신종스팸의 발송동향 및 대응방안 연구

백종훈*, 김영직**

스마트 기기의 보급 확대와 IoT 기반 기술의 발달로 지금까지 휴대전화, 이메일로 양분되던 스팸유통의 현황분석과 대응정책에서 새로운 경로로 등장하는 스팸에 대한 인식 및 대응이 필요한 시점이다. 모바일 메신저 스팸, 웹 팩스 스팸, SNS 스팸, PUSH 알람, 불특정 초대 문자 등과 같이 일상 저변의 각각에 깊숙이 파고 들어오는 신종스팸 유형과 발송기법에 대한 동향과 기초 현황을 분석하여 신종스팸 대응의 개선방안을 제시한다.

* 한국인터넷진흥원 스팸대응팀 주임연구원(baekjoh@kisa.or.kr)
** 한국인터넷진흥원 스팸대응팀 책임연구원(yjkim@kisa.or.kr)

Ⅰ. 서론

스마트폰 보급률의 증가, 전용 하드웨어의 기능을 구현한 소프트웨어의 개발 및 대중화, 앱스토어 등 앱 수요 및 공급 시장의 확장으로 정보를 배포하거나 접근할 수 있는 채널은 날로 다양해지고 있다. 더불어 개별 채널들의 정보 전달 기술의 고도화, 정교화를 바탕으로 광고 효과를 극대화하기 위한 스팸 발송자들의 노력 또한 기술적, 정책적으로 대응 지점을 도출하기가 대단히 난해해지고 있는 실정이라 하겠다.

다양한 검색 채널과 매체들을 통하여 필요한 정보들을 쉽게 검색하고 얻을 수 있게 된 반면, 무익하거나 불필요한 정보들, 특히 제품과 서비스의 마케팅을 위한 영리목적의 스팸들은 이용자가 찾거나 요청하지 않았음에도 불구하고 강제적으로 노출 및 제공되어 피해를 주고 있다. 이렇게 이용자 의사에 반하여 제공되는 영리 목적의 정보는 이전부터 이메일, 전화, 문자, 팩스 등의 매체를 통하여 지속적으로 배포되어 왔으며, 현재는 스마트 단말을 기반으로 하여 자동화/고속화된 채널을 사용하여 이전과 비교하여 월등히 진화한 형태의 스팸들이 유포되고 있는 실정이다.

신종스팸의 등장은 새로운 정보 접근 채널 환경을 찾아보면 알 수 있다. 스마트폰 사용자라면 필수처럼 가입, 사용하고 있는 무료 모바일 메시지 앱을 기반으로 하는 스팸, 팩시밀리 기능을 소프트웨어로 대체할 수 있게 된 인터넷 웹팩스를 이용한 팩스 스팸, 자동화 툴을 이용한 게시판(댓글) 스팸, 블로그를 중심으로 스팸을 생성하는 스플로그 등이 있다.

영리목적의 스팸 발송기술은 지속적으로 진화해 왔으며, 스팸으로 유포되는 내용 또한 단순 광고에서부터 성인, 도박, 대출 등 다양한 범주에 걸쳐 배포되고 있다. 최근에는 광고를 가장한 결제사기나 개인정보 유출 등에 악용되는 보다 위험성을 가지고 있는 내용과 링크를 포함하여 악성코드 또는 바이러스를 유포하는 행태로 진화중이며, 시스템이나 네트워크에 장애를 유발 하거나 좀비PC나 봇넷 확보를 위한 매체로서의 악용 등에 대한 우려도 높아지고 있는 실정이다.

이러한 현황에 대한 적절한 규제와 대응기술의 확보가 요원하다면, 정보 접근매체에 대한 신뢰성은 떨어질 것이며, 이용자들의 고충과 건전한 시장의 발전은 기대하기 어려울 것이다.

1. 스팸의 개념

우리나라는 영리목적의 광고성 정보에 대해 「정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 정보통신망법)」로 규제하고 있다. 국내에서는 동 법의 제50조부터 제50조의8을 위

반하여 영리목적의 광고성 정보를 전송 또는 게시하게 되면 '불법스팸'으로 분류한다. 특히 정보통신망법 개정안이 '14.11.29일부터 시행됨에 따라 모든 전송매체에 대해 사전 수신동의를 받도록 하는 등 수신자의 보호가 크게 강화되었다.

하지만 일반 이용자는 본인의 동의에 따라 수신된 광고성 정보도 수신자의 주관적 판단에 따라 스팸으로 인식하는 경우도 있기 때문에 법에서 규정하고 있는 스팸발생량과 이용자가 체감하는 스팸발생량간 차이가 발생할 수 있다.

법적 정의를 떠나 일반적으로 스팸은 이용자가 받기 싫은 문자나 전화, 이메일 등 전자적 형태의 정보를 모두 포괄하여 인식되고 있지만 각 국가별로 규제 방법에 따라 다르게 정의하고 있어 다소 차이가 있다. 각 국가의 정의를 통해 인식되는 스팸의 공통적인 특징은 아래와 같다.

〈표 1〉 스팸의 특징

특징	내용
전자 메시지	스팸은 전자적으로 발송되며 문자, 전화, 이메일, 인터넷 게시글, 소셜 네트워크 서비스 등 다양한 전자적 형태를 갖고 있음
원하지 않음	수신자가 동의를 했건 하지 않았건 현재 상태에서(광고의 수신 시점)는 수신을 원치 않는 경우가 많음
대량성 · 반복성	스팸은 대게 대량으로 반복적으로 발송됨

2. 전통스팸과 신종스팸의 비교

문자메시지 스팸, 이메일 스팸으로 크게 두 분류로 나뉘던 과거 스팸 대응정책을 바탕으로 현재의 스팸 유통현황과 스팸 대응이 필요한 채널들을 정리하여 보면 그 범위와 발송 현황의 괴리에 있어 큰 차이를 실감한다. 무료 문자앱의 등장으로 급격히 감소하는 SMS/MMS 사용량과 긴 시간동안 성숙하여 온 이메일 스팸의 차단 솔루션을 바탕으로 이용자들의 전통스팸에 대한 고충과 불편 역시, 이용률과 내성에 기반하여 큰 폭으로 감소추세에 있다 하겠다.

모바일 메신저, 웹팩스, 인터넷 커뮤니티 등과 같이 개인이 접근하는 의사소통 채널이 확대됨에 따라 스팸 발송 채널 역시 새로운 방식의 개발과 진화가 진행되고 있는 상황이다. 따라서 신종스팸에 대한 발송 체계 이해와 스팸 생태계 이해를 기반한 대응방안의 수립이 절실하다.

〈 표 2 〉 전통스팸 vs 신종스팸의 구분

구분	전통 스팸	신종 스팸
스팸발송 매체	• 휴대전화 문자메시지 / 이메일	• 모바일 메신저 / 그룹앱 / 웹팩스 / 게시판 / SNS / Push 메시지 / 광고 Popup
노출절차	• 문자함 확인 / 이메일함 확인	• 1:1채팅 / 그룹채팅 / APP설치 웹팩스 수신 / 인터넷 서핑
대응방안	• 휴대전화 스팸 신고 / 이메일 스팸 신고	• 신고방안 미비 (서비스 제공자 자율 대응 중심) • 게시판 스팸의 경우 무차별적 노출로 대응 애로 • 급격히 진화하는 발송기법으로 인해 대응정책의 후행성

무료 문자앱을 이용한 스팸 발송, 앱 설치 이후 Push 기반의 메시지 전송, 검색엔진 또는 유출정보 거래를 바탕으로 한 피싱, 웹 기반의 팩스 전송 시스템을 이용한 전단지 살포 등과 같이 매일 새롭게 등장하는 정보교환 채널이라면 어떠한 형태로라도 영리 목적에 악용되는 통로가 개발되고 있다.

게시판(댓글) 스팸

- 자동화 틀을 이용한 스팸 유포
- 홈페이지 게시판에 스팸 글 게시
- 주로 성인 · 도박 광고를 주제

인터넷 발송 팩스 스팸

- 팩스기기가 아닌 인터넷 팩스를 이용하여 스팸 유포
- 인터넷 팩스의 기능을 이용하여 대량 스팸을 발생
- 수신자는 불필요하게 종이를 낭비하게 됨

SNS 스팸

- 카카오톡, 라인 등의 모바일 메신저를 이용한 스팸 유포
- 메신저를 이용하여 광고 메시지를 전송
- 일반광고부터 피싱사기, 도박, 성인관련 메시지를 유포

스플로그(스팸+블로그)

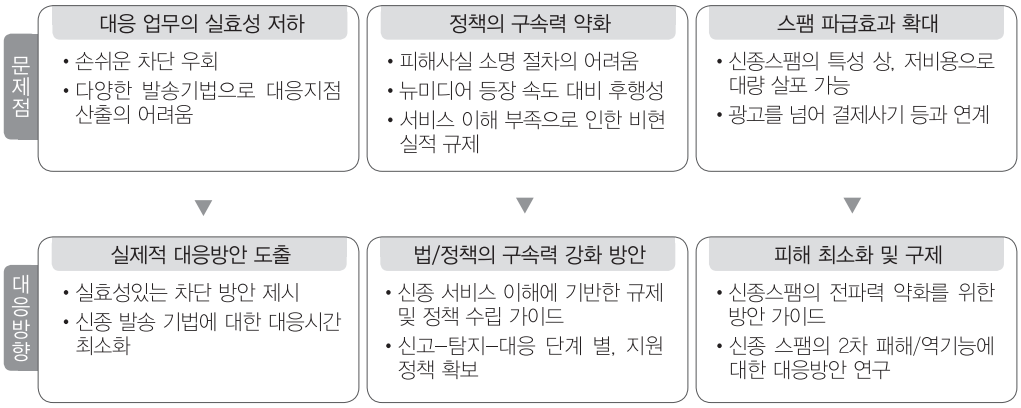
- 광고 또는 검색 엔진 링킹을 올리기 위한 목적
- 블로그 내에 작성된 필요치 않는 포스트나 코멘트 작성
- 검색엔진 신뢰도 감소, 사용자들간의 네트워크 문제 발생

3. 신종스팸 예방연구의 필요성

신종스팸의 예방과 대응방안 수립 시, 발송 기술 및 발송 서비스 환경에 대한 깊이 있는 이해와 제반 연구 없이는, 신종이라는 용어가 환기하듯 그 기반 기술과 지능화 된 유통 모델에 있어서 접근이 어려운 경우가 다수 이다.

단순 문자스팸과 달리 피해의 파급효과와 민생에 미치는 악영향을 고려하여 신종스팸에 대한 예방과 대응을 능동적으로 수행할 수 있는 지식기반 마련을 바탕으로, 지능적이고 피해

범위가 날로 확대되는 신종스팸의 발송체계와 스팸 생태계 이해에 기반한 대응기술 및 규제 방안 수립의 기반자료를 제시하고자 한다.



4. 신종스팸 관련 발송현황 분석

〈표 3〉 스팸 신고접수 현황

(단위 : 건)

구분		2009년	2010년	2011년	2012년	2013년
신고 접수 현황	이메일	28,921	31,923	46,345	39,740	30,948
	전화	35,587,648	70,337,379	53,086,687	32,593,519	21,745,303
	기타	3,377	4,709	34,057	80,803	61,434
	합계	35,619,946	70,374,011	53,167,089	32,714,062	21,837,685

휴대전화와 이메일 등을 통해 보내는 불법스팸이 줄고 있는 반면, 팩스나 게시판 등을 이용한 신종스팸은 크게 늘어난 것으로 나타났다. 한국인터넷진흥원 자료에 따르면 2013년 약 2천만 건의 스팸신고 수는 2012년 대비 약 1천만 건이 감소된 수치이다. 이렇듯 휴대전화 스팸신고 수는 2010년을 정점으로 매년 감소추세에 있다. 이메일 스팸은 2011년 높은 신고 수를 기록하였으나 2012년 39,740건으로 감소하였고 2013년에는 30,948건으로 2009년 수준으로 낮아졌다.

신종스팸으로 이슈가 되고 있는 유통경로는 '게시판(댓글) 스팸', '인터넷 발송 팩스 스팸', 'SNS 스팸'으로 〈표 3〉의 스팸 신고접수 현황에서 기타에 해당한다. SNS 스팸 신고건수는

최초 2011년 소폭 증가하는 추세이고, 팩스 스팸의 경우 2012년까지 증가 하다가 2013년에 다소 감소한 상황이다. 팩스 스팸, 게시판 스팸의 수는 감소하는 추세로 볼 수 있고, SNS의 경우 수치상으로는 증가하였지만 아직까진 그 증가폭이 작다.

이는 SNS 서비스 기반의 스팸 유통이 무시할만한 수준임을 시사한다고 보기는 어렵고, 범람하는 SNS 기반 스팸에 대한 적절한 신고 체계의 정비가 시급함을 방증한다고 해석하는 것이 바람직 할 것이다.

Ⅱ. 신종스팸의 부류와 피해사례 분석

1. 전송 방식에 따른 신종스팸의 분류

과거 동종의 단말간 이루어지던 영리목적의 광고 메시지 전달이 네트워크의 발달로 이종간의 통신 및 발달에 별다른 기술적 어려움이 없는 환경으로 진화하였다.

대표적인 전송방식을 분류하여 본다면 〈표 4〉와 같다.

〈표 4〉 채널별 스팸전송 유형

분류	내용
Web to Phone	• SMS, MMS 문자 메시지의 대량 발송 서비스 • 모바일 무료 문자앱의 PC 또는 Web 기반의 부가 서비스
Phone to Phone	• 전통적인 방식의 SMS, MMS 전송 서비스 • 동일 앱 및 서비스에 기반한 단말 간의 메시지 전송 서비스 • 게임 등과 같은 초대 권유가 가능한 서비스의 초대 메시지
PC to PC	• 모바일 기기 확산 이전의 전통적인 메신저 서비스 • 이메일, 인터넷 팩스 등과 같은 단말 간의 메시지 전송 서비스
Browser 환경 제어 및 Popup	• 시작페이지 고정 등을 이용한 광고노출 • 페이지 열람 시, 광고 팝업
프로그램 및 앱 기반 Push 알람	• 프로그램 설치 시, 팝업 기반의 무작위의 배너광고 표출
동기화 서비스 기반의 스팸	• 일정동기화 서비스 기반의 일정알람 서비스

일정 자동 동기화 기반 스팸의 사례

– 스마트폰의 유용한 앱 중 하나인 일정관리 혹은 캘린더 앱은 구글 캘린더 등의 서비스와 연동되어 사용된다. 일명 '구글 캘린더 스팸'으로 칭하는 동기화 기반 스팸은, 구글이 제공하는 '메일을 통한 일정 공유'기능을 기반으로 한다. 스팸 발송자는 광고를 원하는 내용을 특정 날짜에 일정으로 생성한 후, 무작위로 구글 메일 서비스를 이용하는 이용자들에게 초청 이메일을 보낸다. 초청 이메일을 수신한 수신자는 캘린더에 자동으로 수신된 스팸광고의 일정이 추가된다. 지인간 일정을 자동으로 공유할 수 있도록 한 기능을 악용한 수법이다. 구글 캘린더와 연동하는 일정관리 앱이라면, 어떤 앱이든 스팸의 적용이 가능하다. 일정 공유를 통해 발송되는 스팸의 내용은 성인, 도박, 대출 광고까지 다양하다.

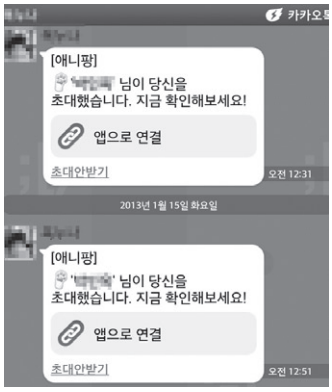
– 일정 자동 동기화 기반 스팸의 등록 절차

– 스팸광고가 일정으로 자동 등록되는 것을 방지하는 방법으로는, 구글 캘린더의 설정화면에서, 설정을 누르고 아래쪽에 있는 '내 캘린더에 초대장 자동 추가' 항목을 '아니요, 회신한 초대장만 표시합니다'로 선택, 저장하면 된다. 하지만, 구글 계정을 처음 생성 시 기본 설정이 '자동추가'로 되어있기 때문에 직접 '회신한 초대장만을 표시합니다'로 설정하지 않은 사용자들은 스팸광고에 노출되어 있다.

2. 내용에 따른 신종스팸의 분류

1) 모바일 게임 등의 신종 비즈니스 모델

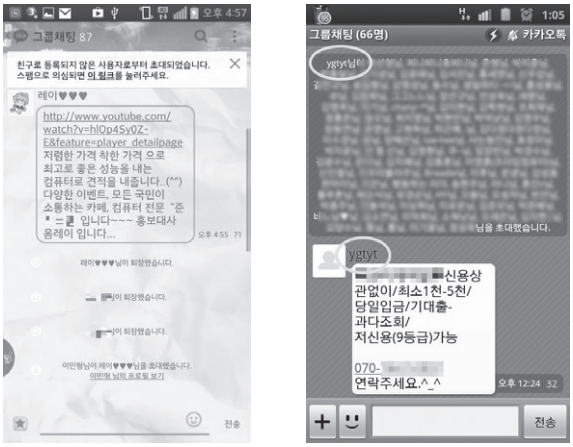
모바일 메신저와 연동되는 게임의 경우, 게임 상에서 사용자의 친구를 초대하면 아이템이나 포인트 등에 대한 다양한 혜택을 받을 수 있다. 이때, 사용자가 지인에게 게임에 초대하는 메시지를 발송하게 된다. 게임 광고 메시지를 발송함으로써 게임유저는 혜택을 얻지만, 게임을 하지 않는 수신자의 경우는 이러한 광고 메시지로 인하여 고충을 겪는다.



[그림 3] 게임초대 메세지

2) 그룹채팅방 스팸

스팸 발송대상자들의 연락처를 등록한 모바일기기에서 메신저앱을 동기화한 후, 메신저에 등록된 사용자들을 대상으로 그룹채팅방을 생성하여 스팸 메시지를 발송한다. 사용자는 원치 않는 스팸 메시지를 수신해야 한다는 점과 불특정 다수에게 사용자의 아이디가 노출되는 상황이 발생한다.



[그림 4] 그룹채팅방 스팸

3) 커뮤니티 앱(밴드/카카오스토리/카카오아지트)의 친구 초대

사용자의 정보에 대해서 개방적인 페이스북과는 성격이 다른 폐쇄형 SNS가 유행이다. 카카오아지트 또는 그룹, 네이버 밴드 같은 경우, 공통관심사를 가진 사람들 간에 채팅, 일정공유, 사진공유, 투표 등의 기능을 제공한다. 카카오스토리는 친구들 간에 사진을 공유하고, 공감대를 형성하는 대표적인 커뮤니티 서비스 중 하나이다.

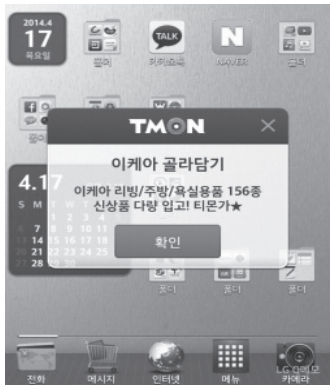
커뮤니티 앱을 사용하는 목적은 업무상 필요, 학교, 친목 도모 등과 같은 다양한 이유로 사용되고 있지만, 판매나 홍보를 목적으로 만들어지기도 한다. 이러한 광고 목적의 커뮤니티들은 광고용 그룹을 생성하고, 해당 그룹에 대한 초대장을 대량으로 배포하여 사용자의 가입을 유도한다.

[그림 5] 커뮤니티 앱 스팸

4) 앱 설치 후, Push 알람을 빙자한 광고

대다수의 모바일앱은 실행과정에서 발생하거나 수신하는 정보를 사용자에게 제공하기 위해서 Push 알람 기능을 제공한다.

그러나 사용자에게 유의미한 정보가 아닌, Push 알람을 통해 불특정 광고를 노출시키는 기법이 유행한다. 이처럼 Push 알람을 통해 광고를 노출하는 앱이 다수 설치된 경우, 앱 당 하나의 Push 알람만 수신한다 하더라도 사용자는 하루에 수십 건의 광고 메시지로 인한 피해에 노출된다.



[그림 6] PUSH를 활용한 스팸

5) 스미싱 기반의 소액결제 사기와 개인정보 유출

스미싱(SMShing)문자를 발송하여 소액결제를 유도하거나 개인정보를 훔쳐가는 수법의 범죄가 날로 기승을 부리고 있다. 모바일 메신저 앱 상에서도 스미싱과 동일한 수법의 문자 메시지가 수신되고 있어 피해가 확산되고 있다.

이를 스팸으로 인한 피해 범주에 포함하여야 하는가에 대해서는 논의가 진행중이지만, 중요한 사실은 불특정 피해자에게 대량으로 발송되는 메시지에 기반 한다는 속성으로 인하여 스팸의 발송기법과 관련 유통환경과 다름이 없어 환기가 필요한 실정이다.

특히, 과거 SMS/MMS 문자 기반의 발송이 스미싱 문자의 주류였다면, 현재는 모바일 메신저앱으로의 범위가 확대되고 있다.

모바일 메신저앱 환경은 SMS 송수신 환경과 달리, 연락처에 등록된 지인들과의 관계를 기반으로 형성되기 때문에, 결혼식이나 돌잔치 등을 사칭한 메시지를 수신 하는 경우 악의적인 목적의 메시지일 수 있다는 의심을 쉽게 덜고, 부주의하게 열람하게 되는 경우가 잦아 보다 쉽게 피해에 노출되는 경향이 있다.

일반 SMS기반의 스미싱 문자 내 포함되는 링크와 마찬가지로, 모바일 메신저 앱을 통해 전송된 링크를 클릭하게 되면, 소액결제를 유도하거나 개인정보 입력을 요구하는 페이지로 유도하여 피해가 발생할 수 있다.

일부 모바일 메시지 앱에서는 친구가 아닌 사용자로부터 링크가 포함된 메시지를 수신하였을 경우, 해당 링크 선택 시 연결 여부를 재확인하는 팝업창이 활성화되고, 사용자에게 링

[그림 7] 모바일 메신저에서의 스미싱

크 연결의 위험성에 대한 경고 및 링크 연결을 재확인하는 보호조치를 제공하기도 한다. 또한 사용자의 프로필 사진 부분에, 해당 사용자가 가입한 국가의 국기를 표시하여 스미싱 문자에 의한 피해를 예방하는 조치를 마련하는 경우도 있다.

Ⅲ. 신종스팸의 주요 발송기술 현황

1. 모바일 메신저 스팸 발송기

SMS 등과 같은 문자메시지와 달리 TCP/IP 기반의 발송 채널을 지원하는 게시판, 카페, 포탈 쪽지, 모바일 메신저앱의 경우 비교적 손쉬운 발송기 구현이 가능하며, 이의 거래 역시 활발한 실정이다.

발송기의 특성은 무료 문자앱 서비스 제공자 및 포탈에서의 차단 정책 우회를 위하여 인증 및 발송속도, 발송유형 등을 설정하는 등의 부가장치를 구비하여 배포된다는 것이다.

[그림 8] 스팸발송기를 이용한 모바일 메신저 스팸전송

2. 기 생성 계정의 거래

신종 서비스의 이용에 필수적인 계정에 대해 스팸 배포대상을 수집하는 방법으로 다른 사람이 보유한 정보를 구매하여 적용할 수 있다. 국내 아이템 거래사이트를 통해서 신규 인기 서비스의 계정이 주요 현금 거래품목으로 주목받고 있다.

계정 판매를 위해 계정이 보유한 아이템 목록과 추가되어 있는 등록된 친구의 수 등의 정보를 제공한다. 이미 거래 시장이 형성되어 거래 방법이 일반화되고 계정들을 생성하여 친구 관계에 있어 일정 수준으로 만든 다음에 판매하는 판매자들이 생겨나고 있다.

생성 계정의 반복 판매로 인해, 친구로 등록된 사람들은 게임 메시지, 기타 스팸 메시지에 의해 상당한 피해를 입게 되는 것이 일반적이다.

3. 무작위 단말번호 생성

모바일 메신저 앱은 연락처에 등록된 전화번호를 이용하여 친구등록이 가능하다. 연락처를 이용한 등록방법의 종류는 2가지가 있는데 사용자가 직접 입력하는 방법이 있고 연락처가 저장되어 있으면 동기화 기능을 통해 자동으로 친구목록을 생성하는 방법이 있다.

스팸 발송자는 활성화되어 있는 전화번호를 수집하지 않고 랜덤으로 전화번호를 발생시켜

[그림 9] 연락처 생성 과정

연락처에 등록한 뒤 모바일 메신저앱의 동기화 기능을 통해서 스팸 수신 대상자로 등록이 가능하다.

해당 기능을 지원하는 앱들도 있어 누구나 손쉽게 랜덤번호를 생성하여 모바일 메신저앱의 친구 대상자등록이 가능하다. 다음은 카톡 친구 랜덤이라는 카톡 친구 생성기 앱의 연락처 생성 과정이다.

4. 개인정보 DB 거래

랜덤 발생기는 정보를 스마트폰에 저장하게 되면 해당 내용으로 친구 목록이 생성이 되고 스팸 수신 대상 목록을 생성할 수 있다. 이와 마찬가지로 인터넷으로 개인 정보 DB를 구매하여 전화번호만 발췌하여 스마트폰에 대량으로 전화번호를 입력하고 해당정보를 모바일 메신저 앱에서 동기화하여 사용자 정보를 입력하여 스팸 수신 대상으로 만들 수 있다.

5. 안드로이드 에뮬레이터 기반 발송기

안드로이드 에뮬레이터를 이용하여 발송환경을 구축하는 사례가 다수이다. 개발 환경 이용 제한과 같은 기술적 보호조치를 해제한 후 UUID 변조 및 준전화 서비스 등을 연계하여 스팸 발송 환경으로 이용한다.

[그림 10] 안드로이드 스팸발송 에뮬레이터

6. 구글보이스 등과 같은 준전화 서비스

문자 메시지를 무료로 주고받는 앱도 있지만 전화를 무료로 이용할 수도 있다. 추가로 전화 요금은 들지 않고 소유자가 보유한 데이터 사용량를 소모하거나 WIFI망이라면 무료로 통화를 할 수 있다. 긴 시간 통화를 하거나 해외로 통화를 하게 될 경우 저렴하게 이용할 수 있어 많은 사람들이 사용하고 있는 추세이다.

〈표〉 준전화 서비스앱 종류 및 기능

제품명	설명
 구글 보이스	• 구글의 행아웃 앱과 연동하여 사용가능 • 전화 통화 무료 • VoIP서비스가 아님, 유/무선인터넷으로도 이용이 가능 • 구글 보이스 서비스를 사용하기 위해서는 구글 계정이 필요 • 미국 내에 다른 전화번호가 있어야 가상 번호를 부여받을 수 있음 • 미국 내에 다른 전화번호가 없다면 미국에서 사용될 수 있는 가상 전화번호를 부여 받은 다음 구글 보이스를 이용할 수 있음 • 한국에서는 구글 보이스 서비스 가입이 불가 • 발급 받은 가상 전화번호를 한국에서 사용가능, 구글 보이스의 가상 번호로 걸려오는 전화를 한국에서 받을 수 있음 • 발급된 가상 전화번호를 이용하여 카카오톡앱을 가입할 경우, 가상 번호를 인식하여 해당 카카오톡 계정이 정지당할 수 있고 계정 삭제가 불가함
 텍스트플러스	• 동일 앱 사용자의 경우 문자 및 통화가능 • 무료 메시지 전송 • 월 정액요금 $2.99로 미국과 캐나다에서 무제한 통화 기능 제공 • 미국과 캐나다의 휴대전화로 무료 문자 및 SMS 메시지 보내기 • 국제 통화 기능 • 문자메시지, SMS, 전화통화를 스마트폰이 아닌 태플릿에서 WIFI망을 통해 사용 가능 • WiFi로 HD지원, 3G, 4G망 지원
 핑거	• 구글 보이스 가입자를 위하여 인증 번호로 사용 가능 • 한국을 제외한 일부 국가(미국 등)에서만 무료서비스 제공 • 미국 전화번호 무료발급 • 무제한 무료 문자 서비스 • 텍스트프리 사용자 간 무료 통화 서비스 • 인터넷 웹을 통해 문자 무료 송수신 • 앱이 OFF 상태여도 수신 가능
 밀리톡	• 아이팟, 아이폰 아이패드만 사용가능 • 밀리톡 계정을 만들거나 SNS 계정을 이용하여 로그인이 가능함(트위터, 페이스북) • 문자 메시지 전송 가능 • 최초 가입시 $0.99로 크레딧을 무료통화(약 15분) 서비스 제공 • 통화에 의한 사용요금 확인 기능 • 인증 시 VPN을 사용하지 않아도 됨

일부 준전화 서비스앱의 경우 나라를 지정하여 가상으로 전화번호를 부여받아 사용할 수 있다. 한마디로 국내에서 새로운 전화번호를 발급받지 않아도 가상 전화번호를 이용하여 모바일 메신저앱의 휴대전화번호 기반의 인증을 받을 수 있으며 익명으로 모바일 메신저앱을 사용할 수 있어 스팸 발송도구로 사용될 수 있게 된다.

모바일 메신저앱의 휴대전화번호 인증을 받을 수 있도록 가상번호를 발급 할 수 있는 서비스는 대표적으로 앞서 설명한 구글보이스, 텍스트플러스, 핑거, 밀리톡 등이 있다.

Ⅳ. 신종스팸 관련 대응기술 현황

신종스팸의 기술적 특성과 다양성으로 인하여, 유통 초기 일원화 된 대응방법 모색과 정책 방향을 설정하기란 대단히 난해한 일이라 할 수 있다. 특히, 시장의 발달과 성장의 단초를 과도하게 제한할 수 있는 위험성이 있어 자율적 대응 노력과 내부규정 수립을 우선적으로 권고, 수립 후 지속적인 대응정책 개발이 바람직하겠다. 현재 운영중인 신종스팸에 대한 대응 기술의 현황은 다음과 같다.

1. 한국인터넷진흥원의 매체 별, 신고 접수

■ **한국인터넷진흥원 – 불법스팸대응센터(HTTP://SPAM.KISA.OR.KR)**

- 한국인터넷진흥원에는 스팸 신고센터를 운영하고 있으며, 스팸에 대한 피해사실이 있을 경우 해당 웹페이지에서 관련 사항을 포함하여 스팸신고서를 작성하면 된다. 만약 허위로 신고하였을 경우, 그로인해 발생하는 모든 민 · 형사상 책임을 신고인이 지게 되어 있다.
- KISA 불법스팸대응센터는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제52조 제3항 제10호에 따른 스팸 민원 고충상담 및 민원처리를 위해 아래의 개인정보를 수집 · 이용하며, 수집된 개인정보는 신고 처리(수사의뢰, 행정처분 등)를 위해 중앙 전파관리소, 검찰, 경찰, 사업자에게 제공될 수 있다. 수집한 개인정보는 개인정보처 리방침에 따라 3년간 안전하게 관리된 후 파기된다.

※ 개인정보 수집 항목 – 성명, 이메일, 전화번호(휴대전화번호), 발신 전화번호

2. 모바일 메신저앱 사업자의 대응 정책

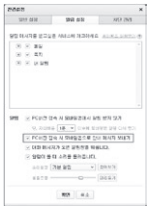
알지 못하는 사람으로부터 메시지를 수신한 경우, 대화화면에서 해당 메시지를 발송한 사용자를 '추가' 또는 '차단'하거나, '스팸신고'할 수 있는 기능을 제공하며, 동일 문자 메시지를 수분내에 대량 발송하는 경우 이용자 계정의 정지 및 메시지 전송 불가 등의 조치를 취한다.

[그림 11] 모바일메신저의 스팸신고 기능

〈표 6〉 메신저 서비스 별 스팸 차단/신고 기능 현황 비교

구 분		카카오톡	마이피플	라인	네이트온
화이트리스트 기능		×	×	○	○
블랙리스트 (차단)기능	친구 목록	○	×	○	○
	대화 창	모르는 상대로부터 메시지 수신시에만 가능			
스팸신고기능		모르는 상대로부터 메시지 수신시에만 가능			×
아이디 검색 허용 여부		○	○	○	○
자동 친구추천 여부		○	○	○	○

〈표 7〉 모바일 메신저앱 서비스별 주요 보안정책 및 기능 현황

구 분	카카오톡	마이피플	라인	네이트온
PC 버전 로그인 시 인증 기능	※ 모바일 메신저로 전송된 인증번호 입력을 통해 로그인할 PC를 인증			
				×
PC 버전 로그인 시 알림 기능	○	○	○	○
			×	×
PC 버전 로그인 정보 확인 기능	○	○	○	○
비밀번호 입력 오류 횟수 제한 여부	×	×	○ (5회) ※ QR코드 인증방식	○ (5회) ※ CAPTCHA 방식
PC 버전 원격 로그아웃 기능	○	○	○	○
				×
PC 버전 잠금모드 기능	○	×	×	○
보안봇 주소록 백업 기능	×	○	×	×
보안봇 위치 추적 기능	×		×	×
보안관련 정보 제공 기능	×	○	○	×

3. 스팸전화 차단앱

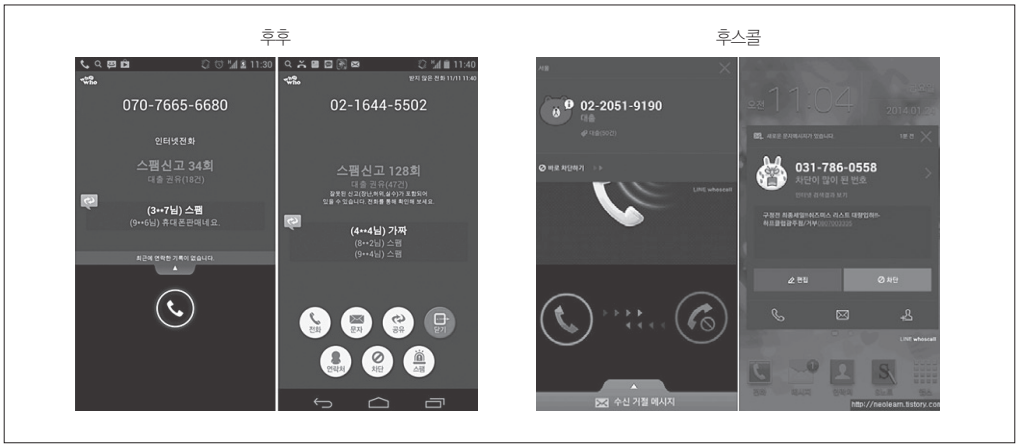
이메일, 문자 메시지, 팩스로 전달되는 문서를 통한 스팸 외에 고정적으로 불편을 겪어왔던 스팸중 하나가 바로 스팸전화이다. 포털, 금융, 통신사의 개인정보 유출 사고로 인하여, 상당수 개인의 유선, 무선전화 정보들이 노출되어 있는 상태이다.

일상생활 속에서 알지 못하는 번호로부터 수신하는 전화는 업무나 개인적으로 나에게 연락하고자 하는 사람일 수 있지만, 결혼중매업체, 카드가입 권유, 보험가입 권유, 휴대폰기기 변경 권유전화까지 상품에 대한 마케팅을 목적으로 걸려온 전화일 가능성 또한 높다. 이러한 스팸 전화로 인해 흩뜨려진 집중력은 업무의 지연을 가져온다.

알지 못하는 번호로부터 수신된 전화는, 업무상 나에게 걸려온 전화인지, 스팸전화인지 받아야 될지 말아야할지 고민하게 된다. 그래서 이러한 스팸전화에 대한 해결책 중 하나로 걸려온 전화가 어떤 전화번호인지 먼저 알고 스팸전화로 확인되었을 경우 받지 않거나 차단하는 기능을 지원하는 앱을 사용할 수 있다. 종류로는 후후, 뭐야이번호, 더 콜 스팸 전화번호, 누구세요, 후잇, 후스콜 등이 있다.

■ **스팸전화 차단 앱의 기능**

- 앱에서 지원하는 DB 스팸전화번호의 다운로드/업데이트(오프라인 이용가능)
- 전화 수신 시, 해당 발신번호에 대한 스팸 정보, 일반 업체 정보등을 제공
- 발신번호가 스팸일 경우, 차단여부, 스팸전화번호에 대한 메모 기능 제공
- 수집한 스팸전화번호 정보 공유기능 제공



[그림 12] 스팸전화 차단 앱

[그림 13] 통신사제공 스팸전화 차단 앱

Ⅴ. 결론

주요 스팸발생 채널인 휴대전화 및 이메일에 대한 스팸대응 정책은 스팸발송 경로 및 스팸 신고 분석을 통해 마련되어 왔다. 예를 들어 휴대전화 스팸은 인터넷 문자발송이나 휴대전화 문자발송과 같은 '발송 환경', 이동통신망이나 PSTN망과 같은 '발송 단'과 '수신 단', 스팸문자를 받게 되는 휴대전화와 같은 '수신 환경' 등 단계별로 스팸발생 취약점을 개선 및 보완해 왔다. 하지만 무엇보다 중요한 것은 스팸 동향의 분석 및 대응에 필요한 정보 수집이 선행되어야 한다는 점이다.

'13년 말부터 스팸문자가 수신단에서 문자 기반의 스팸문차 필터링 서비스에 차단되지 않도록 광고내용을 그림파일로 전송하는 이미지 스팸이 증가하기 시작했다. 스팸대응팀은 KISA에 접수된 신고 건에서 이미지 스팸의 증가추세를 확인한 뒤 이를 필터링 할 수 있도록 이통사와 대응 체계를 구축 하고 있고, 이르면 올해 말 이미지 스팸 차단 서비스가 일부 통신사에서 개시될 예정이다.

이와 같이 스팸정보를 분석하여 최신 스팸트렌드에 선제적 대응을 하기 위해서는 KISA와 사업자간 긴밀한 공조가 중요하다. KISA – 이통사 – 휴대전화 제조사는 '14.5월부터 출시되는 휴대전화(스마트폰)에 간편신고 기능이 탑재되도록 하여 휴대전화 스팸대응을 위한 스팸

신고 정보를 수집 및 분석 할 수 있는 체계를 정비하였다.

신종스팸 대응의 출발점도 동일하다. 신종스팸은 지금도 불법스팸 대응센터 홈페이지에서 신고가 가능하지만 그 절차가 번거로워 KISA에서 신고체계 정비를 추진하고 있다. 그러나 일부에서는 인터넷 서비스의 특성상 서비스 품질 유지와 고객 이탈 방지를 위한 사업자의 자발적인 스팸 관리 노력마만으로도 스팸 대응에 충분하기 때문에 KISA와의 스팸정보 공유는 불필요하다는 주장을 제기하기도 한다. 이같은 주장은 특정 모바일 서비스에서 스팸이 다수 발생하게 되면 해당 이용자가 다른 모바일 서비스로 이동하게 될 터이니 일응 타당한 점이 있다. 하지만 특정 서비스에서 발생하는 스팸동향을 사전에 파악하고 대응방법을 마련하기 위해서는 스팸정보 확보가 선행되어야 하고 효과적인 대응을 위해 사업자와 긴밀한 협조가 요구된다.

스팸정보는 스팸신고를 통해 확보될 수 있어 카카오톡 등 KISA 및 인터넷 사업자간 스팸 신고 정보를 공유할 수 있는 채널이 속히 마련될 필요가 있다. 수집된 정보를 토대로 관련 사업자와 함께 신속하게 스팸유통을 차단할 수 있는 다양한 논의가 가능할 것이다. 최근 국내에 나타난 구글 캘린더 스팸은 물론 다양한 스팸정보가 KISA와 공유 된다면, 이를 분석하여 스팸대응에 효과적인 기술 및 정책을 마련할 수 있을 것이다.

참고문헌

언론보도

뉴데일리경제 (2014). 쏟아지는 스팸, 고객이 직접 막아?

뉴스토마토 (2014). LG유플러스, 12월부터 이미지 스팸도 차단

디지털데일리 (2010). KISA, 아태지역 스팸대응 공조 강화

베타뉴스 (2014). '통장' 빌려주면 사례비로 500만 원 주겠다는 신종스팸 등장

보안뉴스 (2006). 정통부-KISA, 불법스팸 처벌규정 이렇다

세계일보 (2014). 신고된 스팸문자만 3년간 1억 건"

아시아경제 (2014). 오늘 스케줄이 '도박?'…스팸의 진화, 이제 '스팸 일정'까지

정책브리핑 (2014). "이메일, 휴대전화 문자 등에 광고 전송 시 반드시 수신동의를 받아야"

조선비즈 (2013). '스팸톡'된 카카오톡…대책 마련 시급

한국일보 (2014). "법정 출두" 신종스팸메일 기능

ITWORD (2012). 스마트폰을 스팸 봇넷으로 이용한 신종 안드로이드 악성코드 발견

NET SECURITY (2014). Android HijackRAT poised to hit mobile banking users

ZDNET Korea (2012). 개인 정보 유출사고 후폭풍…이용자들 '몸살'

ZDNET Korea (2014). 글자 뒤집힌 신종스팸메일 주의보

연구보고서

방송통신위원회 (2013). 사업자를 위한 불법스팸 방지 안내서

방송통신위원회 (2011). 스팸방지 종합 대책

방송통신위원회 (2011). 이용자를 위한 불법스팸안내서

방송통신위원회 (2010). Smart Korea 强國 도약을 위한 스마트 모바일 시큐리티 종합계획

방송통신위원회 네트워크정보보호팀 (2011). 스마트 모바일 시큐리티 정책 방향

한국정보통신기술협회 (2009). 모바일 플랫폼 표준화 동향 및 향후 전망

한국정보통신기술협회 (2013). 스미싱 사고에 대한 대응지침

주요 논문/서적

Bruce C Brown (2007). The Complete Guide to E-mail Marketing: How to Create Successful, Spam-Free Campaigns to Reach Your Target Audience and Increase Sales

Guido Schryen (2010). Anti-Spam Measures: Analysis and Design

Himanshu Dwivedi (2010). Mobile Application Security

Ken Dunham (2008). Mobile Malware Attacks and Defense

Paul Wholfe (2004). Anti-Spam Tool Kit

U.S. Government (2011). Consumer Guide to Computer Security: Fight Back Against Identity Theft, Malware, Hackers, Spyware, Spam, Botnets, Phishing - Online Privacy - Wireless, Laptop, Hotspot Security