Information Systems Review
Vol. 20, No. 1 March 2018
http://dx.doi.org/10.14329/isr.2018.20.1.061

기업의 스마트폰 메시지에 대한 고객 신뢰도에 관한 연구: 메시지 정교화 모델을 중심으로

The Effect of Message Completeness and Leakage Cues on the Credibility of Mobile Promotion Messages

전 현 준 (Hyun Jun Jeon) 연세대학교 경영학과
최 진 선 (Jin Seon Choe) 연세대학교 경영학과
손 재 열 (Jai-Yeol Son) 연세대학교 경영학과, 교신저자

요 약

지금까지 스마트폰 문자 메시지와 관련한 연구는 보안 및 프라이버시 우려 측면에서 제한적으로 이루어져 왔다. 그러나 기업들이 소비자를 대상으로 프로모션 메시지를 전달할 때 어떤 메시지가 효과적인지 규명하는 시도는 많지 않았다. 본 연구는 스마트폰의 메시지 신뢰도를 저하하는 신호를 정교화 가능성 모델에 적용하여 분석하였다. 메시지의 신호는 내용 상의 신호와 수신자가 세심한 검토 없이 의사결정을 하도록 하는 누설 신호(맞춤법 및 특수문자, 축약 링크, 신뢰할 수 없는 발신자 등)로 나눌 수 있다. 이 중 내용 상의 신호에 조절효과를 주는 요소는 맥락화로 메시지가 자신과 상관있다고 느끼는 정도(관여도)이다. 메시지의 신호가 스마트폰 사용자의 메시지 신뢰도에 주는 영향을 검증하기 위해 모바일에서 쿠폰발행 메시지를 받는 시나리오를 바탕으로 166명 대상의 서베이 실험을 진행하였다. 분석 결과, 누설 신호는 유의한 수준으로 신뢰도에 부정적 영향을 주었고, 내용 상의 결함은 근소한 수준에서 부정적 영향을 주었다. 주목할 점은 고맥락화 메시지에 내용 상의 결함이 있으면 유의한 수준으로 신뢰도에 부정적 영향을 주었으나, 저맥락화된 메시지의 경우에는 신뢰도에 영향을 주지 않았으며, 메시지에 누설 신호가 있으면 맥락화 정도와 상관없이 신뢰도가 저하되었다는 것이다. 이는 기업들이 모바일을 통한 프로모션을 진행할 때 관여도가 높은 상품을 골라 고객 맞춤형으로 문자 메시지를 작성하고, 메시지에는 내용 상의 결함이 없도록 하는 것이 중요하다는 시사점을 제공한다.

키워드 : 메시지 신뢰도, 스마트폰, 정교화 가능성 모델, 누설 신호, 내용 상의 신호, 관여도, 맥락화

Ⅰ. 서 론

산업 내 경쟁이 치열해지고 있는 가운데 바야흐로 소비자의 주목을 끌어 상품 선택의 가능성을 높이는 주목경제(attention economy)의 시대가 도래하였다. 그러나 역설적이게도 소비자들이 수많

은 정보와 자극에 노출되면서 오히려 기업이 제공하는 메시지에 대한 관심은 떨어지고 있는 실정이다. 특히 기업이 스마트폰을 활용해 상품 홍보 메시지를 발송하는 경우, 소비자들은 이러한 메시지를 스미싱(smishing)이라는 새로운 형태의 피싱(phishing) 범죄로 받아들이기도 한다. 피싱은 본래 개인정보(private data)와 낚시(fishing)의 합성어에서 유래한 것으로, 보통 금융기관 또는 공공기관을 가장하여 전화나 전자 메일 등의 채널을 이용해 사용자들의 금융정보나 개인정보를 빼가는 수법을 의미한다(Abu-Nimeh *et al*., 2007). 과거에는 전화로 접근하여 일회성으로 범죄를 저지르는 방식인 보이스 피싱(voice phishing)이 횡행하였으나, 최근 들어 그 수법이 점차 다양해지고 있다. 피싱에서 파생되어 새롭게 출현한 범죄 방식 중 스미싱은 문자메시지(SMS: short message service)를 이용해 피해자들에게 접근하는 방식이다. 문자메시지 내에 기재된 인터넷 주소를 클릭하면 스마트폰에 악성 코드가 설치되고, 피해자가 미처 인지하지 못하는 사이에 소액 결제가 이루어지거나 스마트폰 내에 저장되어 있는 개인정보가 유출되기도 한다. 기존의 피싱 공격 방식과 비교해 볼 때, 스미싱은 스마트폰에 악성코드를 설치하기 때문에 피해를 인지하기 전까지 여러 차례 문제가 발생할 수 있다는 점에서 그 심각성이 크다.

사실 스미싱 등의 피싱은 컴퓨터 공학적인 문제, 즉 기술적인 문제라기보다는 인간의 심리와 관련하여 사용자의 부주의를 교묘히 악용하는 사회공학적인 문제에 가깝다. 실제로 보안에 있어 가장 취약한 요소로 손꼽히는 것이 '부주의한 직원'인데 개인정보와 같이 민감한 정보를 외부로 유출시키거나 특정 시스템을 타깃으로 삼아 악성 프로그램에 감염시키는 등 시스템의 정보 보증을 낮추는데 직원의 부주의가 큰 역할을 한다(EY.com, 2015). 이와 같이 피싱 공격자는 주로 부주의와 같은 수신자의 심리적 요인을 이용해 공격을 감행한다.

메시지 수신자는 심리적 요인으로 피싱의 피해를 입을 수도 있지만, 반대로 이로 인해 피싱 또는 유사 공격을 눈치 채기도 한다. 예를 들어, 수신자가 메시지를 전달받았을 때 메시지 상의 파편적 단서를 통해 피싱 공격을 인지할 수 있다. 수신자가 메시지 상에서 알아차릴 수 있는 파편적 단서를 누설 신호(leakage cue)라고 하는데 심리적인 작용을 통해 수신자로 하여금 받은 메시지가 피싱 메시지임을 눈치 챌 수 있게 한다. 여기서 언급된 누설 신호는 메시지 발신자가 의도하지 않았음에도 불구하고, 피싱 메시지로서의 기만적 본성을 우연히 노출하게 하는 신호(Harrison *et al*., 2016)로 정의된다. 만약 기업들이 상품의 홍보나 기업 캠페인과 관련한 SMS 메시지를 소비자에게 보낼 때, 수신자가 누설 신호로 간주할 만한 요소가 메시지 내에 포함되어 있다면, 이에 대한 수신자의 신뢰도가 감소할 것이고 커뮤니케이션의 효율 또한 떨어질 수 있다.

한국은 2016년 3월 기준 성인의 약 91%가 스마트폰을 보유하고 있는 국가이다. 이 같은 수치는 세계 주요 50개국의 스마트폰 보급률인 69.5%를 훨씬 상회하는 결과이다(박세정, 2016). 또한 국내에서 모바일을 통한 소비도 활발히 이루어지고 있다. 모바일 쇼핑의 규모는 매년 10% 이상 증가해 왔고, 2016년 기준 전자상거래 전체 거래액인 64조 9,134억 원의 절반을 넘는 수준인 34조 7,031억 원에 육박했다. 이는 전체 전자상거래 시장의 약 53.4%에 해당하는 수치이다(홍종선, 2017). 이미 스마트폰이라는 플랫폼이 소비자들에게 가장 많이 활용되는 전자상거래 도구가 된 것이다. 따라서 기업이 국내 소비자들을 대상으로 상품의 홍보나 프로모션을 위해 스마트폰 메시지를 활용하는 것은 고객 접점을 확대할 수 있다는 점에서 바람직하다고 할 수 있다. 그러나 국내에서는 스마트폰을 활용한 서비스에 있어 보안성에 대한 규제가 다른 어떤 요소들보다 엄격히 이루어져 왔으며, 소비자들 역시 이와 마찬가지로 개인 정보보호와 해킹에 대한 우려가 큰 편이다(정기석, 2013). 이 같은 상황을 감안하여 볼 때, 보안에 대한 불안요소를 경감시키고 소비자로 하여금 메시지의 신뢰

도를 높게 인지하도록 하는 방안을 마련하는 것은 기업의 성과를 제고하는 방안이 될 것이다.

지금까지의 연구는 주로 소비자들이 메시지에 대해 지각하는 개인정보 보안에 대한 우려(concern) 측면에 초점을 맞춘 것이 주를 이루었다(Castañeda and Montoro, 2007; Sutanto *et al*., 2013; Wirtz *et al*., 2007; Zhou, 2011). 그러나 본 연구는 기업의 홍보 메시지의 신뢰도를 높이는 방안에 관련한 새로운 관점을 제시하는데 목적을 두고, 메시지 신뢰도에 영향을 주는 주요 요인에 대해 살펴보고자 한다.

이러한 점에 착안하여 본 연구는 스마트폰 환경에서 메시지 신뢰도를 저하하는 신호에 대해 심리학의 정교화 가능성 모델(ELM: elaboration likelihood model)의 프레임워크를 바탕으로 실증적 분석 결과를 제시하고자 한다. 이를 위해, 먼저 정교화 가능성 모델과 이를 스미싱 및 사회공학적 공격의 컨텍스트에 적용한 메시지의 두 가지 신호를 다룬 선행 연구들을 검토하고, 스마트폰 메시지 상에서 이 두 가지 신호가 어떻게 메시지 신뢰도에 영향을 미치는지에 관해 이론적인 논리를 전개하였다. 특히 메시지에 담긴 홍보 콘텐츠와 수신자 사이의 관련성의 정도가 다를 때 메시지 신호가 메시지 신뢰도에 주는 영향도 함께 달라지는지를 관여도(involvement)의 측면에서 관찰하였다. 더불어 메시지의 신뢰도는 메시지에서 제시된 행동을 하고자 하는 의도에 어떠한 영향을 미치는지 설명하는 구조 모형을 개발하였다. 마지막으로 서베이 실험을 활용한 실증분석을 통해 연구모델을 기반으로 제안된 가설을 검증하였으며, 이를 통해 학문적 및 실무적 시사점을 제공하고자 한다.

Ⅱ. 이론적 배경 및 연구모델

2.1 연구모형

기업들이 스마트폰을 통해 상품 등의 홍보 차 전송하는 메시지를 수신자가 받았을 때, 수신자로 하여금 메시지에 제시된 행동을 하도록 유발하는 요인이 무엇인지에 대해 본 연구는 메시지 신호의 관점에서 접근하였다. 다시 말하면, 본 연구는 SMS 신호 상의 어떠한 특징요인들이 메시지의 신뢰도에 영향을 미치는지 살펴보고, 이러한 특징요인들은 메시지와 수신자 사이의 관여도에 따라 그 차이가 어떻게 나타나는지를 확인하고자 한다. 또한 메시지 신뢰도가 결과적으로 어떻게 메시지 수용의사의 형태로 나타나게 되는지에 대해 살펴보고, 이를 논리적으로 설명할 수 있는 이론적 관점을 제시하는 과정을 거친다. 이에 본 연구는 기존의 소비자를 대상으로 하는 설득적 메시지와 관련한 이론인 정교화 가능성 모델(ELM)에서 제시된 중심경로(central route)와 주변경로(peripheral route)의 구조를 스마트폰 메시지 컨텍스트에 적용하고자 한다.

SMS 광고는 수신자에게 쉽게 무시되기 때문에(Wang *et al*., 2002) 메시지의 정교화 과정이 발생하기 어렵다고 보는 시각이 있다. 그러나 SMS를 통한 광고가 오히려 광고에 대한 소비자의 반응을 이끈다는 연구 결과 또한 존재한다. 모바일 광고의 상호 작용 요소가 수신자로 하여금 더 많은 정보를 검색할 수 있게 함으로써 인지 반응을 유도하기 때문이다(Drossos *et al*., 2007). 모바일은 기존의 인터넷 채널 보다 더 많은 상호 작용 요소를 제공하고 있다. 예를 들어 SMS 광고 수신자는 SMS 상의 링크를 통해 더 자세한 내용을 확인하거나, 클릭과 같은 간단한 조작으로 발신자와 즉각적인 통화를 할 수도 있다. 또한 수신자가 발신자에게 메시지를 보내 상호 작용을 하는 것도 가능하다. 즉 모바일 광고는 비자발적 광고 노출 후 링크 접속, 통화, 문자 메시지 등의 방식으로 자발적인 노출이 이루어진다는 점에서 인터넷 광고와 유사한 특징을 가지며, 이러한 특성으로 인해 광고 메시지에 대한 인지적 정보처리 과정이 수반된다. 아울러 국내의 경우 '정보통신망 이용촉진 및 정보보호 등에 관한 법률'에 따라 기업은 사전에 소비자가 수신 동의한 경우에만 스마트폰 문자 광고를 전송할 수 있다. 즉 소비자가 광고를 수신하기 이전인 기업에 사전 동의를 하는 순간부터 모바일 광고 수용 과정이

일어난다고 할 수 있다(남기화, 여정성, 2011). 이외에도 기업이 옵트인(opt-in: 사전에 수신자의 허락을 받은 경우에만 서비스를 제공하는 방식) 문자 메시지 방식을 채택했을 때, 기업의 광고 콘텐츠가 더 효율적으로 소비자의 관심을 끄는 것으로 나타났다(Bamba and Barnes, 2007). 본 연구는 이러한 점을 고려하여 피실험자로 하여금 사전에 특정 통신사를 사용하고 있고, 이 통신사로부터 광고 문자 메시지를 받는 것으로 실험을 설계하였다. 이러한 설정은 스마트폰 광고 메시지의 정교화 가능성을 높이는 장치로 작용된다. 또한 스마트폰의 SMS 광고 메시지 연구 맥락에서도 인터넷 광고와 마찬가지로 정교화 가능성 모델의 틀을 이용해 중심경로와 주변경로로 메시지 처리 과정을 이해하려는 시도가 있었다(Chutijirawong and Kanawattanachai, 2014; 남기화, 여정성, 2011).

본 연구에서는 이러한 선행연구의 관점을 고려하여, 중심경로와 주변경로를 각각 내용 상의 신호(contents cue)와 누설 신호(leakage cue)로 구분한다.

또한 이들 신호가 메시지의 신뢰도에 어떤 영향을 미치고, 수신자에 대한 메시지 관여도가 이들 관계에 어떠한 조절효과를 가지는지 확인해 보고자 한다. 여기서 정교화 가능성 모델의 메시지 관여도는 스마트폰 메시지 컨텍스트 하에서 맥락화로 이해된다. 본 연구에서는 내용 상의 신호에 대한 맥락화의 조절효과를 중점적으로 고려하기 위해 사전에 스마트폰 메시지를 저맥락화와 고맥락화의 명목 변수로 설정하여 모형에 적용하였다.

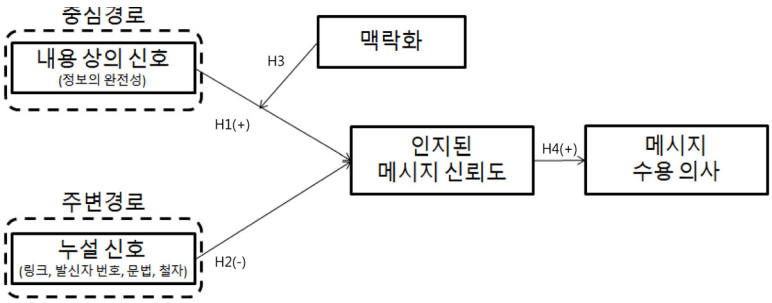
2.2 사회공학(Social Engineering)

스미싱(smishing)은 보안 회사인 맥아피(McAfee)가 피싱(phishing)과 문자메시지(Short Message Service: SMS)를 결합하여 만든 용어다. 이것은 SMS에 포함된 URL을 클릭할 경우, 피해자가 모르는 사이에 스마트폰에 악성코드가 설치되어 개인정보가 탈취되는 사이버범죄 행위다. 즉 스미싱은 스마트폰의 맥락에서 벌어지는 피싱이라 할 수 있다. 피싱은 사회공학적 방법으로 대상자를 속여 그가 지니고 있는 정보를 획득하려 한다(최양서, 서동일, 2016). 그러므로 이는 근본적으로 컴퓨터 기술보다는 인간의 심리와 밀접하게 연결되어 있다(Goel *et al*., 2017).

여기서 사회공학은 비밀스런 정보를 알려주거나 공격자가 원하는 행동을 취하도록 타인을 조작하는 기술을 의미한다(Mitnick and Simon, 2011). 사회공학적 기술을 사용한 피싱 공격은 대상자가 휴리스틱하게 사고하여 의사결정을 내리도록 이끈다. 이러한 과정을 통해 이루어지는 정보 처리 및 의사결정은 인지적으로 많은 부담이 들지 않는 과정이며 사소한 단서에 근거하여 이루어진다.

2.3 정교화 가능성 모델(Elaboration Likelihood Model)

마케팅과 더불어 피싱 연구에서도 활발히 사용되고 있는 모델인 Petty and Cacioppo(1981)의 정교



〈그림 1〉 연구 모델

화 가능성 모델(ELM)은 개인의 의사 결정 및 행동 의사의 형성 과정을 설명하는데 유용하다.

이후 출현한 발전된 정교화 가능성 모델(Petty and Wegener, 1998)은 저부담 및 고부담 사고의 개념을 제시하였다. 발전된 정교화 가능성 모델은 고부담 사고와 연결되는 중심경로(central route) 및 저부담 사고와 연결되는 지엽적 경로(peripheral route)로 이루어진다. 개인이 중심경로를 거쳐 의사 결정을 할 경우 고부담 사고를 통해 명료하고 논리적이며 설명 가능한 태도를 형성하여 행동한다. 그러나 지엽적 경로에는 중심경로에 비해 상대적으로 적은 정도의 인지적 수고, 그리고 덜 명료한 정도의 의식 각성이 포함된다. 즉 지엽적 경로에는 저부담 인지 과정이 반영되는 것이다(Petty and Cacioppo, 1981). Enhanced APCO(antecedents-privacy concerns-outcomes) 모델에 따르면 다음과 같은 요소로 인해 개인은 저부담 사고로 유도되어 프라이버시 관련 행동을 형성하는데, 여기에는 저부담의 인지 과정으로 개인을 유도 하는 요소로 시간 제약 및 인지 요구(time constraints and need for cognition), 감정 및 분위기(emotion and mood), 정보 과부하 및 제한된 인지 자원(information overload and limited cognitive resources) 등이 꼽힌다(Dinev *et al*., 2015).

Dutta-Bergman(2004)의 연구에 따르면, 피싱의 컨텍스트 하에서 정교화 가능성 모델의 중심경로와 지엽적 경로의 요인은 각각 내용 상의 신호(contents cue)와 누설 신호(leakage cue)로 나타난다.

수신자 개인은 피싱 메시지를 접했을 때 일차적으로 메시지의 신호에 주목(attention)하게 되고, 이차적으로 본인이 지닌 지식을 메시지에 연결시키는 정교화(elaboration)의 과정을 거쳐 정보를 처리한다(Petty and Cacioppo, 1981). 첫 번째 과정에서 수신자가 메시지에 담긴 신호에 주목하는 정도에 따라 그것의 내용대로 행동 의사를 형성할 가능성 또한 달라진다. 정교화는 개인이 사전에 보유하고 있는 지식을 그가 본 메시지의 신호와 의식적으로 연결하는 과정이다(Perse, 1990).

정보 처리 과정에서 단순히 신호를 주목하는데 그치기보다는 정교화로 사고 과정을 연결시키는 과정까지 수행한 개인이 메시지의 정보를 더 많이 기억하고 응용할 수 있다(Cialdini, 2009; Eveland *et al*., 2003). 기만 이론(theory of deception)에 따르면 개인은 기만적 사건을 사전에 그가 가지고 있는 지식을 통해 해석한다(Johnson *et al*., 1992). 즉 피싱 공격을 당한 상황에서 기존의 보안 지식과 메시지 내용 상의 신호를 연결시키지 못해 정교화에 실패할 경우 기만을 탐지하지 못하고 피싱 메일에 당할 가능성이 커진다(Vishwanath *et al*., 2011).

2.4 메시지 신뢰도(Message Credibility)

Jakobsson(2007)의 연구에 따르면 메시지에 대해 개인이 갖는 신뢰도는 메시지에 대한 수용의사로 연결되는 성향이 있다. 메시지 신뢰도는 두 가지 요인, 즉 메시지의 내용 상의 신호와 누설 신호로부터 영향을 받는다. 예를 들어 개별맞춤화(personalization)와 같이 수신자가 고려할 만한 정보가 메시지 상에 많이 포함되어 있을수록 메시지의 신뢰도는 높아지는 반면, 철자법, URL링크, 발신자 등의 누설 신호가 포함된 메시지의 신뢰도는 낮은 것으로 나타났다(Jakobsson, 2007). 메시지 신뢰도는 발신자의 의도대로 수신자가 행동하도록 하는 의도에 영향을 주기 때문에 메시지의 효과를 관찰하는데 있어서 반드시 고려해야 할 요인이다. 즉 메시지에 대한 신뢰도는 메시지의 두 가지 신호와 수신자의 행동의도 사이에서 매개변수로 작용한다.

2.5 내용 상의 신호(Contents Cue)

누설 신호가 정교화 가능성 모델의 지엽적 경로를 통해 신뢰도에 영향을 미친다면, 중심경로를 통해 신뢰도에 영향을 미치는 요소는 메시지에 담긴 내용 상의 신호다. 내용 상의 신호는 메시지의 내용이 필요한 내용을 얼마나 담고 있는지의 여부

를 나타내는 개념으로 정보의 완전성(information completeness)으로 표현되기도 한다. 정보의 완전성을 확보하기 위해서는 메시지 상에서 정보의 근거, 출처 및 방법론 등이 온전히 제시되어야 한다. 즉 정보의 완전성은 의사 결정에 필요한 정보가 메시지의 내용 중에 온전하게 갖추어 졌는지를 의미한다. 기존의 연구에서는 건강정보의 맥락에서 정보의 완전성에 대한 인지가 정보 제공 웹사이트에 대한 소비자의 신뢰에 영향을 미친다는 결과를 도출하였다(Dutta-Bergman, 2004). 또한 정보 제공자(source)에 대한 높은 수준의 신뢰는 메시지에 대한 긍정적인 태도를 가진다(Dharmadasa and Alahakoon, 2014). 이와 같은 결과를 근거로 스마트폰 메시지의 내용 상의 신호(즉, 정보의 완전성)는 수신자의 메시지에 대한 신뢰도에 영향을 줄 것으로 예상하였다. 이에 다음과 같은 가설을 제시한다.

H1: 스마트폰 메시지의 내용 상의 신호(메시지 완전성)는 수신자가 인지하는 메시지 신뢰도에 긍정적인 영향을 미칠 것이다.

2.6 누설 신호(Leakage Cue)

누설 신호는 수신자가 메시지에 주목한 뒤 곧바로 메시지의 기만성을 탐지할 수 있는 신호를 의미한다(Harrison *et al*., 2016). 피싱 전자 메일의 컨텍스트로 진행된 기존 연구는 제목(subject line), 위급 신호(urgency cues), 문법 및 철자(grammar and spelling), 전자 메일의 발신자(email's source)를 누설 신호로 지목하였다(Vishwanath *et al*., 2011). 누설 신호가 포함된 전자 메일을 받았을 때 그것은 수신자의 주목을 끌게 된다. 이러한 누설 신호들과 행동 의도의 관계를 정리하면 다음과 같다.

- 전자 메일의 발신자에 대한 주의 정도는 수신자가 피싱 메일에 응답할 가능성을 낮출 것이다.
- 전자 메일의 문법 및 철자에 대한 주의 정도는 수신자가 피싱 메일에 응답할 가능성을 낮출 것이다.
- 위급 신호에 대한 주의도는 수신자가 피싱 메일에 응답할 가능성을 높일 것이다.
- 제목에 대한 주의도는 수신자가 피싱 메일에 응답할 가능성을 높일 것이다.

여기서 위급 신호 및 제목에 대한 주의도가 피싱에 대한 응답 가능성을 높이는 이유는, 두 요소에 수신자가 주의(attention)만 기울이고 이차적으로 정교화(elaboration)를 거치지 못할 경우 휴리스틱하게 사고하여 피싱 메시지의 요구대로 응답하게 되기 때문이다.

본 연구에서는 피싱 메시지의 누설 신호를 역으로 적용한다. 즉 기만적인 메시지가 아닌 기업 등의 조직에서 개인에게 보낸 메시지에 누설 신호가 포함되어 있을 경우, 수신자 개인이 지엽적 경로를 거쳐 사고한 후 메시지에 대한 신뢰도를 어떻게 형성하는지, 그리고 이것은 메시지 수용의사에 어떠한 영향을 갖는지를 확인하고자 한다.

본 연구의 맥락에서 ELM의 지엽적 경로에 기반을 둔 누설 신호로는 링크, 발신자의 출처, 맞춤법 등이 있다.

링크는 수신자 개인이 전자 메일의 신뢰성을 평가하는 기준 중 하나다. 피싱 메일에 포함된 기만적 요소를 찾아보라는 요구의 실험에서 대부분의 피실험자가 URL 링크를 포함한 발신자의 문제를 우선적으로 지적한 기존 연구가 있다(Jakobsson *et al*., 2007). 한편 수신자가 피싱 메일을 받았을 때 가짜 URL 링크를 누르는 경우는 다음과 같다. 우선 도메인 네임의 뜻이나 도메인 네임의 문법에 사전 지식이 없는 경우이다. 이런 상황에서 수신자는 도메인 네임에 권위 있는 기관 혹은 유명 기업의 이름이 있다면 속을 수 있다. 두 번째 경우는 실제 링크와 유사한 겉모습에 기만당하는 경우로, 가령 알파벳 'l' 대신 숫자 '1'을 사용하여 위장된 URL 링크를 꾸미는 경우다.

기존의 피싱 연구 결과, 링크가 의심스러울 경우 피실험자의 14%만이 링크를 클릭하였다(Jakobsson and Ratkiewicz, 2006). 같은 맥락에서 SMS 메시지를

대상으로 하는 본 연구에서도 메시지 상 기재된 링크를 신뢰하기 어려운 경우, 메시지의 신뢰도 역시 낮아질 것으로 예상하였다.

한편 기존 피싱 연구에서 피실험자는 전자 메일 발신 주소 같이 발신자의 신원 또는 소속에 대해 알 수 있는 단서에 민감한 반응을 보였다. 동일한 내용의 피싱 메일을 받았을 때 수신자가 알지 못하는 이로 조작된 발신자에게서 받은 메일의 공격 성공률은 16%에 불과했지만, 알고 있는 사람으로 조작된 발신자에게서 받은 메일의 공격 성공률은 72%에 달했다(Jagatic *et al*., 2006). 한편 모바일 메시지를 통해 이루어지는 스미싱의 컨텍스트에서는 메일 주소가 아닌 발신자의 전화번호가 수신자로 하여금 발신자의 정체를 파악할 수 있는 일차적인 단서가 될 수 있다. 기존 연구에서 SMS 광고의 출처는 신뢰도(credibility)와 같은 개념으로 사용되었으며, 이는 SMS 광고 메시지에 대한 태도에 긍정적인 영향을 주는 것으로 나타났다(Drossos *et al*., 2007). 이와 같은 관점에서 SMS메시지 발신자 출처를 신뢰할 수 없는 경우, 수신자가 인지하는 메시지 신뢰도 역시 낮아질 것으로 예상하였다.

마지막으로 기존 연구에서 문법 및 철자법(grammar and spelling)은 개인이 기만적 전자 메일과 그렇지 않은 전자 메일을 구별할 때 관심을 기울이는 누설 신호의 하나로 지목된 바 있다. 다시 말해 철자법 오류, 띄어쓰기 실수, 비문과 같은 맞춤법의 오류는 메시지의 신뢰도를 저하하는 것이다(Vishwanath *et al*., 2011).

스마트폰 광고 메시지는 소비자 관점에서 정보성 광고와 스팸성 광고로 구분되는데, 특히 스팸성 광고 문자는 다른 채널(인터넷 및 전자 메일)의 스팸성 광고보다 소비자의 성가심을 더 크게 유발한다(남기화, 여정성, 2011). 즉, 소비자가 스마트폰 광고를 스팸성 광고로 인식하게 되면 주의를 깊게 기울이지 않고 이를 곧바로 기만적인 메시지로 판단하게 되는 것이다. 그 결과 메시지에 대한 소비자의 신뢰도 역시 낮아지게 된다. 선행 연구에서 위장된 URL 링크, 신뢰할 수 없는 발신자 출처, 맞춤법 오류 등이 전자 메일에 포함된 경우 수신자는 곧바로 기만을 탐지하였기 때문에(Jakobsson *et al*., 2007; Vishwanath *et al*., 2011) 이와 같은 요소를 본 연구 맥락에도 적용하였다. 즉, 위장된 링크, 낮은 신뢰성의 발신자 출처, 맞춤법 오류의 누설 신호가 스마트폰 광고 메시지에 포함되어 있을 경우, 수신자는 곧바로 낮은 메시지 신뢰도를 형성할 것으로 예상하였다. 따라서 다음과 같은 연구가설을 도출할 수 있다.

H2: 스마트폰 메시지의 누설 신호는 수신자가 인지하는 메시지 신뢰도에 부정적인 영향을 미칠 것이다.

2.7 맥락화(Contextualization)

Goel *et al*.(2017)의 연구는 피싱 취약성에 맥락화(contextualization)의 영향을 밝혀냈다. 이 연구에서는 대학 학부생을 대상으로 습득과 손실의 프레임으로 구분한 메일을 발송하였다. 메일은 각각 금전적인 부분에서의 습득과 손실, 비금전적 부분에서의 습득과 손실, 보안 상의 습득과 손실, 사회적인 부분에서의 습득과 손실의 경우로 나뉘어져 발송되었다. 이때 학부생들은 보편적으로 두루 선호되는 경품 증정보다, 자신들이 수강 신청한 수업의 공지 전자 메일에 더욱 높은 반응도를 보였다. 즉 맥락화의 정도는 메시지의 지시에 따른 행동의도를 높이는 것이다.

메시지의 맥락화는 정교화 가능성 모델에서 관여도(involvement)가 개인의 태도 형성을 조절하는 것과 비슷하다. 메시지 내 정보가 수신자 개인의 상황과 관계된 정도가 높다면 수신자가 메시지에 반응할 가능성이 높아지며, 그 정도가 낮다면 메시지에 반응할 가능성 역시 낮아지는 것이다.

Goel *et al*.(2017)의 연구에서 전자 메일을 발송하고, 메일 상에 링크된 URL을 클릭하는 것으로 메시지 반응성을 관찰하였기 때문에 수신자는 메시지의 내용을 모두 확인하였을 것으로 보았다.

스마트폰을 통한 스미싱 컨텍스트의 본 연구에서도 선행연구와 마찬가지로 맥락화가 높은 경우, 수신자는 메시지의 내용을 모두 확인할 것으로 예상하여, 맥락화의 효과는 내용 상의 신호에 주로 작용할 것으로 보았다. 즉, 맥락화 정도에 따라 내용 상의 신호가 메시지 신뢰도에 주는 영향은 달라질 것으로 가정하였다. 반면 누설 신호에서는 내용 상의 신호와는 달리 맥락화의 조절효과가 나타나지 않을 것으로 예상된다. 앞서 문헌 연구에서 살펴본 바와 같이 누설 신호가 메시지에 존재할 경우, 수신자는 메시지의 내용을 확인하기 이전에 기만성을 탐지하거나 판단하기 때문이다(Harrison *et al*., 2016; Vishwanath *et al*., 2011). 다시 말하면 메시지 내 존재하는 누설 신호로 인해 수신자는 정교화 과정을 거치지 않고 메시지의 신뢰도 여부를 결정짓게 된다. 따라서 맥락화의 조절효과는 메시지의 두 가지 신호 중 내용 상의 신호에만 조절 효과를 가질 것으로 유추하였다. 따라서 다음과 같은 가설을 도출하였다.

H3: 내용 상의 신호가 인지된 메시지 신뢰도에 미치는 영향은 맥락화의 정도에 따라 차이가 있을 것이다.

2.8 메시지 수용의사(Intention to Accept Message)

누설 신호 및 정보의 완전성과 신뢰도의 관계를 연구한 기존 연구들은 피싱의 컨텍스트에서 이루어졌기 때문에 종속변수를 피싱 취약성으로 두었지만(Dutta-Bergman, 2004; Goel *et al*., 2017; Jakobsson *et al*., 2007), 본 연구는 신뢰도를 저하시키는 요소를 제거하여 모바일 메시지를 통한 효율적인 커뮤니케이션 방법을 찾는 것을 목적으로 한다. 신뢰도 높은 메시지의 전달로 인해 메시지의 의도가 제대로 전달되었는지 여부를 확인하기 위해서는 종속변수가 메시지 수용의사(intention to accept message)가 되어야 한다.

Dharmadasa and Alahakoon(2014)은 스마트폰 메시지 컨텍스트 하에서 광고에 대한 높은 신뢰도는 광고에 대한 태도, 브랜드 및 구매 의사에 긍정적인 영향을 미친다는 것을 규명하였다. 이와 같은 연구 결과를 토대로 스마트폰 메시지의 맥락 하에서 메시지의 신뢰도는 메시지 수용의사에 영향을 미치는 것으로 이해를 확장하였다. 이에 다음과 같은 가설을 제시하고자 한다.

H4: 인지된 메시지 신뢰도는 메시지 수용의사에 긍정적인 영향을 미칠 것이다.

Ⅲ. 연구방법

본 연구의 첫 번째 목표는 메시지 신뢰도에 내용 상의 신호 및 누설 신호가 영향을 미치는 정도, 그리고 맥락화의 조절효과를 검증하는 것이다. 더불어 메시지의 신뢰도가 수신자의 메시지 수용의도에 미치는 영향, 즉 수신자가 메시지에 제시된 내용대로 행동의도를 형성하는지 여부를 확인하는 것이 본 연구의 두 번째 목표다. 연구 목적의 달성을 위해 편의표본추출을 통한 표본을 대상으로 서베이 실험을 실시한다.

3.1 서베이 실험(Survey Experiment)

서베이 실험은 서베이의 형식으로 설계된 실험 방식으로, 퀄트릭스(Qualtrics Research Suite)를 통해 웹 기반에서 이루어졌다. 연구는 다음과 같은 절차로 진행되었다. 우선 참여자는 카카오톡 또는 페이스북 등의 채널을 통해 배포된 퀄트릭스 링크를 클릭하여 실험에 참여하게 되며, 도입 단계에서 실험에 대한 간단한 안내를 받는다. 이후 실험 진행을 위해 조작된 상황을 응답자에게 제시하는 시나리오 형식으로 진행되었다. 본 실험에 앞서 대학/대학원생 49명을 대상으로 2회의 예비 실험(pilot test)을 실시하여 실험 시나리오 및 설문 문항을 수정, 보완 후 본 조사에 들어갔다. 시나리오는

〈표 1〉 실험 메시지의 구성

	완전한 정보/고맥락	불완전한 정보/고맥락	완전한 정보/저맥락	불완전한 정보/저맥락
누설 신호 無	발신번호, 링크, 맞춤법 정상/메시지 내용 완전/고맥락의 상황	발신번호, 링크, 맞춤법 정상/메시지 내용 불완전/고맥락의 상황	발신번호, 링크, 맞춤법 정상/메시지 내용 완전/저맥락의 상황	발신번호, 링크, 맞춤법 정상/메시지 내용 불완전/저맥락의 상황
누설 신호 有	발신번호, 링크, 맞춤법 비정상/메시지 내용 완전/고맥락의 상황	발신번호, 링크, 맞춤법 비정상/메시지 내용 불완전/고맥락의 상황	발신번호, 링크, 맞춤법 비정상/메시지 내용 완전/저맥락의 상황	발신번호, 링크, 맞춤법 비정상/메시지 내용 불완전/저맥락의 상황

응답자로 하여금 통신사에서 쿠폰 관련 SMS 메시지를 받은 상황을 자연스럽게 연상하도록 구성되었다. 메시지가 실제 통신사로부터 발송된 것처럼 보이도록 구체적인 발신자로 국내 통신사 한 곳을 선택하고 응답자는 해당 기업을 사용하는 것으로 설정하였다. 응답자가 SMS 메시지를 수신했다는 상황에 과도하게 집중하지 않도록 버스 안에서 음악을 듣다가 메시지를 수신했다는 상황을 만들었다. 이후 두 가지 메시지의 신호 유무(내용 상의 신호 및 누설 신호의 유무)와 맥락화의 조절효과가 메시지 신뢰도에 미치는 영향을 측정하기 위해 각기 다르게 설계된 8가지의 메시지(2×2×2) 중 하나를 무작위로 피실험자에게 노출하는 실험을 진행하였다. <표 1>은 이러한 2×2×2 요인 설계를 구분한 것이다. 실험 진행 직후, 피실험자들을 대상으로 메시지 신뢰도와 메시지 수용 의도를 측정하는 설문에 응답하게 하였다.

설문은 2017년 7월 27일부터 8월 15일까지 진행되었으며, 전체 233명이 서베이 실험에 참여하여 이 중 불성실하게 응답된 것으로 판단되는 67명의 결과를 제외하고, 실제 166명의 설문결과가 데이터분석에 사용되었다. 최종 설문응답자의 인구통계학적 특성은 <표 2>와 같다.

〈표 2〉 설문응답자의 인구통계학적 특성

성별	인원	비율
여	50	30.1%
남	116	69.9%

연령	인원	비율
20세 미만	9	5.4%
20~24	35	21.1%
25~29	98	59.0%
30~39	22	13.3%
40세 이상	2	1.2%

3.2 측정문항의 개발

연구모델을 검증하기 위해 모바일 채널을 통한 소비를 활발히 하고 있는 20~30대 스마트폰 사용자들을 주된 대상으로 서베이 실험을 진행하였다. 측정 문항들은 선행연구에서 사용된 기존 항목들을 사용하거나, 관련 연구의 분류 기준 및 개념적 정의 등을 바탕으로 하여 연구 컨텍스트에 알맞게 수정하여 사용하였다.

〈표 3〉 사전 인터뷰를 통해 파악된 누설 신호 유형

링크	발신번호	맞춤법
URL을 보고, SMS상에 무슨 내용을 담았는지 알 수 있어야 신뢰도가 상승함. 메시지 상 텍스트로 기재할 수 있는 내용을 두고 URL을 참조하라고 할 경우 메시지 신뢰도가 저하됨.	개인전화번호, 유선전화, 인터넷 전화(070)는 메시지 신뢰도가 저하됨. 가장 신뢰도가 높은 것은 전국대표 번호(1588 등)를 사용하였을 때임.	철자법, 띄어쓰기 실수, 비문이 포함된 메시지는 신뢰도가 저하됨. 메시지 내에 특수문자가 포함되는 경우, 메시지 신뢰도가 저하됨.

실험을 진행하기에 앞서 SMS에서 인지된 메시지 신뢰도에 부정적인 영향을 끼치는 누설 신호를 구체적으로 파악하기 위해 서울 소재 대학 학부생 및 대학원생 총 8명을 대상으로 인터뷰를 진행하였다. 인터뷰는 1인당 30분 내외로 진행되었다. 이를

〈표 4〉 변수의 조작적 정의

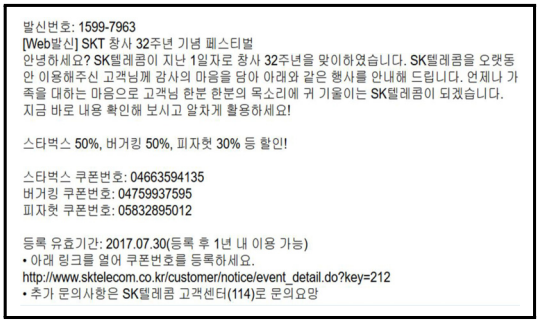
변수	조작적 정의	출처
내용 상의 신호	메시지의 내용 중에 의사결정에 필요한 정보가 갖추어진 정도	Dutta-Bergman(2004)
누설 신호	수신자가 메시지 내용을 검토하는 대신 휴리스틱한 사고 후 의사를 결정하는데 근거가 되는 메시지 상의 오류	Harrison *et al.*(2016) Jagatic *et al.*(2006) Vishwanath *et al.*(2011)
맥락화	메시지가 수신자 자신과 상관 있다고 느끼는 정도	Goel *et al.*(2017), Zaichkowsky(1985)
메시지 신뢰도	메시지에 대한 내용을 신뢰하는 정도	Cheung *et al.*(2012)
메시지 수용의사	메시지에서 제시된 행동을 수신자가 하고자 하는 의도	Mathieson(1991), 허경옥(2015)

통해 기존 피싱 연구에서 알려진 누설 신호가 스마트폰 SMS 환경 하에서도 유효한지를 확인하였고, 본 연구 맥락에서 유효한 누설 신호를 새롭게 발견하였다. 인터뷰 결과는 <표 3>과 같이 각 누설 신호별로 구분하여 정리하였다.

또한 경험 많은 연구자들의 조언을 구해 잘못된 표현이나 측정 상의 오류를 수정하고 피실험자들을 대상으로 하여 2차에 걸친 예비 실험 과정을 통해 측정문항에 대한 신뢰성과 타당성을 검증하였다. 주요 변수들에 대한 조작적 정의와 출처는 <표 4>와 같다.

본 연구에서 설정된 주요변수 중 내용 상의 신호(contents cue)는 정보의 완전성 정도로 측정이 가능하다. 수신된 메시지 내에 의사결정을 내리기에 충분한 정보를 나타내는 개념이 정보의 완전성이다. 정보의 완전성은 Dutta-Bergma(2004)의 연구를 토대로 정보가 빈틈없이 완벽한가?(thorough) 충분한 정보가 담겨 있는가?(contains sufficient information) 필요한 요소가 모두 담겨 있는가?(contains all the necessary elements) 충분한 근거가 담겨 있는가?(contains sufficient evidence) 지지가 되는가?(supported) 완전한가?(complete) 포괄적인가?(extensive) 충분한가?(sufficient)의 8가지 개념을 기반으로 구성하였다.

정보의 완전성 및 불완전성을 반영하여 실제 서베이 실험에서 사용한 SMS 메시지는 <그림 2> 및 <그림 3>과 같다.

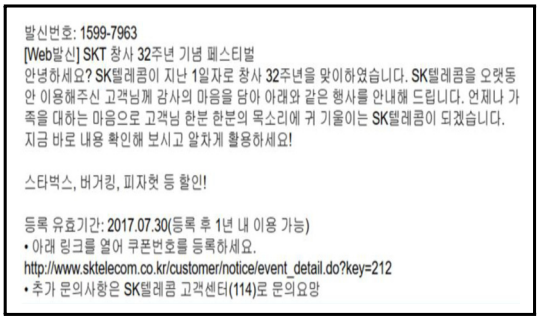

발신번호: 1599-7963
[Web발신] SKT 창사 32주년 기념 페스티벌
안녕하세요? SK텔레콤이 지난 1일자로 창사 32주년을 맞이하였습니다. SK텔레콤을 오랫동안 이용해주신 고객님께 감사의 마음을 담아 아래와 같은 행사를 안내해 드립니다. 언제나 가족을 대하는 마음으로 고객님 한분 한분의 목소리에 귀 기울이는 SK텔레콤이 되겠습니다.
지금 바로 내용 확인해 보시고 알차게 활용하세요!

스타벅스 50%, 버거킹 50%, 피자헛 30% 등 할인!

스타벅스 쿠폰번호: 04663594135
버거킹 쿠폰번호: 04759937595
피자헛 쿠폰번호: 05832895012

등록 유효기간: 2017.07.30(등록 후 1년 내 이용 가능)
• 아래 링크를 열어 쿠폰번호를 등록하세요.
http://www.sktelecom.co.kr/customer/notice/event_detail.do?key=212
• 추가 문의사항은 SK텔레콤 고객센터(114)로 문의요망

〈그림 2〉 정보의 완전성을 나타내는 문자메시지


발신번호: 1599-7963
[Web발신] SKT 창사 32주년 기념 페스티벌
안녕하세요? SK텔레콤이 지난 1일자로 창사 32주년을 맞이하였습니다. SK텔레콤을 오랫동안 이용해주신 고객님께 감사의 마음을 담아 아래와 같은 행사를 안내해 드립니다. 언제나 가족을 대하는 마음으로 고객님 한분 한분의 목소리에 귀 기울이는 SK텔레콤이 되겠습니다.
지금 바로 내용 확인해 보시고 알차게 활용하세요!

스타벅스, 버거킹, 피자헛 등 할인!

등록 유효기간: 2017.07.30(등록 후 1년 내 이용 가능)
• 아래 링크를 열어 쿠폰번호를 등록하세요.
http://www.sktelecom.co.kr/customer/notice/event_detail.do?key=212
• 추가 문의사항은 SK텔레콤 고객센터(114)로 문의요망

〈그림 3〉 정보의 불완전성을 나타내는 문자메시지

아울러 누설 신호의 측정은 Vishwanath(2011)의 연구를 기반으로 하여 본 연구의 컨텍스트인 스마트폰에 맞추어 약간의 수정을 거쳤다. 누설 신호의 측정 문항으로 발신번호(SMS source), 문법 및 철자(grammar and spelling), URL 링크(link)의 여부를 선택하였다. 특히 스마트폰 메시지의 연구 맥

락을 고려할 때, 문법 및 철자 오류 측정 시 특수문자 남발의 유무도 함께 관찰하였다.

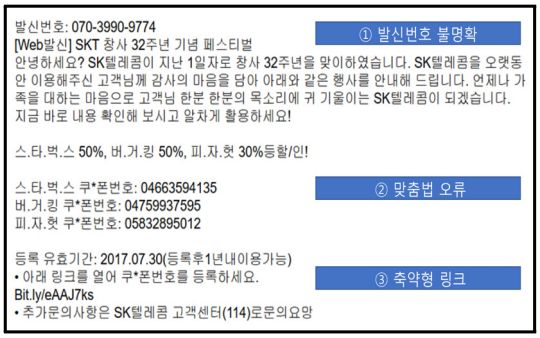

발신번호: 1599-7963
[Web발신] SKT 창사 32주년 기념 페스티벌
안녕하세요? SK텔레콤이 지난 1일자로 창사 32주년을 맞이하였습니다. SK텔레콤을 오랫동안 이용해주신 고객님께 감사의 마음을 담아 아래와 같은 행사를 안내해 드립니다. 언제나 가족을 대하는 마음으로 고객님 한분 한분의 목소리에 귀 기울이는 SK텔레콤이 되겠습니다.
지금 바로 내용 확인해 보시고 알차게 활용하세요!

스타벅스 50%, 버거킹 50%, 피자헛 30% 등 할인!

스타벅스 쿠폰번호: 04663594135
버거킹 쿠폰번호: 04759937595
피자헛 쿠폰번호: 05832895012

등록 유효기간: 2017.07.30(등록 후 1년 내 이용 가능)
• 아래 링크를 열어 쿠폰번호를 등록하세요.
http://www.sktelecom.co.kr/customer/notice/event_detail.do?key=212
• 추가 문의사항은 SK텔레콤 고객센터(114)로 문의요망

〈그림 4〉 누설 신호가 없는 문자메시지



발신번호: 070-3990-9774
[Web발신] SKT 창사 32주년 기념 페스티벌
안녕하세요? SK텔레콤이 지난 1일자로 창사 32주년을 맞이하였습니다. SK텔레콤을 오랫동안 이용해주신 고객님께 감사의 마음을 담아 아래와 같은 행사를 안내해 드립니다. 언제나 가족을 대하는 마음으로 고객님 한분 한분의 목소리에 귀 기울이는 SK텔레콤이 되겠습니다.
지금 바로 내용 확인해 보시고 알차게 활용하세요!

스.타.벅.스 50%, 버.거.킹 50%, 피.자.헛 30%등할/인!

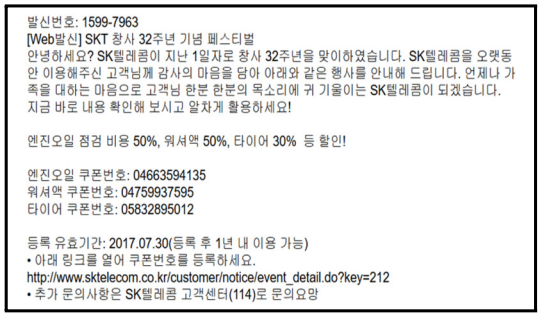
스.타.벅.스 쿠*폰번호: 04663594135
버.거.킹 쿠*폰번호: 04759937595
피.자.헛 쿠*폰번호: 05832895012

등록 유효기간: 2017.07.30(등록후1년내이용가능)
• 아래 링크를 열어 쿠*폰번호를 등록하세요.
Bit.ly/eAAJ7ks
• 추가문의사항은 SK텔레콤 고객센터(114)로문의요망

〈그림 5〉 누설 신호가 있는 문자메시지

누설 신호 유무를 고려한 광고 메시지는 <그림 4> 및 <그림 5>에서 확인할 수 있다.

맥락화는 Zaichkowsky(1985)의 연구를 기반으로 하여 측정하였는데, 본 연구의 피실험 대상이 주로 대학의 학부생임을 감안하여 고맥락화된 메시지는 학부생들이 자주 이용하는 스타벅스, 버거킹, 피자헛에서 사용 가능한 쿠폰 메시지로, 저맥락화된 메시지는 자동차 수리점에서 사용 가능한 쿠폰 메시지로 설정하였다. 아울러 두 가지 메시지 상의 맥락화 설계가 타당한지 확인하기 위해 관여도와 관련한 3개 문항을 추가하여 서베이 실험을 진행하였다. 실제 서베이 실험에 사용된 메시지는 <그림 6> 및 <그림 7>에서 확인할 수 있다.

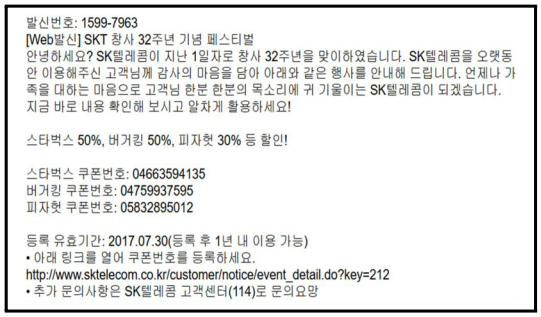

발신번호: 1599-7963
[Web발신] SKT 창사 32주년 기념 페스티벌
안녕하세요? SK텔레콤이 지난 1일자로 창사 32주년을 맞이하였습니다. SK텔레콤을 오랫동안 이용해주신 고객님께 감사의 마음을 담아 아래와 같은 행사를 안내해 드립니다. 언제나 가족을 대하는 마음으로 고객님 한분 한분의 목소리에 귀 기울이는 SK텔레콤이 되겠습니다.
지금 바로 내용 확인해 보시고 알차게 활용하세요!

엔진오일 점검 비용 50%, 워셔액 50%, 타이어 30% 등 할인!

엔진오일 쿠폰번호: 04663594135
워셔액 쿠폰번호: 04759937595
타이어 쿠폰번호: 05832895012

등록 유효기간: 2017.07.30(등록 후 1년 내 이용 가능)
• 아래 링크를 열어 쿠폰번호를 등록하세요.
http://www.sktelecom.co.kr/customer/notice/event_detail.do?key=212
• 추가 문의사항은 SK텔레콤 고객센터(114)로 문의요망

〈그림 6〉 수신자에 저맥락화된 문자메시지


발신번호: 1599-7963
[Web발신] SKT 창사 32주년 기념 페스티벌
안녕하세요? SK텔레콤이 지난 1일자로 창사 32주년을 맞이하였습니다. SK텔레콤을 오랫동안 이용해주신 고객님께 감사의 마음을 담아 아래와 같은 행사를 안내해 드립니다. 언제나 가족을 대하는 마음으로 고객님 한분 한분의 목소리에 귀 기울이는 SK텔레콤이 되겠습니다.
지금 바로 내용 확인해 보시고 알차게 활용하세요!

스타벅스 50%, 버거킹 50%, 피자헛 30% 등 할인!

스타벅스 쿠폰번호: 04663594135
버거킹 쿠폰번호: 04759937595
피자헛 쿠폰번호: 05832895012

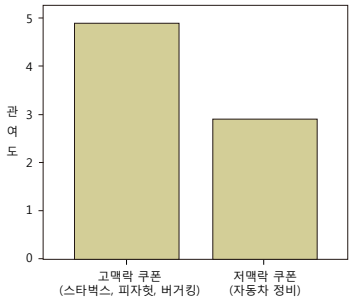
등록 유효기간: 2017.07.30(등록 후 1년 내 이용 가능)
• 아래 링크를 열어 쿠폰번호를 등록하세요.
http://www.sktelecom.co.kr/customer/notice/event_detail.do?key=212
• 추가 문의사항은 SK텔레콤 고객센터(114)로 문의요망

〈그림 7〉 수신자에 고맥락화된 문자메시지

대부분의 설문 응답자가 20대에서 30대 초반에 분포하므로 각각의 맥락화된 메시지 설정이 적절할 것으로 예상되었으나, 맥락화의 자의적 설정으로 인해 야기될 수 있는 오류를 최소화하기 위해 관여도 측정을 위한 3개의 설문 문항을 추가하였다(고맥락화: 2개, 저맥락화: 1개).

이후 두 개 범주의 응답 결과가 유의한 차이를 갖는지 확인하기 위해 독립표본 t검정을 시행하였다. 그 결과, 고맥락화 및 저맥락화 메시지의 평균은 각각 4.87과 2.90(<그림 8> 참고)이며, t값은 10.791($p < 0.01$)로 두 개 메시지 간의 관여도 차이는 유의한 것으로 나타났다.

신뢰도는 Cheung(2012), 메시지 수용의사는 Mathieson(1991)의 연구를 토대로 하여 본 연구에 맞도록 수정하고 보완하여 사용하였다. 본 연구에서 사용된 각각의 문항들은 1점에 해당되는 '매우 그렇지 않음'에서 7점에 해당되는 '매우 그러함'으로 응답할 수 있는 리커트 7점 척도로 구성하였다.



〈그림 8〉 메시지 맥락화에 따른 관여도의 차이

3.3 통제변수

기존의 피싱 연구에서 개인의 피싱 관련 경험 및 관련 지식의 정도에 따라 피싱 취약성이 달라지는 경우가 있었기 때문에(Harrison *et al*., 2016) 종속변수인 메시지 수용의사의 통제변수로 인구통계학적 요소(응답자의 연령, 성별)와 더불어 개인정보가 침해되어 피해를 입은 경험, 스마트폰 하루 사용 시간을 추가하였다. 통제변수의 측정치는 <표 5>와 <표 6>에서 각각 확인할 수 있다.

〈표 5〉 스미싱으로 인한 개인정보 침해 경험

개인정보 침해 경험	인원	비율
없음	75	45.2%
1~3	73	43.9%
4~6	11	6.7%
7~9	2	1.2%
10회 이상	5	3%

〈표 6〉 하루 평균 스마트폰 사용 시간

하루 평균 스마트폰 사용 시간	인원	비율
30분 미만	1	0.6%
30분 이상 1시간 미만	8	4.8%
1시간 이상 2시간 미만	42	25.3%
2시간 이상 4시간 미만	54	32.5%
4시간 이상	61	36.8%

Ⅳ. 분석 및 결과

본 연구에서 각 집단 별(내용 상의 신호 유무, 누설 신호 유무, 맥락화 정도) 메시지 신뢰도의 차이를 확인하기 위해 가설 H1에서 H3까지는SPSS (version 24.0)을 사용한 분산분석(ANOVA)으로 검증하고, H4는 메시지 수용의사에 대한 인지된 메시지 신뢰도의 영향을 살펴보고자 같은 분석 도구인 SPSS를 활용하여 회귀분석을 시행하였다.

4.1 조작점검(Manipulation Check)

연구 가설을 검증하기에 앞서 서베이 실험에서 조작된 세 가지 유형의 변인인 내용 상의 신호, 누설 신호, 맥락화에 대한 조작 점검을 시행하였다. 피실험자들은 안내문과 시나리오에 이어 조작 점검 문항에 대한 응답을 완료하였다. 이를 통해 서베이 실험 문항들이 의도한대로 조작되었는지 확인하였다. ANOVA를 통해 검증한 결과 모든 변인 조작이 성공적으로 이루어진 것이 <표 7>에서 확인

〈표 7〉 조작 점검 결과

ANOVA	CC 점검 문항 1		CC 점검 문항 2		LC 점검 문항 1		LC 점검 문항 2		LC 점검 문항 3		Context 점검문항 1	
	F	Sig.	F	Sig.	F	Sig.	F	Sig.	F	Sig.	F	Sig.
내용 상의 신호 (Contents cue)	169.049	.000	71.154	.000								
누설 신호 (Leakage Cue)					29.945	.000	15.258	.000	8.077	.000		
맥락화 (Contextualization)											50.154	.000

* $p < 0.01$.

되었다. 여기서 내용 상의 신호를 확인하는 문항은 2개, 지엽적 경로 상의 누설 신호를 확인하는 문항은 3개, 맥락화를 위한 문항은 1개로 구성하였다.

4.2 동일방법편의(Common Method Bias)

동일방법편의의 잠재 가능성을 확인하기 위해 단일 요인 검사(Harman's one-factor extraction test)를 실시하였다. 이 분석법은 도구 변수 사이의 분산 대부분을 단일한 방법 요인이 설명할 수 있는지 여부를 확인하는 방법이다. 만약 단일한 방법이 총 분산을 50% 넘게 설명하는 경우, 동일방법편의가 존재할 수 있다고 본다(Nov and Ye, 2008). 검사 결과 본 연구에서는 첫 번째 요인이 총 분산의 31% 만을 설명하는 것으로 나타났다. 따라서 동일방법편의에 대한 우려는 낮다고 볼 수 있다.

4.3 가설 검정

4.3.1 메시지의 신호(내용 상의 신호와 누설 신호)가 메시지의 신뢰도에 미치는 영향 및 맥락화의 조절 효과

본 절에서는 내용 상의 신호가 메시지 신뢰도에 미치는 영향(H1), 누설 신호가 메시지 신뢰도에 미치는 영향(H2), 그리고 내용 상의 신호가 메시지 신뢰도에 미치는 영향에 있어서 맥락화의 조절 효과(H3)에 대한 연구가설을 검증한다. 이를 위해 이원 분산분석(Two-way ANOVA)을 실행하였다.

가설 검증을 시행하기 전 분산분석의 가정에 대한 평가를 실시하였다. Kolmogorov-smirnov을 통해 정규성(normality) 검증을 실시하였고, 모집단들이 정규분포를 이루고 있음을 확인하였다(정용준, 김예진, 2016). 또한 모집단들이 서로 동일한 분산을 가지는지 여부는 Levene 기법을 적용하여 검증하였다. 자료로부터 계산된 F(7, 158)값은 1.753(p = .100)으로 등분산성을 만족시켰다.

가설 검증을 위한 분산분석의 결과는 <표 8>에 나타나 있다. 완전한 정보가 담긴 메시지를 제공받은 집단과 불완전한 정보가 담긴 메시지를 수신한 집단 간의 신뢰도 차이는 근소한 정도로 유의미한 결과가 나타났다(p = .079). 따라서 정보의 완전성에 문제가 있을 경우 신뢰도가 저하된다는 가설 H1은 근소한 수준에서 지지된다. 메시지에 누설 신호가 존재하는 집단과 그렇지 않은 집단 사이의 신뢰도는 분석 결과 통계적으로 유의한 수준에서 뚜렷하게 차이가 나타났으므로 누설 신호가 메시지 신뢰도에 부정적인 영향을 끼칠 것이라는 가설 H2가 지지되었다.

〈표 8〉 내용 상의 신호, 누설 신호, 맥락화 조절 효과에 대한 분산분석 결과[1)]

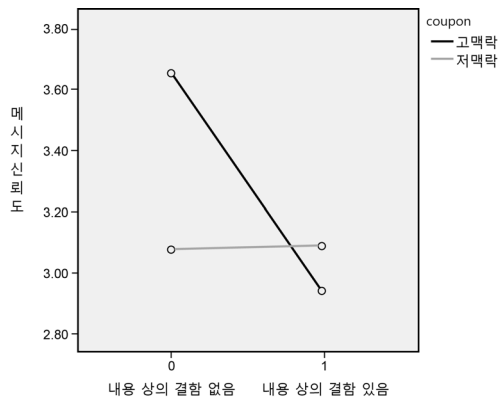
	Mean Square	F	p-value	Effect Size (Eta2)
Contents cue	5.152	3.135	.079	.019
Leakage Cue	48.431	29.468	.000	.157
Contents cue × Context	5.520	3.359	.069	.021
Leakage Cue × Context	3.395	2.066	.153	.013

마지막으로, 내용 상의 신호가 인지된 메시지 신뢰도에 미치는 영향은 맥락화의 정도에 따라 차이가 있을 것이라는 가설 H3을 검증하기 위해 ANOVA 분석 외에 조절효과 분석을 추가적으로 실시하였다. <그림 9>는 내용 상의 신호에 대한 응답자들의 메시지 신뢰도를 저맥락과 고맥락의 두 집단으로 나누어 그 평균을 비교한 그래프이고, <그림 10>은 누설 신호의 여부에 따라 응답자들의 메시지 신뢰도를 저맥락과 고맥락 두 집단으로 나누어 각각의 평균을 비교한 그래프이다.

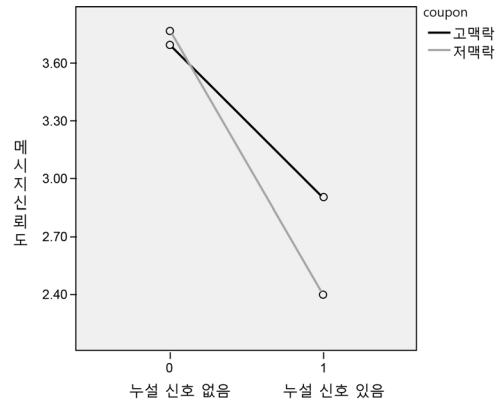
두 그래프를 보면 <그림 9>에서는 고맥락과 저맥락 두 집단 간 메시지 신뢰도의 차이가 뚜렷이 나타나지만, <그림 10>에서는 두 집단 간 메시지

1) 독립변수들 및 조절변수는 다음과 같이 코딩 되었다. Contents cue(정보의 완전성 = 0, 정보의 불완전성 = 1); Leakage cue(없음 = 0, 있음 = 1); Contextualization(상관 높음 = 0, 상관 낮음 = 1).

신뢰도에 분명한 차이가 나타나지 않는다. 특히 고맥락 메시지를 수신 했을 때 내용 상의 신호에 문제가 있는 경우(즉, 정보의 불완전성이 있는 경우) 수신자가 인지하는 메시지의 신뢰도가 급격히 저하되는 것으로 나타났다. 이 같은 결과는 내용 상의 신호가 메시지 신뢰도에 주는 영향에 있어 맥락화의 조절 효과가 존재한다는 가설 H3의 결과를 더욱 명백하게 보여준다. 아울러 이것은 가설 설정 단계에서 누설 신호에는 맥락화의 조절 효과가 존재하지 않을 것이라고 하였던 당초 예상을 뒷받침해 주고 있다.



〈그림 9〉 내용 상의 신호에 대한 맥락화의 조절효과 분석



〈그림10〉 누설 신호에 대한 맥락화의 조절효과 분석

4.3.2 메시지 신뢰도가 메시지 수용의사에 미치는 효과

인지된 메시지 신뢰도는 메시지 수용의사에 긍정적인 영향을 미칠 것이라는 가설 H4는 회귀분석을 통해 검증되었다.

종속변수를 메시지의 수용의사로 설정하였을 때 회귀 모형의 F값은 91.325($p < 0.01$)로, 99% 신뢰수준에서 모형이 적절한 것으로 나타났으며, 수정된 R^2의 값은 0.354로 독립변수가 종속변수를 35.4% 설명하고 있다. 회귀모형의 결과는 <표 9>에서 제시된 바와 같다. 즉, 인지된 메시지 신뢰도는 메시지 수용의사에 긍정적인 영향을 미치는 것으로 검증되었다.

〈표 9〉 메시지 수용의사에 대한 메시지 신뢰도의 회귀 분석 결과

	비표준화 계수		표준화 계수	t	p-value
	B	표준오차	베타		
메시지 신뢰도	.753	.079	.598	9.556	.000
수정된 R^2	0.354				
F	91.325				

Ⅴ. 결 론

5.1 연구의 시사점

본 연구의 목적은 메시지 신뢰도에 내용 상의 신호 및 누설 신호가 미치는 영향을 살펴보고, 동시에 이 두 가지 신호에서 맥락화의 조절효과를 확인하는 것이다. 더불어 메시지의 신뢰도가 수신자의 메시지 수용 의사에 미치는 영향, 즉 수신자가 메시지에 제시된 내용대로 행동하고자 하는 의도를 형성하는지 여부를 확인하고자 하였다. 이를 규명하기 위해 서베이 실험을 시행하였으며, 메시지의 두 가지 신호가 메시지 신뢰도에 영향을 끼치는 것을 확인할 수 있었다. 본 연구의 결과를 통해 맥락화가 정교화 가능성 모델에서 어떻게 작용하는지를 밝혀내었으며, 모바일 메시지에서 작용

하는 누설 신호에는 어떤 요소들이 있는지 구체적으로 찾아내었다. 본 연구의 학술적 및 실무적인 시사점은 다음과 같다.

5.1.1 학문적 시사점

기존 연구는 정교화 가능성 모델에서 관여도(involvement)의 조절효과를 밝히거나 그것을 응용하는데 그쳤지만, 본 연구는 주어진 메시지에 대해 수신자가 느끼는 맥락화(contextualization)의 정도가 중심경로를 조절하는 것을 보았다. 서베이 실험 결과 맥락화의 조절효과가 내용 상의 신호에만 나타난 점은 주목할 만하다. 이는 메시지가 본인과 관련 있는 내용이면 수신자로 하여금 내용 상의 신호에 집중하도록 하고, 메시지에 누설 신호가 포함되어 있을 시에는 맥락화의 정도와 상관없이 신뢰도가 저하되었음을 의미한다.

맥락화와 피싱 취약성의 관계를 규명한 선행연구에서는 주어진 피싱 메시지가 맥락화된 정도에 따라 피싱 취약성이 달라짐을 밝혔다(Goel *et al*., 2017). 누설 신호와 관련된 기존 연구들은 웹사이트 및 전자 메일의 컨텍스트 하에서 연구를 진행하는 것이 주를 이루었다. 그러나 본 연구는 정교화 가능성 모델을 활용한 메시지 신뢰도 변화를 스마트폰 메시지의 맥락에서 진행하였다. 또한 기존 연구 환경과는 다르게 스마트폰 메시지 환경에서 작용하는 누설 신호인 축약형 URL, 전국 대표번호가 아닌 발신번호, 특수 문자의 남발을 발견하였다.

5.1.2 실무적 시사점

기존 연구는 대부분 피싱 메시지에 대한 개인의 사생활 침해 우려(privacy concern)에 초점을 맞춰 진행되어 왔다. 본 연구에서는 피싱 메시지가 아닌, 기업의 홍보용 메시지를 소비자가 수신하였을 때 메시지의 두 가지 신호(내용 상의 신호와 누설 신호)가 메시지 신뢰도에 어떤 영향을 미치는지를 관찰하였다. 특히 메시지의 맥락화가 이 경로에 어떻게 작용하는지 분석하여 고맥락화의 경우에는 중심경로인 내용 상의 신호에 주목하게 하고, 누설 신호가 포함되었을 시에는 맥락화의 여부에 관계없이 메시지 신뢰도가 저하된다는 것을 규명하였다. 이러한 발견은 기존의 맥락화 연구와 차별화되며 기업에게 제공하는 시사점 역시 매우 의미 있다.

정교화 가능성 모델 및 맥락화를 사용한 기존의 피싱 연구는 피싱 메시지의 사회공학적인 요소를 강조하여, 수신자로 하여금 피싱 공격을 방지하도록 하는 방안을 강구하였다. 이는 개인 관점에서 보안을 제고할 수 있는 방안이기는 하지만, 소비자들에게 기업의 홍보 및 마케팅을 위한 효과성 높은 메시지를 전달하는데 관심을 두고 있는 기업에게는 큰 도움이 되지 못한다. 본 연구의 결과는 기업의 홍보 메시지를 소비자에게 효율적으로 전달할 수 있는 방법을 마련하는데 다양하게 응용 가능하다.

구체적으로 살펴보면 다음과 같다. 기업이 고객에게 모바일을 통한 프로모션을 진행할 때 신뢰도 및 메시지 수용의사를 높이기 위해서는 정확한 고객 목표 설정을 통해 개별 고객들에게 관여도가 높은 상품(또는 서비스)을 골라 맞춤형 프로모션을 진행해야 한다. 또한 내용 상의 신호(contents cue)에 생긴 결함과 누설 신호(leakage cue)는 메시지 신뢰도를 저하시키며, 이는 결국 쿠폰 다운로드 권유 등 메시지에 제시된 사항을 수신자가 따르지 않게 할 가능성을 높인다. 따라서 메시지 완전성(즉, 내용 상의 신호) 측면에서 수신자의 의사결정을 이끌어 낼 정보가 구체적으로 존재해야 한다. 본 연구에서 규명해 낸 누설 신호인 의심스러운 URL 링크(축약형 링크), 발신번호, 맞춤법 및 특수문자에도 각별히 주의해야 한다. 기업이 소비자에게 스마트폰 메시지를 보낼 때, 용량 등의 문제로 인해 가능한 간략하게 내용을 구성하는 경향이 있다. 하지만 본 연구의 결과 축약형 URL 주소를 사용할 경우, 수신자가 인지하는 메시지 신뢰도가 떨어지는 것으로 나타났기 때문에 URL 링크는 축약형 대신 기업의 이름이 확실하게 드러나는 주소를 사용해야 한다. 발신번호는 인터넷 전화 번호 대신 전국 대표번호를 사용하는 편이 수신자의 메시지에 대한 신뢰도 저하를 막을 수 있다. 또한 맞춤

법의 경우, 철자와 문법 요소 외에도 특수문자의 과도한 사용을 자제해야 한다는 것을 밝혀냈다.

5.2 연구의 한계 및 향후 연구

이러한 학문적, 실용적 의의에도 불구하고 본 연구는 다음과 같은 한계점을 가지고 있는 것으로 판단된다. 우선 온라인을 통한 서베이 실험으로 연구를 진행하여 횡단적인 조사로 데이터를 수집하였다는 점을 지적할 수 있다. 이러한 경우 동일방법편의의 문제가 발생할 수 있다. 이를 방지하고자 종속변수를 측정하는 항목을 설문지 앞부분에 배치하였다. 아울러 하만의 단일 요인 검사도 병행하여 실시하였다. 이러한 결과를 바탕으로 동일방법편의의 문제는 본 연구에서 크게 영향을 받지 않은 것으로 볼 수 있다. 그러나 추후 연구에서는 종단적 연구를 통한 데이터 수집을 병행하여 보다 심도 있는 분석을 도모할 수 있을 것이다.

또한 서베이 실험 참여자를 편의표본추출(convenient sampling)로 모집하였다는 문제가 있다. 본 연구는 응답자의 참여를 넓히기 위한 목적으로 편의를 고려해 카카오톡이나 페이스북을 활용해 설문을 링크 방식으로 배포하였으며, 대부분의 참여자는 서울지역 3개 대학의 학부생 및 대학원생으로 이루어져 있다. 이 때문에 표본으로 선택된 학부생과 직장인의 비율을 비교해 보았을 때 전자가 압도적으로 많았다. 이러한 방식은 연구 결과의 외적 타당성(external validity)을 확보하는데 한계를 가진다. 따라서 본 연구는 자료 수집의 제약으로 인해 특정 집단을 중심으로 편의표본추출을 시행하였으므로 연구 결과를 일반화하는데 문제점을 안고 있다. 다만 서베이 실험 표본이 대부분 20~30대에서 추출되었다는 점은 일견 장점이 될 수 있다. 소비 채널로 모바일을 활용하는 세대가 대부분 20대에서 30대에 분포하고 있기 때문이다(이중배, 2015).

연구의 외적 타당성과 관련된 또 다른 문제로 실험 방식을 꼽을 수 있다. 참여자에게 실제 스마트폰 문자 메시지를 보내고 반응을 포착하는 대신 시나리오로 실험의 상황을 제시한 후 설문에 응답하도록 했기 때문에 연구의 외적 타당성이 현장실험(field experiment)에 비해서는 다소 부족할 수 있다. 향후 연구에서는 현장 실험을 통한 데이터 수집을 하는 방안을 고려해 볼 수 있을 것이다.

마지막으로 실험 설계 시 독립 변인을 누설 신호 유무로 설정하여 진행하였기 때문에 누설 신호의 세 가지 요소인 맞춤법, 링크, 발신자의 개별적 효과를 측정하는데 어려움이 있었다. 향후 연구에서는 이러한 누설 신호를 세부적으로 구별하여 실무적 함의를 높이고자 한다.

최근에는 많은 스마트폰 사용자가 SMS 외의 수단(소셜 미디어, 메신저 등)을 커뮤니케이션 용도로 사용하고 있다. 기업 대표성을 지닌 메시지를 전달하거나 본인 인증 등의 수단으로써 SMS는 여전히 유용하지만, 향후 연구에서는 최근 많은 사용자들로부터 각광을 받고 있는 카카오톡, 라인 등의 메신저 채널까지 연구 대상으로 확대할 필요가 있다. 이러한 채널까지 반영한다면 한 층 더 발전된 실무적 시사점을 제공할 수 있을 것으로 기대된다.

참 고 문 헌

[1] 남기화, 여정성, “모바일 광고의 단계별 수용과정에 관한 연구”, *소비자학연구*, 제22권, 제4호, 2011, pp. 1-28.

[2] 박세정, “세계 스마트폰 보급률 70% 육박… 세계1위 한국은 몇%?”, 디지털타임스, 2016.7.2, Available at http://www.dt.co.kr/contents.html?article_no=2016070102100151780001.

[3] 이중배, “2015 라이프 스타일과 소비 성향: 10대부터 50대까지”, 슬로우뉴스, 2015.9.3, Available at http://slownews.kr/45332.

[4] 정기석, “국내 모바일 간편결제 활성화 방안에 관한 연구”, *융합보안논문지*, 제15권, 제4호, 2013, pp. 79-88.

[5] 정용준, 김예진, “상관분석 및 의사결정나무분석을 통한 하수처리시설의 에너지 소비량과

운영인자의 관계 분석", *Journal of Korean Society on Water Environment*, 제32권, 제3호, 2016, pp. 253-260.

[6] 최양서, 서동일, "사회공학적 공격방법을 통한 개인정보 유출기술 및 대응방안 분석", *정보보호학회지*, 제16권, 제1호, 2006, pp. 40-48.

[7] 허경옥, "소비자의 구매의사결정 행동유형이 TV 광고에 대한 소비자신뢰도 및 수용도에 미치는 영향", *소비자문제연구*, 제26권, 제2호, 2015, pp. 1-22.

[8] 홍종선, "'토종 1호' 소셜커머스 창업 신현성 티몬 이사회 의장 "알면 알수록 도전하는 게 힘들다, 나도 두렵다", 주간동아, 2017.8.2, Available at http://weekly.donga.com/3/all/11/1012634/1.

[9] Abu-Nimeh, S., D. Nappa, X. Wang, and S. Nair, "A comparison of machine learning techniques for phishing detection", In *Proceedings of the Anti-Phishing Working Groups 2nd Annual eCrime Researchers Summit*, 2007, pp. 60-69.

[10] Bamba, F. and S. J. Barnes, "SMS advertising, permission and the consumer: A study", *Business Process Management Journal*, Vol.13, 2007, pp. 815-829.

[11] Castañeda, J. A. and F. J. Montoro, "The effect of Internet general privacy concern on customer behavior", *Electronic Commerce Research*, Vol.7, No.2, 2007, pp. 117-141.

[12] Cheung, C. M. Y., C. L. Sia, and K. K. Kuan, "Is this review believable? A study of factors affecting the credibility of online consumer reviews from an ELM perspective", *Journal of the Association for Information Systems*, Vol.13, 2012, pp. 618-635.

[13] Chutijirawong, N. and P. Kanawattanachai, "The role and impact of context-driven personalisation technology on customer acceptance of advertising via short message service (SMS)", *International Journal of Mobile Communications*, Vol.12, No.6, 2014, pp. 578-602.

[14] Cialdini, R. B., *Influence: Science and Practice*, Pearson Education, Boston, 2009.

[15] Dharmadasa, P. and T. Alahakoon, "An empirical study of factors influencing consumer attitudes towards SMS advertising", *International Journal of Online Marketing (IJOM)*, Vol.4, No.3, 2014, pp. 1-13.

[16] Dinev, T., A. R. McConnell, and H. Jeff Smith, "Research commentary-informing privacy research through information systems, psychology, and behavioral economics: Thinking outside the "APCO" Box", *Information Systems Research*, Vol.26 No.4, 2015, pp. 639-655.

[17] Drossos, D., G. M. Giaglis, G. Lekakos, F. Kokkinaki, and M. G. Stavraki, "Determinants of effective SMS advertising: An experimental study", *Journal of Interactive Advertising*, Vol.7, No.2, 2007, pp. 16-27.

[18] Drossos, D., G. M. Glaglis, G. Lekakos, F. Kokkinaki, and M. G. Stavraki, "Determinants of effective SMS advertising: An experimental study", *Journal of Interactive Advertising*, Vol.7, No.2, 2007, pp. 16-27.

[19] Dutta-Bergman, M. J., "The impact of completeness and Web use motivation on the credibility of e-health information", *Journal of Communication*, Vol.54, No.2, 2004, pp. 253-269.

[20] Eveland, W. P., D. V. Shah, and N. Kwak, "Assessing causality in the cognitive mediation model: A panel study of motivations, information processing, and learning during campaign", *Communication Research*, Vol.30, 2003, pp. 359-386.

[21] EY.com, "Creating trust in the digital world", EY's Global Information Security Survey 2015, 2015.

[22] Goel, S., K. Williams, and E. Dincelli, "Got phished? Internet security and human vulnerability",

Journal of the Association for Information Systems, Vol.1, No.1, 2017, pp. 22-44.

[23] Harrison, B., E. Svetieva, and A. Vishwanath, "Individual processing of phishing emails How attention and elaboration protect against phishing", *Online Information Review*, Vol.40, No.2, 2016, pp. 265-281.

[24] Jagatic, T., N. Johnson, M. Jakobsson, and F. Menczer, *Social Phishing*, School of Informatics and Department of Computer Science, Indiana University, 2006, Available at http://www.indiana.edu/~phishing/social-network-experience/phishing-preprint.pdf.

[25] Jakobsson, M. and J. Ratkiewicz, "Designing ethical phishing experiments: A study of (ROT13) rOnl query features", In *Proceedings of the 15th International Conference on World Wide Web*, 2006, pp. 513-522.

[26] Jakobsson, M., A. Tsow, A. Shah, E. Blevis, and Y. K. Lim, "What instills trust? A qualitative study of phishing", In *Proceedings of the 11th International Conference on Financial Cryptography*, 2007, pp. 356-361.

[27] Jakobsson, M., *The human factor in phishing, Privacy and Security of Consumer Information*, Indiana University, Bloomington, IN, 2007.

[28] Johnson, P. E., S. Grazioli, K. Jamal, and I .A. Zualkernan, "Success and failure in expert reasoning", *Organizational Behavior and Human Decision Processes*, Vol.53, 1992, pp. 173-203.

[29] Mathieson, K., "Predicting user intentions: Comparing the technology acceptance model with the theory of planned behavior", *Information Systems Research*, Vol.2, 1991, pp. 173-191.

[30] Mitnick, K. and W. L. Simon, *The Art of Deception: Controlling the Human Element of Security*, New York, John Wiley & Sons, 2011.

[31] Nov, O. and C. Ye, "Users' personality and perceived ease of use of digital libraries: The case for resistance to change", *Journal of the American Society for Information Science and Technology*, Vol.53, 2008, pp. 845-851.

[32] Perse, E. M., "Audience selectivity and involvement in the newer media environment", *Communication Research*, Vol.17, 1990, pp. 675-697.

[33] Petty, R. E. and D. T. Wegener *Attitude Change: Multiple Roles for Persuasion Variables*, New York, McGraw-Hill, 1998.

[34] Petty, R. E. and J. T. Cacioppo, *Attitudes and Persuasion: Classic and Contemporary Approaches*, William C. Brown, Dubuque, IA, 1981.

[35] Sutanto, J., E. Palme, C. H. Tan, and C. W. Phang, "Addressing the personalization-privacy paradox: An empirical assessment from a field experiment on smartphone users", *Mis Quarterly*, Vol.37, No.4, 2013, pp. 1141-1164.

[36] Vishwanath, A., T. Herath, R. Chen, J. Wang, and H. R. Rao, "Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model", *Decision Support Systems*, Vol.51, 2011, pp. 576-586.

[37] Wang, C., P. Zhang, R. Choi, and M. DíEredita, "Understanding consumers attitude toward advertising", Eighth Americas Conference on Information Systems, 2002, Available at http://www.sigh-ci.org/amcis02/RIP/Dishaw.pdf.

[38] Wirtz, J., M. O. Lwin, and J. D. Williams, "Causes and consequences of consumer online privacy concern", *International Journal of Service Industry Management*, Vol.18, No.4, 2007, pp. 326-348.

[39] Zaichkowsky, J. L., "Measuring the involvement construct", *The Journal of Consumer Research*, Vol.12, 1985, pp. 341-352.

[40] Zhou, T., "The impact of privacy concern on user adoption of location-based services", *Industrial Management and Data Systems*, Vol.111, No.2, 2011, pp. 212-226.

Information Systems Review
Volume 20 Number 1
March 2018

The Effect of Message Completeness and Leakage Cues on the Credibility of Mobile Promotion Messages

Hyun Jun Jeon* · Jin Seon Choe* · Jai-Yeol Son**

Abstract

Individuals often receive smishing campaigns (mobile phishing messages), which they treat as spam. Thus, firms should understand how their customers distinguish their promotion messages from smishing. However, only a few studies examined this important issue. The present study employs the elaboration likelihood model to develop research hypotheses on the relationship between message cue and message credibility. The message cue in this study is classified as content cue, which is found in the content of promotion messages, and as leakage cue, which is found in peripheral information in the message. Leakage cue includes orthography (inclusion of special characters)and an abbreviated link sent by a faithless sender. We also propose that contextualization has a moderating effect on the relationship between content cue and credibility. We conducted a survey experiment to examine the effect of message cues on message credibility in the context of respondents receiving discount coupons through mobile messages. The result of data analysis based on 166 responses suggests that leakage cue had a negative effect on message credibility. A message with defective content cue has a marginally negative effect on message credibility. In particular, defective content cue in a high-contextual message has a strong negative impact on message credibility. This effect was not observed in low-contextual messages. Moreover, message credibility is significantly low regardless of the degree of contextualization if there is a leakage cue in the message. Our findings suggest that mobile promotion messages should be customized for message receivers and should have no leakage cues.

Keywords: ***Message Credibility, Smart Phone, Elaboration Likelihood Model, Leakage Cue, Contents Cue, Involvement, Contextualization***

* School of Business, Yonsei University
** Corresponding Author, School of Business, Yonsei University

◐ 저 자 소 개 ◑

전 현 준 (hjjun@withconsumer.org)

연세대학교 경영학과에서 정보시스템 전공으로 석사 학위를 취득하였고, 현재 '(사) 소비자와 함께'에서 프로젝트 매니저로 근무 중이다. 주요 관심분야는 온라인 상의 사용자 행위 등이다.

최 진 선 (jschoe@yonsei.ac.kr)

이화여자대학교 경영전문대학원에서 석사 학위를 취득하였으며, 연세대학교 경영학과 정보시스템 전공 박사 과정에 재학 중이다. 주요 관심분야는 모바일 플랫폼, 정보 검색 행위, E-Commerce 등이다.

손 재 열 (json@yonsei.ac.kr)

현재 연세대학교 경영학과 정보시스템 교수로 재직 중이다. 캐나다 University of British Columbia의 Sauder School of Business에서 경영정보시스템 분야 교수를 역임하였다. 미국 Georgia Institute of Technology에서 information technology management 박사 학위를 취득하였다. 연구 관심분야는 온라인 상의 사용자 행위, 정보보안, 조직 간 시스템 등이다. MIS Quarterly, Journal of Management Information Systems, Journal of the Association for Information Systems 등의 저널에 논문을 발표하였다.

논문접수일 : 2018년 01월 16일 **게재확정일 : 2018년 03월 15일**
1차 수정일 : 2018년 03월 02일 **2차 수정일 : 2018년 03월 14일**