Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.32, NO.5, Oct. 2022 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2022.32.5.791

메신저피싱 경험사례 분석을 통한 대응방안 연구

남 소 원,[1†] 이 학 선,[2] 이 상 진[3‡]
[1,2,3]고려대학교 (대학원생, 학생, 교수)

A Study on Countermeasures through Messenger Phishing Experience Analysis

Sowon Nam,[1†] Haksun Lee,[2] Sangjin Lee[3‡]
[1,2,3]Korea University (Graduate Student, Undergraduate Student, Professor)

요 약

최근 몇 년간 보이스피싱 관련 사기 피해는 감소하는 추세이지만, 신종 범죄 수법인 메신저피싱 피해는 매년 늘고 있다. 본 연구에서는 메신저피싱 사례가 담긴 SNS의 게시물을 분석하여 신유형인 지인 사칭유형과 허위 결제 사칭 유형의 범죄 동향을 파악하였다. 분석을 통해 메시지를 구성한 주요 단어와 패턴, 사용된 전화번호의 유사성과 관계성 등을 범죄 속성으로 도출하였고 이를 바탕으로 범죄조직을 그룹화하였다. 분석 결과를 토대로 수사기관에서 수집한 범죄정보를 민간 사업자에 전파하여 메신저피싱 피해를 예방하는 공조 체계와 범죄조직 그룹화를 통해 예측한 메신저피싱에 대응하는 방안을 제시한다.

ABSTRACT

In recent years, the number of scams related to voice phishing has been on the decline, but the number of messenger phishing attacks, a new type of crime, is increasing. In this study, by analyzing SNS posts containing messenger phishing cases, criminal trends of the main methods, imposture of trusted relative and fake payment were identified. Through the analysis, main words and patterns composing the message and the similarity and continuity of the phone numbers used were derived as criminal attributes, and criminal organizations were grouped. As the results of the analysis, we propose a cooperative system to prevent damage from messenger phishing by disseminating the criminal information collected by investigative agencies to private operators, and a plan to respond to messenger phishing predicted through grouping of criminal organizations.

Keywords: Messenger Phishing, Voice Phishing, Trusted Relative Scam, Imposture Message

I. 서 론

퓨 리서치 센터의 조사에 의하면, 2019년 우리나라 성인의 스마트폰 보유율은 95%로 27개 선진 경제국가 중 일위이다[1]. 정보통신의 발달과 함께 범죄조직도 지능화되고 있다. 유출된 개인정보로 포털과 메신저 계정을 해킹하여 주소록에서 범죄에 필요한 정보를 얻는 식으로 수법이 진화하고 있다[2].

메신저피싱(messenger phishing)은 문자와 메신저로 지인 등을 사칭하여 메시지 수신자를 속인 뒤 금전을 갈취하는 범죄이다.

금융감독원에 따르면 '21년 보이스피싱 피해 금액은 총 1,682억 원으로 전년(2,353억 원) 대비 671억 원(△28.5%) 감소한 반면 메신저피싱 피해액은 전년 대비 165.7%(+618억 원) 급증한 991억 원으로 사기 수법이 보이스피싱에서 메신저피싱으로 전환된 것으로 보았다[3].

본 논문에서는 메신저피싱 경험사례가 담긴 인스타그램(instagram) 게시글을 분석하여 신규 사칭

Received(08. 04. 2022), Accepted(09. 23. 2022)
† 주저자, southwish@korea.ac.kr
‡ 교신저자, sangjin@korea.ac.kr(Corresponding author)

유형의 범죄 속성을 파악하고 이에 따른 대응 방안을 제시한다. 3절에서는 메신저피싱 사례를 수집하고 지인 사칭유형과 허위 결제 사칭유형에 대해 살펴본다. 4절에서는 사칭유형의 속성을 분석하고 범죄조직을 그룹화한다. 5절에서는 수사기관과 민간 사업자의 메신저피싱 차단 공조 체계와 범죄조직 그룹화를 통해 메신저피싱을 예측하여 대응하는 방안을 제시한다.

본 논문에서는 문자 서비스와 메신저 서비스를 구분하기 위해 메신저피싱의 메시지를 “문자”와 “모바일 메시지”로 구분하며 문자와 모바일 메시지 모두를 언급할 때는 “메시지”라고 칭한다.

II. 관련 연구

김경진 등[4]은 통신사기피해환급법의 전기통신금융사기가 대면편취형 범죄를 포섭하지 못하는 문제점을 지적하며 법 개정의 필요성을 제시하였다.

유재두[5]는 네이버와 카카오톡에 피싱 사기 계정 삭제 방안을 제시하였다.

배지효 등[6]은 메신저피싱 대화에서 단어 연관도를 분석하여 범죄가 의심되는 대화를 탐지하는 방안을 제시하였다.

조성규 등[7]은 사용자 PC의 IP 주소와 메신저 서버에서 접속한 IP 주소를 비교하여 비정상 접속에 대해 경고 알림을 주는 방안을 제시하였다.

장영호 등[8]은 스마트폰 뱅킹 구동 중 원격제어 앱을 차단하는 메신저피싱 대응방안을 제시하였다.

임희서[9]는 피싱아이즈 앱에서 수집한 데이터를 분석하여 보이스피싱, 스미싱, 악성앱 사기 피해 경향 및 유형을 분석하였다.

정부 관련 기관은 메신저피싱에 대한 대국민 주의를 위해 보도자료[3][10]를 배포하고 있으며 민간 사업자들은 범죄 예방을 위해 보안기술을 고도화하고 있다[11].

위와 같은 선행 연구와 여러 노력에도 메신저피싱 범죄는 증가하고 있으며 사칭유형에 대한 심층 분석과 대응방안을 다룬 연구가 부족한 실정이다.

III. 메신저피싱 경험사례

이 절에서는 인스타그램에 게시된 메신저피싱 경험사례의 수집과 신유형인 지인 사칭유형과 허위 결제 사칭유형에 대해 살펴본다[2].

3.1 메신저피싱 경험사례 수집

본 논문에서는 인스타그램에서 ”보이스피싱[1]“ 키워드로 검색되는 1만 8천여 개 사진을 수집하였다. 수집된 사진은 ’13년 9월부터 ‘22년 4월 1일까지 약 9년 동안 게시된 것이다. 인물 및 사물 사진 등과 같이 메신저피싱과 관련 없는 사진은 수집 대상에서 제외하였다.

경찰대학교에서 제공하는 피싱아이즈 보고서에 있는 사칭유형 별 주요 단어를 지인 사칭유형(”폰“, ”파손“, ”고장“, ”엄마“, ”수리“ 등)과 허위 결제 사칭유형(”결제“, ”국제“, ”구매“, ”승인“, ”문의“, ”고객센터“ 등)의 분류 기준으로 선정하였다[9]. 수집한 사진에서 OCR로 추출한 문자열을 대상으로 분류 단어 매칭과 육안 검증을 통해 메신저피싱 사칭유형을 분류하였다. 그 결과 인스타그램에서 지인 사칭유형의 경험사례 2,821건과 허위 결제 사칭유형의 경험사례 470건을 수집하였다.

메신저피싱 경험사례는 게시자가 수신한 사칭 메시지를 Fig. 1.과 같이 캡처한 것으로 다음과 같은 범죄 관련 정보가 포함되어 있다.

① 문자 발신 번호(sender number)
② 메시지 수신 날짜와 요일
③ 메시지 수신 시간
④ 메시지 내용
⑤ 문자 내 번호(implied number)

사진이 잘렸거나 정보가 마스킹된 경우에는 위의 5가지 범죄 관련 정보 중 일부만 추출되었다.

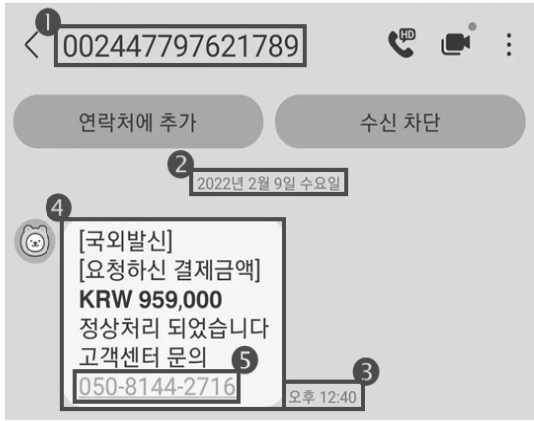

Fig. 1. Example of Collected Pictures

1) 대부분 게시자는 메신저피싱을 보이스피싱으로 인지함

3.2 지인 사칭유형

지인 사칭유형은 가족과 지인을 사칭하여 휴대폰 파손 등의 불가피한 상황을 알리며 신분증, 카드번호 등의 개인정보를 탈취하여 자금을 편취하는 식으로 발생한다[12].

금융감독원에 따르면 해당 유형은 자녀를 사칭하여 부모의 이성적 판단이 와해되는 취약점을 공략하여 주로 50대 이상에서 피해가 발생한다[3][13].

지인 사칭유형의 발생 추이는 Fig. 2.와 같다. 해당 유형은 '18년 9월에 처음 확인되어 '21년 1월에 발생량이 최고점을 찍고 감소하고 있다.

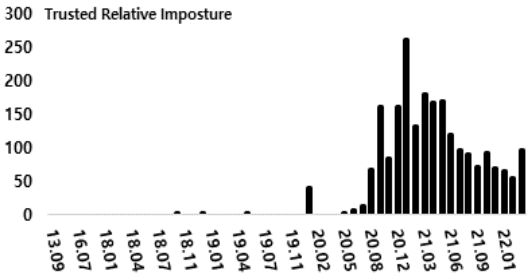

Fig. 2. Occurrence Trend of Trusted Relative Imposture

3.3 허위 결제 사칭유형

허위 결제 사칭유형은 특정 상품 및 금액에 대한 결제를 가장하여 문자 내 포함된 고객센터 번호로 전화를 유도한 뒤 명의도용 수사 협조를 사유로 금전을 갈취하는 식으로 발생한다.

허위 결제 사칭유형의 발생 추이는 Fig. 3.과 같다. 해당 유형은 '13년 9월에 처음 확인되었고 점점 증가하는 추세이다.

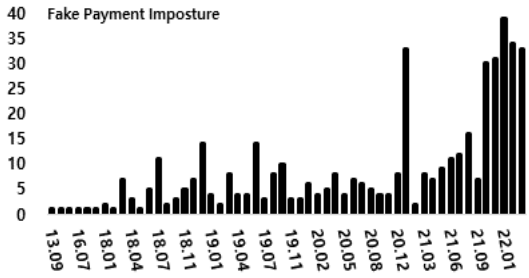

Fig. 3. Occurrence Trend of Fake Payment Imposture

IV. 메신저피싱 속성 분석

이 절에서는 지인 사칭유형과 허위 결제 사칭유형의 속성을 분석하고 이를 바탕으로 범죄조직을 그룹화한다.

4.1 메신저피싱 수신 시점

이 절에서는 메신저피싱 메시지를 수신한 시점에 대해 살펴본다.

4.1.1 메시지 수신 요일

전체 메신저피싱 메시지는 평일 평균 292건, 주말은 평일의 42% 수준으로 수신량이 적었다. Table 1.과 같이 지인 사칭유형은 허위 결제 사칭유형과 달리 주말도 메시지 수신량이 많았다.

Table 1. Message Received Day of the Week

Week	Trusted Relative Imposture	Fake Payment Imposture
Mon	250	51
Tue	259	81
Wed	243	44
Thu	215	43
Fri	235	39
Sat	179	2
Sun	66	0

4.1.2 메시지 수신 시간

메신저피싱 메시지는 Fig. 4.와 같이 9시부터 12시까지 가장 많이 수신되었으며 오후로 갈수록 수신

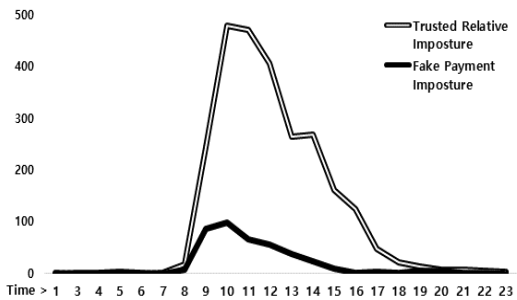

Fig. 4. Message Received Time

량이 감소하였다. 두 유형 모두 9시부터 18시까지 메시지 수신이 확인되었으며 10시에 가장 많은 메시지가 수신되었다.

4.2 메시지 특성 분석

이 절에서는 메신저피싱에서 사용된 메시지에 있는 주요 단어와 이들 단어의 패턴을 살펴본다.

4.2.1 메시지 구성 단어

메신저피싱에서는 특정 단어들이 반복적으로 사용되었다.

지인 사칭유형에서는 Table 2.와 같이 자녀를 사칭하며 “엄마”, “아빠”를 호칭하거나 “폰”, “액정”, “고장”, “센터”, “수리”, “부탁”과 같은 단어를 사용하면서 휴대폰 고장을 사유로 도움을 요청하였다. 또한, 연락을 요청하며 “번호”, “추가”, “답장”, “문자”, “카톡”, “톡줘”와 같은 단어가 사용되었다.

허위 결제 사칭유형에서는 Table 3.과 같이 결제 사실을 가장하기 위해 “승인”, “결제”, “완료”와 같은 단어가 사용되었으며 해외 결제를 가장할 때는 “해외”, “국제”, “국외”와 같은 단어가 사용되었다.

허위 결제 사칭유형의 메시지에서 반복적으로 사용되는 결제금액의 빈도를 확인하였다.

발생 횟수가 2회 이상인 결제금액은 57개이며 가장 많이 사용된 금액은 “959,000”원으로 Table 4.와 같다.

결제금액에 대해 시간에 따른 발생 추이는 Fig. 5.와 같다. ‘18년 6월 이전 20만 원, 이후 50만 원이 주로 사용되었다. ‘21년 10월 이후 100만 원에 근접한 금액이 사용되었으며 시간의 흐름에 따라 금액이 상승하였다.

Table 2. Frequently Used Keywords in Trusted Relative Imposture

No.	Keyword	Occurrences	No.	Keyword	Occurrences
1	문자	4,308	11	액정	906
2	폰	3,478	12	연락처	785
3	엄마	2,996	13	메시지	655
4	수리	1,429	14	통화	648
5	고장	1,376	15	답장	621
6	부탁	1,211	16	나라	484
7	지금	1,183	17	센터	384
8	번호	1,089	18	카톡	318
9	추가	1,084	19	바빠	239
10	아빠	963	20	톡줘	173

Table 3. Frequently Used Keywords in Payment Imposture

No.	Keyword	Occurrences	No.	Keyword	Occurrences
1	승인	526	11	번호	162
2	발신	432	12	Web	146
3	결제	385	13	요청	112
4	완료	331	14	아닐시	111
5	문의	278	15	KRW	98
6	해외	219	16	소비자	92
7	님	200	17	배송	91
8	국제	189	18	국외	89
9	문자	172	19	인증	80
10	본인	167	20	주문	76

Table 4.에서 가장 많이 사용된 “959,000”원이 포함된 메시지를 Table 5.와 같이 비교하였다. 메시지는 서로 일치하지 않았으며 “요청하신결제금액”, “서비스고객센터” 문구가 반복하여 사용되었다.

이로 인해 범죄자(사람)가 유사한 내용을 반복하여 작성하면서 같은 숫자를 무의식적으로 사용한 것

Table 4. Frequently Used Amounts in Fake Payment Imposture

No.	Amount	Occurrences
1	959,000	29
2	969,000	20
3	464,000	16
4	960,520	12
5	248,700	10
6	1,640,000	8
8	1,680,000	6
9	876,000	6
10	475,000	5

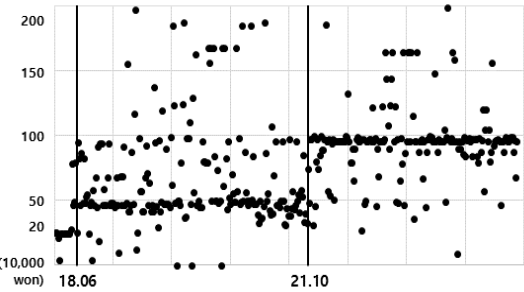

Fig. 5. Occurrence Trend of Amounts in Fake Payment Imposture

Table 5. 9 Messages of the 29 Imposture Messages Including 959,000 won

1	2	3
〔결제〕 확인코드:9**8 〔KRW959,000〕 본인구매상품아닐시 꼭문의주세요 고객센터 070-7893-2**1	〔결제〕 확인코드:9**8 〔KRW959,000〕 본인구매상품아닐시 꼭문의주세요 고객센터 070-7893-1**3	〔국제발신〕 〔결제〕 확인코드:9**8 〔KRW959,000〕 본인구매상품아닐시문의 배송관련고객센터 070-7893-3**9
4	5	6
〔결제내역〕 승인코드:1**3 KRW959,000원 〔승인〕 본인아닐시신고요망 배송관련고객센터 070-7847-5**3	〔국외발신〕 요청하신결제금액 KRW959,000 결제되었습니다 서비스고객센터 050-5061-5**4	〔국외발신〕 요청하신결제금액 KRW959,000 〔승인〕되었습니다 서비스고객센터 070-7893-2**9
7	8	9
〔국제발신〕 요청하신결제금액 KRW959,000 〔승인〕되었습니다 서비스고객센터 032-655-1**7	〔국제발신〕 요청하신결제금액 KRW959,000 〔승인〕되었습니다 서비스고객센터 070-7893-3**7	〔국외발신〕 요청하신결제금액 KRW959,000 결제완료되었습니다 서비스고객센터 070-7893-3**3

으로 보인다〔14〕. 또한, 고객센터 번호인 “070-7893-XXXX” 형태의 인터넷 전화번호가 6차례 발견되어 번호의 유사성을 보였다.

4.2.2 메시지 내용 구성 패턴

이 절에서는 4.2.1절의 메시지 주요 단어 조합에 따른 메시지 패턴을 살펴보았다.

지인 사칭유형에서 총 1,294개의 패턴이 확인되었고 2회 이상 발생한 패턴은 348개이다. 가장 많이 사용된 패턴의 경우 Table 6.과 같이 32차례 발생

Table 6. Frequently Used Keyword Combination Patterns in Trusted Relative Imposture

No.	Pattern of Keyword Combination	Occurrences
1	엄마, 폰, 고장, 번호, 문자, 부탁	32
2	엄마, 폰, 액정, 문자, 부탁	24
3	엄마, 폰, 고장, 수리, 번호, 문자, 부탁	21
4	엄마, 폰, 고장, 수리, 지금, 피시, 문자, 나라, 부탁	15
5	엄마, 폰, 고장, 문자,	14

Table 7. Frequently Used Keyword Combination Patterns by Fake Payment Imposture

No.	Pattern of Keyword Combination	Occurrences
1	Web, 발신, 결제, 248,700, 완료, 익월, 청구	7
2	국외, 발신, 고객, 님, 신청하신, 완료, 문의	5
3	국제, 발신, 님, 번호, 해외, 인증, 직구	4
4	Web, 발신, 결제, 완료, 익월, 청구, 문의	4
5	Web, 발신, 결제, 완료, 익월, 청구	4

하였다.

허위 결제 사칭유형에서 총 375개의 패턴이 확인되었고 2회 이상 발생한 패턴은 49개이다. 가장 많이 사용된 패턴의 경우 Table 7.과 같이 7차례 발생하였다. 이를 통해 메신저피싱 메시지를 패턴화할 수 있을 것이다.

4.3 메신저피싱 사용 메신저

이 절에서는 메신저피싱에서 메신저가 악용된 사례를 살펴본다. 지인 사칭유형의 문자에서 카카오톡 친구추가를 요청하거나 전화번호가 포함된 경우가 335건, 카카오톡 아이디가 포함된 경우가 12건으로 확인되었다. 모바일 메시지로 지인 사칭유형이 시작된 경우는 605건으로 확인되었다. 종합적으로 전체 지인 사칭유형 중 33%(952건)가 카카오톡을 통해 발생하였다.

금융감독원에 따르면 최근 카카오톡을 통한 메신저피싱 피해 건수가 ‘18년 81.7%, ’19년 90.2%, ‘20.1월~9월 중 85.6%로 증가하고 있다〔12〕. 허위결제 사칭유형에서는 카카오톡을 통한 발생 사례가 확인되지 않았다.

4.4 메신저피싱 사용 전화번호

이 절에서는 메신저피싱에서 사용된 전화번호에 대해 살펴보았다.

4.4.1 전화번호 종류

이 절에서는 메신저피싱에 사용된 전화번호의 종류를 살펴보았다. 메신저피싱에 사용된 전화번호는

문자 발신 번호(sender number)와 문자 내용에 포함된 문자 내 번호(implied number)로 구분하였다.

전화번호는 앞 2~4자리를 기준으로 식별번호와 비교하여 분류하였다. 국제 전화번호는 “001”, “002” 등 식별번호와 “+44”, “+46” 등 국가번호로 구분하였다. 유선 전화번호는 “02”, “031” 등 지역번호, 인터넷 전화번호는 “070”, 안심 전화번호[2]는 “050”, 대표 전화[3] 번호는 통신사에서 현재 확인되는 앞 4자리(1522, 1644 등) 번호로 구분하였다.

Table 8.과 같이 지인 사칭유형의 경우 메시지 발송에 이동 전화번호가 99%(1,218개) 사용되었다. 허위 결제 사칭의 경우 국제 전화번호 67%(233개), 유선 전화번호 20%(71개), 인터넷 전화번호 11%(38개) 순으로 사용되었다.

Table 9.와 같이 문자 내 번호에는 지인 사칭유형의 경우 이동 전화번호만 사용하였다. 허위 결제 사칭유형의 경우 유선 전화번호, 인터넷 전화번호, 안심 전화번호, 대표 전화번호를 사용하였다. 문자 내 번호에서는 문자 발신 번호와 다르게 “050”으로 시작하는 안심 전화번호가 사용되었다.

종합적으로 메신저피싱에서는 이동 전화번호, 국제 전화번호, 유선 전화번호가 주로 사용되었다.

Table 8. Distribution of Sender Numbers in Different Phone Number Types

Type	Trusted Relative Imposture	Fake Payment Imposture
International Phone Number	12	233
Mobile Phone Number	1,218	5
Landline Phone Number	2	71
Internet Phone Number	1	38
Representative Phone Number	1	4

2) 가상의 개인 번호로 통화 연결하는 서비스 개인의 전화번호가 노출되지 않도록 하는 서비스의 안심 전화번호

3) 대표전화번호는 여러 개 일반번호를 대표번호로 통합하여 자동 연결해주는 서비스 번호. 8자리로 기억하기 쉬워 관공서, 대기업 등의 콜센터 전화번호로 사용됨. https://대표번호.net/전국대표번호-조회/

Table 9. Distribution of Implied Numbers in Different Phone Number Types

Type	Trusted Relative Imposture	Fake Payment Imposture
International Phone Number	0	3
Mobile Phone Number	113	0
Landline Phone Number	0	218
Internet Phone Number	0	122
Representative Phone Number	0	17
Private Phone Number	0	63

4.4.2 이동 전화번호 개통 통신사

’04년 이전 이동 전화번호는 〔식별번호〕-〔국번〕-〔사번〕으로 구성되어 식별번호로 개통 통신사를 구분하였다. ’04년 010통합번호제도[4]가 시행되며 식별번호를 “010”으로 통합하며 국번을 통신사 별로 배정하여 구분할 수 있도록 하였다. 이때 이동전화사업자에게 배정된 고유한 국번을 원배정국번이라고 한다.

통신사를 이동하여도 원배정국번의 통신사는 변경되지 않으며 번호가 해지되면 개통한 통신사로 귀속된다. 메신저피싱에서 사용된 이동 전화번호의 원배정국번 조회[5]를 통해 개통 통신사를 확인하였다.

과학기술정보통신부에 따르면 메신저피싱 이동 전화번호가 수집된 기간인 ‘13년부터 ’21년까지 8년 평균 이동통신 3사의 점유율은 SKT 44.04%, KT 26.27%, LGU+ 19.85%이다〔15〕.

Table 10.과 같이 점유율 대비 KT 개통으로 확인된 이동 전화번호는 63%(773개)로 가장 많이 발생하였으며 점유율이 가장 높은 SKT 개통 전화번호는 1%(22개)로 가장 적었다.

수사기관은 ‘21년 4월부터 2개월간 보이스피싱 등에 사용된 2만7,039대의 대포폰[6]을 적발하였다. 적

4) 010통합번호통합제도 : 국가자원인 번호의 효율적인 이용과 번호의 브랜드화를 방지하기 위한 목적으로 통신 사업자 식별번호(011, 016, 019 등)을 ‘010’으로 통합하는 제도로 통신사 별 가운데 4자리에 차이를 두어 구분될 수 있도록 하였다.

5) http://sdisk.iptime.org/phone.php

6) 개통 명의자와 실제 사용자가 다른 휴대폰

Table 10. Originally Allocated Mobile Phone Numbers Used for Messenger Phishing per Carrier

Carrier	SKT	KT	LGT
Number	22	773	396

발된 대포폰의 개통처는 알뜰폰 통신사[7]가 92%(2만5,142개)를 차지하였다[16].

알뜰폰 통신사는 사업장용 국번을 통신사 망을 대여하는 통신사로부터 받는다[17]. 따라서, KT 개통 전화번호 중 KT 통신망을 재판매하는 알뜰폰 통신사 개통 전화번호가 포함된 것으로 보인다.

4.4.3 국제 전화번호 사용 통신사

국제 전화번호는 [식별번호]-[국가번호]-(지역/서비스 번호)-[실제 전화번호]로 구성된다. 메신저피싱에 사용된 국제 전화번호의 식별번호로 통신사를 살펴보았다.

식별번호는 SK텔링크(006, 00700), KT(001), LGU+(002), 한국케이블(00777)로 169개의 국제 전화번호를 구분할 수 있으며 식별번호 없이 "+국가번호"로 시작되는 번호가 29개였다.

정보통신정책연구원[18]에 따르면 '13년부터 '19년까지 국제전화 주요 통신사업자 평균 점유율은 SK텔링크 31.9%, KT 25.3%, LGU+ 19.1%로 확인되었다. 메신저피싱 범죄에 악용된 국제전화사업자는 Table 11.과 같이 국제전화사업자의 점유율 대비 SK텔링크 69%(118개), LGU+ 26%(44개) 순으로 사용이 많았다.

Table 11. International Phone Number Operator Used for Messenger Phishing

Carrier	SK Telink	KT	LG U+	Korea Cable
Number	118	6	44	1

4.4.4 전화번호 사용기간

메신저피싱에 사용된 전화번호의 사용기간을 살펴보았다. Table 12.와 같이 사용기간이 1일로 확인된 전화번호는 58%(126개)로 가장 많이 발생하였다. 한 달 이내로 사용기간이 확인된 전화번호는 89%(192개)를 차지하였다. 6개월 이상 사용된 전화번호는 3건으로 193일, 199일, 335일이 확인되었다.

Table 12. Usage Period of Messenger Phishing Numbers

Usage Period	Occurrences
One Day	126
One Week	36
One Month	30
3 Months	20
6 Months	1
One Year	3

4.4.5 전화번호 유사성

이 절에서는 메신저피싱에 사용된 전화번호 간의 유사성을 살펴본다.

메신저피싱에 사용된 전화번호는 Table 13.과 같이 전화번호의 유사성을 보였다. "070-7893-XXXX" 형태의 인터넷 전화번호는 뒤 4자리가 "1**7"부터 "3**6"까지 오름차순으로 35개가 확인되었다. Table 13.에 나타낸 전화번호 외에도 "070-7847-XXXX" 형태 등 다수의 전화번호에서 유사성이 확인되었다.

결제승인 문자사기 제보모음 블로그[19][20]에서도 "070-7893-XXXX" 형태 62개, "02-830-XXXX" 형태 275개, "02-900-XXXX" 형태 46개 등의 번호가 확인되었으며 Table 13.의 전화번호와 일치하였다.

Table 13. Similarity of Messenger Phishing Numbers

International Phone Number	Landline Phone Number	Internet Phone Number
0069198100**24	029002**5	07078931**7
0069198100**91	029002**8	07078931**6
0069198100**81	029004**8	07078931**8
0069198100**22	029005**2	07078931**1
0069198100**02	029006**1	07078931**4
0069198100**37	029006**3	07078931**6
	029007**8	07078931**9

7) 기간통신사업자의 전기통신회선설비를 이용하여 도매제공의무서비스를 단순재판매하는 사업자

0064676943**00	029008**6	07078931**9
0064676943**02	029008**4	07078931**5
0064676943**07		07078931**7
0064676943**12	028300**7	07078931**5
0064676943**15	028301**6	07078931**1
0064676943**37	028301**4	07078931**3
0064676943**39	028301**4	07078931**0
0064676943**47	028301**0	07078931**7
0064676943**48	028301**5	07078931**3
0064676943**49	028302**7	07078931**1
0064676943**54	028303**9	07078931**4
0064676943**63	028303**3	07078931**9
0064676943**64	028303**6	07078932**7
0064676943**70	028304**9	07078932**0
0064676943**72	028304**0	07078932**0
0064676943**73	028304**7	07078932**4
0064676943**76	028305**0	07078932**6
0064676943**80	028305**2	07078932**1
0064676943**84	028306**4	07078932**2
	028307**2	07078932**7
	028307**5	07078932**9
	028308**3	07078932**4
		07078932**2
		07078932**8
		07078933**9
		07078933**7
		07078933**3
		07078933**6

4.4.6 문자 발신 번호와 문자 내 번호 간 관계성

메신저피싱 경험사례 중 문자 발신 번호와 문자 내 번호가 모두 추출된 경우는 지인 사칭유형에서 12건, 허위 결제 사칭유형에서 350건이 확인되었다. 해당 사례에서 Fig. 6.과 같이 문자 발신 번호와 문자 내 번호의 18가지 관계성이 나타났다.

Fig. 6.에서 화살표의 시작은 문자 발신 번호와 끝은 문자 내 번호를 의미한다.

사칭유형 간에 번호를 교차하여 사용하는 사례는 확인되지 않았다.

4.5 메신저피싱 범죄조직 그룹화

이 절에서는 메신저피싱의 범죄 속성을 기반으로 그룹화의 가능성을 살펴보았다. 그룹화는 메신저피싱의 속성 중 문자의 패턴, 전화번호의 유사성, 문자 발신 번호와 문자 내 번호의 관계성을 바탕으로 시도하였다.

4.4.6절에서 파악된 Fig. 6.의 관계성 7번의 메시지 내용은 Table 14.와 같으며 문자 패턴 유형 중 A3에 속하는 문자 3개를 추가로 확인하였다. 메시지의 문자 내 번호는 "070-7893-XXXX"의 형태를 보이며 4.4.5절에서 확인한 유사성을 확인할 수 있었다.

이를 통해 범죄조직이 다량의 전화번호를 확보하며 유사성이 나타난 것으로 보인다. 그룹1은 메신저피싱에서 사용된 전화번호의 유사성, 문자의 유사 패

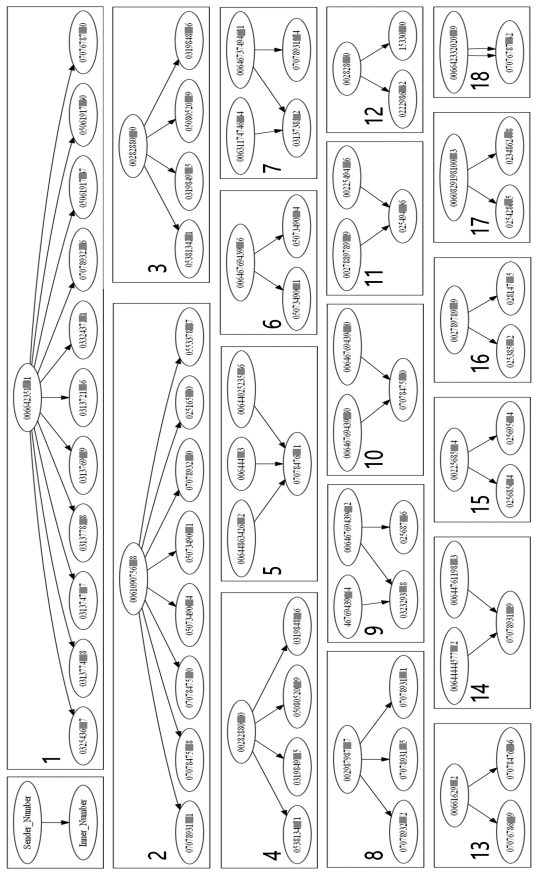

Fig. 6. Relationship Between Sender Numbers and Implied Numbers

Table 14. Grouping based on Messenger Phishing Characteristics

Group	Relationship	Sender Number	Implied Number	Message Pattern Type	SMS Message Content
1	7	00631174746**4	0313738**2	A1	〔국제발신〕인증번호 32** KRW 572,100원승인 본인아닐경우 소비자 고객센터 문의:031-373-8**2
		00646737494**1	0313738**2	A2	〔국제발신〕해외승인 41** V11 다이슨 청소기 KRW 582,000주문완료본인아닐시신고문의:031-373-8**2
		00646737494**1	07078931**4	A3	〔국외발신〕6*5***해외승인 ₩940,520 일시불 10/30 배송예정 LK포스트몰 배송문의:070-7893-1**4
	-	00664566**2	07078931**7	A3	〔국제발신〕3*2*해외승인 ₩960,520 일시불 11/04 09:20배송예정LK포스트몰배송문의 070-7893-1**7
	-	-	07078931**9	A3	〔국제발신〕5*3***해외승인 ₩960,520 일시불11/02 09:20배송예정LK포스트몰배송문의 070-7893-1**9
	-	-	07078931**8	A3	〔국제발신〕5*3*해외승인 960,520 일시불 11/02 09:20배송예정LK포스트몰배송문의 070-7893-1**8

턴, 문자 발신 번호와 문자 내 번호의 관계성이 모두 확인되었다. 그룹1은 동일한 범죄조직에서 발송한 것으로 추정된다. 가시성을 부여하기 위해 Fig. 7.과 같이 도식화하였다.

Fig. 7.에서 유사성을 보이는 번호는 대표 형태를 지정하여 ①과 같이 표기하였으며 같은 번호 동일한 색과 점선을 이용하여 ②와 같이 표기하였다. 문자 발신 번호는 메시지 패턴이 담긴 칸의 상단에 ③과 같이 표기하였다. 칸 내부에는 Table 14.의 문자 패턴 유형 A3를 대표 패턴으로 ④와 같이 배치하고 A3 패턴이 발생한 횟수를 ⑤와 같이 표기하였다. 칸 하단에는 문자 내 번호를 ⑥과 같이 표기하였다.

메신저피싱에 사용된 전화번호 중 유사성을 보인 번호에 대해 문자 발신 번호와 문자 내 번호의 관계성, 문자 패턴을 바탕으로 그룹화를 시도하였다.

Fig. 8.과 같이 그룹화한 범죄조직의 명칭을

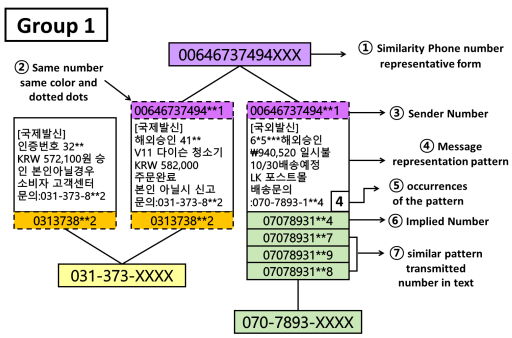

Fig. 7. Group 1 Diagram

'Octopus"라고 명명하였다. 전체 허위 결제 사칭유형의 사례 470건 중 28%(132건)가 Octopus에 속하였다. Table 14.의 그룹1도 Octopus에 포함되며 가시성을 위해 도식은 전체 그룹의 일부만 표현하였다.

Octopus는 '19년 8월부터 현재까지 약 32개월 동안 허위 결제 사칭유형으로 메신저피싱 범죄를 일삼았다. Octopus가 전송한 문자 내용은 전문이 일치하는 경우가 드물었고 결제금액, 번호 등이 달랐다.

Octopus는 활동 초기 유선 전화번호를 사용하여 냉장고, 에어컨 등과 같은 특정 상품에 대한 결제 사칭 문자를 발송하였으며 문자 내 번호의 경우 문자 발신 번호와 일치하는 유선 전화번호를 사용하였다. '19년도 말부터는 국제 전화번호를 사용하며 해외 결제 사칭 문자를 전송하였으며 문자 내 번호에는 유선 전화번호를 주로 사용하다가 '21년 6월부터는 인터넷 전화번호를 사용하였다. 이후 '21년 9월부터는 문자 내 번호에 유선 전화번호와 안심 전화번호를 사용하기 시작하였다.

Octopus는 Table 15.와 같이 '21년까지 "KG모빌리언스", "네이버페이" 등을 사칭하였다. 사칭 대상인 KG모빌리언스는 KG이니시스와 '19년 1월에 PG사 사칭 문자주의를 고객에게 당부한 바 있으며 금융감독원은 '19년 9월, '20년 9월, '22년 1월에 허위 결제 문자 주의보를 발령하였다〔21〕~〔24〕. Octopus는 '22년부터 Table 15.와 같이 문자 내용에 사칭 대상을 포함하지 않고 결제금액과 고객센

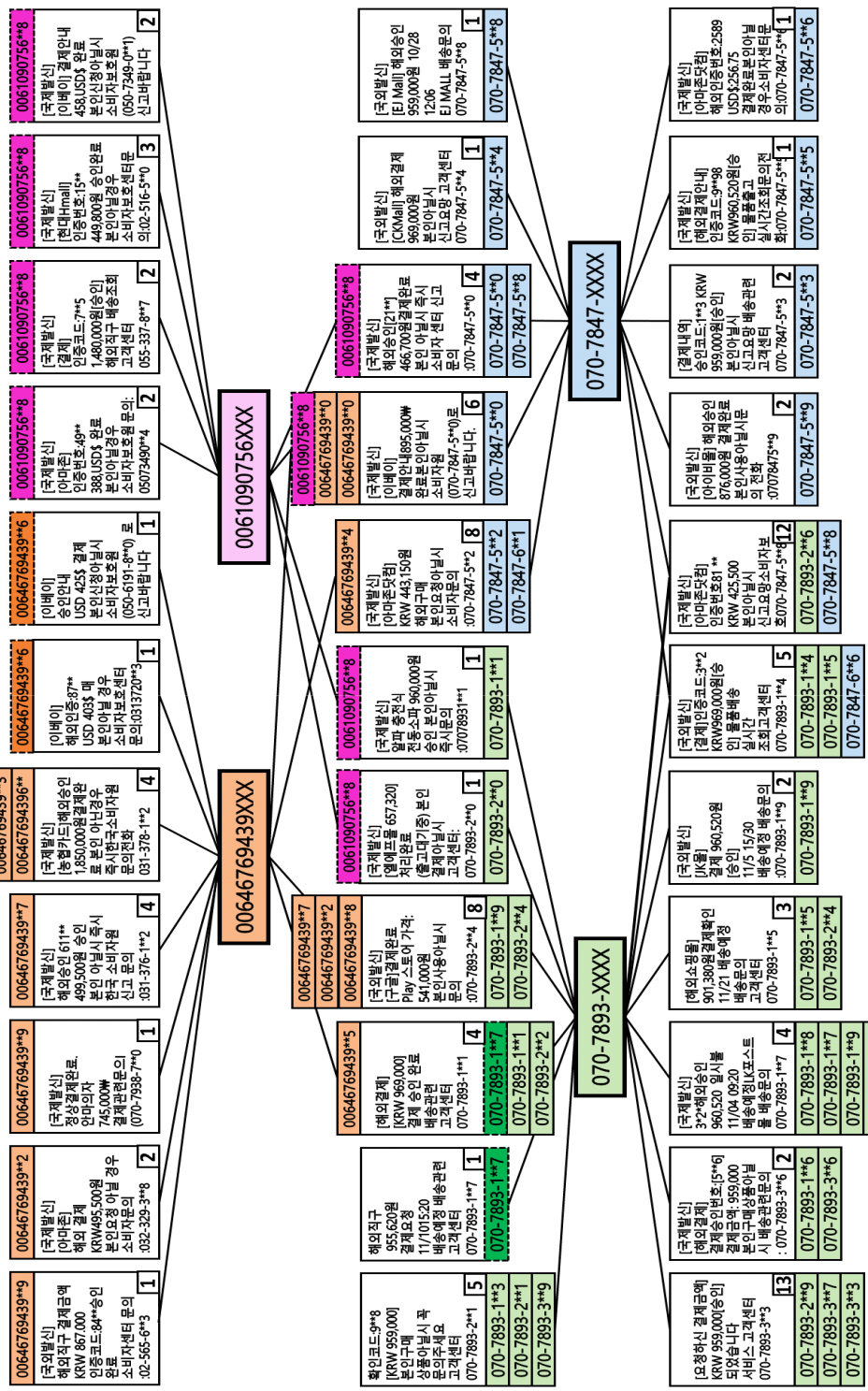

Fig. 8. Octopus Criminal Organization Grouping Result

Table 15. Example of Fake Payment Imposture Messages from the Octopus Group

Message Received Date	Message Content
19.09.20	〔Web 발신〕 KG모빌리언스 475.000원 승인완료 요청일:2019/09/20 이용해주셔서 감사합니다
20.04.20	〔Web 발신〕 〔네이버pay〕 삼성 지펠 냉장고 제품번호:755314 1,680,000원 승인 문의:02-830-1**5
21.10.08	〔국외발신〕 〔구글〕 결제완료 Play 스토어 가격:458,500원 본인사용아닐시 신고문의:070-7893-1**9
22.01.20	〔국제발신〕 〔결제〕 인증코드:7**5 1,480,000원〔승인〕 해외직구배송조회고객센터055-337-8**7
22.02.09	〔국외발신〕 〔요청하신 결제금액〕 KRW 959,000 정상처리 되었습니다 고객센터 문의 050-8144-2**6
22.03.14	〔국제발신〕 해외승인〔411**〕 468,800원 결제완료본인아닐시즉시소비자센터신고문의:02-564-4**6

터 전화번호만 사용하는 식으로 수법이 변화하였다.

V. 메신저피싱 대응방안

이 절에서는 수사기관과 민간 사업자 공조에 따른 메신저피싱 대응방안에 대해 살펴본다.

5.1 수사기관과 민간 사업자 공조 체계

메신저피싱은 민간 사업자의 서비스를 악용하기 때문에 범죄에 신속하고 효과적으로 대응하기 위해서는 수사기관과 민간 사업자의 공조가 필요하다.

인스타그램에 게시된 메신저피싱 경험사례는 범죄시도가 대부분 미수에 그쳤으나 『형법』 제352조 미수범 처벌 조항을 근거로 각 사례를 수집하여 범죄정보를 수집하고 수사하여야 한다.

수사기관은 피해 신고 접수 단계부터 범죄 관련 정보(메시지 내용, 수신 시점, 발신 번호 등)을 정형화하여 수집하고 분석하여 민간 사업자에게 서비스 통제 기준을 실시간으로 전파하는 체계를 마련하여야 한다. 민간 사업자는 전달받은 서비스 통제 기준을 범죄자원과 범죄행위에 적용해야 한다.

5.2 메신저피싱 범죄자원 통제

메신저피싱 범죄자원 통제는 범죄자의 전화번호와 메신저 계정을 무력화시키는 것이다.

수사기관은 다양한 범죄번호의 개통 통신사를 조회할 수 있는 체계를 마련하고 4.4.5절의 유사성을 보이는 다량의 범죄번호가 개통된 통신사를 수사하여야 한다.

과학기술정보통신부는 손쉬운 비대면 선불 알뜰폰 개통〔25〕으로 인한 대포폰 양산을 막기 위해 알뜰폰 사업자가 회선 개통 시 본인인증 절차를 강화하도록 하여야 한다. 또한, 명의도용을 하여 여러 알뜰폰 사업자로부터 다량의 회선을 개통하는 행위를 막기 위해 전체 통신사업자를 총합하여 1인 명의로 가입 가능한 회선 수를 제한하여야 한다.

『통신사기피해환급법』 제13조의3제1항에 따르면 수사기관은 과학기술정보통신부를 통해서만 범죄에 이용된 전화번호를 중지할 수 있다. 이는 절차적으로 범죄자원 통제를 지연시킨다. 신속한 통제를 하려면, 수사기관이 통신사에 직접 이용중지를 요청할 수 있게 법안이 개정되어야 한다.

카카오톡은 무료 전화번호 서비스를 사용하여 수신한 문자의 번호를 입력하면 손쉽게 계정을 생성할 수 있다〔26〕. 계정 생성에 사용된 전화번호가 이용중지 되어도 가입 이후 추가 인증 절차가 없어 계정을 계속 사용할 수 있다. 따라서 카카오톡이 메신저피싱에 악용되는 것을 막기 위해서는 서비스 계정 생성 시 본인인증을 강화하고 가입 후에도 일정 기간이 지나면 전화번호를 재인증하거나 『통신사기피해환급법』 제13조의3제1항에 부가통신역무 제공 중지할 수 있도록 개정하여 카카오톡과 같은 부가통신사업자도 통제 주체에 포괄하여야 한다.

5.3 메신저피싱 범죄행위 통제

메신저피싱 범죄행위 통제는 서비스 이용자가 사칭 범죄에 노출되지 않도록 주의 알림을 주거나 메시지 수신과 전화 연결을 차단하는 것이다.

범죄행위 통제 행위는 4.1절을 토대로 "메신저피싱 집중대응 시간"을 두어 주중 9시부터 18시까지 운영하여야 한다. 통제 기간은 한 달로 4.4.4절의 범죄번호의 사용기간이 한 달 이내인 경우가 89%인 점과 통제 시작 일자에 범죄번호가 해지되어 다른 이용자가 해당 전화번호를 신규로 개통할 수 있는 에이

징 기간[27]을 함께 고려하였다.

이통3사는 『정보통신망 이용촉진 및 정보보호 등에 관한 법률』 제50조의4제4항에 근거해 광고성 문자를 차단해야 하며 스팸 차단을 위한 문자 필터링 시스템을 갖추고 있다. 이통3사는 수사기관으로부터 문사 수신차단 기준을 공유받아 기술적으로 메신저피싱 메시지를 통제할 수 있으나 법적으로 차단 근거가 미비하다.

전화 연결 차단은 이통3사 중 SKT만 이용약관에 근거하여 음성 스팸 필터링 시스템(VSFS)를 운영하고 있으며 보이스피싱 등 전국에서 신고된 범죄번호를 수사기관으로부터 전달받아 고객의 수발신을 차단하고 있다[28].

『통신사기피해환급법』 제2조에 따르면 "전기통신금융사기"는 피해자가 계좌이체로 재산상 피해를 입은 경우로 국한되어 있다.

이통3사가 범죄행위를 통제하기 위해서는 "전기통신금융사기"에 사칭문자 발송과 사칭전화 통화를 포괄하도록 개정하고 금전적인 피해가 발생하지 않았더라도 중복으로 신고된 범죄 의심 전화번호에 대해 메시지 수신차단과 전화연결 차단 조치를 할 수 있도록 『통신사기피해환급법』 제13조의3제1항을 개정하여야 한다.

5.4 범죄조직 그룹화를 통한 메시지 탐지방안

이 절에서는 4.5절의 메신저피싱 그룹화 기술을 활용해 신고되지 않은 메신저피싱 문자를 사전 탐지하여 문자 수신자에게 알림을 주는 방안을 제시한다.

Fig. 9.는 메신저피싱 그룹화의 예시로 "Sender Num"은 문자 발신 번호를 의미하며 "Implied Num"은 문자 내 번호를 의미한다. 번호 간의 유사성을 같은 알파벳과 숫자로 표현하였다. "Message Pattern"은 문자 내용의 대표 패턴을 의미한다. 각 요소의 관계성은 화살표로 나타내었다. "Implied Num C2"의 경우 "Implied Num C1, C3, C4"와 유사성을 보이는 잠재적 범죄번호지만 문자를 발송하지 않았다.

Fig. 10.에서는 새로운 발신 번호로 "Implied Num C2"와 "Implied Num C3"를 사용하여 유사한 패턴의 사칭문자가 발송되었으며 문자 간의 관계성을 파악할 수 있다. 수사기관으로 신고가 접수되기 전 통신망에서 문자가 발송될 때 범죄조직 그룹화를 통해 탐지하고 수신자에게 알림을 주어 피해를 예방할 수 있다.

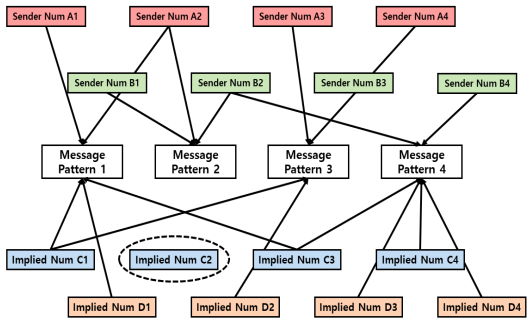

Fig. 9. Messenger Phishing Grouping Example

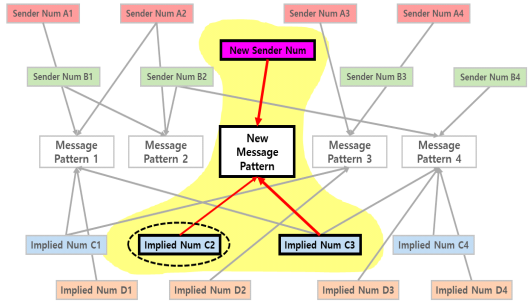

Fig. 10. Diagram of Predictive Blocking Through Messenger Phishing Grouping

VI. 결 론

정보통신의 발달에 따라 전기통신금융사기를 일삼는 범죄조직 또한 지능화되어가고 있다. 보이스피싱 범죄는 줄어들고 있으며 메신저피싱 범죄가 증가하고 있다. 이에 따라 메신저피싱에 대응하기 위한 여러 연구들이 수행되고 있으며 변화하는 범죄 수법에 대한 대응방안 마련이 강조되고 있다.

본 논문에서는 인스타그램에서 수집한 메신저피싱 경험사례를 분석하여 주요 사칭유형인 지인 사칭유형과 허위 결제 사칭유형에 대해 범죄에 사용된 전화번호의 종류, 유사성, 관계성 등과 같은 범죄 속성을 도출하고 범죄조직을 그룹화하였다. 이를 바탕으로 한 수사기관과 민간 사업자의 공조 체계와 범죄조직 그룹화를 통한 메신저피싱 메시지의 탐지방안을 제시하였다.

본 논문에서 도출한 메신저피싱 범죄의 속성들과 대응방안이 범죄 피해 예방에 도움이 될 것으로 기대한다. 본 논문에서는 신유형인 사칭유형인 지인 사칭

유형과 허위 결제 사칭유형을 대상으로 분석하였으나 향후에는 대출빙자형, 기관사칭형 등의 메신저피싱 사칭유형을 종합적인 관점으로 분류하여 범죄 피해를 예방할 수 있는 대응방안을 도출하고자 한다.

References

[1] Pew Research Center, "Smartphone ownership is growing rapidly around the world, but not always equally" https://www.pewresearch.org/global/2019/02/05/smartphone-ownership-is-growing-rapidly-around-the-world-but-not-always-equally/, Accessed, Jun, 2022

[2] Gi-bum Kim, Hun-yung Gwon, Hyun-min Park, Jong-hwa Song, Hyun-ji Moon, Sang-pil Yun, Ji-hun Lim and Sae-rom Hyun, "A Study of Policy and Technical Measures against Emerging Voice Phishing", Ministry of Science and ICT Report, 2020.

[3] Financial Supervisory Service, "Analysis of Voice Phishing Damage in '21" https://www.fss.or.kr/fss/bbs/B0000188/view.do?nttId=55444&menuNo=200218&cl1Cd=&sdate=&edate=&searchCnd=1&searchWrd=%EB%B3%B4%EC%9D%B4%EC%8A%A4%ED%94%BC%EC%8B%B1+%ED%94%BC%ED%95%B4&pageIndex=1, Accessed, Jun, 2022

[4] Kyung-jin Kim and Joon-bae Suh, "A Study on the Trend of Voice Phishing and Policy Recommendations", Security Study, no. 66, pp. 111-128, Mar. 2021.

[5] Jae-doo Yu, "A Study on the Current Status and Cases and Countermeasures of New SNS Phishing", Korean Criminal Psychology Review, vol. 14, no. 4, pp. 103-116, Dec. 2018.

[6] Ji-hyo Bae, Su-yeol Chae, Myeong-jun Song and Kyeong-chan Bang, "Detection method through analysis of messenger phishing conversation", Korea Telecommunications Society, 2019.

[7] Sung-kyu Cho and Jun Moon Seog, "A Study on Countermeasures against Messenger Phishing using ARIT Technique", Journal of the Korea Information Processing Society Conference, vol. 2, no. 5, pp. 223-230, 2013.

[8] Young-ho Jung and Hyung-jun Ha, "Messenger Phishing Crime : Trends and Responses", Journal of Criminal Investigation Studies, vol. 8, no. 1, pp. 31-54, 2022.

[9] Infinigru, "Phishing Eyes Voice Phishing Static Report" https://bigdata-policing.kr/filedownload?idx=132&attached_idx=REPT_15&table=report, Accessed, Sep, 2022

[10] PolicyNews, "Beware of 'messenger phishing' impersonating family and acquaintances", https://www.korea.kr/news/policyNewsView.do?newsId=148901587, Accessed, July, 2022

[11] Seoul, "Samsung Electronics and SKT to block voice phishing" https://www.seoul.co.kr/news/newsView.php?id=20220519021009, Accessed, July, 2022

[12] Financial Supervisory Service, "Beware of voice phishing impersonating family members or friends through messengers such as text messages or Kakao Talk" https://www.fss.or.kr/fss/bbs/B0000188/view.do?nttId=15990&menuNo=200218&cl1Cd=&sdate=&edate=&searchCnd=1&searchWrd=%EC%B9%B4%EC%B9%B4%EC%98%A4%ED%86%A1&pageIndex=1, Accessed, July, 2022

[13] Financial Supervisory Service, "Voice Phishing Victim Survey Results"

https://www.fss.or.kr/fss/bbs/B0000188/view.do?nttId=16403&menuNo=200218&cl1Cd=&sdate=&edate=&searchCnd=1&searchWrd=%EB%B3%B4%EC%9D%B4%EC%8A%A4%ED%94%BC%EC%8B%B1+%ED%94%BC%ED%95%B4%EC%9E%90+%EC%84%A4%EB%AC%B8&pageIndex=1, Accessed, July, 2022

〔14〕 Soog-kyung Moon, "A study on the using pattern analysis of four-digit personalidentification numbers - A university case", Journal of Digital Convergence, vol. 10, no. 10, pp. 529-538, Nov. 2012.

〔15〕 Statistics KOREA Government Official Work Conference, "Local/mobile phone subscribers", https://www.index.go.kr/potal/main/EachDtlPageDetail.do?idx_cd=2755, Accessed, July, 2022

〔16〕 Hani, "Cannon phone detections soared 8 times… There were many thefts of 'low-priced phones' and 'foreign names'" https://www.hani.co.kr/arti/society/society_general/1001196.html, Accessed, July, 2022

〔17〕 Naver Blog, "Guidance of 010 number by telecommunication company, original assigned station number and 010 conversion number" https://m.blog.naver.com/osh1213/130172042541, Accessed, Aug, 2022

〔18〕 Ra Seong-hyeon, Yeom Su-hyeon, Lee Min-seok, Kim Hyeon-su, Jeong Kwang-jae, Yeo Jae-hyun, Kim Min-cheol, Moon A-ram, Kang In-gyu, Lee Bo-gyeom, Park Sang-mi, Jin Jin-min, Yoon Do-won, Jeon Seong-ho, Hwang Hye-in, Hong Hyeon-ki, Byun Jeong-wook and Lee Sol-hee, "Communication market competition evaluation (2020)", Journal of Information and Communication Policy Research Institute, 1-616, 2020.

〔19〕 Naver Blog "Smartphone payment approval Text scam (Smishing voice phishing) Spam sending Contact phone number Report collection" https://blog.naver.com/autoarc/221559576006, Accessed, Aug, 2022

〔20〕 Naver Blog, "Smartphone payment approval Text scam (Smishing voice phishing) Spam sending Contact phone number Report collection" https://blog.naver.com/autoarc/221685138640, Accessed, Aug, 2022

〔21〕 Inicis, "Beware of characters impersonated by PG companies PG Association, consumer caution request" https://www.inicis.com/blog/archives/119515, Accessed, Aug, 2022

〔22〕 Financial Supervisory Service, "Beware of smishing damage that pretends to be a small payment for a Chuseok delivery service" https://www.fss.or.kr/fss/bbs/B0000188/view.do?nttId=15239&menuNo=200218&cl1Cd=&sdate=&edate=&searchCnd=1&searchWrd=%EC%86%8C%EC%95%A1%EA%B2%B0%EC%A0%9C&pageIndex=1, Accessed, Aug, 2022

〔23〕 Financial Supervisory Service, "Press release to prevent damage from telecommunication financial fraud during Chuseok holidays" https://www.fss.or.kr/fss/bbs/B0000188/view.do?nttId=15936&menuNo=200218&cl1Cd=&sdate=&edate=&searchCnd=1&searchWrd=%EC%8A%A4%EB%AF%B8%EC%8B%B1&pageIndex=1, Accessed, Aug, 2022

〔24〕 Financial Supervisory Service, "Smishing voice phishing warning impersonating government subsidy for courier delivery during explanation days" https://www.fss.or.kr/fss/bbs/B0000188/view.do?nttId=16742&menuNo=200218&

cl1Cd=&sdate=&edate=&searchCnd=1&searchWrd=%EC%8A%A4%EB%AF%B8%EC%8B%B1&pageIndex=1, Accessed, Aug, 2022
[25] Newsis, "Prepaid cheap phone 'pierced by fake ID'... Non-face-to-face opening loopholes" https://mobile.newsis.com/view.html?ar_id=NISX20211002_0001601175, Accessed, Aug, 2022
[26] Itslim, "Create an account without a KakaoTalk phone number" https://itslim.tistory.com/306, Accessed, Aug, 2022
[27] Digitaltoday, "The reason why the three mobile carriers ban the reuse of mobile communication numbers for a certain period of time" https://www.digitaltoday.co.kr/news/articleView.html?idxno=200977, Accessed, Aug, 2022
[28] Hankyung, "SKT blocked 30,000 voice phishing cases last year" https://www.hankyung.com/it/article/2022062292901, Accessed, Aug, 2022

〈저자소개〉

남 소 원 (Sowon Nam) 정회원
2019년 2월: 서울과학기술대학교 산업정보시스템공학과, 컴퓨터공학과 졸업
2019년 9월~현재: 고려대학교 정보보호대학원 정보보호학과 석사과정
〈관심분야〉 정보보호, 디지털포렌식

이 학 선 (Haksun Lee) 학생회원
2019년 3월~현재: 고려대학교 사이버국방학과 학사과정
〈관심분야〉 웹 보안, 유틸리티 보안

이 상 진 (Sangjin Lee) 종신회원
1989년 10월~1999년 2월: ETRI 선임 연구원
1999년 3월~2001년 8월: 고려대학교 자연과학대학 조교수
2001년 9월~현재: 고려대학교 정보보호대학원 교수
2008년 3월~현재: 고려대학교 디지털포렌식연구센터 센터장
〈관심분야〉 디지털포렌식, 심층암호, 해시암호