Research Paper Informatization Policy Vol. 31, No.2 (2024), pp.082-104
https://doi.org/10.22693/NIAIP.2024.31.2.082

스마트 IoT 서비스 사용자의 개인정보 보호 행동 준수: 소프트웨어 업데이트 유도를 위한 메세지 디자인 특성에 관한 실증 연구*, **

이 호 진*** · 김 형 진**** · 이 호 근*****

요 약

사물인터넷(IoT)의 발전으로 이른바 '연결된 생활(Connected Living)'이 가능해지면서 스마트 홈 서비스가 급격한 성장세를 보이고 있다. 그런데 스마트 홈 카메라를 통한 개인정보 유출 피해가 늘어나고 있으나, 사용자들은 걱정을 하면서도 개인정보 보호 행동에는 소극적인 성향을 보이고 있다. 본 연구는 스마트 홈 카메라의 소프트웨어 업데이트 알림 메시지를 어떻게 디자인하는 것이 사용자의 보안행동 준수(업데이트 설치)에 효과적인지를 이론적으로 설명하고 검증하였다. 실제 사용자 120명이 참여한 설문 실험을 통해 확인한 결과, 감정적 소구(공포 유발을 위한 보안침해 경고 이미지), 이성적 소구(업데이트 미설치 시 발생할 수 있는 부정적 결과(영상 유출)를 강조한 손실 프레이밍 메시지))의 효과가 모두 확인되었다. 본 연구의 결과는 스마트 홈 카메라 사용자의 위협 판단(Threat Appraisal) 및 보호 동기(Protection Motivation) 형성에 효과적인 메시지 디자인 특성(Message Design Features)에 대한 이론적 해석을 제공하며, 실무적인 가이드라인 마련에 도움이 될 수 있다.

주제어 : IoT 서비스, 스마트 홈 카메라, 개인정보 보호 행동, 사용자 준수, 보호 동기, 소프트웨어 업데이트, 메시지 디자인 특성, 공포 소구, 이득-손실 메시지 프레이밍

Smart IoT Service Users' Compliance with Personal Information Protection Behavior: An Empirical Study on the Message Design Features to Induce Installation of Software Updates*, **

Lee, Ho-Jin*** · Kim, Hyung-Jin**** · Lee, Ho-Geun*****

Abstract

Smart home services are growing rapidly as the development of the Internet of Things (IoT) opens the era of the so-called "Connected Living." Although personal information leaks through smart home cameras are increasing, however, users—while concerned—tend to take passive measures to protect their personal information. This study theoretically explained and verified how to design effective software update notification messages for smart home cameras to ensure that users comply with the recommended security behavior (i.e., update installation). In a survey experiment participated in by 120 actual users, the effectiveness of both emotional appeals (i.e., security breach warning images for fear appeals) and rational appeals (i.e., loss-framed messages emphasizing the negative consequences of not installing the updates) were confirmed. The results of this study provide theoretical interpretations and practical guidelines on the message design features that are effective for threat appraisals (i.e., severity, vulnerability) of smart home camera users and their protection motivation.

Keywords : IoT service, smart home camera, personal information protection behavior, end-user compliance, protection motivation, software updates, message design features, fear appeals, gain-loss message framing

Received May 29, 2024; Revised May 31, 2024; Accepted Jun 5, 2024

* This work was supported by Yonsei Business Research Institute

** This article is revision of the first author's master's thesis from Yonsei University.

*** First Author, Cell Leader, DOUZONE Bizon (mailrorok@gmail.com, https://orcid.org/0009-0005-7131-5282)

**** Corresponding Author, Chief Officer, Industrial Convergence Regulation Office, Korea Institute of Industrial Technology (kimhyungjin@kitech.re.kr, https://orcid.org/0000-0002-9188-2736)

***** Co-Author, Professor, Yonsei University, School of Business (h.lee@yonsei.ac.kr, https://orcid.org/0000-0002-5438-8552)

I. 서론

지금으로부터 20여 년 전, 사물 인터넷(Internet of Things, 이하 IoT)이란 용어는 PC기반의 인터넷을 넘어 우리 주변 다양한 사물에 센서와 네트워크 기술이 탑재되는 새로운 세상을 의미하는 용어로 등장했다. 그리고 최근에는 전문 기술 분야뿐만 아니라 우리의 일상생활 속 깊숙이까지 들어와 '연결된 생활(Connected Living)'이라는 새로운 트렌드의 중심이 되었다. 일례로, 여러 가지 홈 디바이스들을 유무선 네트워크로 연결한 스마트 홈 서비스(Smart Home Service)가 대중적인 인기를 끌고 있다. 인공지능 스피커, 월패드(Wall Pad), 홈 카메라, 스마트 플러그와 조명, IoT 가전 등 스마트 홈 서비스를 구성하는 IoT 디바이스들도 점차 다양화되고 있다.

스마트 홈 서비스는 소비자로 하여금 주거공간에서 필요한 다양한 기기 제어 및 자동화, 모니터링 등을 가능하게 해준다(Hayes, 2024). 출근 전 깜빡 잊고 끄지 못한 거실 등을 모바일 앱을 통해 원격으로 소등하거나, 기온이 갑자기 떨어진 날 집에 도착하기 전에 보일러를 미리 켤 수 있다는 것은 IoT 기술이 가져다 준 전에 없던 편리함이다. 또, 아이들이나 반려동물이 하루 종일 안전하게 지내고 있는지 걱정되는 가구들에게 홈 카메라는 편리함 이상으로 중요한 니즈를 충족시켜주고 있다.

이런 인기에 힘입어 전 세계 스마트 홈 가구 수는 하루가 다르게 증가하고 있으며, 2025년 4억 8천만 가구로 증가할 것으로 예상된다(Statista, 2024). 글로벌 스마트 홈 시장은 2022년 790억 달러 수준으로 평가되었으며, 2023년부터 2030년까지 27%가 넘는 연평균복합성장률(Compound Average Growth Rate, CACR)을 보일 것으로 예상되고 있다(Grand View Research, 2023a).

스마트 홈 서비스 중에서 보안 관련 서비스(Smart Home Security)는 홈 에너지 절약(Energy Saving) 서비스와 함께 수요 증가가 가장 두드러진 분야이다(Grand View Research, 2023a). 원격 실시간 모니터링, 얼굴 인식 등을 통해 외부 침입을 억제하고, 침입 행위를 감지, 신속한 알림을 제공해주는 등 스마트 감시 시스템(Smart Surveillance System)으로서의 역할이 인기를 얻고 있기 때문이다. 실제로 전 세계 스마트 홈 카메라 시장은 2023년 현재 약 81억 달러에 달하며, 2030년까지 19.2%의 성장률(CACR)이 기대된다(Grand View Research, 2023b).

그런데, 이러한 확산 추세 이면으로 우려 섞인 목소리도 높아지고 있다. 홈 카메라를 통한 개인정보 유출 때문이다. 기존 폐쇄회로 감시 카메라(CCTV)와 달리, IP기반의 스마트 홈 카메라는 인터넷을 통해 데이터(녹화 영상 등) 전송, 양방향 오디오, 원격 접속 등이 가능하고 클라우드 서버 연결을 통한 실시간 스트리밍을 제공한다. 그런데, 역설적이게도 이러한 스마트 기기로서의 효용이 외부의 위협으로부터 타깃이 될 수 있는 것이다. 대부분의 스마트 홈 기기들은 이른바 '저사양 IoT 디바이스'로, 낮은 수준의 보안 기술이 적용되어 있어 보안에 상대적으로 취약한 것으로 알려져 있다(Lee, et al., 2018). 실제로, 몇 가지 프로그램만 활용하면 인터넷을 통해 타인의 웹캠에 쉽게 접근하여 촬영 화면을 보는 게 가능할 정도이다(Kim, 2016; Lee, 2019).

그럼에도 불구하고, 사용자의 개인정보보호 실천 비율이 상대적으로 높지 않아 불안함을 더하고 있다. 개인정보보호란 특정 개인을 식별할 수 있는 이름, 주민등록번호, 영상 등의 정보들을 동의 없이 유출하려는 위협으로부터 보호하기 위한 다양한 활동을 말한다(Korea Information Security Industry Association, 2021).

선행 연구들은 분산 환경의 정보시스템이나 PC, 모바일과 같은 개인 정보기기의 보안 유지를 위한 최선의 방법은 소프트웨어를 최신 버전으로 신속하게 업데이트 하는 것이라고 주장해왔다(Mathur & Chetty, 2017; Möller, et al., 2012). 그러나, 최근 발표된 정부 통계에 따르면, 스마트 홈 카메라에 대한 보안 조치로 소프트웨어를 업데이트하고 있는 사용자는 전체 응답자 중 42.4% 수준에 그치고 있다(Korea

Information Security Industry Association, 2021). 흥미로운 것은 응답자 중 74.1%는 IP 카메라를 통한 '많은 종류의 영상 데이터 발생 및 처리로 인한 개인정보 침해 위협 증가'를 우려하고 있으며, '영상정보 노출에 따른 2차 범죄(주거침입, 성범죄 등)를 우려'하는 비율도 61.5%에 달했다. 즉, 사용자들은 스마트 홈 카메라 이용으로 인한 보안 위협들을 인지하고는 있지만, 인지된 위협에 대한 실질적인 개인정보 보호 행동에는 상대적으로 소극적인 모습을 보였다.

본 연구는 이와 같은 프라이버시 패러독스(Privacy Paradox) 현상에 대한 이해를 바탕으로, 스마트 홈 카메라 사용자의 개인정보 보호 행동(소프트웨어 업데이트)을 효과적으로 유도할 수 있는 방법을 찾고자 하였다. 시스템 보안 및 정보 보호는 기술적 향상(Technological Advance)을 통한 대처뿐만 아니라, 사용자 행위 관점의 변화가 반드시 필요하기 때문이다(Lee, 2021; Möller, et al., 2012; Wash, et al., 2014).

이와 같은 연구 목적을 위해 본 연구는 보호동기이론(Protection Motivation Theory)을 토대로, 스마트 홈 카메라의 소프트웨어 업데이트 알림 메시지(Software Update Message)를 어떻게 디자인하는 것이 효과적인지를 공포 소구(Fear Appeal)와 이득-손실 프레이밍(Gain-Loss Framing) 관점에서 이론적으로 설계하고 검증하였다. 본 연구의 결과는 스마트 홈 카메라 사용자의 위협 판단(Threat Appraisal) 및 보호 동기(Protection Motivation) 형성에 효과적인 메시지 디자인 특성들(Message Design Features)에 대한 이론적 해석을 제공하며, 실무적인 가이드라인 마련에 도움이 될 수 있다.

Ⅱ. 이론적 배경

1. 스마트 홈 프라이버시 침해

정보 프라이버시(Information Privacy)는 개인 정보를 수집하고 활용하는 정보 기술이 발달하면서 등장한 개념으로, 최근 들어 정보의 주체인 개인들이 본인과 관련된 정보에 대한 통제권을 침해당하는 사례들이 늘어나고 있다. 일례로, 40만 개가 넘는 가정용 웰패드가 해킹되어 사생활 영상과 사진이 유출된 사례가 국내에서도 발생할 정도로, IoT 확산에 따른 프라이버시 침해는 어느덧 중요한 사회적 문제가 되었다(Lee, 2023). 이에 따라, 프라이버시 염려(Privacy Concern), 즉 동의 없이 개인 정보가 유출되거나 합의되지 않은 목적으로 활용됨에 따른 사생활 침해 및 그로 인한 금전적·물리적 피해를 걱정하는 사람들도 많아졌다.

스마트 홈을 구성하는 IoT 기기들의 보안 위협을 분석한 연구들에 따르면, 홈캠이나 로봇 청소기 등과 같이 실내용 카메라를 내장한 디바이스와 관련된 프라이버시 침해 가능성이 단연 눈에 띈다(Kim, 2016; Yoo, 2022). 네트워크에 연결된 IP 카메라에 불법 접근하여 개인의 사생활을 실시간으로 엿보거나, 촬영된 사진 및 영상을 외부로 유출하는 경우 개인의 사생활이 심각하게 침해 받기 때문이다. 실제로, 2018년 반려동물 확인용 홈 카메라를 해킹해서 수 만 명의 일상을 훔쳐본 사건이 있기도 했다(Lyu & Kwon, 2021).

선행 연구들은 IoT 서비스를 구성하는 요소들(IoT 디바이스, 네트워크, 플랫폼 등) 중에서 보안 위협이 가장 큰 대상으로 디바이스를 손꼽고 있다(Yoo, 2022). 대부분 저전력, 경량화, 소형화 제품으로 낮은 처리 성능과 부족한 메모리를 특징으로 하고 있어서 PC 환경에서 사용하는 보안 솔루션을 적용할 수 없기 때문이다. 최소한의 기능들로 구현한 저사양 제품이기 때문에 보안에 취약한 태생적 한계를 갖고 있는 것이다(Lee, et al., 2018). 이에 따라, 경량화 암호화 알고리즘을 이용한 데이터의 암/복호화 방법이나, SDN(Software Defined Network) 환경에서의 인증 방법 등 기술적 대처 방안에 관한 연구들(예: Majeed, 2017; Salman, et al., 2017)이 이어지고 있다.

그러나 기술적 향상을 통해 보안 위협을 낮추거나 대비하는 방법 외에 사용자의 행동 관점에서 정보 프

라이버시 침해를 줄일 수 있는 방안들에 대한 중요성도 강조되고 있다(Möller, et al. 2012; Wash, et al., 2014). 아무리 기술적 보안 수준을 높인다고 하더라도 사용자 개입(User Intervention) 없이는 실현되지 못하는 경우가 있기 때문이다.

선행 연구에 따르면, 정보기기 기업들은 소프트웨어 업데이트를 신속하게 마련하여 배포함으로써 보안 위협에 대비하고 있으나, 사용자들은 다양한 이유(재부팅해야 하는 번거로움 등)로 업데이트 설치를 미루거나 간과하는 경향이 있다(Mathur & Chetty, 2017; Wash, et al., 2014). 또한, 프라이버시 침해를 염려하면서도 누구나 추측할 수 있는 공장셋팅 비밀번호(가령, 0000)를 변경 없이 사용하고 있는 사용자들도 주변에서 쉽게 찾을 수 있다. 때문에, 보안 기술이 아니라 사용자 행동 관점에서 대안을 찾고자 하는 연구자들이 많아지고 있는 것이다(예: Anderson & Agarwal, 2010; Angst & Agarwal, 2009; Park, 2017).

2. 소프트웨어 업데이트

대부분의 소프트웨어 업데이트는 이전 버전의 버그(bug)를 바로 잡거나, 보안 취약성을 보완하거나, 새로운 기능을 추가하는 등 다양한 목적을 위해 준비된다. 그런데, 보안과 관련해서는 신속하게 보안 패치나 새로운 버전을 배포하는 것이 피해 확산을 막는 데 무엇보다 중요하다. 때문에, 기업 입장에서는 사용자들이 가급적 빨리 최신 버전의 소프트웨어를 설치하는 이른바 사용자 준수(End-User Compliance) 행위가 절실하기까지 하다.

그러나 안타깝게도 대부분의 보안 침해 사례는 해당 보안 취약성을 개선하기 위한 최신 버전의 소프트웨어가 배포되었음에도 불구하고 사용자가 설치하지 않아 발생하는 것으로 알려져 있다(Microsoft, 2012; Symantec Corporation, 2013). 모바일 앱에 대한 사용자 업데이트를 분석한 Möller, et al.(2012)에 따르면, 업데이트 버전이 공개된 지 일주일 이후에도 사용자의 절반이 보안에 취약한 이전 버전의 앱을 사용하고 있는 것으로 나타났다.

뿐만 아니라, 사용자의 업데이트 설치가 늦어질수록 보안 위협에 노출될 가능성은 급격히 높아진다(Bilge & Dumitras, 2012). 최신 업데이트 공개와 함께 해당 보안 취약성이 공식적으로 알려지기 때문이다(Microsoft, 2012). Microsoft가 Windows ME부터 자동 업데이트(Automated Updates) 기능을 추가하게 된 이유가 바로 여기에 있다(Mathur & Chetty, 2017).

보안 위협에 대해 사용자들은 결코 시스템 관리자처럼 생각하지 않으며, 선택할 수만 있다면 그들이 바라는 다른 목적을 위해서 낮은 보안 수준도 무시하는 경향이 있다(Wash, et al., 2014). 때문에, 사용자들에게 보안이 중요해지는 순간은 대부분 침해 사례가 발생한 이후인 경우가 많다.

이러한 배경에서 연구자들은 사용자가 업데이트를 설치하도록 유도하기 위해 노력해왔다. 그리고 그러한 방법의 일환으로 업데이트 알림 메시지 디자인에 대한 연구가 주목을 받았다. 예를 들어, Fagan, et al.(2015a,b)은 C-HIP 모델(Communication-Human Information Processing Model)(Conzola & Wogalter, 2001)과 ARI 모델(Affect-Reason-Involvement Model)(Buck, et al., 2004)의 관점에서 다양한 업데이트 알림 메시지 디자인에 대한 사용자 태도를 분석하였다. 그 결과, 알림 메세지는 사용자의 주목을 끌 수 있어야 하며(Attention-Grabbing), 업데이트의 목적과 결과 등에 대해 설명하고 사용자가 이해할 수 있도록 해야 한다고 했다(Understandable). 또한, 성가시거나(Annoying) 혼란스럽지(Confusing) 않아야 업데이트를 망설이거나 거부하는 부정적인 반응이 줄어든다고 하였다.

한편, 보호동기이론(Protection Motivation Theory)의 관점에서 사용자의 보안 행동 준수 또는 이행을 이해하고자 한 선행연구들도 본 연구의 이론적 기반이 될 수 있다. 소프트웨어 업데이트를 설치하는 목적이 보안 위협으로부터 사용자를 보호하기 위

한 것이기 때문이다. 인간은 위협으로부터 스스로를 보호하고자 하는 동기가 생겼을 때 행동에 변화를 준다(Rogers, 1975). 선행 연구들은 이러한 보호 동기를 유발하기 위한 방법으로 공포 소구에 많은 관심을 기울여 왔다(Lee, et al., 2013).

3. 공포 소구(fear appeals)

소프트웨어 업데이트 알림 메시지는 위험에 관한 커뮤니케이션(Risk Communication) 또는 설득 커뮤니케이션(Persuasive Communication)의 일종이다(Johnston & Warkentin, 2010). 보안 관련 위협 및 대안(Countervailing Measures)에 관한 내용을 제공하며 사용자로 하여금 권장 행동을 하도록 동기를 부여하는 것을 목적으로 하기 때문이다. 설득 커뮤니케이션은 인간의 태도나, 의도, 행동을 변화시키는 데 효과적인 방법이며(Fishbein & Ajzen, 1975), 이러한 관점에서 사용자의 보안 행동(데이터 백업, 멀웨어 방지 프로그램 사용 등)을 이해하고자 한 선행 연구들은 주로 보호동기이론에 기반을 두고 있다(Boss, et al., 2015).

보호동기이론에 따르면 개인들은 위협으로부터 본인(혹은 본인이 소속된 조직)을 보호하려는 동기 부여가 되면 특정 행동을 하거나 행동에 변화를 준다. 이러한 행동은 두 가지 평가 프로세스(Appraisal Processes) - 위협 평가(위협의 심각성과 위협에 대한 취약성), 대안 평가(권장 행동의 효과성과 자기 효능감) -를 통해서 생긴 보호 동기에 의해서 발생한다(Rogers, 1975; 1983). 즉, 심각한 결과를 초래하는 위협일수록(Threat Severity), 해당 위협에 본인이 취약하다고 판단될수록(Threat Vulnerability) 더 높은 수준의 보호 동기가 생기고 권장 행동을 따를 가능성도 커진다. 다른 한편으로는, 대처 방안으로 제시된 권장 행동이 위협에 대해 효과적이라고 판단될수록(Response Efficacy), 권장 행동과 관련된 자기 효능감이 클수록(Self-Efficacy) 보호 동기는 커진다.

보호동기이론은 공포 소구에 관한 여러 이론들의 진화 과정에서 등장한 이론 중 하나로, 질병이나 보안 위협 등 여러 분야의 연구뿐만 아니라 광고나 캠페인 등에서도 자주 활용되는 이론이다(Lee, et al., 2013). 여기서 공포 소구란 상대방으로 하여금 위협으로 인한 공포를 느끼게 하여 태도나 행동에 변화를 유도하는 설득 커뮤니케이션 방법이다(Witte & Allen, 2000). 따라서, 위협을 묘사하거나 관련하여 발생할 수 있는 끔찍한 결과를 설명하는 메시지 형태로 주로 디자인된다(Hale, et al., 1995; Witte, 1992). 흡연이나 음주 관련 건강 캠페인에서 폐암과 같은 질병 정보나 이미지를 제공하는 것이 공포 소구를 활용한 좋은 예이다.

이러한 공포 소구의 효과는 최근 보안 관련 컨텍스트에서도 자주 확인된다. 관련 연구들에 따르면 스파이웨어 방지 프로그램 사용, 데이터 백업, 스마트폰 보안수칙 준수, 강력한 인터넷 비밀번호 설정하기 등 사용자의 다양한 보안 행동을 유도하는 데 공포 소구가 효과적인 것으로 나타났다(Johnston & Warkentin, 2010; Kim & Kim, 2023; Mwagwabi, et al., 2014; Park, et al., 2017; Zhang & McDowell, 2009).

4. 이득-손실 프레이밍(gain-loss framing)

행동 변화를 위한 설득 커뮤니케이션의 성공을 결정짓는 요인들은 크게 메시지에 관한 것과 메시지 수신자에 관한 것으로 구분될 수 있다(Angst & Agarwal, 2009). 메시지 프레이밍은 메시지 내용이 구성되는 방식을 말하며, 설득 대상 행동이 가져올 결과 및 인과관계를 주로 설명한다(Wilson, et al., 1998). 메시지 프레이밍이 설득 커뮤니케이션에서 중요한 근본적인 이유는 정보를 얻고 이해하는 과정을 통해서 태도나 행동의 변화가 이뤄지기 때문이다(Kenrick, et al., 2005).

이득-손실 프레이밍은 건강관리습관(예: 운동, 금연, 유방자가점검)이나 생활안전(예: 유아용 차량보호장치 사용), 보안행동(예: 개인 컴퓨터 보안 조치)에 이르기까지 다양한 분야의 설득 커뮤니케이션에서 등장하는 대표적인 메시지 프레이밍 기법이다(Block &

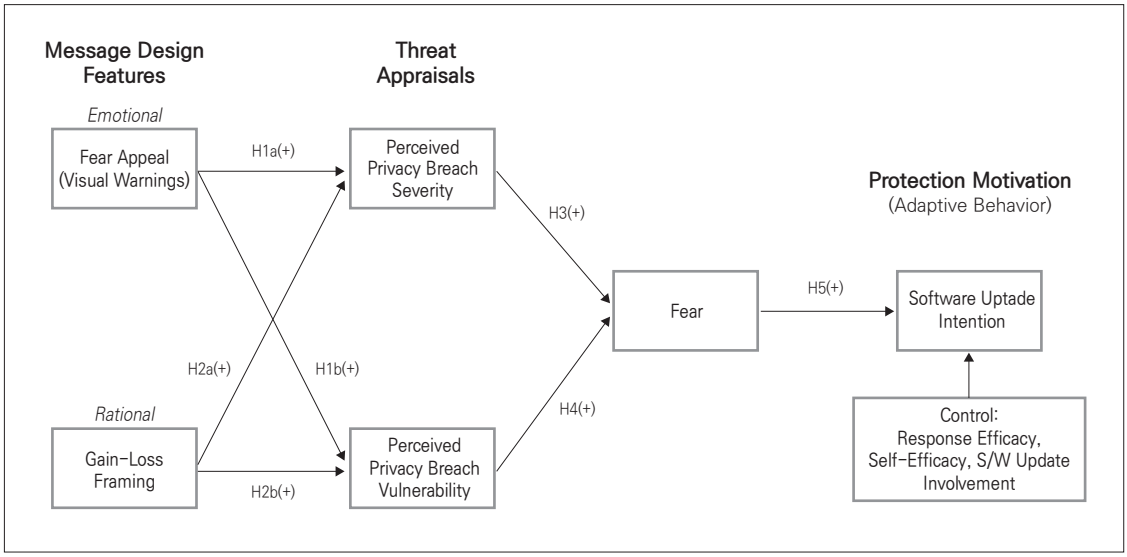
Keller, 1995; Rothman, et al., 1993; Meyerowitz & Chaiken, 1987). 두 프레이밍의 차이는 권장 행동을 했을 때(Compliance)의 긍정적 결과를 강조하느냐(이득 프레이밍), 하지 않을 때(Noncompliance)의 부정적 결과를 강조하느냐(손실 프레이밍)로 구분된다.

전망 이론(Prospect Theory)에 따르면, 본질적으로 동일한 정보라고 하더라도 메시지를 어떻게 프레이밍(이득 vs. 손실)하느냐에 따라 메시지 수용자의 결정이 달라진다(Kahneman & Tversky, 1979). 인간의 행동은 항상 합리적 선택(Rational Choices)의 형태가 아니라는 것이다. 구체적으로, 발생할 수 있는 긍정적인 결과(Potential Positive Consequence)가 강조되면, 인간은 위험을 회피하기 위해 상대적으로 확실한(Certain) 결과물(Outcomes)이 있는 선택을 한다. 반면에, 발생할 수 있는 부정적 결과(Potential Negative Consequence)가 강조되면, 위험을 추구하는 성향을 보이며 상대적으로 결과물이 불확실한(Uncertain) 경우를 선택한다(Tversky & Kahneman, 1981, 1986). 다시 말해, 이득 프레이밍 메시지를 받으면 확실한 이득을, 손실 프레이밍 메시지를 받으면 불확실한 손실을 선택한다는 것이다.

이러한 행동 성향은 이득에 비해 손실에 더 민감하며 손실에 대한 반응이 더 극단적이라는 것을 의미한다(Tversky & Kahneman, 1984). 따라서, 행동 변화를 유도하기 위한 설득 커뮤니케이션을 디자인할 때 어떤 프레이밍 메시지를 활용할 것인지가 결과에 중요할 수 있다. 예를 들어, 부정적인 결과(피해 등)가 초래될 가능성이 큰 컨텍스트에서는 손실 프레이밍 메시지가 더 효과적인 것으로 알려져 있다(Meyerowitz & Chaiken, 1987; Rodriguez-Priego, et al., 2020).

Ⅲ. 연구 모형 및 연구 가설

앞서 설명한 선행 연구 및 관련 이론들을 기반으로 〈그림 1〉과 같은 연구모형을 도출하였다. 본 연구는 스마트 홈 카메라 사용자의 개인정보 보호 행동(소프트웨어 업데이트)을 유도할 수 있는 방법으로 업데이트 알림 메시지를 어떻게 디자인하는 것이 효과적인지를 이



〈그림 1〉 연구 모델
〈Fig. 1〉 Research Model

론적으로 설명하고자 하였다.

ARI Model(Buck, et al., 2004)에 따르면, 사람은 감정적 소구(Emotional Appeals)와 이성적 소구(Rational Appeals)에 의해 설득된다. 설득 커뮤니케이션에서 감정적 소구란 수신자의 감정을 유발하여 설득하는 방법으로, 불안하거나 불길한 느낌을 주는 경고 이미지를 사용하는 경우가 대표적이다. 반면, 이성적 소구는 논리적인 수단을 통해 설득시키는 방법으로, 권장 행동이 왜 필요한지가 정확히 설명된 메시지를 활용하는 방법이 있다(Fagan, et al., 2015a).

본 연구에서는 앞서 설명한 공포 소구와 메시지 프레이밍을 각각 감정적 소구와 이성적 소구 측면의 메시지 디자인 특성(Message Design Features)로 보았다. 그리고 이러한 메시지 디자인 특성들이 사용자의 위협 평가 과정 및 행동 변화에 얼마나 효과적인지를 설명하기 위해 보호동기이론의 주요 요인들(인지된 심각성, 인지된 취약성, 공포)을 본 연구의 컨텍스트에 맞게 변수로 반영하였다.

1. 메시지 디자인 특성과 사용자 위협 평가

1) 공포 소구

위험 커뮤니케이션에 관한 선행 연구들은 위험한 상황이 발생할 수 있다는 것에 대한 수신자의 감각이나 인지 정도를 높이기 위해 다양한 메시지 기법을 활용하였다(Lipkus, 2007; Schneider, et al., 2001). 그 중에서 시각적 메시지는 당사자의 주의를 끄는 데 탁월할 뿐만 아니라, 메시지의 전체 느낌을 빠르고 쉽게 감각적으로 이해하는 데도 도움을 준다(Lipkus, 2007; Townsend & Kahn, 2014). 예를 들어, 위험 안내를 위한 경고 표시(Warning Sign)는 위험 요소나 위협으로부터의 주의 필요성, 또는 불길한 결과(피해 등)가 발생할 수 있음을 직관적으로 전달함으로써, 수신자로 하여금 불안감을 느끼게 하는 감정적 소구 효과가 있다(Buck, et al., 2004).

한편, 공포 소구 방법에 관한 연구에서도 시각적 이미지의 효과가 발견된다. Park(2017)은 해커 이미지를 활용한 공포 소구가 비밀번호 관련 위협에 대한 사용자 공포를 높이고 나아가 비밀번호 변경 의도에 긍정적인 영향을 준다는 것을 확인하였다. 또, Park, et al.(2017)은 인터넷 비밀번호 유출 위험에 관한 공포 소구를 위해 누군가 몰래 엿보는 시각적 이미지를 함께 활용하였다.

이와 같은 연구 결과들을 바탕으로 본 연구에서는 보안 침해 상황을 나타내는 경고 이미지를 활용한 공포 소구가 스마트 홈 카메라 사용자의 위협 평가에 긍정적인 효과가 있을 것으로 가정하였다. 사용자가 업데이트 알림 화면에 노출되었을 때 전에 없던 보안 침해 경고 이미지를 보게 된다면 업데이트 미설치에 따른 피해의 심각성과 본인에게도 발생할 수 있음을 더 크게 인지할 수 있다.

H1a: 시각적 경고 메시지를 활용한 공포 소구는 스마트 홈 카메라 사생활 침해에 대한 인지된 심각성에 긍정적인 영향을 미칠 것이다.

H1b: 시각적 경고 메시지를 활용한 공포 소구는 스마트 홈 카메라 사생활 침해에 대한 인지된 취약성에 긍정적인 영향을 미칠 것이다.

2) 이득-손실 프레이밍

Rodriguez-Priego, et al.(2020)은 이득 프레이밍 메시지에 비해 손실 프레이밍 메시지가 인터넷 쇼핑 과정에서 사용자의 보안 행동(회원가입 시 최소한의 정보만 입력, 보안 수준이 높은 암호 사용, 로그아웃 등) 증가에 더 효과적이라고 하였다. 손실 프레이밍 효과를 바탕으로, Anderson and Agarwal(2010)은 개인 컴퓨터에 보안 조치를 하지 않았을 때의 부정적 결과(예: 사진, 금융 등 개인 정보에 접근)에 대한 사용자의 염려가 보안 조치 의도에 긍정적인 효과가 있음을 밝혔다.

이처럼, 메시지 프레이밍 방식(이득 vs. 손실)에 따라 설득 커뮤니케이션에 미치는 영향이 다를 수 있

다(Tversky & Kahneman, 1981; Wilson, et al., 1998). 특히, 선행 연구들은 부정적인 결과(피해 등)가 초래될 가능성이 큰 컨텍스트에서는 손실 프레이밍 메시지가 더 효과적이라고 하였다(Meyerowitz & Chaiken, 1987; Rodriguez-Priego, et al., 2020). 또한, 이러한 손실 프레이밍의 상대적 영향력은 모바일처럼 짧은 메시지의 경우에도 나타난다(Steindle, et al., 2015).

이와 같은 선행 연구 결과들을 바탕으로, 본 연구에서는 스마트 홈 카메라 보안 침해로 인한 손실을 강조한 메시지 프레이밍이 사용자의 위협 평가에 긍정적인 효과가 있을 것으로 가정하였다. 사용자가 업데이트 알림 화면에 노출되었을 때 업데이트 미설치에 따른 손실 상황이 강조된 메시지를 보게 된다면 본인의 일상이 촬영된 영상 등이 외부로 유출될 경우의 심각성과 본인에게도 발생할 수 있음을 더 크게 인지할 수 있다.

H2a: 손실 메시지 프레이밍은 스마트 홈 카메라 사생활 침해에 대한 인지된 심각성에 긍정적인 영향을 미칠 것이다.

H2b: 손실 메시지 프레이밍은 스마트 홈 카메라 사생활 침해에 대한 인지된 취약성에 긍정적인 영향을 미칠 것이다.

2. 사용자 위협 평가와 사용자 공포

Boss, et al.(2015)는 보호동기이론에 기반을 둔 정보보안 관련 선행 연구들을 분석하면서 당사자들이 느끼는 공포를 별도의 개념으로 직접 측정하지 않은 점을 지적하고 그 필요성을 강조하였다. 공포 유발을 위한 외부 자극(공포 소구) 및 그에 따른 당사자의 위협 평가(위협의 심각성 및 취약성)가 실제로 일정 수준 이상의 공포를 느끼게 하는지를 정확히 알기 위해서는 공포에 대한 측정이 필요하다는 것이다. 사람마다 위협으로 느끼는 대상이 각기 다를 수 있기 때문이다(Witte & Allen, 2000).

보호동기이론을 적용한 많은 선행 연구들은 위협이 가져올 피해의 심각 정도와 발생 확률 또는 가능성을 알리는 방식으로 공포 소구를 적용한 경우가 많았다(Boss, et al., 2015; Johnston & Warkentin, 2010; Witte, 1992). 즉, 위협의 심각성과 위협에 대한 취약성은 공포를 느끼게 하는 대표적인 선행 요인이다(Witte, 1992). 본 연구의 컨텍스트에서도 스마트 홈 카메라 사용자가 본인의 일상이 촬영된 영상 등이 외부로 유출될 경우의 심각성과 그럴 가능성을 크게 인식할수록 사용자가 느끼는 보안 침해 관련 공포는 클 것으로 기대할 수 있다.

H3: 스마트 홈 카메라 사생활 침해에 대한 인지된 심각성은 사용자가 느끼는 공포 수준에 긍정적인 영향을 미칠 것이다.

H4: 스마트 홈 카메라 사생활 침해에 대한 인지된 취약성은 사용자가 느끼는 공포 수준에 긍정적인 영향을 미칠 것이다.

3. 사용자 공포와 소프트웨어 업데이트 의도

보호동기이론의 전신인 병행과정모델(Parallel Process Model)에 따르면, 위협에 대한 평가 이후에 두 가지 유형의 행동 반응이 나타난다(Witte, 1992; 1994). 첫 번째로 공포 제어(Fear Control)는 거부나 회피와 같은 감정 기반의 반응으로, 불편한 감정(공포 등)을 줄이기 위한 목적이다. 따라서 위협을 줄이는 등의 실질적인 효과에는 도움이 되지 않는다. 반면에 또 다른 유형인 위험 제어(Danger Control)는 위협으로 인한 위험한 상황에 직접적으로 대처하기 위한 것이다(de Hoog, et al., 2007; Leventhal, 1970). 즉, 위험 제어는 위협을 줄이기 위한 목적 지향성을 가진 적응 반응(Adaptive Responses)이다(Rogers, 1975).

위협에 대한 대처 방안으로 제시되는 권장 행동에 대한 수신자의 이행 의도(즉, 보호 동기), 실제 행동, 행

동의 변화 등은 모두 적응 반응의 범주에 속한다. 예를 들어, 본 연구에서는 스마트 홈 카메라 보안 침해 위협에 직접적으로 대처하기 위한 업데이트 설치 의도가 여기에 해당된다. 보호동기이론에 따르면 사용자의 공포감이 클수록 이러한 보호 동기는 증가한다(Leventhal, 1970). 따라서 본 연구의 컨텍스트에서도 사생활 영상 유출 위협에 대해 공포를 크게 느낄수록 스마트 홈 카메라 업데이트 의도가 증가할 것으로 기대하였다.

H5: 스마트 홈 카메라 사생활 침해 관련 사용자의 공포는 소프트웨어 업데이트 의도에 긍정적인 영향을 미칠 것이다.

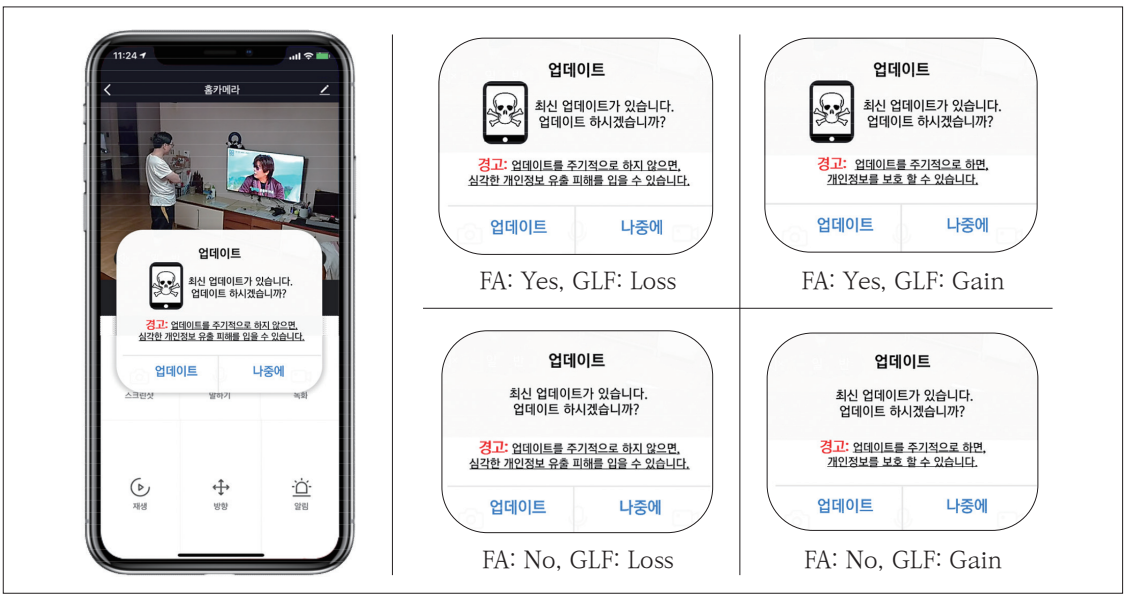
Ⅳ. 연구 방법

1. 실험 설계

본 연구에서 제안한 연구모형 및 가설을 검증하기 위하여 스마트 홈 카메라의 소프트웨어 업데이트 상황을 고려한 설문 실험(Survey Experiment)을 설계하였다. 설문 실험은 실험 방법이 가진 인과관계 설명력(Causal Power)과 설문 방법이 가진 일반화 가능성(Generalizability)을 동시에 취할 수 있는 연구 방법으로 최근 다양한 사회과학 분야 연구에서 활용되고 있다(Mullinix, 2015).

본 연구에서는 독립변수들의 효과를 검증하기 위해 실험 방법을 설계하였으며, 나머지 변수들 간의 관계는 실험 참여자들의 설문 데이터를 분석하여 확인하였다. 먼저 실험 설계를 위해, 메시지 디자인 요소로 반영한 공포 소구(있음 vs. 없음)와 메세지 프레이밍(손실 vs. 이득)은 각각 두 그룹씩, 총 4가지(2x2) 실험 처치(Treatment)에 따라 그룹을 구분하였다.

공포 소구를 위한 실험 처치는 피실험자가 업데이트 알림 화면에 노출되었을 때 볼 수 있는 보안 침해 경고 이미지를 활용하였다(〈그림 2〉 참조). 일반적으로 스마트 홈 카메라의 소프트웨어 업데이트는 모바일 환경에



〈그림 2〉 실험 처치

〈Fig. 2〉 Experiment Treatment by Group

서 앱 업데이트를 통해 이뤄진다. 개인 컴퓨터를 사용한 인터넷 기반 업데이트 상황과 달리 스마트폰 환경은 업데이트 알림 메시지 창의 크기가 작은 점을 고려하여 보안 침해 경고 이미지는 모바일 환경에서 자주 사용되는 픽토그램(Pictogram)을 사용하였다.

다음으로, 메시지 프레이밍을 위한 실험 처치를 위해서는 업데이트 알림 메시지 창에 표시될 결과(Consequence) 문구를 서로 다르게 구성하였다. 즉, 손실 프레이밍 메세지는 업데이트를 하지 않았을 때의 개인정보 유출 피해라는 부정적 결과를, 이득 프레이밍은 업데이트를 했을 때의 긍정적 결과(개인 정보가 보호됨)를 강조하는 내용으로 구성하였다.

추가로, 설문 실험 상황의 현실적 유사성을 높이기 위해, 실험에 사용된 업데이트 화면을 일반적인 스마트폰 사용 시 접하는 알림 화면과 흡사하게 디자인하였다(Fagan, et al., 2015a). 또한, 실험 참가자들로 하여금 본인들이 가정에서 홈 카메라를 사용하는 상황에 몰입하여 응답할 수 있도록 카메라가 거실을 보여주고 있는 이미지를 배경 이미지로 활용하였다.

2. 측정 항목

본 연구에서 사용된 변수별 측정 항목들은 선행연구에서 검증된 내용들을 스마트 홈 카메라 컨텍스트에 맞게 항목별로 수정하여 사용하였으며, 모두 7점 척도로 측정되었다. 먼저, 인지된 사생활 침해 심각성

〈표 1〉 측정항목
〈Table 1〉 Measurement Items

Variables	Items	Reference
Perceived Privacy Breach Severity (PPBS)	- If my personal information (e.g., recorded videos) is leaked through the home camera, it causes me major problems. - If my personal information (e.g., recorded videos) is leaked through the home camera, I would suffer a lot of pain. - If my personal information (e.g., recorded videos) is leaked through the home camera, it would be significant.	Johnston and Warkentin (2010); Boss, et al., (2015)
Perceived Privacy Breach Vulnerability (PPBV)	- The home camera is at risk for my personal information (e.g., recorded videos) being leaked to others. - It is possible that my personal information (e.g., recorded videos) will be leaked to others through the home camera. - It is likely that my personal information (e.g., recorded videos) will be leaked to others through the home camera.	Johnston and Warkentin (2010)
Fear	- I am frightened that my personal information (e.g., recorded videos) may be leaked to others through the home camera. - I am worried that my personal information (e.g., recorded videos) may be leaked to others through the home camera. - I am scared that my personal information (e.g., recorded videos) may be leaked to others through the home camera. - I am anxious that my personal information (e.g., recorded videos) may be leaked to others through the home camera.	Milne, et al., (2002)
Software Update Intention (SUI)	- I intend to update the software for my home camera. - I plan to update the software for my home camera. - I predict I will update the software for my home camera.	Johnston and Warkentin (2010)

(PPBS)은 데이터 백업을 안 할 경우에 발생할 수 있는 위협(데이터 손실)의 심각성 정도를 측정한 Boss, et al.(2015)의 측정항목, 스파이웨어 방지 프로그램을 사용하지 않을 경우에 발생할 수 있는 위협(스파이웨어 감염)의 심각성 정도를 측정한 Johnston and Warkentin(2010)의 측정항목을 수정하여 사용하였다. 유사하게, 인지된 사생활 침해 취약성(PPBV)은 Johnston and Warkentin(2010)에서 사용된 '스파이웨어 위협 취약성' 변수의 측정항목을 본 연구에 맞게 수정 적용하였다.

다음으로, 공포 변수는 위협으로 인한 걱정, 공포, 불안, 두려움 등으로 측정한 Milne, et al.(2002)의 측정항목을 사용하였다. 본 연구에서 보호 동기를 의미하는 소프트웨어 업데이트 의도 변수(SUI)는 스파이웨어 방지 프로그램 사용 의도를 측정한 Johnston and Warkentin(2010)의 항목들을 활용하여 측정하였다. 끝으로, 독립변수로 반영하여 실험 처치한 공포 소구(FA)와 이득-손실 메시지 프레이밍(GLF)에 대한 조작 점검을 위해 관련 문항을 설문 항목에 추가하여 측정하였다.

3. 실험 절차

실험은 스마트 홈 카메라의 모바일 앱 업데이트 상황을 가정한 시나리오를 모든 피실험자에게 먼저 제공하고, 이어서 그룹별로 각기 다른 메시지 디자인이 반영된 업데이트 알림을 보게 한 후, 마지막으로 설문에 응답하는 순서로 이뤄졌다. 시나리오는 피실험자를 그룹별로 랜덤 배정한 후 제공되었으며, 피실험자가 가정에 스마트 홈 카메라를 설치하여 사용하고 있는 중인데 당일 카메라 조작을 위해서 모바일 앱을 열었을 때 업데이트 알림을 보게 된 상황을 가정하였다. 또한, 피실험자의 공통된 이해를 위해 실험에서 등장하는 개인정보는 스마트 홈 카메라로 촬영된 영상임을 안내하였다.

본실험에 앞서 사전실험을 통해 실험 조작 점검 및 측정 항목의 적절성을 확인하였다. 사전실험의 타당성을 높이기 위해 피실험자는 실제 스마트 홈 카메라 사용자를 대상으로 하였다. 직장인 28명(그룹별 7명)이 사전실험에 참여하였으며, 참여자 모두에게 4,000원 상당의 기프티콘 보상이 제공되었다. 메시지 내용의 명확한 정도, 강압적인지 정도 등(Fagan, et al., 2015a; Steindl, et al., 2015) 사전실험의 결과를 바탕으로 일부 설문 문항에 대한 소폭의 수정이 이뤄졌으며, 전체적으로 설문 문항 및 그룹별 실험 처치상의 문제는 없는 것으로 확인되었다.

본실험은 설문 실험의 장점(일반화 가능성)을 활용하기 위해 설문조사 전문 기업(https://opensurvey.io/)을 통해 표본을 확보하고 데이터를 수집하였다. 설문은 온라인으로 이뤄졌으며, 본격적인 실험 참여 전에 본 연구의 컨텍스트에 맞는 기본 요건(스마트 홈 카메라 사용 경험이 있는 사람)에 관한 질문을 통해, 충족하지 못한 참여자는 제외되었다. 본 연구의 실험 처치를 고려하여 각 그룹별 40명씩 총 160명을 무작위 모집하였으며, 연령(20/30/40대) 및 성별에 따라 균등배분하였다.

Ⅴ. 데이터 분석 및 결과

1. 인구통계학적 특성

실험에 참여한 160명의 응답 중에서 불성실한 실험 참여 등으로 간주되는 응답을 제외하고 총 120개(그룹별 30개)의 데이터가 실제 분석에서 사용되었다. 응답 표본 중 여성은 61명(49.2%), 남성은 59명(50.8%)의 비중을 보였다. 연령대는 20대, 30대 그리고 40대가 각각 31.7%, 34.2%, 34.2%로 나타났다. 따라서 인구통계학적 특성 관점에서 주요 사용자 그룹이 누락되거나 집중되는 등 표본 구성에 특별히 우려되는 점은 발견되지 않았다. 그 외에 응답자의 스마트 홈 카메라 이용 행태 측면에서는 사용 기간이 3개월 미만부터 1년 이상까지로 골고루 분포되어 있었으며, 사용 목적은 사생활과 관련된 안전(가족, 반려동물 등)과 보안이 가장 많은 비중을 차지하고 있었다.

2. 조작 점검(manipulation check)

주요 분석에 앞서, 공포 소구에 대한 실험 처치가 응답자에게 제대로 인지되었는지를 파악하기 위해 조작 점검 질문에 대한 응답을 확인하였다. '개인정보 침해(해킹) 위험을 나타내는 특정 아이콘을 포함하고 있다'라는 질문에 대한 응답을 확인한 결과, 실험 처치와 반대로 응답한 경우가 일부 발견되었다. 불성실한 실험 참여 등 결과를 왜곡할 가능성을 철저히 배제하기 위해 해당 표본들은 최종 분석 전에 제외하였다.

공포 소구에 대한 조작 점검을 위해 선행 연구들과 같이(Boss, et al., 2015), 위협의 심각성과 취약성에 대한 그룹 간 차이를 분석한 결과, 모두 $p<0.01$ 수준에서 차이를 보였다(PPBS: M_{yes}=6.33, M_{no}=5.91, t=-3.486, PPBV: M_{yes}=5.77, M_{no}=5.38, t=-2.676). 한편, 이득-손실 메시지 프레이밍 조작 점검 문항('업데이트를 주기적으로 할 경우의 긍정적인 결과를 설명하고 있다', '업데이트를 주기적으로 안 할 경우의 부정적인 결과를 설명하고 있다')에 대해서도 그룹 간 차이를 확인하였다. 그 결과, 의도한 것과 같이 그룹 간 유의한 차이를 보였다(손실 프레이밍 메시지: F(1,118)=48.815, p=0.000 ; 이득 프레이밍 메시지: F(1,118)=76.685, p=0.000). 결과적으로, 두 가지 메시지 디자인 특성에 대한 실험 처치가 모두 의도된 대로 정상 반영된 것으로 판단하였다.

3. 동일방법편의(common method bias)

본 연구가 설문 실험 참가자의 응답으로 모든 변수를 측정한 점을 고려하여 동일방법편의 유무를 확인하였다. 하만의 단일 요인 검정(Harman's one-factor Test) 결과, 전체 분산의 가장 많은 비중을 차지하는 첫 번째 요인이 총 분산의 28%이어서 동일방법편의는 없는 것으로 판단하였다. 단일 요인 검정에서는 첫 번째 요인이 전체 분산의 대부분(예: 50%)을 차지할 경우 동일방법편의가 존재하는 것으로 판단한다(Nov & Ye, 2008).

〈표 2〉 신뢰성 및 집중 타당성 분석
〈Table 2〉 Reliability and Convergent Validity Test

Factors	Loadings	Cronbach's α	CR	AVE
Perceived Privacy Breach Severity (PPBS)	0.802	0.791	0.877	0.705
	0.828			
	0.887			
Perceived Privacy Breach Vulnerability (PPBV)	0.874	0.817	0.891	0.732
	0.856			
	0.836			
Fear	0.823	0.891	0.924	0.754
	0.853			
	0.888			
	0.908			
Software Update Intention (SUI)	0.893	0.875	0.923	0.800
	0.918			
	0.871			

〈표 3〉 판별 타당성 분석
〈Table 3〉 Discriminant Validity Test

Factors	1	2	3	4	5	6
1. Fear	0.868					
2. Perceived Privacy Breach Severity	0.399	0.840				
3. Software Update Intention	0.405	0.238	0.894			
4. Fear Appeals	0.299	0.307	0.209	1.000		
5. Perceived Privacy Breach Vulnerability	0.586	0.346	0.308	0.240	0.856	
6. Gain-Loss Framing	0.313	0.341	0.318	0.000	0.218	1.000

4. 측정모형(measurement model) 분석

구조모형 분석을 통한 가설 분석 이전에 SmartPLS를 활용하여 측정 모형을 분석하였다. 먼저, 변수별 크론바흐 알파계수(Cronbach's Alpha)와 합성 신뢰도(Composite Reliability)를 확인한 결과 모두 기준치(0.7) 이상으로 나타나 측정 모형의 신뢰성이 확보된 것으로 판단되었다(〈표 2〉 참조).

다음으로, 타당성은 수렴 타당성(Convergent Validity)과 판별 타당성(Discriminant Validity)을 통해 확인하였다. 수렴 타당성은 측정 항목들이 이론적으로 설명하려는 변수를 실제 얼마나 잘 설명하는지에 관한 것으로, 변수에 대한 측정항목의 실제 관련 정도를 의미한다. 수렴 타당성에 대한 확인은 요인 적재량(Factor Loadings)이 0.7이상인지, 평균분산추출값(AVE; Average Variance Extracted)이 0.5 이상인지로 판단할 수 있는데, 〈표 2〉와 같이 두 기준 모두 충족된 것으로 확인되었다.

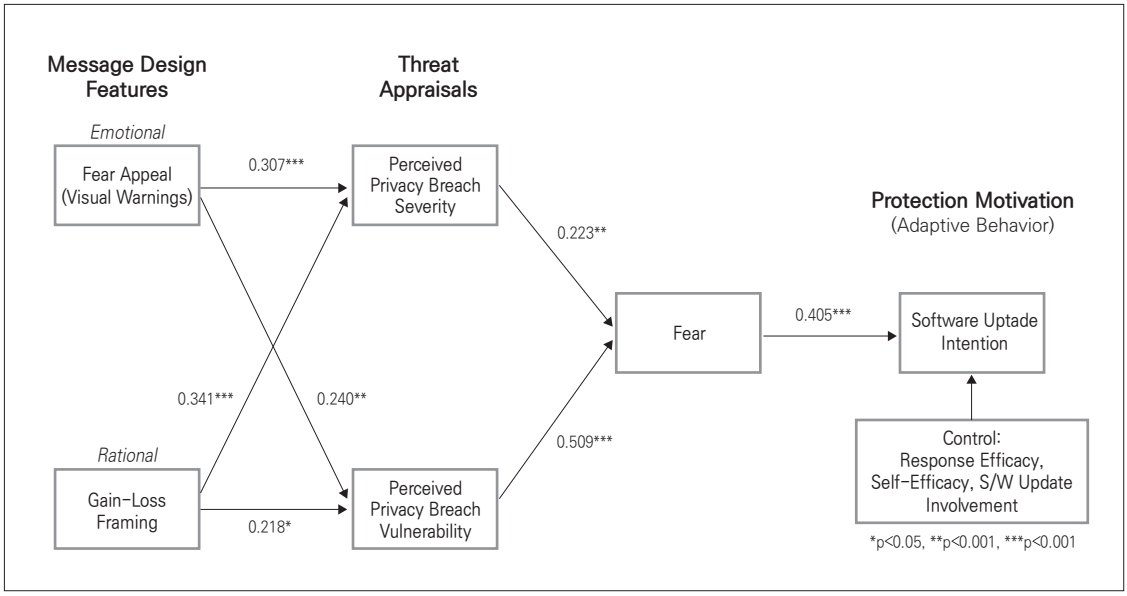
판별 타당성은 측정항목들이 해당 변수를 제외한 다른 변수와의 상관관계가 적을 때 확보된다. 변수 간 상관관계와 AVE의 제곱근을 비교하여 확인한 결과, 〈표 3〉에서와 같이 대각선의 굵은 수치(각 변수의 AVE제곱근값)들이 모두 다른 변수와의 상관계수보다 큰 것으로 확인되었다. 이에 따라, 측정 모형의 신뢰성 및 타당성 측면에서 전반적으로 구조 모형을 분석하는 데에 문제가 없다고 판단하였다.

5. 구조모형(structural model) 분석

구조 모형의 경로 분석을 위해 SmartPLS 3.3.2를 이용하였으며, 경로계수의 유의성은 1,000회 부트스랩 샘플링(Bootstrap Sampling)을 통해 확인하였다. PLS(Partial Least Squares)는 샘플 수에 대한 제약이 적은 등 다양한 장점으로 많은 연구자들이 사용하는 분석 방법이다(Lee, et al., 2023; Li, et al., 2022; Kim, et al., 2013, 2016b, 2019, 2021).

구조모형 분석 결과 〈그림 3〉과 같이 모든 가설이 채택되었다. 먼저, 공포 소구와 이득-손실 프레이밍은 사용자의 인지된 사생활 침해 심각성(PPBS)과 취약성(PPBV)에 모두 유의미한 긍정 효과를 보였다(H1a: β=0.307, t=3.893; H1b: β=0.240, t=2.995; H2a: β=0.341, t=4.359; H2b: β=0.218, t=2.482). 다음으로, 공포 소구와 메시지 프레이밍에 의한 위협 평가 프로세스는 사용자의 공포를 높이는 것으로 나타났다(H3: β=0.223, t=2.965; H4: β=0.509, t=6.798). 끝으로, 본 연구에서 기대한 것과 같이 사용자가 느끼는 공포는 보호 동기를 높이는 데 유의미한 영향이 있는 것으로 확인되었다(H5: β=0.405, t=5.542).

끝으로, 통제 변수로 반영한 반응 효능감(Response Efficacy), 자기 효능감, 보호 행동 관여도 중에서는 보



〈그림 3〉 구조모형 분석
〈Fig. 3〉 Structural Model Test

호 행동 관여도가 p〈0.05 수준에서 유의미한 영향이 확인되었다. 즉, 공포 소구와 손실 프레이밍 메시지에 의한 영향과 별도로, 사용자 스스로 스마트 홈 카메라 소프트웨어 업데이트에 대해 얼마나 관심을 갖고 중요하게 생각하는지가 보호 행동에 영향을 주는 것으로 나타났다.

Ⅵ. 시사점 및 향후 연구

1. 이론적 시사점

본 연구의 이론적 시사점은 다음과 같다. 먼저, 본 연구는 사용자들의 개인정보 보호 행동으로서 소프트웨어 업데이트에 영향을 줄 수 있는 메시지 디자인 특성(Message Design Features)을 이론적 관점에서 검증하였다. 설득 커뮤니케이션의 관점에서 업데이트 메시지 자체가 중요하다는 것은 여러 이론(예: Conzola and Wogalter(2001)의 C-HIP Model, Buck, et al.(2004)의 ARI Model)에 의해서도 뒷받침된다.

본 연구는 스마트 홈 카메라의 사생활 보호를 위한 소프트웨어 업데이트 상황에서 공포 소구 형태의 메시지(감정적 소구)와 이득-손실 프레이밍 형태의 메시지(이성적 소구)가 사용자의 위협 평가 프로세스(인지된 심각성 및 취약성)에 유의미한 영향을 준다는 것을 이론적으로 설명하였다. 사용자의 권장 행동 준수를 보호동기이론 관점에서 설명하고자 한 선행 연구들은 보호동기를 유발하는 외부 자극으로서 공포 소구에만 주로 집중해왔다(Boss, et al., 2015). 본 연구는 여기에 ARI model의 이론적 시각을 추가함으로써, 공포 소구와 메시지 프레이밍을 메시지 디자인 특성으로 개념화하였다. 즉, 감정적 소구로서 공포 소구를, ARI model의 또 다른 소구 형태인 이성적 소구는 이득/손실 메시지 프레이밍으로 반영하고 이 두 가지 디자인 특성들이 보호 동기 형성에 미치는 영향을 확인하였다. 이처럼 본 연구는 보호동기이론의 앞 단을 ARI model과 이론적으로 연결함으로써, 보호동기이론을 공포소구 외 다양한 설득 메시지 기법에 관한 효과(보호 동기 형성 여

부)를 설명할 수 있는 영역으로 확장하였다.

본 연구의 이러한 이론적 시도는 개인정보·보안 침해와 관련하여 사용자 행동 관점의 연구와 전략이 요구되고 있는 점을 고려할 때 더욱 의미가 있다. 기술적으로는 보안 취약성이 최초 발견된 이후 평균 1.2개월 이내로 해당 위협에 대비한 소프트웨어 업데이트가 준비되고 있는 데 반해, 정작 실제 개인정보·보안 침해 사례는 사용자의 부주의에 의한 경우가 많기 때문이다(Wash, et al., 2014). 소프트웨어 업데이트를 제때 설치하게 유도하는 등 사용자의 보안 행동 준수를 증가시킬 수 있는 외부 자극으로서, 알림 메시지를 활용한 효과적인 소구 전략을 위해 다양한 이론적 시도가 필요한 이유이다. 본 연구는 이러한 이론적 시도로서의 의미를 갖는다.

다음으로, 본 연구의 결과는 보호동기이론의 주요 요인 간 영향 관계, 나아가 보호 동기가 형성되는 메커니즘이 모바일 앱 환경에서는 다를 수 있음을 시사한다. 보호동기이론에 따르면 위협에 대한 평가뿐만 아니라 대안에 대한 평가(Coping Appraisal) - 반응 효능감, 자기 효능감 -도 위협으로부터 본인을 보호하려는 보호 동기 형성에 중요한 영향을 준다(Boss, et al., 2015). 그런데 본 연구에서는 반응 효능감과 자기 효능감 모두 보호 동기에 유의미한 영향이 없는 것으로 나타나, 다음과 같은 이유를 짐작해보게 한다.

개인정보 위협에 대한 대처 방안(업데이트)이 효과적인지를 정확히 판단하기 위해서는 해당 소프트웨어 업데이트의 목적이나 배경, 내용 등 상세 내용에 대한 이해가 필수적이다(Fagan, et al., 2015a). 그러나, 본 연구에서 사용된 알림 메시지 디자인처럼 모바일에서는 업데이트 알림 시 화면 공간의 제약으로 인해 해당 업데이트에 관한 자세한 정보를 표시하는 것이 사실상 불가능하다. 링크를 통해 추가 정보를 확인할 수 있도록 한 경우도 있으나, 사용자들이 무시하기 쉽다.

또, 모바일 앱 업데이트는 대부분의 스마트폰 사용자들이 쉽게 해낼 수 있을 정도의 기본적인 역량을 요구하는 과정이다. 즉, 높은 수준의 자기 효능감을 필요로 하지 않는다. 이에 비해, 복잡한 시스템의 보안 관련 업데이트의 경우는 시작 버튼을 누르기만 하면 되는 것이 아닌, 여러 단계에 걸친 기술적 과정(명령어 입력 등)을 직접 진행시켜야 하는 수준의 기술적 역량을 요구하는 경우가 있다. 이러한 맥락에서 볼 때, 보호동기이론이 설명하는 대안 평가(Coping Appraisal)와 보호동기 형성 간의 인과적 관계는 모바일 환경과 같은 새로운 컨텍스트에서는 다르게 나타날 수 있다. 다만, 이에 대한 명확한 확인을 위해서는 다양한 실증 연구가 필요할 것이다.

2. 실무적 시사점

본 연구는 실무적으로도 의미 있는 시사점을 제공한다. 특히, 본 연구에서 사용된 메시지 디자인은 스마트홈 카메라 사용자들의 개인정보 보호 행동 준수를 높일 수 있는 구체적인 메시지 디자인에 대한 가이드라인을 제공한다. 구체적으로, 시각적 이미지 선택 및 포함 여부는 예상되는 공포 소구 효과의 측면에서 비교·결정할 필요가 있으며, 메시지 내용 자체는 손실 프레이밍을 통해 개인정보 보호 행동 미준수 상황의 부정적 결과를 효과적으로 표현했는지를 점검할 필요가 있다.

소프트웨어 업데이트를 망설이거나 지연하는 이유를 알림 메시지 디자인에 초점을 두고 분석한 Fagan, et al.(2015a,b)에 따르면, 크게 네 가지의 중요한 디자인 특성이 있다. 업데이트 관련 중요한 내용(목적, 이유, 세부사항 등)을 담고 있어야 하고(Importance), 눈에 잘 띄어야 하고(Noticeability), 거슬리지 않아야 하며(Annoyance), 혼란스럽지 않아야 한다(Confusion). 이 특성들은 본 연구에서 사용된 두 가지 메시지 디자인이 보호동기이론 및 관련 이론들의 관점에서 왜 효과적이었는지를 실무자들이 더 세부적으로 이해하는 데 도움을 줄 수 있다.

먼저, 보안 침해를 경고하는 해킹 이미지는 일반적으로 위험 안내를 목적으로 사용되는 경고 표시(Warning Sign)처럼 위험 요소나 위협으로부터의 주의 필요성, 또는 불길한 결과(피해 등)에 대한 경고를

직관적으로 전달하는 효과가 있다. 즉, 시각적으로 쉽게 눈에 띄는 것은 물론(Noticeability) 메세지가 담고 있는 내용(주의 필요)이 중요함을(Importance) 직관적으로 전달함으로써, 사용자로 하여금 불안감을 느끼게 하는 데 효과적이다(Emotional Appeals). 해킹 이미지에 내포된 이러한 디자인 측면의 속성들은 스마트 홈 카메라는 물론 이와 유사한 개인 정보기기 사용자들을 위한 '감정적 소구' 개발 시 실무적으로 중요한 고려요소가 될 수 있다.

다음으로, 업데이트 설치 여부에 따른 부정적 결과를 강조하는 메시지 프레이밍도 실제 디자인에 적용하기 위해서는 세부적인 기법이 필요하다. 무엇보다도, 손실 상황을 대표하는 결과(Consequence)를 적절하게 선택해야 한다. C-HIP Model에 따르면 메시지는 상대방이 믿고 생각하는 바와 일치해야 설득력이 있기 때문이다(Conzola & Wogalter, 2001). 본 연구에서는 스마트 홈 카메라와 관련하여 누구나 공감할 수 있는 보안 피해로, 사용자의 주거 공간과 사적인 모습이 촬영된 영상들이 불법적으로 유출되는 상황을 가정하였다. 그리고, 전망 이론의 가정을 고려하여, 이러한 손실 프레이밍과 본질적으로 동일한 정보를 내포한 이득 프레이밍 메세지를 구성하였다 (Kahneman & Tversky, 1979).

본 연구의 결과를 토대로 볼 때, 이처럼 개인 사생활 영상의 유출 피해가 발생하는 상황을 부정적 결과로서 프레이밍한 메시지는 사용자로 하여금 권장 행동(업데이트 설치)의 필요성 등에 대한 혼란을 줄임으로써(confusion) 이성적인 판단을 돕는 데 효과적이라고 할 수 있다(Rational Appeals). 따라서, 스마트 홈 카메라 및 이와 유사한 개인정보 유출 위협이 높은 컨텍스트에서 '이성적 판단'에 기반한 사용자 보안행동 유도가 필요할 때 이와 같은 디자인 접근 방식을 활용할 수 있을 것이다.

끝으로, 본 연구의 결과를 토대로 스마트 IoT 환경에서의 개인정보보호에 관한 정책적·제도적 방향에 대해서도 생각해 볼 수 있다. 'Privacy by Design'은 IT 서비스의 기획 단계부터 전체 생애주기에 걸쳐 사용자의 프라이버시와 데이터를 보호하자는 개념으로 우리나라를 비롯한 전 세계 많은 국가에서 개인정보보호에 관한 정책 방향의 토대가 되고 있다(Korea Development Institute, 2016). Privacy by Design을 실제로 구현하기 위한 8가지 디자인 전략(Danezis, et al., 2014)에는 IoT 서비스 등이 법적 혹은 정책적으로 준수해야 하는 요구사항을 입증(Demonstrate)할 수 있도록 해야함을 포함하고 있다. 또한, 설계 및 분석 단계에서는 사용자의 개인정보 등을 보호할 수 있는 기능 및 설정을 포함하도록 설계될 필요가 있다(Kim, et al., 2016a).

이러한 정책적 관점에서 볼 때 본 연구의 결과는 스마트 홈 카메라와 같은 IoT 서비스 설계 시 사용자의 보안 행동 준수를 유도할 수 있는 효과적인 메시지 알림 방식을 필수적으로 포함하도록 하고, 이러한 기능을 포함했음을 입증하도록 하는 방안을 생각해 볼 수 있게 한다. 경량, 저전력의 암호 기술을 포함하도록 하는 기술적인 요구사항 뿐만 아니라 이와 같은 사용자의 보호동기 유발을 위한 디자인 특성도 함께 요구사항으로 반영된다면 사용자 행동 관점의 중요성이 정책적으로 구현되는 의미 있는 결과가 될 수 있을 것이다.

3. 연구의 한계 및 향후 연구

본 연구는 다음과 같은 한계점을 갖고 있다. 먼저, 공포 소구를 위해 단일 이미지를 사용하였다. 선행 연구에 따르면 업데이트 알림 메시지는 다양한 디자인 요소들(레이아웃, 색상, 버튼, 폰트 등)로 구성될 수 있으며, 사용자들의 태도 역시 전반적인 요소들에 대한 복합적인 반응으로 나타난다(Fagan, et al., 2015b). 따라서 보안 침해를 경고하는 해킹 이미지 외 다른 부가적인 디자인 요소들을 활용한 공포 소구를 고려해 볼 수 있다. 특히, 스마트 홈 카메라 업데이트처럼 모바일의 화면 공간 제약이 있는 상황에서 효과적인 공포 소구 방법이 추가된다면 실무적으로 효과적일 수 있다.

다음으로, 본 연구의 메시지 프레이밍은 업데이트 설치 여부에 따른 선언적 결과(보호할 수 있다 또는 유출될 수 있다)를 기술하는 형태로 디자인 되었는데, 설득력 측면에서 보완될 필요가 있다. Angst and Agarwal(2009)은 개인 건강 기록의 유출 염려가 있는 전자건강기록(Electronic Health Records) 시스템에 대한 사용자의 태도와 수용 여부에 관한 연구에서, 실제 통계를 기반으로 한 프레이밍 메시지를 사용하였다. 예를 들어, '4만 4천명에서 9만 8천여 명의 사람들이 매년 의료기록 착오로 병원에서 사망한다' 등 통계 정보들을 이득 프레이밍 메시지에 포함하였다. 이와 같은 사실 기반의 정보가 설득 커뮤니케이션에서 활용될 경우 사용자의 이성적 판단에 보다 효과적일 수 있다.

본 연구의 또 다른 한계점은 보호동기이론에 관한 선행연구들에서 종종 등장하는 사용자 공포의 매개효과는 확인하지 않았다. 본 연구의 주요 관심은 두 가지 메시지 디자인 특성이 사용자의 위협 평가 과정에 미치는 영향에 대한 것이기 때문이다. 또한, 보호동기이론에 관한 선행연구들에서도 공포의 매개효과는 컨텍스트별로 서로 다르게 나타나고 있다(Boss, et al., 2015). 다만, 보호동기이론이 공포 소구를 중요하게 다루고 있는 점을 고려한다면 스마트 홈 카메라 또는 유사 IoT 기반 정보기기 컨텍스트에서도 사용자 공포는 중요한 변수임에 틀림없다. 따라서 연구 모델 개발 시 연구 목적에 따른 신중한 결정이 요구된다.

끝으로, 사용자의 업데이트 준수를 높이기 위한 감정적, 이성적 소구의 진정한 효과는 선행 연구에서 제안한 바와 같이 이행 의도만이 아닌 실제 행동에 대한 측정이 필요하다(Boss, et al., 2015). 관련하여, 알림 메시지 디자인 및 그에 따른 사용자의 업데이트에 의한 보안 효과가 자동 업데이트에 의한 보안 효과 수준에 미칠 수 있는지에 대한 실증 기반의 종단 연구(Longitudinal Study)는 흥미로운 주제가 될 수 있다. 구글 플레이와 같은 플랫폼 기반 마켓플레이스에서는 멀웨어와 같은 악성 프로그램 여부 등만 사전 체크하고 있고, 모바일 앱의 업데이트를 자동으로 설정하는 것도 사용자의 개입과 선택에 의해서만 가능하다(Moller, et al., 2012). 따라서 사용자의 보안 행동 준수를 유발하기 위한 메시지 디자인 기법 개발 및 그에 따른 실제 효과를 측정하는 것은 실무적으로 매우 중요한 시사점을 제공할 수 있다.

■ References

Anderson, C. & Agarwal, R. (2010). "Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions." *MIS quarterly, 34*(3), 613-643.

Angst, C. & Agarwal, R. (2009). "Adoption of Electronic Health Records in The Presence of Privacy Concerns: The Elaboration Likelihood Model and Individual Persuasion." *MIS quarterly, 33*(2), 339-370.

Bilge, L. & Dumitras, T. (2012). *Before We Knew It: An Empirical Study of Zero-Day Attacks in the Real World.* Paper presented at the ACM Conference on Computer and Communications Security, October 16-18.

Block, L. & Keller, P. (1995). "When to Accentuate the Negative: The Effects of Perceived Efficacy And Message Framing on Intentions to Perform a Health-Related Behavior." *Journal Of Marketing Research, 32*(2), 192-203.

Boss, S., Galletta, D., Lowry, P., Moody, G. & Polak, P. (2015). "What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear That Motivate Protective Security Behaviors." *MIS Quarterly, 39*(4), 837-864.

Buck, R., Anderson, E., Chaudhuri, A. & Ray, I. (2004). "Emotion and Reason in Persuasion: Applying

The Ari Model And The CASE Scale." *Journal of Business Research, 57*(6), 647-656.

Conzola, V. & Wogalter, M. (2001). "A Communication-Human Information Processing (C-Hip) Approach to Warning Effectiveness in the Workplace." *Journal of Risk Research, 4*(4), 309-322.

Danezis, G., Domingo-Ferrer, J., Hansen, M., Hoepman, J., Metayer, D., Tirtea, R. & Schiffner, S. (2014). *Privacy and Data Protection by Design - from Policy to Engineering.* Attiki: ENISA.

de Hoog, N., Stroebe, W. & de Wit, J. (2007). "The Impact of Vulnerability to And Severity of a Health Risk on Processing and Acceptance of Fear-Arousing Communications: A Meta-Analysis." *Review of General Psychology, 11*(3), 258-285.

Fagan, M., Khan, M. & Buck, R. (2015a). "A Study of Users' Experiences and Beliefs About Software Update Messages." *Computers in Human Behavior, 51*, 504-519.

Fagan, M., Khan, M. & Nguyen, N. (2015b). "How Does This Message Make You Feel? A Study of User Perspectives on Software Update/Warning Message Design." *Human-centric Computing and Information Sciences, 5*(1), 36.

Felt, A., Ha, E., Egelman, S., Haney, A., Chin, E. & Wagner, D. (2012). *Android Permissions: User Attention, Comprehension, and Behavior.* Paper presented at the Eighth Symposium on Usable Privacy and Security, July 11-13.

Fishbein, M. & Ajzen, I. (1975). *Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research,* Reading, MA: Addison-Wesley.

Great View Research (2023a). "Smart Home Market Size, Share & Trends Analysis Report By Products (Lighting Control, Security & Access Controls), By Application (New Construction, Retrofit), By Protocols (Wireless, Wired), By Region, And Segment Forecasts, 2023 - 2030." https://www.grandviewresearch.com/industry-analysis/smart-homes-industry (Retrieved on February 1, 2024)

Great View Research (2023b). "Smart Home Security Camera Market Size, Share & Trends Analysis Report By Technology (Wired Camera,Wireless Camera), By Application (Doorbell Camera, Indoor Camera, Outdoor Camera), By Region, And SegmentForecasts, 2023 - 2030." https://www.grandviewresearch.com/industry-analysis/smart-home-security-camera-market (Retrieved on February 1, 2024)

Hale, J., Lemieux, R. & Mongeau, P. (1995). "Cognitive Processing of Fear-Arousing Message Content." *Communication Research, 22*(4), 459-474.

Hayes, A. (2024). "Smart Home: Definition, How They Work, Pros and Cons." *Investopia,* April 12.

Johnston, A. & Warkentin, M. (2010). "Fear Appeals and Information Security Behaviors: An Empirical Study." *MIS quarterly, 34*(3), 549-566.

Kahneman, D. & Tversky, A. (1979). "Prospect Theory: An Analysis of Decision under Risk." *Econometrica, 47,* 263-292.

Kenrick, D., Neuberg, S. & Cialdini, R. (2005). "Attitudes and Persuasion," in Kenrick, D., Neuberg, S., & Cialdini, R. (ed.) *Social Psychology: Unraveling the Mystery,* Boston: Allyn & Bacon.

Kim, M. (2016). "Privacy Protection Technologies on IoT Environments: Case Study of Networked

Cameras." *The Journal of the Korea Contents Association, 16*(9), 329-338.

{김미희 (2016). 사물인터넷(IoT) 환경에서 프라이버시 보호 기술: 네트워크 카메라 사례 연구. 〈한국콘텐츠학회 논문지〉, 16권 9호, 329-338.}

Kim, S. & Kim, J. (2023). "The Effect of Involvement and Message Framing in Smartphone Security Behavior." *The Journal of Internet Electronic Commerce Research, 23*(1), 1-15.

{김상희·김진성 (2023). 스마트폰 보안행동에 대한 관여도와 메시지 프레이밍의 효과. 〈인터넷전자상거래연구〉, 23권 1호, 1-15.}

Kim, H., Ding, X. & Lee, H. (2021). "An Empirical Investigation of Customer Loyalty in Chinese Smartphone Markets with Large-Scale Data: Apple, Samsung, and Xiaomi Cases." In Lee, W., Leung, C. & Nasridinov, A. (ed.) *Big Data Analyses, Services, and Smart Data,* Singapore: Springer.

Kim, H., Hong, S. & Park, S. (2016a). "A Study on Personal Information Protection Guideline : Through Research Case Study Analysis in Internet of Things Environment." *Journal of Security Engineering, 13*(2), 155-168.

{김혜리·홍승필·박수민 (2016a). 개인정보보호 가이드라인 연구 : 사물인터넷 환경의 개인정보 보호 사례 연구 분석을 통해. 〈보안공학연구논문지〉, 13권 2호, 155-168.}

Kim, H., Kim, I. & Lee, H. (2016b). "Third-Party Mobile App Developers' Continued Participation in Platform-Centric Ecosystems: An Empirical Investigation of Two Different Mechanisms." *International Journal of Information Management, 36*, 44-59.

Kim, H., Lee, Y. & Lee, H. (2019). "Negative Transition of Smart Device Utility: Empirical Study on IT-Enabled Work Flexibility, After-Hours Work Connectivity, and Work-Life Conflict." *Informatization Policy, 26*(4), 36-61.

{김형진·이윤지·이호근 (2019). 스마트기기 효용의 부정적 전이: IT기반 업무 유연성, 근무시간 외 업무 연결성, 일-삶 갈등에 관한 실증 연구. 〈정보화정책〉, 26권 4호, 36-61.}

Kim, H., Shin, B. & Lee, H. (2013). "The Mediating Role of Psychological Contract Breach in IS Outsourcing: Inter-Firm Governance Perspective." *European Journal of Information Systems, 22*, 529-547.

Korea Development Institute (2016). "Three-Year Implementation Plan for the Internet of Things (IoT) Information Security Roadmap." https://eiec.kdi.re.kr/skin_2016/common/epicdownload.jsp?num=143619&filenum=2 (Retrieved on April 20, 2024).

{KDI (2016). "사물인터넷(IoT) 정보보호 로드맵 3개년 시행계획." https://eiec.kdi.re.kr/skin_2016/common/epicdownload.jsp?num=143619&filenum=2 (검색일:2024.04.20.)}

Korea Information Security Industry Association (2022). *Survey on Information Security.* Seoul: Korea Information Security Industry Association.

{한국정보보호산업협회 (2022). 〈2021 정보보호실태조사〉. 서울: 한국정보보호산업협회.}

Lee, B., Sohn, Y., Seo, D., Jwa, B., Hong, H. & Lee, J. (2013). "A Research Synthesis of Fear Appeal Studies over the Past 40 Years: A Meta-Analysis of Fear Appeals in Korea." *The Korean Journal of Advertising and Public Relations, 15*(3), 126-155.

{이병관·손영곤·서동명·좌보경·홍현호·이진우 (2013). 지난 40년 간 공포소구 연구의 통합 - 국내 공포소구

연구에 대한 메타분석. 〈한국광고홍보학보〉, 15권 3호, 126-155.}

Lee, H. (2019). "IoT is the Prey of Hackers... Security 'Red Flag'." *AI TIMES,* April 8.

{이한재 (2019). "해커들의먹잇감IoT…보안'적신호'." 〈AI 타임스〉. 4월 8일.}

Lee, H. (2021). "Smart Home Camera User's Update Motivation :Intended Privacy Protection Behavior Using Fear Appeals And Message Framing." Master's Thesis, Department of Business Administration, Yonsei University.

{이호진 (2021). 〈스마트 홈 카메라 사용자의 업데이트 행동 동기: 공포 소구와 메시지 프레이밍을 이용한 의도된 개인 정보 보호 행동〉. 연세대학교 대학원 석사학위 논문.}

Lee, J., Kim, H. & Lee, H. (2023). "An Empirical Study on the User Experience Model of Music Streaming Service." *Informatization Policy, 30*(3), 92-121.

{이정아·김형진·이호근 (2023). 음악 스트리밍 서비스 사용자 경험 모델에 관한 실증 연구. 〈정보화정책〉, 30권 3호, 92-121.}

Lee, K., Kim, B. & Cho, J. (2018). "Negative Transition of Smart Device Utility: Empirical Study on IT-Enabled Work Flexibility, After-Hours Work Connectivity, and Work-Life Conflict." *Journal of KIISE, 45*(4), 321-331.

{이기영·김병선·조진성 (2018). 저사양 IoT 디바이스의 안전한 부트 및 업데이트를 위한 보안 시스템 설계 및 구현. 〈정보과학회논문지〉, 45권 4호, 321-331.}

Lee, S. (2023). "Poor IoT Security, Private Lives of 400,000 People were Exposed." *SisaIN*, January 13.

{이상원 (2023). "허술한 사물인터넷 보안, 40만명의 사생활이 노출됐다." 〈시사IN〉. 1월 13일.}

Leventhal, H. (1970). "Findings and theory in the study of fear communications." In Berkowitz, L. (ed.) *Advances in Experimental Social Psychology,* 119-186. New York: Academic Press.

Li, Y., Kim, H. & Lee, H. (2022). "Why Do Users Participate in Hashtag Challenges in a Shortform Video Platform? The Role of Para-Social Interaction." *Informatization Policy, 29*(3), 82-104.

{이의경·김형진·이호근 (2022). 숏폼 비디오 플랫폼에서 사용자는 왜 해시태그 챌린에 참여하는가? : 준사회적 상호작용을 중심으로. 〈정보화정책〉, 29권 3호, 82-104.}

Lipkus I. (2007). "Numeric, Verbal, and Visual Formats of Conveying Health Risks: Suggested Best Practices and Future Recommendations." *Medical Decision Making, 27*(4), 696-713.

Lyu, J. & Kwon, S. (2021). "A Study on the Privacy Paradox in the IoT-based Smart Home Camera Usage Environment: Focusing on a Comparative Study of User Experience." *Journal Of Information Technology Applications & Management, 28*(6), 145-161.

{루진단·권순동 (2021). IoT 기반 스마트 홈카메라 이용환경에서의 프라이버시 패러독스 현상에 관한 연구: 사용경험 비교연구를 중심으로. 〈한국데이터전략학회지〉, 28권 6호, 145-161.}

Majeed, A. (2017). Internet of Things(IoT): *A Verification Framework.* Paper presented at the 2017 IEEE 7th Annual, Computing and Communication Workshop and Conference, January 9-11.

Mathur, A. & Chetty, M. (2017). *Impact of User Characteristics on Attitudes Towards Automatic Mobile Application Updates.* Paper presented at the Thirteenth Symposium on Usable Privacy and Security, July 12-14.

Meyerowitz, B. & Chaiken, S. (1987). "The Effect of Message Framing on Breast Self-Examination Attitudes, Intentions, and Behavior." *Journal of Personality and Social Psychology, 52*(3), 500.

Microsoft (2012). *Microsoft Security Intelligence Report Volume 13 (January - June 2012)*, Washington: Microsoft.

Milne, S., Orbell, S. & Sheeran, P. (2002). "Combining Motivational and Volitional Interventions to Promote Exercise Participation: Protection Motivation Theory and Implementation Intentions," *British Journal of Health Psychology, 7*, 163-184.

Möller, A., Michahelles, F., Diewald, S., Roalter, L., & Kranz, M. (2012). *Update Behavior in App Markets and Security Implications: A Case Study in Google Play.* Paper presented at the 3rd International Workshop Held in Conjunction with Mobile HCI, September 21-24.

Mullinix, K., Leeper, T., Druckman, J. & Freese, J. (2015). "The Generalizability of Survey Experiments." *Journal of Experimental Political Science, 2*(2), 109-138.

Mwagwabi, F., McGill, T. & Dixon, M. (2014). *Improving Compliance with Password Guidelines: How User Perceptions of Passwords and Security Threats Affect Compliance with Guidelines.* Paper presented at 2014 47th Hawaii International Conference on System Sciences, January 6-9.

Nov, O. & Ye, C. (2008). "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, 59*(5), 845-851.

Park, J. (2017). *Designing Fear Appeal Cues to Enhance Security Protection of Users: Leveraging from Cognitive Bias of Humans.* Paper presented at the 2017 KMIS Spring Conference, June 9-10.

Park, J., Kim, J. & Kim, B. (2017). "Online Users' Password Security Behavior : The Effects of Fear Appeals and Message Framing, and Mechanism of Password Security Behavior." *Journal of Information Technology Services, 16*(3), 147-165.

{박재영·김전도·김범수 (2017). 온라인 사용자의 비밀번호 보호행위: 공포 소구와 메시지 프레이밍 효과, 그리고 비밀번호 보호행위의 동기요인. 〈한국IT서비스학회지〉, 16권 3호, 147-165.}

Rogers, R. (1975). "A Protection Motivation Theory of Fear Appeals and Attitude Change." *The Journal of Psychology, 91*(1), 93-114.

Rogers, R. (1983). "Cognitive and Physiological Processes in Fear Appeals and Attitude Change: A Revised Theory of Protection Motivation." In Cacioppo, J. & Petty, R. (ed.) *Social Psychophysiology: A Sourcebook,* 153-176. New York: Guilford.

Rothman, A., Salovey, P., Antone, C., Keough, K. & Martin, C. (1993). "The Influence of Message Framing on Intentions to Perform Health Behaviors." *Journal of Experimental Social Psychology, 29*(5), 408-433.

Salman, O., Elhajj, I., Chehab, A. & Kayssi, A. (2017). *Software Defined IoT Security Framework.* Paper presented at the SDS 2017 4th Conference, May 8-11.

Schneider, T., Salovey, P., Pallonen, U., Mundorf, N. & Smith, N. (2001). "Visual and Auditory Message Framing Effects on Tobacco Smoking." *Journal of Applied Social Psychology, 31*(4), 667-682.

Statista (2024), "Number of Smart Homes forecast

in the World from 2017 to 2025(in millions)." https://www.statista.com/statistics/1252975/smart-home-households-worldwide/, (Retrieved on March 8).

Steindl, C., Jonas, E., Sittenthaler, S., Traut-Mattausch, E. & Greenberg, J. (2015). "Understanding Psychological Reactance New Developments and Findings," *Zeitschrift für Psychologie, 223*(4), 205-214.

Symantec Corporation (2013). "Internet Security Threat Report 2013 Volume 18, 2013." https://www.insight.com/content/dam/insight/en_US/pdfs/symantec/symantec-corp-internet-security-threat-report-volume-18.pdf, (Retrieved on March 2).

Townsend, C. & Kahn, B. (2014). "The Visual Preference Heuristic: The Influence of Visual versus Verbal Depiction of Assortment Processing, Perceived Variety, and Choice Overload." *Journal of Consumer Research, 40*(5), 993-1015.

Tsai, H. Y. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J. & Cotten, S. R. (2016). "Understanding online safety behaviors: A protection motivation theory perspective." *Computers & Security, 59,* 138-150.

Tversky, A. & Kahneman, D. (1981). "The Framing of Decisions and The Psychology of Choice." *Science, 211*(4481), 453-458.

Tversky, A. & Kahneman, D. (1984). "Choice, Values and Frames." *American Psychologist, 39*(4), 341-350.

Tversky, A. & Kahneman, D. (1986). "Rational Choice and the Framing of Decisions." *Journal of Business, 59*(4), S251-S278.

Wash, R., Rader, E., Vaniea, K. & Rizor, M. (2014). *Out of the Loop: How Automated Software Updates Cause Unintended Security Consequences.* Paper presented at the 10th Symposium on Usable Privacy and Security, July 9-11.

Wilson, D., Purdon, S. & Wallston, K. (1988). "Compliance to Health Recommendations: A Theoretical Overview of Message Framing." *Health Education Research, 3*(2), 161-171.

Witte, K. (1992). "Putting the Fear Back into Fear Appeals: The Extended Parallel Process Model." Communications Monographs, 59(4), 329-349.

Witte, K. (1994). "Fear Control and Danger Control: A Test of the Extended Parallel Process Model (EPPM)." *Communication Monographs, 61*(2), 113-134

Witte, K. & Allen, M. (2000). "A Meta-Analysis of Fear Appeals: Implications for Effective Public Health Campaigns." *Health Education & Behavior, 27*(5), 591-615.

Yoo, Y. (2022). "Cloud security authentication platform design to prevent user authority theft and abnormal operation during remote control of smart home Internet of Things (IoT) devices." *Journal of Convergence Security, 22*(4), 99-107.

{유용한 (2022). 스마트 홈 사물인터넷 기기(IoT)의 원격 제어 시 사용자 권한 탈취 및 이상조작 방지를 위한 클라우드 보안인증 플랫폼 설계. 〈융합보안논문지〉, 22권 4호, 99-107.}

Zhang, L. & McDowell, W. (2009). "Am I Really at Risk? Determinants of Online Users' Intentions to Use Strong Passwords." *Journal of Internet Commerce, 8*(3-4), 180-197.

[부록]

〈표 3〉 측정항목

〈Table 3〉 Measurement Items

변수	측정항목	출처
인지된 사생활 침해 심각성	스마트 홈 카메라를 통해 나의 개인 정보(영상)가 유출된다면, - 나에게 심각한 문제가 초래될 것이다. - 나는 많은 고통을 겪을 것이다. - 나에게 중대한 일일 것이다.	Johnston and Warkentin (2010); Boss, et al., (2015)
인지된 사생활 침해 취약성	- 스마트 홈 카메라는 나의 개인 정보(영상)가 다른 사람에 유출될 위험이 있다. - 스마트 홈 카메라를 통해 나의 개인 정보(영상)가 다른 사람에 유출될 가능성이 있다. - 스마트 홈 카메라를 통해 나의 개인 정보(영상)가 다른 사람에 유출될 것 같다.	Johnston and Warkentin (2010)
공포	- 스마트 홈 카메라를 통해 나의 개인 정보(영상)가 유출될 수도 있다는 것에 겁이 난다. - 스마트 홈 카메라를 통해 나의 개인 정보(영상)가 유출될까봐 걱정이 된다. - 스마트 홈 카메라를 통해 나의 개인 정보(영상)가 유출될까봐 두렵다. - 스마트 홈 카메라를 통해 나의 개인 정보(영상)가 유출될까봐 불안하다.	Milne, et al., (2002)
소프트웨어 업데이트 의도	- 나는 스마트 홈 카메라의 소프트웨어를 업데이트 할 의도가 있다. - 나는 스마트 홈 카메라의 소프트웨어 업데이트를 계획할 것이다. - 나는 스마트 홈 카메라의 소프트웨어를 업데이트 할 것 같다.	Johnston and Warkentin (2010)