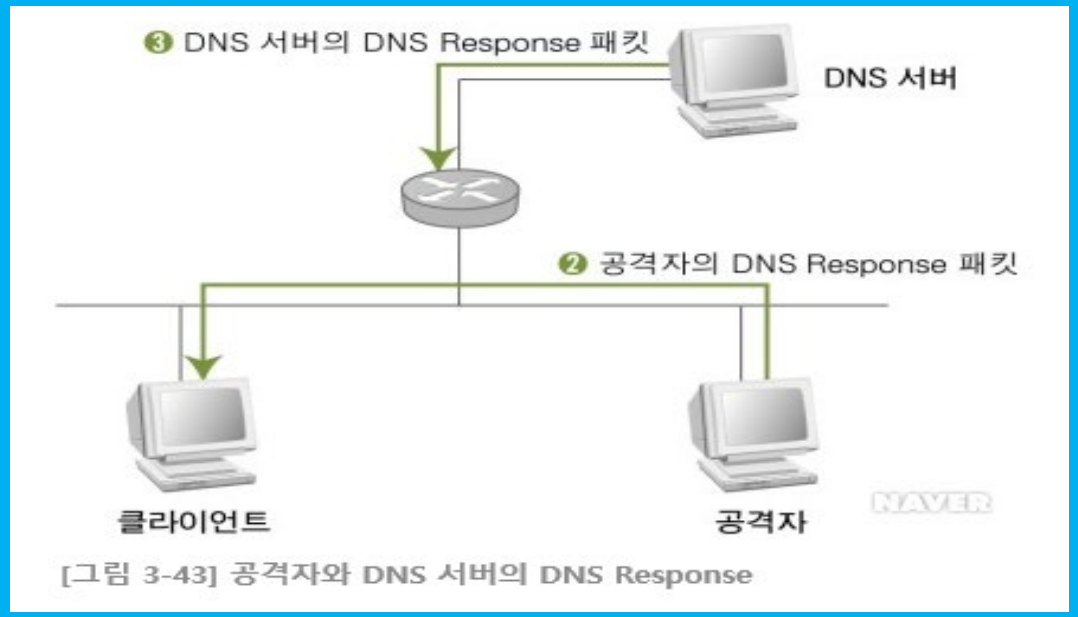
[그림 3-42] DNS Query

① 클라이언트가 DNS 서버로 DNS Query 패킷을 보내는 것을 확인한다. 스위칭 환경일 경우에는 클라이언트 DNS Query 패킷을 보내면 이를 받아야 하므로 ARP 스푸핑과 같은 선행 작업이 필요하다. 만약 허브를 쓰고 있다면 모든 패킷이 자신에게도 전달되므로 클라이언트가 DNS Query 패킷을 보내는 것을 자연스럽게 확인할 수 있다.

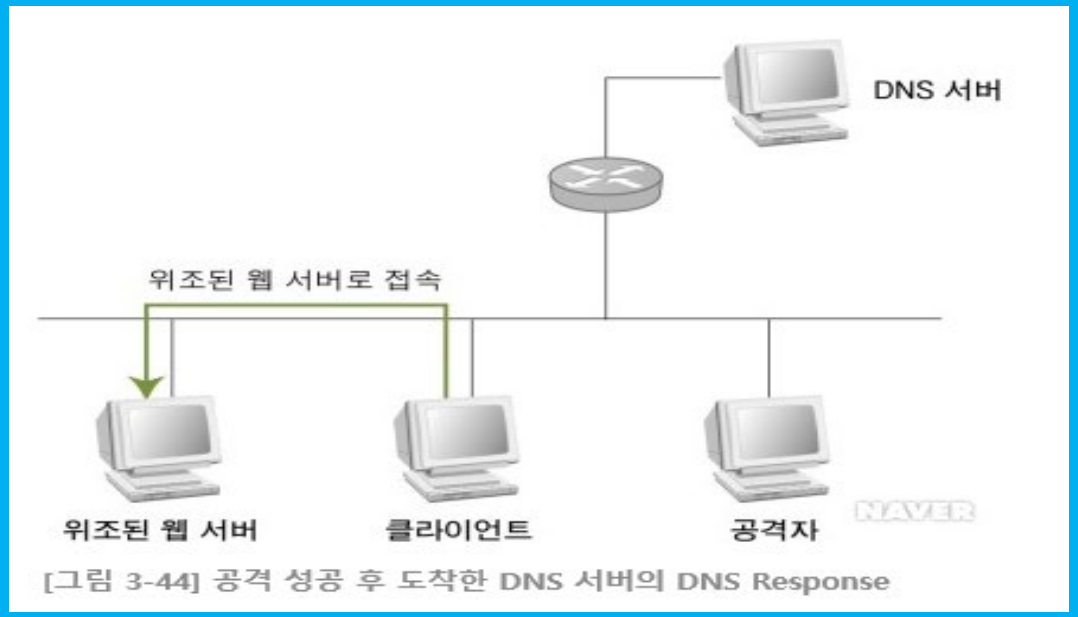
② 공격자는 로컬에 존재하므로 지리적으로 DNS 서버보다 가깝다. 따라서 DNS 서버가 올바른 DNS Response 패킷을 보내주기 전에 클라이언트에게 위조된 DNS Response 패킷을 보낼 수 있다.

해킹 기법

DNS 스푸핑



[그림 3-43] 공격자와 DNS 서버의 DNS Response

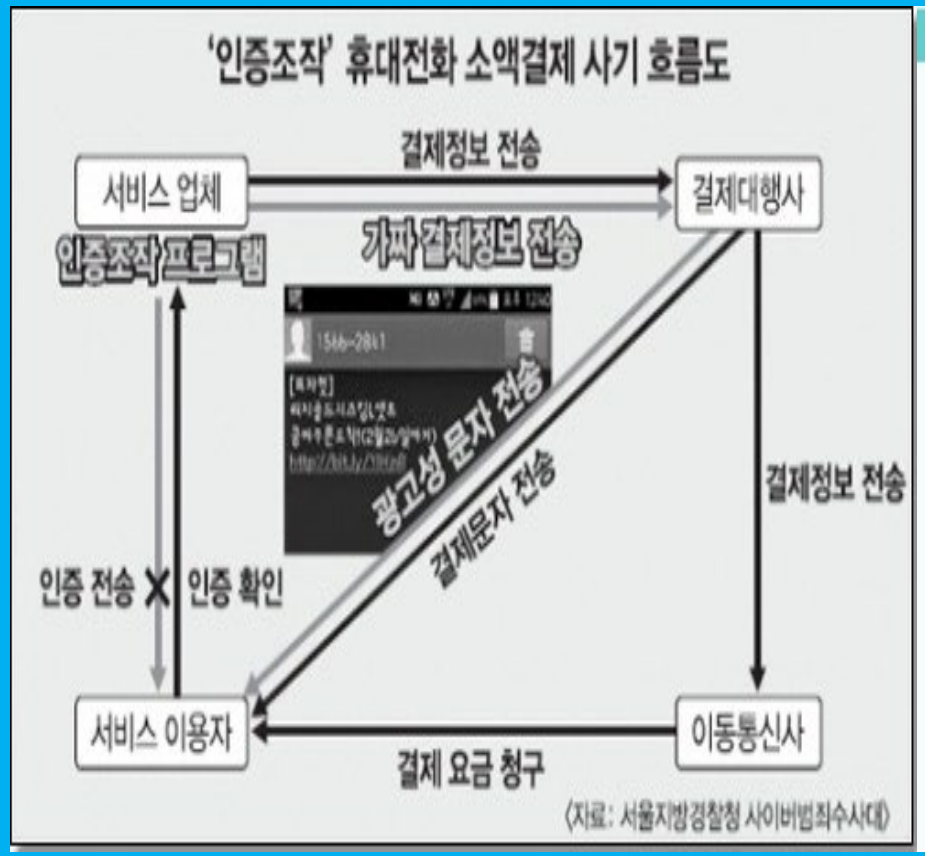


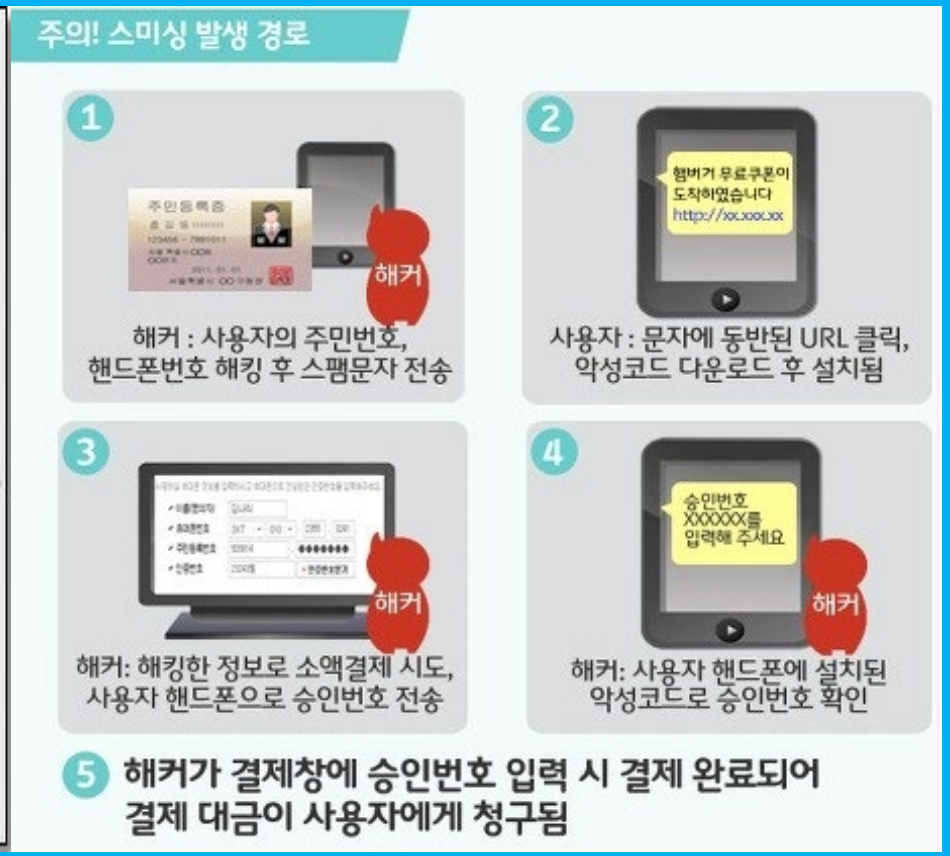
[그림 3-44] 공격 성공 후 도착한 DNS 서버의 DNS Response

③ 클라이언트는 공격자가 보낸 DNS Response 패킷을 올바른 패킷으로 인식하고 웹에 접속한다. 지리적으로 멀리 떨어진 DNS 서버가 보낸 DNS Response 패킷은 버린다.

해킹 기법

악성코드 이용


'인증조작' 휴대전화 소액결제 사기 흐름도
서비스 업체
결제정보 전송
결제대행사
인증조작프로그램
가짜 결제정보 전송
광고성 문자 전송
결제문자 전송
결제정보 전송
인증 전송
인증 확인
서비스 이용자
이동통신사
결제 요금 청구
〈자료: 서울지방경찰청 사이버범죄수사대〉

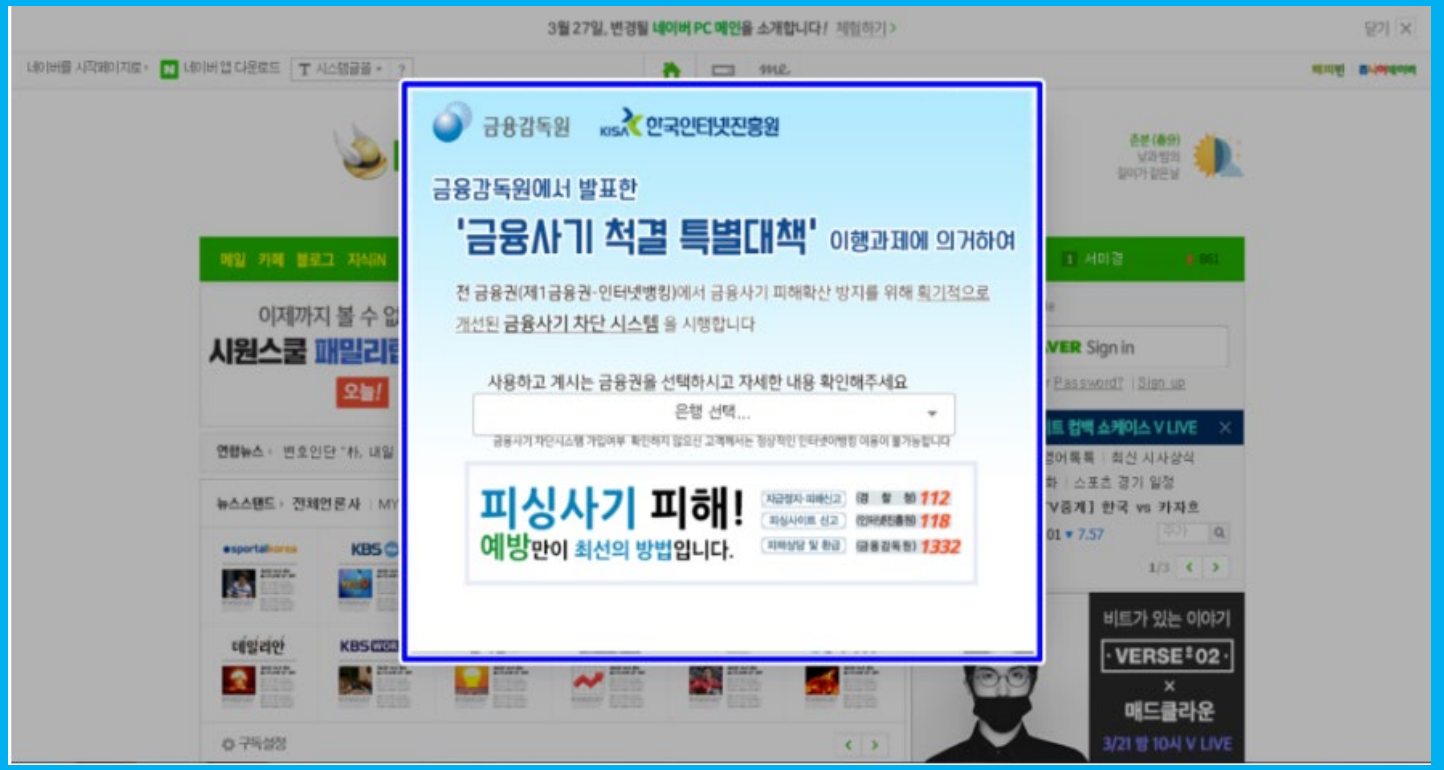

주의! 스미싱 발생 경로
1
해커
해커 : 사용자의 주민번호, 핸드폰번호 해킹 후 스팸문자 전송
2
햄버거 무료쿠폰이 도착하였습니다
http://xx.xxx.xx
사용자 : 문자에 동반된 URL 클릭, 악성코드 다운로드 후 설치됨
3
해커
해커: 해킹한 정보로 소액결제 시도, 사용자 핸드폰으로 승인번호 전송
4
승인번호 XXXXXX를 입력해 주세요
해커
해커: 사용자 핸드폰에 설치된 악성코드로 승인번호 확인
5 해커가 결제창에 승인번호 입력 시 결제 완료되어 결제 대금이 사용자에게 청구됨

해킹 사례

페이스북 방문자 추적 또는 각종 사회이슈에 대한 서명운동을 미끼로 불법 수집한 페이스북 액서스 토큰 정보 수 십만 건을 '좋아요' 또는 '팔로우' 횟수를 조작하는데 악용한 온라인마케팅업자들이 경찰에 적발됐다.
액서스 토큰은 특정 페이스북 계정에 접근할 수 있는 임시 보안권한으로, 암호문 형태의 문자열을 말한다.
이 정보는 페이스북 계정에서 타임라인 글작성, 좋아요 추가, 팔로워·친구 신청, 이름·나이·친구·연락처 조회 등 대부분의 주요 기능을 로그인 없이 실행할 수 있는 권한이 포함돼 있다. 부산경찰청 사이버수사대는 1일 A(22)씨 등 온라인마케팅업체 3곳의 운영자 등 5명을 정보통신망법 위반 등의 혐의로 불구속 입건했다고 밝혔다.

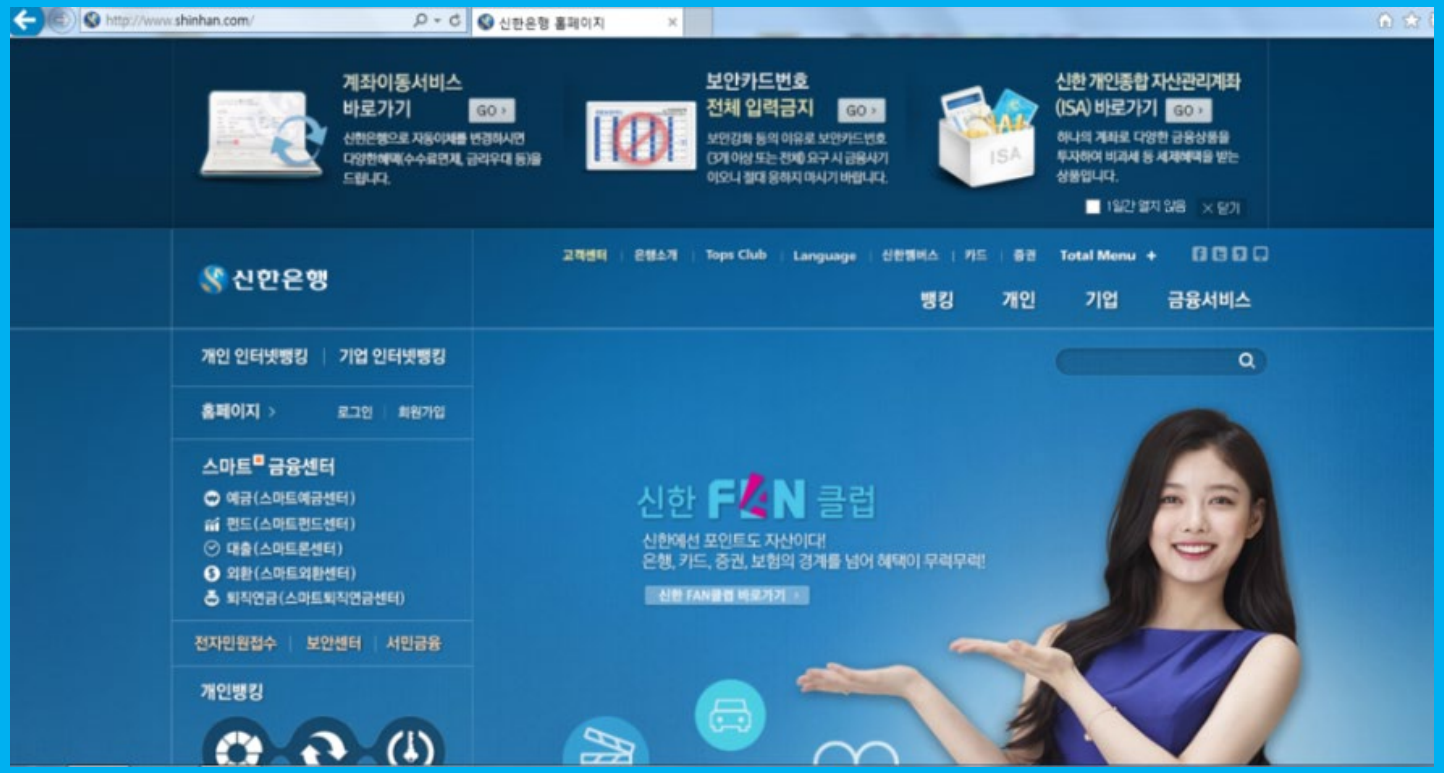
출처 :http://www.newsis.com/view/?id=NISX20171101_0000134925&cID=10811&pID=10800

피싱 예시



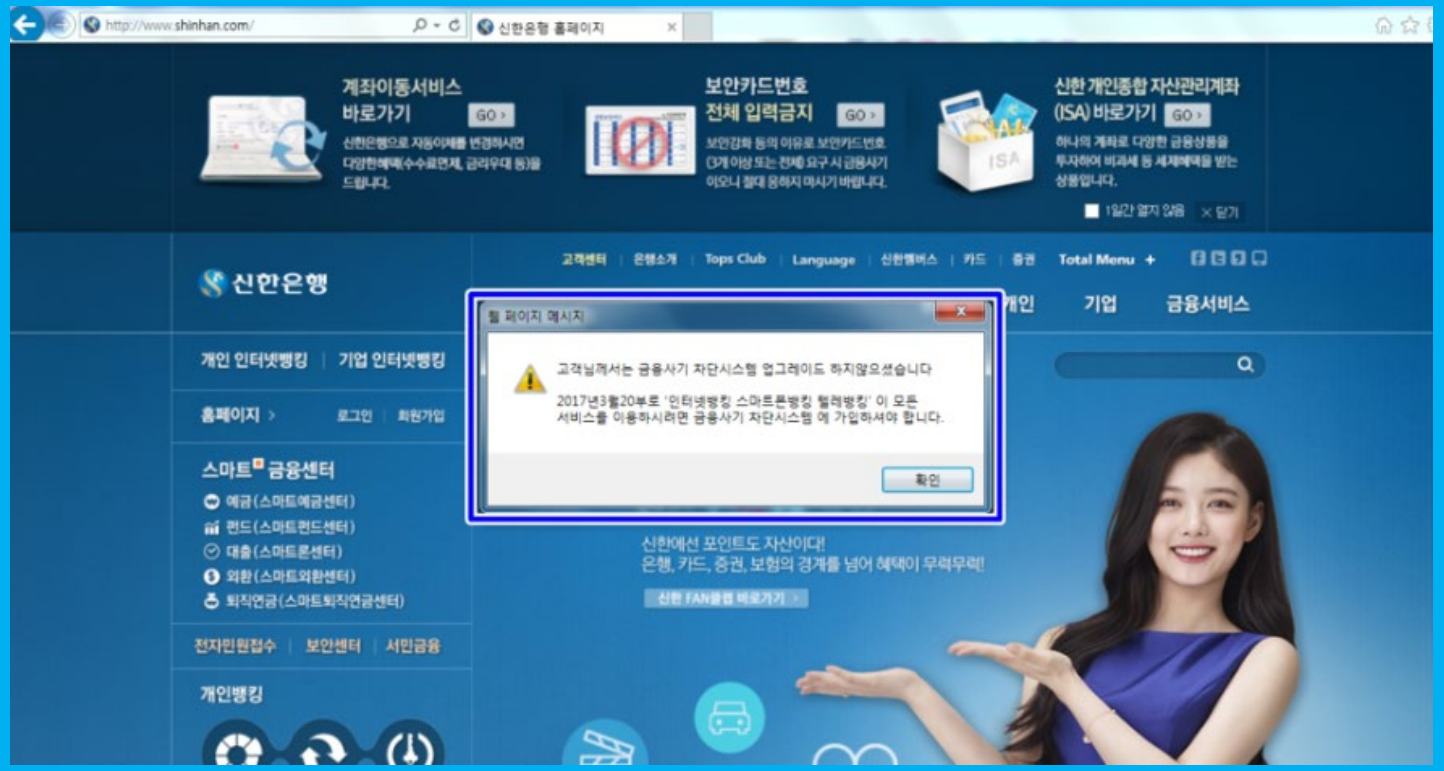
1. 피싱 사이트 접속을 시키기 위한 URL 혹은 링크

피싱 예시



2. 신뢰성 있는 사이트 혹은 기존에 있던 사이트처럼 구성

피싱 예시



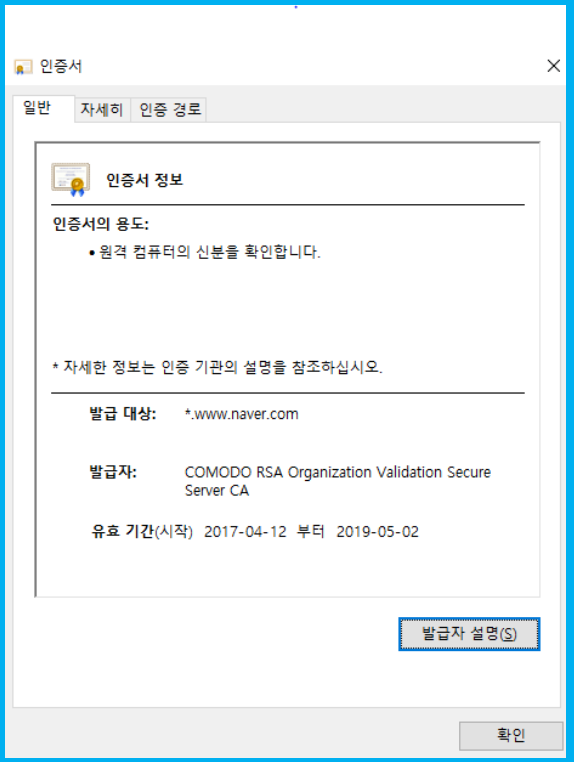
3. 개인정보 수집을 위한 피싱 기법

피싱 예시

3. 개인정보 수집을 위한 피싱 기법

예 방 법

- 인증된 사이트를 통해 연결된 링크나 URL이 아니면 접속하지 않는다.
  (사이트의 인증서 확인)



- 개인정보 수집 혹은 여러 서비스를 통제할 수 있는 권한을 허가해달라는 요청이 있는지 확인한다.

- 모바일 어플리케이션 설치 시 앱 스토어나 신뢰성이 확인된 곳이 아니면 설치하지 않는다.

- 사이트나 어플리케이션 로그인 시 이중암호 (OTP, 보안코드)등을 사용한다.


THANKS