중고거래플랫폼에서 나타나는 개인정보 유출 현황 및 제안

장민경 [1], 김지원 [1], 박혜원 [1], 임수진 [1], 김명주 [2]
[1] 서울여자대학교 정보보호학과
[2] 서울여자대학교 정보보호학과 교수
skyups10@swu.ac.kr, eldorado15@swu.ac.kr, hwp45_76@swu.ac.kr, sjclass9898@naver.com, mjkim@swu.ac.kr

Privacy Data Leakage Problem and its Solution in the Used Product Trading Markets

Min-Kyung Jang[1], Ji-Won Kim[1], Hye-won Park[1], Su-Jin Lim[1], Myuhng-Joo Kim[2]
[1]Dept. of Information Security, Seoul Women's University
[2]Professor, Dept. of Information Security, Seoul Women's University

요 약

중고 거래 플랫폼 사용이 증가함에 따라 각 중고 거래 플랫폼에 많은 사진과 글이 업로드되고 있다. 플랫폼에 올린 사진과 글을 통해 일차적으로 해당 이용자의 나이대, 사는 동네, 가족 관계, 신체 사이즈, 특정 제품 취향을 알 수 있다. 중고 거래 플랫폼에서 전화번호를 얻게 될 경우, 이차적으로 카카오톡을 통해 이용자의 얼굴 사진, 연동된 계정을 알 수 있다. 이때 얻은 얼굴 정보와 이름, 계정을 통해 인스타그램, 카카오스토리, 페이스북 등 SNS 를 통한 해당 이용자의 추가적인 개인정보들을 얻을 수 있다. 이처럼 이용자가 작성한 글을 통해 사적인 정보가 드러남으로써 심각한 개인정보 유출로 이어질 수 있다. 중고 거래 플랫폼 이용자의 직접적인 입력으로 인한 개인정보 노출을 예방하기 위해서는 이용자에게 게시물에 포함된 개인정보와 개인정보 유출의 위험성을 인지시켜 유출 위험성이 높은 개인정보는 게시하지 않도록 해야 한다. 본 논문에서는 중고 거래 판매 게시물 기반 개인정보 유출 워크플로우를 작성하여 중고 거래 플랫폼에서 나타나는 개인정보 유출의 현황을 분석하고 이를 방지하기 위한 방법을 제안했다.

1. 서론

오늘날 정보통신기술의 발전으로 인터넷과 스마트폰 등 디지털 기기가 생활화됨과 동시에 인터넷과 스마트폰을 이용한 중고 거래가 날로 늘어가고 있다. 대표적인 중고 거래 플랫폼에는 당근마켓이 있다[1]. 당근마켓은 '당신 근처의 직거래 마켓'의 약자로 동네에서 중고 직거래를 할 수 있는 지역 기반 중고 거래 스마트폰 애플리케이션 서비스이다. 현재 와이즈앱(앱과 소매시장의 사용자 행태 분석 데이터 제공 서비스) 2021 년 12 월 기준, 월간 1,676 만 명이 이용하고 있는 대표적인 중고 거래 플랫폼이다[2].

이러한 지역 기반의 당근마켓의 중고 거래는 택배 거래의 불편함과 신뢰성 문제를 해결함으로써 다른 중고 거래 플랫폼과 차별점을 제공하여 가까운 거리에서 거래가 이루어져 직거래에 용이하고, 당근마켓 모든 이용자가 동네 인증을 받아 안심하고 중고 거래를 할 수 있다는 장점이 있다[3]. 반면, 중고 거래 플랫폼 이용자가 작성한 글과 올린 사진에서 쉽게 이용자의 개인정보들을 얻을 수 있어 얻은 개인정보들을 이용한 사기 범죄, 성범죄 등 범죄에 노출될 가능성이 크다. 매너 온도가 높은 사람일수록 거래 시 좋은 평가를 받으려는 성향이 높으므로 중고 거래 플랫폼 이용자가 작성한 글과 올린 사진을 통한 개인정보 유출의 위험성이 매너 온도가 낮은 사람에 비해 더 높다. 지역 기반 직거래 특성상 사는 지역과 얼굴을 알 수 있으므로 더욱 위험성이 높다[4]. 더구나 중고 거래 플랫폼 이용자가 작성한 글 내 전화번호가 있는 경우 직접 거래하지 않고도 번호와 연동된 카카오톡 등 여러 SNS 계정 내에 있는 개인정보까지 유출될 수 있다.

본 논문은 현재 중고 거래 플랫폼의 개인정보 유출 위험성에 대한 경각심을 주는 것을 목적으로 하고 있다. 판매 글과 사진들을 통해 개인정보 유출 워크플

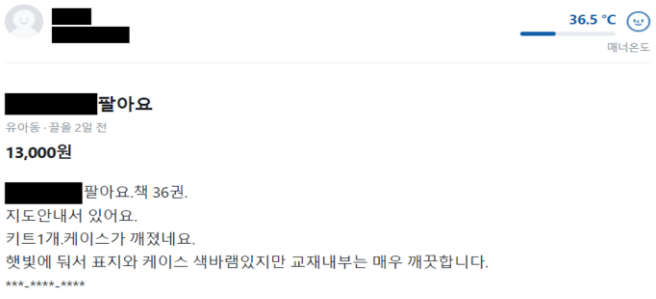
로우로 작성하여 개인정보 유출 현황을 분석하고 그리고 개인과 기업의 차원에서 작성한 글과 올린 사진을 통한 개인정보 유출을 방지하는 방법을 제공하고자 한다.

2. 중고 거래 플랫폼의 프라이버시 침해 실태

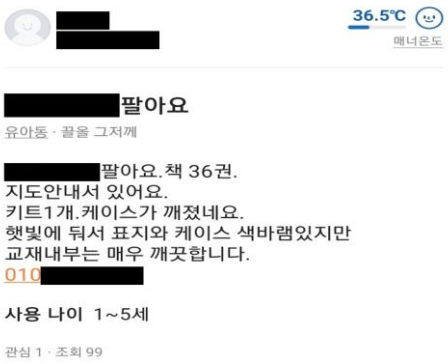
2021 년 4 월 27 일 당근마켓의 한 이용자는 중고 거래하며 교환했던 번호로 카카오톡을 통해 본인의 얼굴과 가족의 얼굴, 심지어 아들 연락처까지 유출되어 거래 상대방에게 돈을 빌려 달라는 협박에 시달리는 사건이 있었다[5]. 이 외에도 당근마켓에서는 지역 기반 거래라는 점을 악용하여 여성 이용자들을 노린 성희롱, 스토킹 범죄도 빈번하게 발생하고 있다[6]. 프라이버시 침해가 발생하는 원인에 대해 중고 거래 플랫폼의 기술적인 특징과 그로 인해 유출되는 개인정보 현황을 분석하고자 한다. 당근마켓, 중고나라, 번개 장터 등 여러 중고 거래 플랫폼 중 국내 최대 중고 거래 플랫폼인 당근마켓을 집중적으로 분석을 진행했다[7].

3. 중고 거래 플랫폼 개인정보 항목 분석

당근마켓은 모든 이용자에게 가입과 동시에 영문 대소문자와 숫자로 이루어진 16 자리 고유 코드를 부여하는데, ‘https://www.daangn.com/u/’ 링크 뒤에 붙으며 닉네임 및 사는 지역이 바뀌어도 코드는 변경되지 않는다. 이 고유 코드를 통해 이용자를 추적할 수 있지만 당근마켓 애플리케이션에서 프로필 링크 복사를 통해 손쉽게 타인과 공유할 수 있다. 본 논문은 당근마켓 이용자의 판매 상품 게시물에서의 개인정보 유출 실태를 파악하기 위해 고유 코드를 사용하여 웹 크롤러 코드를 작성하여 진행하였다. 웹 크롤러(Web Crawler)는 웹 사이트, 하이퍼링크, 데이터, 정보 자원을 자동화한 방법으로 수집, 분류, 저장하는 것을 의미한다[8].



(그림 1) 판매글 속 전화번호 은닉 화면

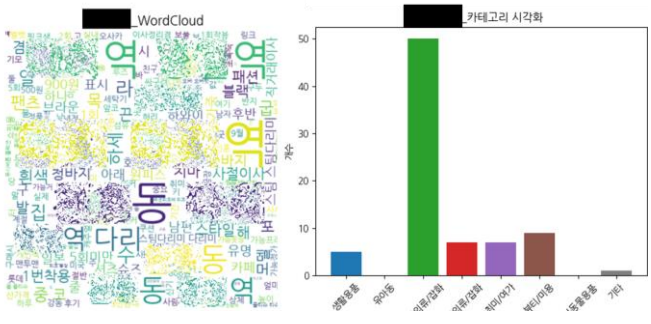


(그림 2) 판매글 속 전화번호 노출 화면

(그림 1)은 웹 페이지로 조회된 판매 글에서 전화번호가 숨김 처리되어 나타난 화면이다. 당근마켓 게시글에서 전화번호로 추측되는 숫자로 이루어진 문자열이 나열되면 웹 페이지에서 ‘***-****-****’ 형태로 마스킹 되어 조회된다.

이와 반대로 모바일 애플리케이션에서 같은 게시물을 조회하면 (그림 2)와 같이 전화번호가 마스킹되지 않고 그대로 노출됨을 알 수 있다. 본 논문에서는 당근마켓에서 전화번호를 이처럼 비식별 처리한다는 점을 이용하여 ‘***-****-****’ 문자열을 탐색함으로써 오히려 전화번호를 쉽게 추적하여 획득할 수 있었다.

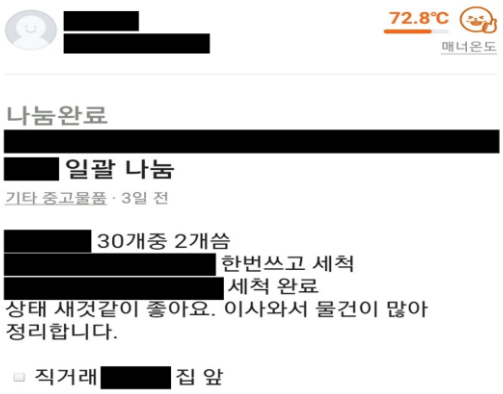
정확한 분석 결과를 위해 불용어 사전을 작성하여 개인정보 관련 데이터를 전처리 및 가공하여 분석했다. 기존의 불용어 사전의 경우, 토큰화 후에 조사, 접속사 등을 제거하는 방식을 사용하나 당근마켓 게시글의 경우 쓰이는 용어가 한정되어 있어 조사나 접속사와 같은 단어들뿐 아니라 명사, 형용사도 정의한 불용어 사전을 토대로 제거하였다. 크롤링이라는 단순한 방법으로 (그림 3)과 같이 생각보다 많은 개인정보가 노출될 위험이 크다는 사실을 발견했다.



(그림 3) 개인정보 추출 결과 화면

(그림 4)는 이미 거래 완료 처리된 거래 게시물을 통해 한 계정에서 얻은 정보 화면이다. 거래 완료된

판매 상품 게시물도 누락되는 정보 없이 판매 중인 게시물과 같은 형식을 취하고 있음을 알 수 있다.



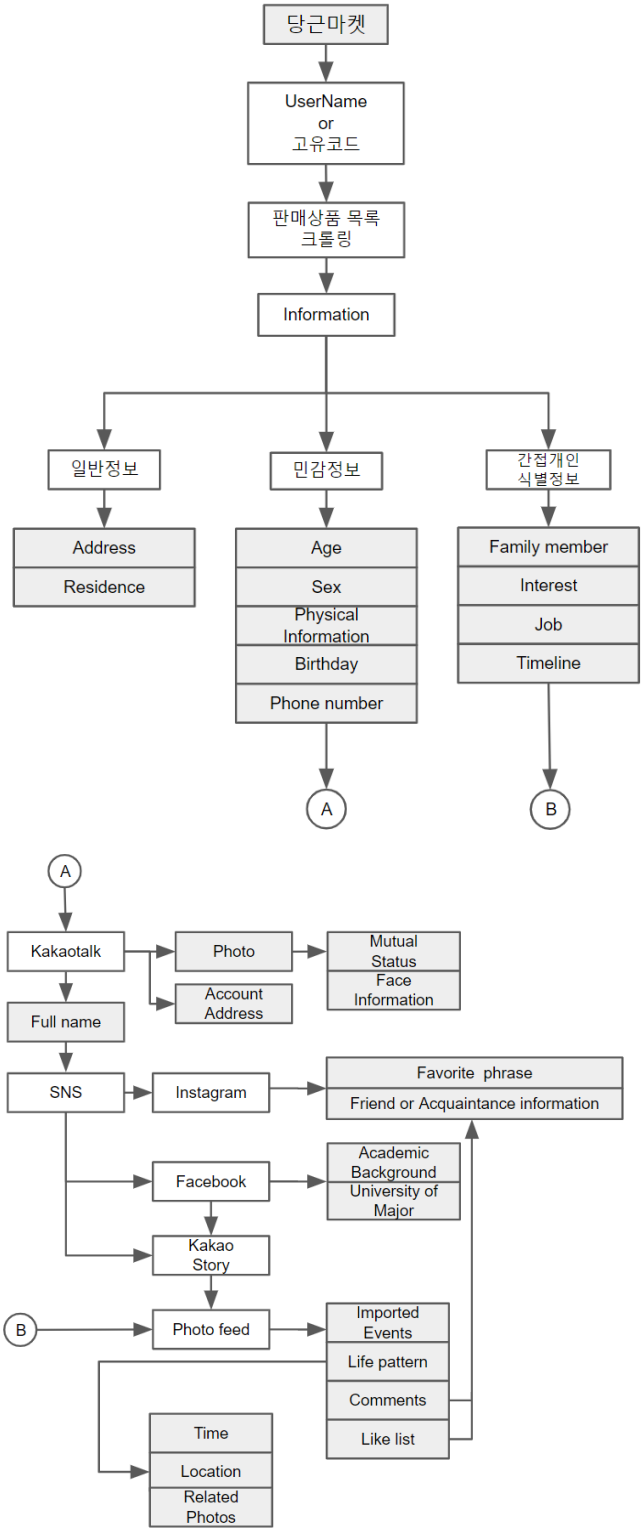
(그림 4) 거래 완료 상품 게시물 화면

4. 판매 게시물 기반 개인정보 유출 워크플로우

현재 대부분의 당근마켓 이용자는 개인정보 유출의 위험성을 인지하여 최대한 개인정보 노출을 삼가는 편이다. 그러나 전화번호를 올린 이용자일수록 경각심이 낮아서 더 많은 개인정보를 유출할 가능성이 크다고 판단할 수 있다. 한편 판매상품의 고유주소를 분석한 결과, 이용자의 계정과 관계없이 최근에 올린 글일수록 판매상품 고유주소의 마지막 숫자들이 크고, 과거에 올린 글일수록 작다는 사실도 발견했다.

(그림 5) 전화번호 추출 코드 결과 화면

(그림 5)은 게시물에 전화번호가 존재할 경우 화면에 개인정보가 존재한다는 메시지를 출력하는 화면이다. 판매상품 고유주소를 이용하여 특정 기간 동안 올린 게시물 중 전화번호를 유출한 이용자의 계정만 무작위로 추출해 해당 계정을 분석한 결과, 전화번호를 유출하지 않은 이용자보다 많은 개인정보를 발견할 수 있었다.



(그림 6) 당근마켓 개인정보 유출 워크플로우

(그림 6)은 크롤링 및 판매 글 분석을 통해 당근마켓에서 개인정보가 유출되는 과정에 대하여 작성한 워크플로우이다. 이용자명 혹은 고유 코드를 통해 프로필 페이지에 접근하면 거주 지역, 판매 물품 목록, 거래 후기 등에서 얻을 수 있는 글과 사진 정보를 통

해 나이, 성별, 전화번호, 신체정보, 가족 정보 등을 알 수 있다. 이후 개인정보 검색은 게시물에 전화번호가 업로드 되었다는 가정하에 이루어진다. 전화번호를 이용해 카카오톡 계정을 검색하면 이용자가 설정한 본인의 이름, 이전 프로필 사진 목록 및 카카오스토리로 연결된다. 이때 이용자의 이름은 본명에 가까울 가능성이 높으며 프로필 사진을 통해 신체정보가 노출된다. 또한 카카오스토리에 게시글이 작성되어 있다면 사진을 직접 분석해 사진에 내재된 신체정보, 가족정보, 고용정보 등의 개인정보를 알 수 있다. 마찬가지로 당근마켓 상품 게시물에 올린 사진을 통해 직접 개인정보를 알아내는 방법도 가능하다. 이처럼 당근마켓 이용자가 물품 판매 시 전화번호를 게시한 경우, 거래하지 않고도 번호와 연동된 SNS 계정을 통해 사진, 가족 관계, 출생연도, 출신 학교, 대인관계, 방문한 장소 등 개인정보가 추가로 유출될 위험성이 높다는 것을 알 수 있다.

5. 개인정보 보호를 위한 제안 사항

개인정보의 가치가 높아짐에 따라 개인정보를 수집하는 기업에 그에 상응하는 개인정보보호 관련 조치를 요구하는 것은 당연한 일이다[9].

판매 완료된 게시글은 개인정보를 유추할 수 있는 단어와 사진은 지우고 거래 물품과 가격만 남길 수 있게 해야 한다. 당근마켓 내 검색 기능을 이용하여 ‘010-12’까지만 입력 후 검색했을 때, 게시물에 올린 전화번호의 ‘010’과 게시글 내용에서 ‘12 시간’, ‘12 만 원’, ‘12 개’ 등 ‘12’를 찾아낼 수 있는 글이 검색됨을 알 수 있다. 이 경우는 내용에 ‘12’가 있는 글에 한정된다는 단점이 있지만 높은 확률로 전화번호가 게시되어 있었다.

따라서 이용자가 개인정보가 포함된 게시물 작성 후 등록을 요청하면 기업은 게시물에서 개인정보의 유형대로 추정되는 패턴을 정규 표현 식을 이용해 인식하여 개인정보가 검출되면 애플리케이션 내에서도 표시 제한 보호 조치를 수행해야 한다[10].

6. 결론

본 논문에서는 중고 거래 플랫폼 이용자가 작성한 글 또는 올린 사진을 통해 '크롤링'이라는 단순한 방법으로 추출할 수 있는 개인정보를 분석했다. 다른 중고 거래 플랫폼에서도 이와 같은 개인정보 유출 동향이 발견되었다. 이러한 내용을 바탕으로 본 논문은 개인정보 유출 워크플로우 제시 및 개인정보 노출에 대한 기업과 개인의 실천 방안을 제안하였다.

향후 중고 거래 플랫폼 이용자의 고유 계정 링크를 입력 받으면 자동으로 글, 사진 정보를 수집해 개인정보 노출 위험도를 시각화하여 보여줄 수 있는 웹사이트 개발을 진행할 예정이며 이것이 구현되면 개인정보 노출 위험성에 대한 경각심을 보다 더 높일 수 있을 것으로 기대한다.

참고문헌

[1] Y. Z. Lin, “Influence Factors on the Intention of Continuous Use of Local-Based and Nationwide-Based Online Second-hand Trading Platform:Focused on ‘danggeun market’ and ‘Junggonara’”, 국내석사학위 논문 서울대학교 대학원, 2021

[2] 박응서, “한국인 37% 중고거래 앱 이용… 이용자 수 당근마켓, 번개장터, 중고나라 순”, Techworld Online News, 2022 년 1 월 25 일, https://www.epnc.co.kr/news/ articleView.html? idxno= 219246

[3] 김윤진, “동네 사람과 거래… 이웃 간 연결 핵심” 마켓에서 출발해 커뮤니티 부활시켜”, Dong-A Business Review, 2019 년 11 월 1 일,https://dbr.donga.com/article/view/1203/ article_no/ 9348

[4] G. Y. Park & S. I. Kim , "A Study on User Experience of the Security in Online Trading of used goods", Journal of Digital Convergence, Vol. 19, No. 7, pp. 313-318, 2021.

[5] 김명일, “당근마켓 거래 뒤 ‘돈 빌려달라’ 협박…같은 동네 사는데 어쩌나”, 한경사회, 2021 년 4 월 27 일, https://www.hankyung.com/society/article/ 2021042714547

[6] 박정환 · 박하얀, '착샷' 요구에 성추행까지…당근마켓 '성범죄 주의보', 노컷뉴스, 2021 년 1 월 4 일, https://www.nocutnews.co.kr/news/5474511

[7] S. P. Kim, “A Study on the User Structure Analysis of Second Hand Market Apps”, Journal of the Korea Academia-Industrial, Vol. 22, No. 7, pp. 449-458, 2021

[8] D. M. Seo & H. M. Jung, “Intelligent Web Crawler for Supporting Big Data Analysis Services”, Journal of the Korea Contents Association, Vol. 13, No. 12, pp. 575~584, 2013

[9] Korea Information Security Agency, “개인정보보호 교육 시리즈-개인정보보호 왜 중요할까요”, Information security news, No.130, pp. 10-11, 2008

[10] K. S. Lee & H. B. Ahn, "A Study on a Prevention Method for Personal Information Exposure", Convergence Security Journal, Vol. 12, No. 1, pp. 71-77, 2012