Facebook Hacking

중부대학교 정보보호학과, 정보보안개론 이병천 교수님

91714117 안지현

목차

1 주제 소개 &
선정 동기

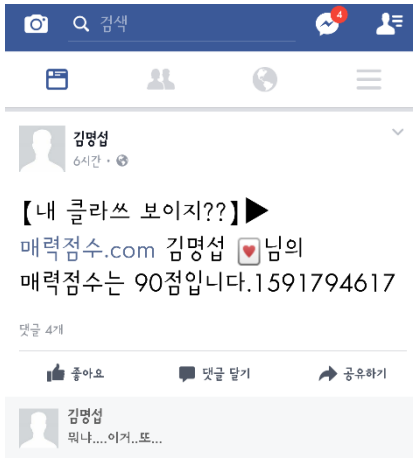
2 설명

3 시연, +α

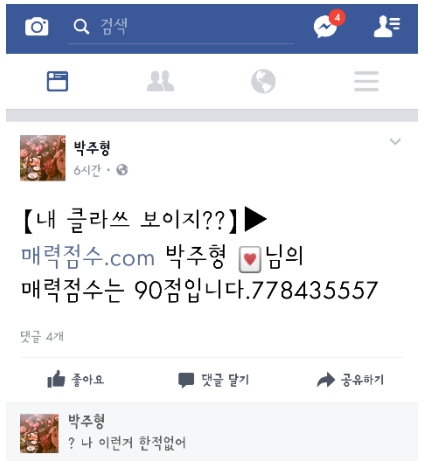
4 결론 &
보안(예방) 방법

Why? Facebook Hacking

모두가 이용하는 SNS,
페이스북



방문자 추적기/ 염탐꾼 탐지 등
친구들 사이에서 유행하던 것



수상한 프로그램,
원리는 무엇일까?

프로그램을 실행하는 사람들의 심리

▶ 이 서비스는 '굳이 내 타임라인까지 방문했다→나에 대해 궁금해한다→나에게 관심이 있다→나를 좋아하는 것은 아닐까?!' 라는 사고의 흐름을 따라가는 사람에게 혹할 만한 기능이다.

▶방문자 추적기 업체 입장

실제 자신의 타임라인을 방문한 사람 데이터를 페이스북으로부터 받아서 제공하는 것은 당연히 아닙니다. 업체 측은 "방문자 추적기는 5가지 가설을 세워서 기능을 넣었다" 라며 "100% 완벽하게 추적을 완료하는 게 아니라, 5가지 방법을 교차해서 방문자를 예측하는 서비스" 라고 설명했습니다.

* 출처 : http://www.bloter.net/archives/264264

▶어떤 경우에 친구 추천 목록에 뜨는지?

1. 상대방의 이름을 검색해서 들어 온 경우
2. 상대방의 페이스북에 자주 들어갔을 경우 (주기적 염탐)
: 이 경우 페이스북은 친밀한 관계라고 판단해 친구 추천 목록 '최상단'에 뜰 수 있다.
3. 페이스북 계정과 휴대폰 번호를 연동한 사람의 번호가 저장됐을 경우
: 과거 소개팅 했던 이성, 아르바이트 했던 곳의 사장님, 전 직장 동료 등이 뜰 수 있다. 상대가 아직 당신의 번호를 지우지 않았다는 것을 의미하기도 한다.
4. 페이스북과 연동된 이메일을 가진 사람과 이메일을 주고받은 경우
: 페이스북과 같은 이메일 주소를 사용하는 경우 해당 이메일로 서로 주고받은 적이 있을 때 페이스북은 친분이 있다고 판단해 추천하게 된다.
5. 자신이 입력해 놓은 정보와 비슷한 사람의 경우
: 학교, 직장, 출신지 등 비슷한 정보를 입력한 사람이라면 친구 추천 목록에 뜨게 된다.

설 명

토큰(Token) → Access token in F.B

▶토큰(Token) 이란 ?

전자상거래 카드 결제 시 보안 수준을 강화하고 위변조를 막기 위하여 신용카드번호를 고유 토큰으로 대체하는 것을 말한다.
토큰화하면 독자적 암호화, 자체 보안 설정으로 특정 상점 · 기기 · 거래 형식 · 경로를 제한할 수 있다.
따라서 특정 가맹점과 채널에서만 사용할 수 있기 때문에 가맹점 간 정보를 공유할 수 없고, 외부로 유출되어도 개인정보를 알 수 없는 쓰레기 정보가 된다.
* 요약 : 보안 정보를 담는 무작위의 문자열

* 출처 : [네이버 지식백과] 토큰화 (시사상식사전, 박문각)

▶권한 탈취 시 가능해 지는 것 ?

로그인 시 로그인 상태 그대로 사용하는 권한.
예를들면 포스팅/좋아요/게시 글 공유/친구 맺기/개인 정보 접근 등 가능

방문자 추적 사이트 같은 곳에서는 이 권한을 가져다가 방문자의 정보를 보는 것이기 때문에 개인정보 유출, 권한 탈취 등 보안적인 측면에서 매우 위험하다고 할 수 있다.

하지만 아이디나 비밀번호를 알 수는 없다.
비유를 하자면 ' 집 도어락 비밀번호는 안 알려주지만 카드키를 넘겨주는 것 '

설명

대표 사이트 '페북미' + 광고 사이트 '아이라이크 페북' 도 가세

재미로 하는 '방문자 추적기/ 염탐꾼 찾기/ 절친 찾기/ 스토커 찾기/ 팔로우 부스터'

설명 (광고 사이트를 이용하는 광고주들의 목적:광고비 절감)

방문자 추적기 사이트 '리미트 연구소 '

해당 사이트는 사용자의 토큰을 수집함.
그러나 법적으로 아무런 문제가 되지 않음,

설 명

법(法) 건드리기

이용 약관

Limit Lab은 여러분의 facebook엑세스토큰을 수집해 Limit Lab서비스 제공을 위하여 사용할 수 있습니다.

여러분에게 Limit Lab서비스를 제공하기 위하여, Limit Lab은 여러분의 facebook엑세스토큰에 대한 어떤 권리를 부여할 것을 필요로 합니다. 예를 들면, Limit Lab은 여러분 facebook엑세스토큰을 수집해 그 데이터를 바탕으로 통계 및 품앗이 서비스를 진행할수있고 데이터 손실을 막고 백업을 만들 필요등이 있습니다. 이와 유사하게, Limit Lab은 Limit Lab 서비스상 여러분의 개인 정보를 마케팅에 활용할수 있습니다. 여러분이 Limit Lab서비스에 facebook엑세스토큰을 제공하는 경우, Limit Lab서비스에만 이용될것을 말씀드리며 제공받아 수집된 facebook엑세스토큰의 경우 계정을 탈퇴한 후에도 보존기간동안 존속될 것입니다.

여러분은 Limit Lab에게 여러분이 Limit Lab서비스에 제공한 데이터를 사용할 수 있는 facebook엑세스토큰을 수집하는 데 필요한 모든 법적 권리를 가지고 있거나 취득하여야 합니다. Limit Lab이 여러분이 제공한 facebook엑세스토큰이 Limit Lab의 정책에 위반되는 것으로 결정하는 경우, Limit Lab은 그 데이터를 삭제하거나 이를 게시하는 것을 거절할 수 있습니다. 그러나 Limit Lab은 여러분 또는 다른 사용자의 facebook엑세스토큰을 전부 검토할 의무를 부담하지는 않습니다. 여러분의 권리가 침해되었다고 믿는 경우, 여러분은 Limit Lab의 고객센터를 통하여 도움을 받을 수 있습니다.

여러분의 Limit Lab서비스 이용은 여러분에게 다른 이용자들로부터 제공된 데이터에 관한 권리를 부여하지 않습니다. Limit Lab서비스를 통하여 이용가능하게 된 다른 이용자들의 데이터를 사용하기 위하여, 여러분은 그 데이터의 소유자로부터 개별적으로 허락을 받아야 합니다.

다 같은 원리인 '엑세스 토큰' 탈취를 이용하여 합법적으로 계정 탈취 중이다! 심지어 활발히 활동 중.

설 명

페이스북 공식 입장

Facebook
2013년 5월 2일 ·

내 Facebook 방문자 추적은 불가능합니다!

대부분 방문자 추적이 가능하다고 하는 앱/프로그램 등은 내 타임라인에 남긴 댓글, 좋아요 수 등을 기준으로 순위를 보여줄 뿐이오니 의심스러운 프로그램은 다운받지 않는 것이 좋답니다.
이상한 앱은 살포시 '신고'해주세요!

고객 센터 | 질문하기 | 로그인 | 계정 만들기

홈 | Facebook 사용 | 계정 관리 | 개인정보보호 및 안전 | 정책 및 신고

- 로그인 및 비밀번호
- 프로필 및 설정
- Facebook상의 이름
- **계정 보안 유지하기**
- 보안 기능 및 팁
- 로그인 알림 및 2단계 인증
- **스팸 및 사기 방지**
- 알림
- 광고 기본 설정
- 내 정보에 액세스하기
- 계정 비활성화 또는 삭제

Facebook에서 사기를 예방하려면?

데스크톱 도움말 | **모바일 브라우저 도움말** | 기타 고객 센터 | 게시물 공유하기

Facebook에서는 사기범들이 회원님이 좋아하는 사람의 계정을 가짜로 만들거나 기존 Facebook 계정 또는 페이지를 해킹하는 사기 형태가 등장한 바 있습니다. 이들은 허위 계정이나 해킹된 계정으로 송금을 유도합니다. 사기로 생각되는 메시지를 받은 경우 응답하지 마세요. 금융 사기 메시지를 받았다면 신고해주세요.

다음은 주의해야 하는 일반적인 사기 형태입니다.

- **연애 사기**: 주로 모르는 사람한테 로맨틱한 메시지를 보내 이혼하거나 배우자가 죽었거나 결혼생활이 불행한 척하는 유형입니다. 온라인 관계를 맺어 항공편이나 비자에 필요한 돈을 요구하는 형식으로, 신뢰를 쌓기 위해 몇 주간 대화를 지속한 후 돈을 요구하는 방식을 사용합니다.
- **복권 사기**: 복권 사기는 흔히 회원님이 아는 사람 또는 단체(예:정부 기관, Facebook)를 사칭한 계정 또는 페이지를 통해 발생합니다. 이들은 회원님이 복권에 당첨되었으며 소액의 선불 수수료를 입금하면 당첨금을 보내준다고 하면서 회원님의 거주지 주소나 은행 계좌와 같은 개인 정보를 요구합니다.
- **대출 사기**: 대출 사기범은 낮은 이자율에 적은 선급금으로 즉시 대출 가능하다는 메시지를 보내거나 게시물을 남깁니다.
- **액세스 토큰 도용:** Facebook 계정 또는 페이지에 대한 액세스를 요청하는 링크가 회원님과 공유됩니다. 이 링크는 합법적인 앱의 링크로 보일 수 있지만 스팸 유포자들이 회원님의 계정에 대한 액세스 권한을 얻고 스팸을 퍼뜨리기 위해 사용하는 방법입니다.

설 명

방문자 추적기 사이트 '페북미 '

페이스북 방문자 친구 초간단 확인

공유하기 6,623개

페북미는 토큰 필요없음!!

로그인

바로 위의 버튼으로 페북에 로그인 후(꼭),
하단의 사용 방법을 읽고 따라하세요.

페북로그인 버튼이 안나온다면 2초만 기다려주세요

아래 사용법을 읽고 소스를 붙여넣으세요

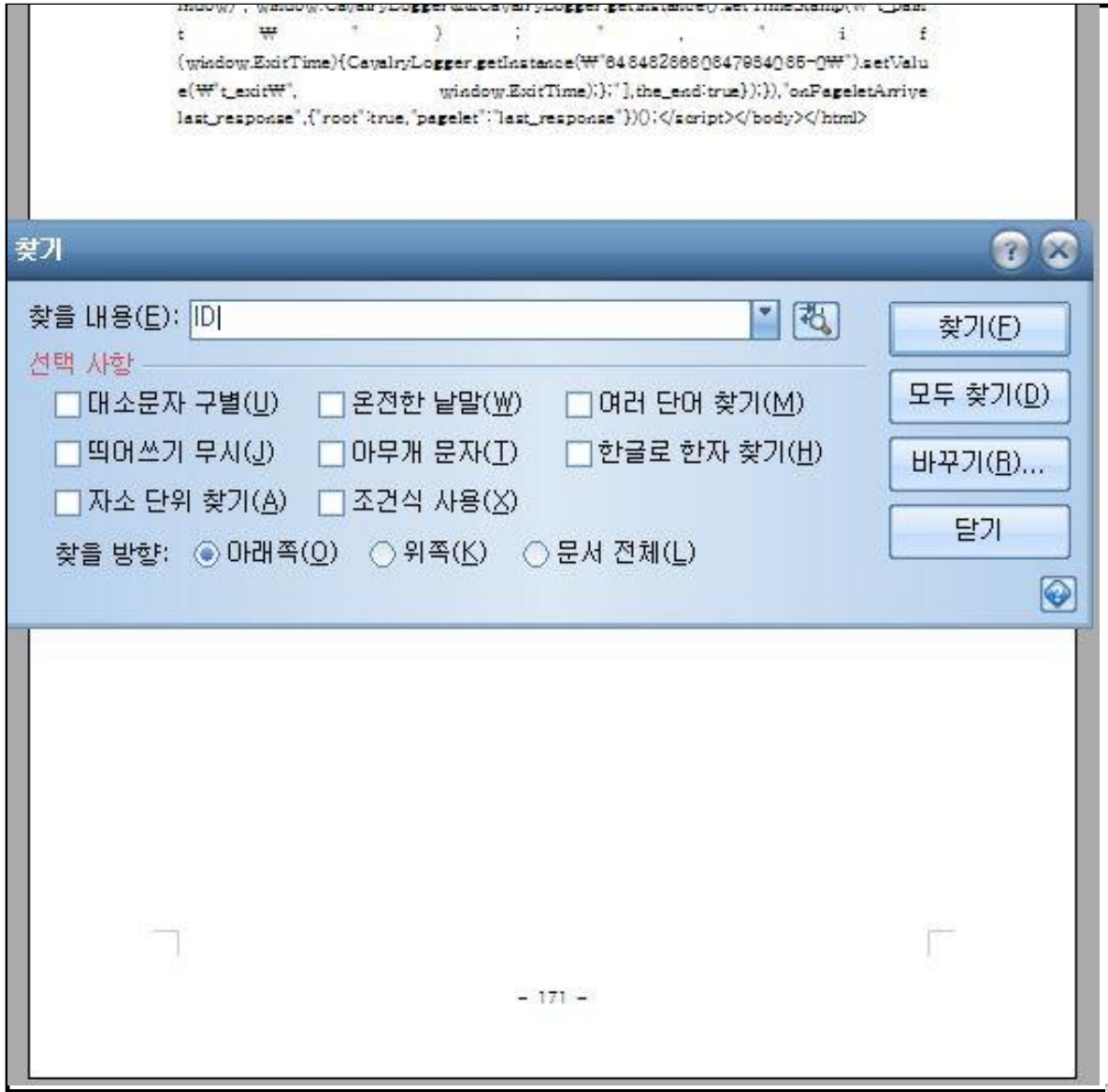
추적

스마트폰 사용법	PC 사용법

0. 본문의 facebook 로그인 버튼을 눌러서 로그인 합니다.
1. 페이스북으로 이동
2. Ctrl + U (소스보기) 후
3. Ctrl + A (전체선택) -> Ctrl + C (복사)
4. 소스 붙여넣고 추적 버튼 클릭

궁금한 친구나 장소를 검색해보세요.
안지현
홈
친구 찾기
안지현
뉴스피드
Messenger
바로가기
PPT의 모든 것
둘러보기
게시물 작성
사진/동영상 앨범
안지현님, 무슨 생각을 하고 계신가요?
사진/동영상
기분/활동
강지혜님이 댓글에 답글을 남겼습니다.
Sponsored
광고
SK브로드밴드(SK broadband)
SK브로드밴드(SK
F12
DOM 탐색기
콘솔
디버거
네트워크
성능
메모리
에뮬레이션
www.facebook[1]
1 <!DOCTYPE html>
2 <html lang="ko" id="facebook" class="no_js">
3 <head><meta charset="utf-8" /><meta name="referrer" content="default" id="meta_referrer" /><script>window._cstart=+new Date();</script>
<script>function envFlush(a){function b(c)
{for(var d in a)c[d]=a[d];}if(window.requireLazy){window.requireLazy(['Env'],b);}else{window.Env=window.Env||{};b(window.Env);}}envFlush(
{"ajaxpipe_token":"AXiICcpIdQ43Zt3N","timeslice_heartbeat_config":{"pollIntervalMs":33,"idleGapThresholdMs":60,"ignoredTimesliceNames":
{"requestAnimationFrame":true,"Event listenHandler mousemove":true,"Event listenHandler mouseover":true,"Event listenHandler mouseout":true,
"Event listenHandler scroll":true},"enableOnRequire":false},"shouldLogCounters":true,"timeslice_categories":{"react_render":true,"reflow":true},
"dom_mutation_flag":true});</script><style></style><script>__DEV__=0;CavalryLogger=window.CavalryLogger||function(a){this.lid=a;
this.transition=false;this.metric_collected=false;this.is_detailed_profiler=false;this.instrumentation_started=false;this.pagelet_metrics={};
this.events={};this.ongoing_watch={};this.values={t_cstart:window._cstart};this.piggy_values={};this.bootloader_metrics={};
this.resource_to_pagelet_mapping={};this.e2eLogged=false;if(this.initializeInstrumentation)this.initializeInstrumentation();};

시 연


찾기
찾을 내용(E): ID
선택 사항
대소문자 구별(U)
온전한 낱말(W)
여러 단어 찾기(M)
띄어쓰기 무시(J)
아무개 문자(T)
한글로 한자 찾기(H)
자소 단위 찾기(A)
조건식 사용(X)
찾을 방향: 아래쪽(O) 위쪽(K) 문서 전체(L)
찾기(F)
모두 찾기(D)
바꾸기(R)...
닫기
- 171 -

찾기
찾을 내용(E): 한지호
선택 사항
대소문자 구별(U)
띄어쓰기 무시(J)
자소 단위 찾기(A)
찾을 방향: 아래쪽

시 연

▶추가적인 앱 설치

HTC Sense 앱에서 수신하는 정보: 회원님의 공개 프로필, 친구 리스트, 이메일 주소, 사용자 지정 친구 리스트, 메시지, 친구 요청, 뉴스피드, 결혼/연애 상태, 결혼/연애 관심 대상, 생년월일, 채팅 상태, 노트, 경력, 상태 업데이트, 학력, 이벤트, 그룹, 출신지, 관심사, 거주지, 사진, 질문, 종교관과 정치관, 팔로우와 팔로워, 동영상, 웹사이트, 설명, 좋아요, 책 활동, 음악 활동, 뉴스 활동, 동영상 활동, 게임 활동 및 친구의 결혼/연애 상태, 결혼/연애 관심 대상, 생년월일, 채팅 상태, 노트, 경력, 상태 업데이트, 학력, 이벤트, 그룹, 출신지, 관심사, 거주 도시, 사진, 질문, 종교관과 정치관, 팔로우와 팔로워, 동영상, 웹사이트, 설명, 좋아요, 책 활동, 음악 활동, 뉴스 활동, 동영상 활동, 게임 활동.

방문자 추적기를 한 번 사용하게 되면 HTC sense 앱에 대한 승인창이 뜨는데 대부분의 사람들은 잘 읽지 않는다.

▶왜 다른 앱을 썼을까?

서비스를 만든 업체는 페이스북 마케팅 업체인데, 권한을 받는 앱은 전혀 무관한 'HTC sense' 입니다. HTC 센스는 HTC에서 제작한 스마트폰의 전용 그래픽 사용자 인터페이스를 말합니다. 스마트폰에서 사용자 조작에 필요한 그래픽 요소들을 지칭한다고 이해하시면 좋을 것 같습니다. 사실 어떤 앱인지 살피지 않았어도 해당 서비스와 전혀 관련이 없다는 건 쉽게 알 수 있습니다.
굳이 사용자가 직접 토큰을 직접 '복사-붙여넣기' 하게 만들지 않아도, 개발자가 직접 페이스북에서 앱을 만들고 해당 앱을 통해 권한을 받는 식으로도 운용할 수 있습니다. 하지만 이 경우 커뮤니티 정책 위반으로 앱을 만든 계정이 날아가 버리면 그간 들인 공이 허사가 됩니다.
타사의 잘 알려진 앱을 우회해서 사용하면, 페이스북 정책 위반으로 본계정이 날아가더라도 웹사이트에 기반을 둔 서비스는 유지할 수 있습니다. 일종의 안전장치죠. 해당 계정이 커뮤니티 정책 위반으로 삭제된 것이 확인됐습니다.

보안/예방 방법

1. 비밀번호를 당장 변경한다.

2. 비밀번호를 주기적으로 변경한다.

3. (비밀번호를 바꾸었음에도 불구하고 글이 계속 올라오는 경우)
페이스북 설정메뉴>앱>해당 프로그램 삭제

4. 이렇게 생긴 것 말고도 '코드를 넣어라, 주소를 복사하라' 등의 지시가 있는 것은 php파일이나 주소를 이용하여 토큰을 탈취하고 있으므로 주의하자.

5. 활동 로그를 살펴서 원하지 않는 계정 활동이 있었는지 주기적으로 점검하자.

6. 개인정보보호는 사용자 역할이 중요하다.
→사용자 스스로 추적기의 사용을 자제하고 보안에 각별한 주의를 기울여야 한다.

QnA

감사합니다