Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.33, NO.2, Apr. 2023 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2023.33.2.353

비대면 금융거래 사용자 확인 개선방안 연구 - 메신저피싱 사례를 중심으로*

김 은 비,[1†] 정 익 래[2‡]
[1,2]고려대학교 (대학원생, 교수)

A Study on the Improvement of User Identification of Non-Face-to-Face Financial Transactions with Messenger Phishing Case*

Eun Bi Kim,[1†] Ik Rae Jeong[2‡]
[1,2]Korea University (Graduate student, Professor)

요 약

전기통신금융사기 범죄인 메신저 피싱은 스마트폰 원격제어와 비대면 금융거래를 악용한 것으로 재산 피해는 물론이고 피해자들의 신용과 채무문제가 발생해 이차 피해가 심각하다. 이러한 금융사고는 피해자들의 부주의도 있겠지만 현재 메신저 피싱 범죄 수법은 지능적이며, 비대면 사용자 확인 절차의 허점을 파고든 결과로도 볼 수 있다. 본 연구에서는 메신저 피싱이 비대면 금융거래 시 사용자 확인 절차의 허점을 어떻게 악용하고 있는지 사례를 중심으로 분석하고, 실험을 통해 더 안전한 금융거래를 위한 비대면 확인 항목별로 개선점을 제언한다.

ABSTRACT

Messenger phishing, communications frauds crime, exploits remote control of smartphones and non-face-to-face financial transactions, causing property damage due to money transfers, as well as account opening and loans in the name of victims. Such financial accidents may be careless of victims, but the current messenger phishing criminal method is intelligent and can be seen as digging into loopholes in the non-face-to-face user verification process. In this paper we analyze how messenger phishing uses loopholes in user identification procedures in non-face-to-face financial transactions. Through experiments, it is suggested to improve the non-face-to-face verification process for safer financial transactions.

Keywords: Messenger phishing, Remote control, Non-face-to-face financial transactions

I. 서 론

금융위원회에서 2015년 5월 '계좌 개설시 실명확인 방식 합리화 방안'을 발표하고, 그 해 11월에 비대면 거래를 중심으로 하는 인터넷 전용은행이 출범하면서, 영업점을 방문하지 않고 PC나 스마트폰을 통해 간단한 본인인증만 거친 후 계좌개설, 송금, 대출 등의 모든 금융거래를 비대면으로 할 수 있게 되었다.

2021년 말 기준 국내은행의 모바일 뱅킹 등록 고객수는 1억 5,337만명으로 2020년 대비 13.5% 증가했고, 인터넷 뱅킹(모바일 뱅킹 포함, 일평균)을 통해 자금이체·대출신청서비스 이용건수 및 금액은 1,732만건, 70.6조원이며, 이 중 모바일 뱅킹의 이용건수는 1,436만건, 12.9조원으로 전년대비 각각 22.9%, 36.6% 증가했다. 특히 대출신청서비스 이

Received(12. 22. 2022), Modified(03. 06. 2023), Accepted(03. 24. 2023)
* 본 논문은 금융보안원·금융정보보호협의회·금융보안포럼이 주최한 「제6회 금융보안원 논문공모전」에서 우수논문으로 선정된 논문을 수정 보완한 논문입니다.
† 주저자, sertworld@police.go.kr
‡ 교신저자, irjeong@korea.ac.kr(Corresponding author)

용건수는 2021년 3만건으로 전년대비 증가율 47.6%, 대출신청 이용 금액은 7,545억원으로 56.9% 증가하는 등 큰 폭으로 확대되었다[1].

이처럼 인터넷·모바일뱅킹 서비스를 통한 비대면 금융거래가 크게 증가한 것은 금융거래의 편의성 향상을 반영하는 지표임과 동시에 누구나 비대면 금융거래를 손쉽게 이용할 수 있는 것을 뜻하기도 한다.

반면, 모바일 뱅킹 이용자의 스마트폰에는 비대면 금융거래를 할 수 있는 개인정보, 금융정보들이 저장되어 있는데, 이런 중요 정보들이 저장된 스마트폰이 해킹된다면 그 피해는 걷잡을 수 없게 된다.

특히, 메신저 피싱 범죄로 인하여 금융정보 유출과 금전적인 피해가 발생하더라도, 금융기관에서는 금융위원회에서 가이드로 제시한 '계좌 개설시 실명확인 방식 합리화 방안'을 준수하여 금융거래 사용자 확인을 진행하였다는 이유로 금융사고의 책임을 피해자에게 부담[1]시키고 있다.

본 연구에서는 비대면 금융거래의 사용자 확인 절차가 너무 간편한 것은 아닌지, 수많은 금융거래 서비스가 하자 없이 제대로 제공되고 있는지를 전반적으로 검토해 본다. 현재 메신저 피싱 범죄 수법을 중심으로, 비대면 금융거래에 필요한 본인 확인 절차 중 미처 고려하지 못한 요소들이 실제 범죄에서 어떻게 악용되었는지 사례를 바탕으로 분석하고, 그 대응방안으로 개선되어야 할 요건을 제시하고자 한다.

II. 관련 선행 연구

메신저 피싱을 중점적으로 다룬 선행연구는, 메신저 피싱 범행에 주로 사용되는 통신사, 문자수발신 시간, 전화번호 등의 범죄정보를 데이터베이스로 축적하여 수사기관과 민간업체간의 대응체계와 범죄행위를 사전에 차단하기 위한 관련 법 개정을 제안한 연구[2], 메신저 피싱에 사용되는 단어를 분석하여 피싱으로 의심되는 대화의 탐지 방안을 제안한 연구[3], 메신저 피싱 수사 사례를 바탕으로 수사기관의 신속한 수사를 위한 금융기관, 민간업체의 공조체계 구축과 모바일뱅킹 구동 중에는 원격제어 어플을 차단하는 방안을 제안한 연구[4] 등이 있다.

또한, 현재 비대면 금융거래에서의 비대면 인증 항목별로 발생할 수 있는 취약점을 다룬 연구[5], 비대면 금융거래가 확산됨에 따라 금융사고 방지를 위한 금융소비자의 법적, 제도적 대책을 다룬 연구[6], 금융당국에서 시행하고 있는 전자거래 당사자의 본인확인 정책을 검토하고 비대면 실명인증 제반 사항을 다룬 연구[7] 등 비대면 금융거래 정책들을 다룬 연구들이 있다.

위와 같은 선행연구들이 있음에도 메신저 피싱의 범죄는 증가하고 있고, 현재 메신저 피싱에서 악용되는 비대면 금융거래로 인해 그 피해액 또한 큰 폭으로 증가하였다. 메신저 피싱과 비대면 금융거래를 접목시켜 그 대응방안을 세밀하게 다룬 연구는 아직 부족한 실정이다.

III. 메신저 피싱 실태와 피해사례

3.1 메신저 피싱 관련 통계

메신저 피싱 범죄가 처음 화제가 되었던 것은 2000년대 초반으로, PC 메신저를 통해 직장 동료, 가족을 사칭하며, 급전을 빌미로 계좌이체를 요구하며 금전을 탈취하는 수법이었다. 그 뒤 몇 년간은 발생이 잦아들다가, 정보통신기술 발달과 스마트폰 사용이 대중화 되면서 모바일 메신저 또는 휴대폰 문자를 사용한 메신저 피싱 범죄 발생이 증가하기 시작하였다.

결과적으로, Fig. 1.과 같이 2021년 기준 발생한 전체 사이버금융범죄[2] 중 메신저 피싱 비율이 58.6%로 과반수 이상을 차지하고 있다. 경찰청이 2019년부터 본격적으로 메신저 피싱 통계를 관리한 것을 감안하여도 최근 3년간 메신저 피싱의 발생건수가 8배 가까이 급증하였다.

메신저 피싱의 심각성을 말해주는 또 다른 통계는 2021년 금융감독원에서 보도한 자료이다. 해당 자료에 따르면 보이스 피싱 피해액은 감소하였으나, 메신저 피싱 피해액은 증가하였다. 특히 2020년 상반기에 비해 2021년 상반기 피해액은 466억원으로 동기간에 비해 165.4% 대폭 증가하였다. 이는 보이스 피싱(기관사칭 유형)에서 메신저 피싱으로 범행 수법

1) 은행이 공인인증서로 본인확인 절차를 거쳤다면 은행에 책임을 물을 수 없는 만큼 대출약정은 유효하다는 취지로, 금융사기 조직에 공인인증서를 도용당해 대출 피해를 입었어도 대출원리금을 모두 상환할 의무가 있다는 판결임. (서울중앙지방법원 2020. 12. 24. 선고 2019가합580780 판결 〔채무부존재확인〕)

2) 경찰청에서는 피싱, 파밍, 스미싱, 메모리해킹, 몸캠피싱, 메신저 피싱, 기타금융범죄 7개 항목을 사이버금융범죄로 분류하고 있다.

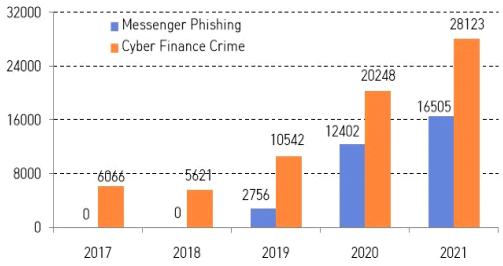
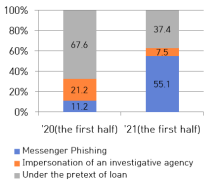


Fig. 1. Messenger Phishing - Cyber Finance Crime Statistics(Occurrence)



Type		2019	2020	the first half	2021 (the first half)	Increase or decrease year-on-year (rate)
an impersonation type	Messenger Phishing	342	373	176	466	↑290 (165.4%)
	Investigative agency	1,872	414	334	63	↓271 (81.1%)
Under the pretext of loan		4,506	1,566	1,067	316	↓751 (70.4%)

(Unit : one hundred million)

Fig. 2. Communications frauds crime damage status

이 변하고 있으며[8] 메신저 피싱으로 인한 피해금이 보이스피싱을 넘었음을 의미한다.

이렇게 단시간에 메신저 피싱 피해금이 급증하게 된 배경은 현재의 메신저 피싱 범행 수법과 밀접한 관련이 있다.

3.2 메신저 피싱 범행 수법

현재 가장 많이 발생하는 메신저 피싱 범행 수법은 피해자의 자녀를 사칭하면서 모바일 메신저, 문자로 연락해 피해자를 속인 뒤, 피해자의 스마트폰에 "팀뷰어"와 같은 원격제어 어플을 설치하게 한다. 원격제어 어플이 설치되면, 피해자의 스마트폰에 접속한 후, 범인이 직접 피해자 명의로 금융거래를 하는 수법이다. 피해자로부터 신분증 사진과 모바일 뱅킹을 이용할 수 있는 비밀번호와 같은 금융정보만 추가적으로 알아내면, 피해자 스마트폰으로 할 수 있는 모든 비대면 금융거래를 진행할 수 있다. 메신저 피싱에 악용되는 원격제어 어플은 별도의 악성코드가 아닌 정상적인 프로그램으로, 피해자 스마트폰에 이런 원격제어 어플이 정상설치 가능한데, 이로 인해 모바일 뱅킹 서비스를 이용하고 있다면, 메신저 피싱으로 막대한 피해를 입을 수 있다.

3.3 메신저 피싱 범죄에서 악용되는 비대면 거래

Table. 1.은 메신저 피싱 범죄로 피해자 스마트폰에 원격제어 어플을 설치하여 접속한 후, 피해자 명의로 실행했던 비대면 거래를 분석한 것이다. 계좌이체는 물론 피해자 명의로 신규 계좌 개설, 대출 실행, 예적금 해지, 주식거래도 하였다. 또한 인증서까지 재발급 받았고, 모바일 뱅킹의 로그인 방식이 바이오인증이면 이를 간편 비밀번호 입력 방식으로 변경하였다.

피해자가 범인에게 정보를 알려주지 않은 계좌에서도 금융거래가 발생하였는데, 이는 금융기관이 "오픈뱅킹" 서비스를 제공하고 있기 때문이다. 범인은 이 점을 악용해 피해자 명의로 된 금융계좌를 모두 알아낸 후 해당 계좌들의 잔고를 갈취한다[9].

메신저 피싱 피해금을 이체할 때, 수십개의 타인 명의 계좌로 나눠서 이체하는데, 정상적인 개인·회사의 계좌로도 이체하여 수사기관의 추적을 어렵게 하

Table 1. Non-face-to-face transactions from messenger phishing

Damage Type	Method of crime
Certificate	Certificate discard, reissue
Login method	Change biometric authentication method to password method
Sign up open-banking services	Check all financial accounts of the victim
Account transfer	Transferring to dozens of crime financial accounts
Termination of deposit	Transfer a canceled deposit to a criminal account
Selling Crypto	Transfer to a criminal account after selling Crypto
A new credit(card) loan	Transfer the loan to the criminal account
A new mortgage loan	
In-app billing	Purchase gift certificates and game items with in-app billing
Opening a new account	Using Internet Banks
Opening of a cell-phone	Using MVNO

고 있다. 금융기관에서는 「전기통신금융사기 피해금 환급에 관한 특별법」에 따라 전기통신사기 피해금이 이체된 상대 계좌를 지급정지하는데, 이로 인해 정상적으로 사용하던 사람들은 갑자기 본인 계좌를 사용할 수 없는 또 다른 피해가 발생한다.

스마트폰 신규 개통의 경우 금융 거래는 아니지만 범인이 이차적으로 비대면 금융거래를 위해 악용하는 방법이다. 온라인을 통해 피해자 명의로 스마트폰을 새롭게 개통하면 그 뒤로는 피해자의 기존 스마트폰을 원격조종할 필요없이, 피해자 명의로 할 수 있는 모든 비대면 금융거래를 진행한다. 이런 사실을 꽤 많은 시간이 흐른 뒤에야 피해자는 알 수 있어, 그 전까지는 예측 불가능한 이차 피해가 계속해서 발생한다.

IV. 비대면 사용자 확인 절차 현황

4.1 국내 비대면 확인 방식

그동안 금융실명법 및 전자금융거래법에 의해 직접 대면을 통한 금융거래 사용자 확인만이 인정되었기 때문에 인터넷전문은행 및 비대면 인증 관련 업무를 수행할 수 없었다. 그러나 2015년 5월 금융위원회 금융개혁회의를 통해 '개좌 개설시 실명확인 방식 합리화 방안'이 발표[10]되면서, 기존의 금융실명법 및 전자금융거래법에 대한 실무적 확대 해석을 통해 금융거래 사용자 본인 확인을 직접 대면 방식뿐만 아니라, 비대면 방식까지 허용하였다[5].

Table 2. A Study on the Rationalization of User Identification Method when Opening an Account

Category	Detailed Category	Note
A mandatory requirement	① Submit a copy of ID Card	Adopting 2 of these
	②Video call	
	③Check when delivering financial access item	
	④Using existing account	
	⑤the equivalent of this (biometric authentication, etc)	
Recommen-dations	⑥Using the results of other agencies' checks (Cell-phone verification, etc)	Adopting 1 of these
	⑦Verification of multiple personal information	

금융위원회에서 비대면 확인 방식을 도입한 해외 사례를 분석한 후, 우리나라 여건에 맞는 비대면 확인 방식을 Table. 2.와 같이 "필수사항"과 "권고사항"으로 나누어 다중확인 방식을 제시하였다.

이에, 각 금융기관은 내부 여건과 실정에 맞게 "필수사항" 중 두 가지와 추가적으로 "권고사항" 중 한 가지를 채택하여 비대면으로 금융거래 사용자 본인확인을 하고 있다[11].

4.2 금융기관의 비대면 확인 절차 실태

4.2.1 간편 위주의 비대면 확인

각 금융기관에서는 비대면 사용자 확인 방법 중 필수방식을 선택할 때 최대한 빠르고, 간편한 방식을 채택하고 있다. 비대면 금융거래 사용자 입장에서도 복잡하지 않고, 영업점 방문 없이 최소한의 시간이 소비되는 것을 선호하기 때문이다. 실제로 각 금융기관의 모바일 뱅킹을 이용해보면 비대면 계좌개설과 대출이 간편하고 빠르다며 광고하는 것을 볼 수 있다.

신분증 사본(사진)을 제출하고, 본인 명의의 계좌를 인증받은 후 본인 명의 휴대폰으로 문자전송된 인증번호를 입력하면 개인의 신용문제와 직결되는 대출이 단 몇 분 만에 완료될 정도로 비대면 사용자 확인 절차가 간편하다.

4.2.2 일방적인 사용자 입력 위주의 비대면 확인

메신저 피싱 범죄 수법은 현재 시행하고 있는 비대면 금융거래 사용자 확인 절차의 허점을 정확하게 악용하고 있다. Fig. 3.은 메신저 피싱에서의 원격제어 프로그램을 통해 이루어진 비대면 금융거래의 절차를 요약한 것이다.

피해자들을 속이기 위해 ①, ②의 선행행위가 있고, 이를 통해 확보한 피해자들의 정보를 가지고 ③부터 원격제어를 통해 피해자의 명의로 직접 비대면 금융거래를 한다.

이렇게 제3자인 범인이 피해자 명의로 비대면 거래가 가능한 것은 대부분의 금융기관에서 "신분증 사본 제출", "기존계좌 활용", "휴대폰 문자 인증"으로 비대면 확인을 하는데, 이 확인 방법들은 금융거래 사용자의 일방적인 인증이다. 즉, 금융기관이 명의자

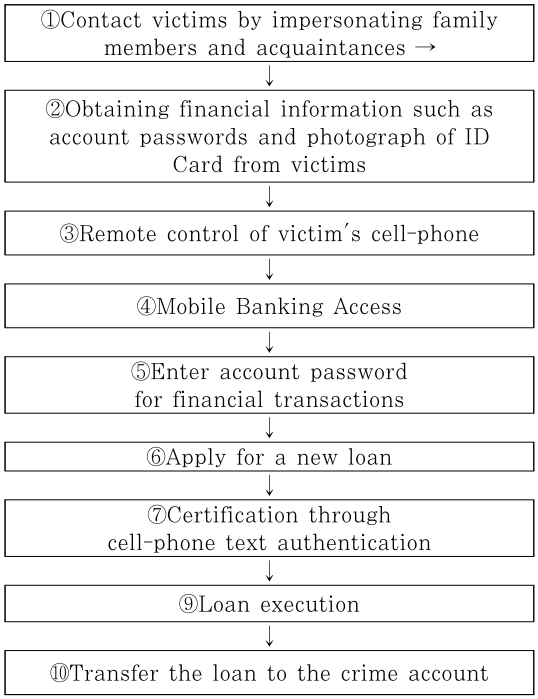


Fig. 3. Proceed with Messenger Phishing

와 금융거래를 신청한 사람이 실제로 동일인인지에 대한 추가 보완적인 확인 절차가 없기 때문이다. 금융거래 사용자의 일방적인 정보 제공만으로 인증이 완료되기 때문에, 메신저 피싱 피해를 입어 자신의 의사와는 상관없이 범인이 원격조종으로 비대면 금융거래를 실행하여도 금융기관에서는 그 거래가 비정상적인지 알 수 없다.

피해자가 속아서 범인에게 개인·금융정보를 전송해주었다 하더라도, 피해자의 신용에 직접적인 영향을 미치는 대출이 쉽게 실행되는 것은 피해자의 부주의로만 결론지을 것은 아니다. 비대면 금융거래가 정상적인 사용자들에게는 신속성과 편의성을 제공하나, 원격제어 어플을 악용한 메신저 피싱과 같은 예외적인 상황에서의 비대면 사용자 확인 절차에 대해서는 정밀하게 점검해 봐야 할 것으로 보인다.

V. 비대면 사용자 확인 절차 개선점

5.1 비대면 사용자 확인 항목별 문제점

Table. 3.은 2022년 1월부터 6월까지 경기도남부경찰청에 접수[3]된 메신저 피싱 사건들의 비대면 금융거래와 사용자 확인 방식을 분석한 것이다. 메신저 피싱 112건 중 원격제어 어플을 이용해 비대면 계좌개설, 신용대출과 같은 중요거래가 발생한 피해는 62건으로 절반을 차지한다.

62건 모두 신분증 사본제출, 타행계좌 인증, 스마트폰 문자인증을 통해 진행된 것으로, 금융기관과 금융거래 사용자간의 영상통화나 음성통화 같은 양방향 인증이나 원격제어 어플로는 입력할 수 없는 생체인증은 사용되지 않았다.

이러한 통계를 바탕으로 본 절에서는 대부분의 금융기관에서 채택한 비대면 사용자 확인 방식의 취약점을 분석하고 개선 방안을 제시하고자 한다. 확인 방식 중 "접근매체 전달시 확인" 방식은 실시간으로 진행되는 것이 아니기 때문에 분석에서 제외한다.

5.1.1 실명증표 사본제출

사본 제출된 신분증의 진위여부를 확인하는 것으로, 사본 제출 방식은 신분증 원본을 사진촬영하여 제출하는 방식이다. 금융기관은 "주민등록증(운전면허증) 진위확인 시스템"을 도입해[12] 제출된 신분증의 위·변조 여부를 검증하고, 정상적인 신분증으로 확인되면 실명 확인을 완료한다. 신분증을 소지하고 있는 국민이라면 간편하고 쉽게 사본 제출을 통해 비대면으로 사용자를 확인할 수 있다.

문제는 신분증 실물(원본)이 아닌 촬영되었거나 인쇄된 신분증을 재촬영하더라도 가능하다는 것이다. 즉, 실명확인증표 사본제출만으로는 명의자가 직접 금융거래를 신청했는지 알 수 없다. 이러한 허점을 악용해 메신저 피싱 범인은 피해자로부터 신분증 사진을 전송받아 금융거래에 필요한 비대면 사용자 확인을 진행한다.

금융거래뿐만 아니라 스마트폰 신규 개통 절차에서도 전송받은 신분증 사진으로 사용자를 확인하는데 문제가 없다. 실제로 메신저 피싱에서 피해자 명의로 스마트폰을 신규 개통한 후, 소액결제를 하거나 피해자 명의로 계좌를 새롭게 개설하여 대출하기 때문에, 신분증 사본으로 인증된 비대면 거래의 피해는 고스란히 피해자가 떠안고 있다[13][14].

3) 경기남부 지역 경찰관서에서 접수받은 메신저 피싱 사건 중 피해액이 일정 기준치 이상되는 건들은 경기도남부경찰청(사이버범죄수사대)로 이첩된다. 해당 통계는 사이버범죄수사대로 이관된 메신저 피싱 건수이다.

Table 3. Non-face-to-face User Identification method statistics

	account transfer	Opening a new account	Loan execution(44)					Termination of deposit
			credit loan	card loan	stock mortgage	endowment mortgage	deposit mortgage	
	50	12	6	22	8	6	2	6
Submit a copy of ID Card	-	12	6	4	-	2	-	-
Video call	-	-	-	-	-	-	-	-
Using existing account	-	12	6	1	6	-	2	2
Biometric authentication	-	-	-	-	-	-	-	-
Check when delivering financial access item	-	-	-	-	-	-	-	-
SMS verification	-	12	6	20	6	6	2	6

5.1.2 영상통화

금융기관과 금융거래 사용자 간 양방향으로 확인하는 방식이다. 금융기관이 금융거래 사용자와 명의인의 일치 여부를 육안으로 직접 확인하므로, 신뢰성이 높으면서도 금융기관의 책임감 또한 부여된다.

실제로 S은행에서는 본인 명의의 휴대폰을 가지고 있지 않아 휴대폰을 통한 인증을 할 수 없는 고객에 대해서는 개인정보 변경이나 신규 적금 가입과 같은 일부 금융거래는 영상통화로 인증하는 항목이 있다. 금융기관 직원이 영상통화를 통해 직접 금융거래 사용자 얼굴을 확인하고 신분증 원본을 소지하고 있는지, 신분증 정보가 일치하는지 확인한다.

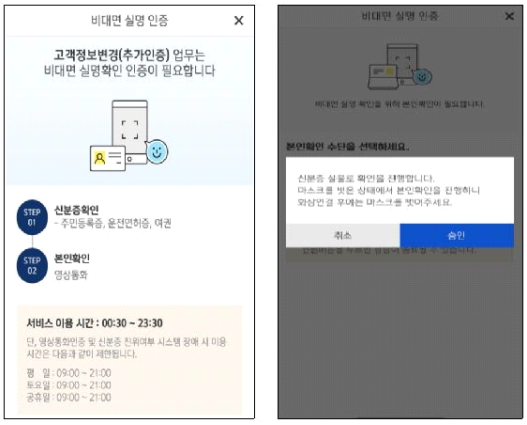


Fig. 4. S Bank's "Video Call" Certification Process

그런데 영상통화를 필수 확인 수단으로 채택한 경우는 많지 않다. 금융위원회가 비대면 사용자 확인 방식을 자율적으로 선택할 수 있도록 했고, 금융기관 직원이 상주해야 한다는 점과 고객이 영상통화가 가능한 영상장비가 있어야 한다는 한계 때문이다. 금융거래 사용자들도 불가피하게 영상통화를 꼭 해야 하는 상황이 아니면 영상통화 방식은 선택하지 않는다.

5.1.3 기존계좌 활용

이미 개설된 기존 계좌를 통해 금융거래 사용자를 확인하는 방식이다. 대면이든 비대면이든 이미 금융기관에서 사용자 확인을 거친 정상적인 계좌를 보유한다는 점을 전제조건으로 착안한 방식이다. 따라서 이미 입출금 계좌를 1개 이상 보유한 고객은 상대적으로 간단하고 쉽게 확인할 수 있어, 대부분의 금융기관에서 신분증 사본과 함께 확인하는 절차 중 한 가지로 채택했다.

그러나 기존 계좌 활용방식의 허점이 메신저 피싱 범죄에서 악용된다. 기존 금융정보는 명의자 본인만이 알아야 하는데, 범인에게 속은 피해자는 계좌 비밀번호와 같은 자신의 정보를 알려준다.

피해자가 특정 은행의 정보만 알려준다 하더라도, 범인은 "오픈뱅킹"을 신청해, 피해자가 알려주지 않은 타행 계좌정보까지 모두 확인할 수 있다. 게다가 범인이 피해자 모르게 신규 개설한 피해자 명의의 계좌를 악용하면 현재 비대면 사용자 확인 절차로는 인지할 방법이 없다.

기존계좌 활용 방식의 단점으로 지적되었던 “명의 도용, 피싱 등에 이용, 한 개의 대포통장으로 복수 계좌 개설 등 부작용”이 메신저 피싱 범행에 그대로 적용되고 있다. 신분증 사본 제출과 마찬가지로 계좌 인증 신청자가 명의자 본인인지, 행위자의 동일성이 확인되지 않는 일방적인 인증 절차이기 때문이다.

5.1.4 바이오 인증(기타 이에 준하는 방법)

개인의 고유한 생체정보, 바이오 정보를 통해 비대면 사용자 확인을 하는 방식이다. 바이오 정보는 등록한 당사자 외에는 인증할 수 없는 강력한 방식이지만 모든 스마트폰이 생체인식 기능이 탑재되어 있지 않고, 금융기관에서도 바이오 인증을 필수적으로 채택하고 있지 않다.

또한, 현재 바이오 인증은 금융거래 사용자 본인이 직접 등록하였는지 확인하지 않고, 스마트폰에 등록된 바이오 정보와 비교하는 방식이다. 단순히 스마트폰에 등록된 바이오 정보와 비교하는 것으로는 신원확인의 허점이 있다.

바이오 방식에서 비밀번호 입력과 같은 다른 방식으로 변경할 때, 새로운 바이오 정보로 재등록할 때 기존에 등록되었던 정보와 다르다는 것을 인지하거나 명의자에게 별도로 알리지 않는 점도 메신저 피싱 범죄에서 그대로 악용되었다.

피해자가 모바일 뱅킹 로그인이나 금융거래 사용자 확인을 바이오 방식으로 설정해 두었더라도, 범인은 이미 피해자 스마트폰 제어권을 가지고 있기 때문에 간편 비밀번호 입력이나 패턴 입력 방식으로 변경하여, 비대면 금융거래를 진행한다.

5.1.5 스마트폰 문자인증(타기관 확인결과 활용)

스마트폰 문자인증 방식은 수신되는 문자 내용상의 인증번호를 확인해서 입력하는 것으로, 비대면 사용자 확인 방식에서 필수사항과 함께 가장 많이 사용된다.

문자 인증 방식은 스마트폰 명의자 본인만이 수신된 인증번호를 확인하고, 인증번호 내용은 타인에게 절대 알려주지 않는다는 점이 전제되어야 한다. 그러나 메신저 피싱에서는 피해자 스마트폰을 원격제어하거나 피해자 명의로 스마트폰을 신규 개통하는 등 스마트폰을 제어하는 주체가 제3자이기 때문에 해당 전제는 무력화된다. 스마트폰 문자 인증은 정보유출과 신원확인에 취약하므로, 비대면 사용자 확인 결과로 신뢰하기에는 위험성이 높다.

5.2 비대면 사용자 확인 방식 개선사항

비대면 사용자 확인 방식의 허점으로 인해 원격제어 어플을 사용한 메신저 피싱에서 피해자가 인지하지 못하는 피해가 급증하고 있다. 이러한 문제점을 해결하기 위해 제시한 실명 확인 방식별 개선사항은 다음과 같다.

5.2.1 실명확인증표 사본 제출

현재 실명확인증표 사본 제출 방식은 신분증 앞면에 기재된 개인정보의 위조유무, 진위 확인 위주로만 검증하기 때문에 제출된 신분증 사진이 실물을 직접 촬영한 결과물인지, 이미 촬영된 신분증 사진을 재촬영한 것은 아닌지 확인하여야 한다.

개선사항으로는 모바일 뱅킹 어플에서 사용하는 신분증 촬영 기능을 활용하되, ①파일 업로드가 아닌 직접 촬영만 가능하도록 하고, 촬영 시 ②신분증 앞, 뒷면 외에도 옆면을 촬영케 하거나, ③신분증만이 아닌 금융거래 사용자와 같이 촬영, 또는 신분증과 타임 스탬프를 찍게 하는 특정한 조건을 추가하고, 제출된 신분증 사진을 ④금융기관에서 최종 확인하는 절차까지 진행한다. 금융기관에서 최종적으로 확인하기 전까지는 신규 비대면 금융거래는 할 수 없도록 해야 한다.

메신저 피싱은 피해자 스마트폰을 직접 원격제어하는만큼 실시간을 요하는 범행이다. 위와 같이 신분증 앞면 촬영만으로 비대면 사용자 확인이 완료되는 것이 아니고, 확인 과정에 상당한 시간과 공수가 들어가게 된다면 메신저 피싱 범행이 빠르게 진행되는 것을 제어할 수 있다.

또한, 피해자로부터 얻은 신분증 사진은 휴대폰을 개통할 때 악용하기 때문에 비대면 금융거래 뿐만 아니라 휴대폰 온라인 개통과 같은 사용자 명의로 새롭게 개설, 개통할 때에도 미리 촬영된 사진 파일 업로드 방식은 제한해야 할 것이다.

5.2.2 영상통화

메신저 피싱 범행 중 범인이 피해자 스마트폰을 원격제어하는 동안에는 피해자에게 걸려오는 영상통

화, 음성통화는 원격지에 있는 범인의 기기로 전환하여 받을 수 없다. 따라서, 비대면으로 중요 금융거래(계좌개설, 대출신청)를 진행할 때에는 영상통화를 반드시 필수로 도입하는 것을 제안한다. 현재 국민 대다수가 카메라 기능이 기본으로 장착된 스마트폰을 이용하고 있기 때문에 영상통화가 필수로 도입되는 것에는 부담이 적다.

영상통화 시에는 금융기관이 금융거래 사용자의 기본적인 개인정보, 현재 신분증을 소지하고 있는지, 계좌개설이나 대출신청의 이유, 사전에 메신저 피싱과 같은 의심되는 연락을 받은 사실이 있는지 등 간단한 질의응답도 병행하도록 한다.

위와 같이 개인의 신용과 관련된 계좌개설, 대출신청 시 금융기관에서 명의자를 상대로 영상통화를 필수로 시행하고 양방향으로 비대면 사용자 확인 절차를 거친다면, 메신저 피싱 범죄로 인해 피해자 모르게 금융거래가 진행되는 이차 피해를 방지할 수 있다.

5.2.3 기존계좌 활용

기존 계좌의 사용 지속 기간과 개설한 지 얼마 안 된 신규 계좌로 인증하였는지를 확인하고, 자동응답의 ARS 방식이 아닌 AI 방식 또는 금융기관에서 가입자와 직접 전화 통화하는 절차를 추가한다.

메신저 피싱 범인들이 피해자의 스마트폰을 원격제어하는 동안에는 범행이 발각될 수 있는 상황을 최소화하고, 전화통화는 원격지 기기로 전환하여 통화하는 것이 불가능하기 때문에 범인들은 피해자 스마트폰으로 걸려오는 전화는 받지 않는다.

따라서, 기존 계좌 활용은 금융기관에서 명의자 본인이 신청한 것인지 다시 한번 확인하는 추가 절차가 필요하다. 즉, 금융기관 직원이 직접 비대면 금융거래 사용자에게 전화를 걸어 양방향 소통을 하거나, AI 방식의 음성통화로 무작위 숫자를 부르고 키패드로 입력하는 방식을 추가 도입해야 한다.

5.2.4 바이오 인증

메신저 피싱 조직이 피해자의 스마트폰을 원격제어하는 중에는 키패드·키보드 입력은 할 수 있지만 Fig. 5.와 같이 카메라와 생체인식 기능은 원격지 기기로 전환할 수 없어, 홍채, 안면인식과 지문인식은 불가능하다.

따라서, 단순히 스마트폰에 등록된 바이오정보와

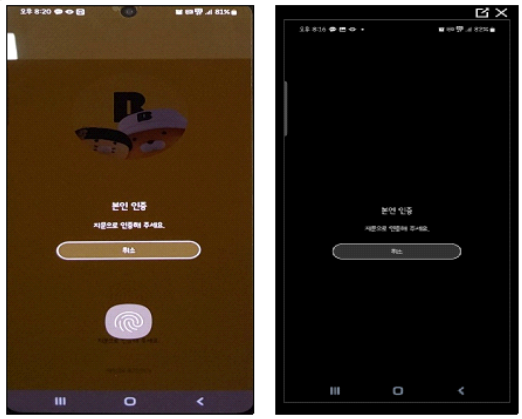


Fig. 5. Biometrics screen between remote location and remote target device

같은지 비교하는 것으로 사용자 확인을 하는 것이 아닌, 금융기관에서 비대면 사용자 확인에 필요한 바이오 정보의 최초 등록은 적어도 금융기관 영업점에 방문하거나 영상통화를 활용, 양방향 소통을 통해 금융거래 사용자와 바이오 정보 등록자가 동일한지 확인하는 절차가 필요하다.

바이오 인증에서 간편 비밀번호 입력이나 패턴 입력과 같이 다른 방식으로 변경 시에는 명의자에게 통보하고, 변경한 날은 일일 계좌 이체한도를 감소시키거나 신규 대출 제한 등의 일정 시간 금융거래를 제한하는 추가 보완적인 사항도 필요하다.

5.2.5 비대면 사용자 확인 항목 구분 개선

개선안으로 제시한 비대면 사용자 확인 항목별 필수사항과 선택사항의 결과를 정리하면 Table. 4와 같다. 영상통화는 필수항목으로 하며, 권고항목별로는 상호보완적인 방안을 제안하였다. 문자 인증 방식은 선택사항으로 그대로 두되, 확인 결과로서의 유효성은 배제하도록 한다.

원격제어 어플이 사용되어도 안전하게 비대면 사용자 확인을 하려면 대상이 되는 스마트폰으로만 실제 본인인지 인증할 수 있는 항목이 도입되어야 한다. 음성·영상통화, 카메라를 이용한 실시간 촬영, 바이오 인증이 그 예이다.

이 기능들이 모바일 뱅킹에서 비대면 금융거래를 진행할 때 사용자 확인 과정에 필수로 추가된다면 메신저 피싱의 피해액을 상당수 줄일 수 있을 것이다.

Table 4. User Identification Method (Improvement plan)

Category	Detailed Category	Note
Mandatory requirement	①Video call	①Check the ID Card ②Basic Information Questions
Recommendation (Adopting 2 of these)	②Submit a copy of ID Card	①Confirmation of financial institutions ②Add conditions of ID card copy
	③Check when delivering financial access item	
	③Using existing account	①Voice calls
	④Biometric authentication	①Notify user ②Restrictions on transactions
	⑤Verification of multiple personal information	
Optional	⑥Using the results of other agencies checks (Cell-phone verification, etc)	

VI. 결 론

금융위원회에서 비대면 실명확인 가이드라인을 발표할 때, "비대면 확인 과정에서 명의 도용 금융사기나 대포통장 발급 등 부작용 가능성을 최대한 차단할 것"이라고 자신하였다.

그러나 디지털 기술이 급속도로 발달함과 동시에 이전까지는 전혀 볼 수 없었던 비대면 금융거래를 악용한 신종 수법의 금융사기가 발생하고 있다. 전기통신금융사기의 피해는 끊이지 않고 있으며, 금융당국의 대책 또한 뒷수습에 불과한 양상을 보이고 있다.

국민들에게 비대면 금융거래라는 편의성만 제공하면서, 오히려 금융기관의 책임은 면책하고 있다. 사회 공학 기법에 당한 피해자들의 부주의도 있지만, 허술한 비대면 금융거래 사용자 확인 방식으로 인해 피해자가 의도하지도 않은 대출과 같은 추가 피해까지 피해자에게 전가하는 것은 개선해야 한다.

우리나라보다 비대면 금융거래를 먼저 시행하고 있던 일본, 프랑스의 경우, 금융기관이 금융거래 사용자들에게 우편을 보내 대면으로 본인임을 확인하거나 금융기관과 사용자간의 영상통화 같은 방식들을 사용한다. 이런 방식은 일방적인 인증이 아닌 양방향으로 사용자를 확인한다는 점이 핵심이다.

다시 과거로 돌아가 영업점 방문을 통한 대면 거래 전면 실시까지는 아니더라도, 안전한 비대면 금융거래를 위해 금융기관과 거래 사용자 간 비대면이지만 양방향 방식의 절차를 필수적으로 이행하도록 가이드라인을 개정하거나, 원격제어 어플로 실행할 수 없는 실시간 카메라 촬영, 영상·음성통화 등 좀 더 안전한 비대면 방식을 도입하여야 한다.

References

[1] Bank of Korea, "Status of use of Internet banking services by domestic banks in 2021", https://eiec.kdi.re.kr/policy/materialView.do?num=224135, Accessed, June. 2022

[2] So-won Nam, Hak-sun Lee, Sang-jin Lee, "A Study on Countermeasures through Messenger Phishing Experience Analys," Journal of The Korea Institute of Information Security & Cryptology, 32(5), pp. 791-805, Oct. 2022

[3] Ji-hyo Bae, Su-yeol Chae, Myeong-jun Song, Kyeong-chan Bang, "Detection method through analysis of messenger phishing conversation," KICS Fall Conference 2019 Program, pp. 537-538, Nov. 2019

[4] Young-ho Jung, Hyung-jun Ha, "Messenger Phishing Crime : Trends and Responses," Journal of Criminal investigation Studies, 8(1), pp. 31-54, June. 2022

[5] Hyeon-min Kim, Jin-ho Lee, "A Study on the Safe Non-face-to-face Certification of Financial Companies," e-Finance and Financial Security, pp.

33-63, Nov. 2016
〔6〕 Tae-jun Park, "A Study on the Protection of Financial Consumers by the Spread of Non-face-to-face Financial Transactions," Master's thesis, Graduate School of Policy Studies, Korea University, Feb. 2019
〔7〕 Eung-jun Jeon, "A Study on the Customer Identification in Electronic Financial Transactions," Journal of Korea Infomation Law, 19(3), pp. 239-265, Dec. 2015
〔8〕 Financial Supervisory Service, "Voice phishing damage status in the first half of 2021", https://eiec.kdi.re.kr/policy/materialView.do?num=217836, Accessed, Jan. 2022
〔9〕 Segye Times, "Vulnerable authentication·Open banking…all accounts are stolen even if one place is breached", https://www.segye.com/newsView/20201124519835, Accessed, Apr. 2022
〔10〕 Financial Services Commission, "A Study on the Rationalization of Real Name Identification Method when Opening an Account", https://www.fsc.go.kr/no010101/71573, Accessed, Jan. 2022
〔11〕 Hae-jin An, "Non-facing authentication Security threat analysis and security measures Establishment of checklist basis for minimizing non-facing authentication security threats," Master's thesis, Graduate School of Information and Telecommunications, Konkuk University, Feb. 2018
〔12〕 Financial Services Commission, "Reorganization of 'non-face-to-face real-name verification guidelines' to revitalize corporate online financial transactions", https://www.fsc.go.kr/no010101/74052, Accessed, Apr. 2022
〔13〕 BizHanKook, "Non-face-to-face certified financial damage, why are financial companies not responsible?", http://www.bizhankook.com/bk/article/24086, Accessed, Aug. 2022
〔14〕 Hani, "Non-face-to-face loans are vulnerable to consumer protection…There's a growing voice for stricter regulations", https://www.hani.co.kr/arti/economy/finance/1027635.html, Accessed, Mar. 2022

〈저자소개〉

김 은 비 (Eun Bi Kim) 정회원
2013년 2월: 인천대학교 컴퓨터공학과 졸업
2023년 2월: 고려대학교 디지털포렌식학과 석사
〈관심분야〉 정보보호, 컴퓨터공학, 디지털포렌식

정 익 래 (Ik Rae Jeong) 종신회원
1998년 2월: 고려대학교 전산학과 졸업
2000년 2월: 고려대학교 전산학과 석사
2004년 8월: 고려대학교 정보보호학과 박사
2006년 3월~2008년 2월: 한국전자통신연구원 암호기술연구팀 선임연구원
2008년 3월~현재: 고려대학교 정보보호대학원 교수
〈관심분야〉 암호 이론, 프라이버시 향상 기술 (PET), 데이터베이스 보안, 생체인