보도일시: 2020. 6. 24.(수) 10 시 이후 사용해주시기 바랍니다.

국민과 함께하는 따뜻하고 믿음직한 경찰

경 찰 청 브리핑 www.police.go.kr

경찰청 · 방송통신위원회 · 금융위원회 · 금융감독원

경찰청 · 방송통신위원회 · 금융위원회 · 금융감독원 공동 보도자료

경 찰 청	사이버수사과장 총경 최종상(02-3150-1605), 경정 이명원(02-3150-0235)
방송통신위원회	이용자보호과장 천지현(02-2110-1540), 주무관 신희승 (02-2110-1542)
금융위원회	전자금융과 사무관 유원규(02-2100-2974)
금융감독원	불법금융대응단 팀장 이선진(02-3145-8521), 수석 문성훈(02-3145-8534)

가족 또는 지인 사칭해 개인정보와 돈을 요구하는 메신저 피싱 근절 위해 관계기관 힘 모아

경찰청(청장 민갑룡), 방송통신위원회(위원장 한상혁), 금융위원회(위원장 은성수), 금융감독원(원장 윤석헌)은 반부패정책협의회(6. 22.)에서 논의된 '민생침해 불법행위 엄정대응'의 일환으로 서민경제를 위협하는 '메신저 피싱' 근절에 힘을 모아 대응하기로 하였다.

언택트 사회로의 전환이 가속화되면서 전형적인 언택트 범죄인 '메신저 피싱'은 갈수록 피해 규모가 증가하는 추세이며, 올해(1~4월)는 약 128억 원의 피해가 발생한 것으로 집계되었다.

출처 : 금융감독원

최근 3년간 메신저 피싱 피해 현황

피해 규모	'18년		'19년		'20년
	총계	1~4월	총계	1~4월	1~4월
금액 (억 원)	216	37	342	84	128
건수 (건)	9,607	1,662	8,306	2,416	3,273

최근 3년간 1~4월중 피해 추이



메신저 피싱은 카카오톡 등 SNS에서 가족·지인을 사칭해 피해자에게 금원을 요구하는 방법이 일반적인 수법이다.(붙임1 참고)

▸**일반적인 메신저 피싱 수법**

- "엄마, 지금 뭐해?", "많이 바빠? 바쁜거 아니면 톡 해줘"와 같이 가족 또는 지인을 사칭하며, 피해자 상태를 파악하기 위해 질문
- 액정파손, 충전단자 파손, 공인인증서오류 등으로 휴대전화를 사용할 수 없어, PC로 메시지(카톡 등)를 보낸다고 하면서 접근
- 긴급한 송금, 선배에게 빌린 돈 상환, 대출금 상환, 친구 사정으로 대신 입금 등의 이유로 지금 당장 급히 돈이 필요하다며 다급한 상황을 연출

최근에는 문화상품권의 핀번호를 요구하거나, 스마트폰에 '원격제어 어플' 설치를 유도하는 등 새로운 수법들도 발생하고 있다.

▸**문화상품권 구매 후 핀번호 전송 요구**

- 계좌에 대한 지급정지를 피하기 위해 최근 주로 이용되는 수법으로, '문화상품권을 구매해야 하는데 카드 문제로 결제가 되지 않으니, 문화상품권 구매 후 핀번호를 보내주면 구매대금을 보내주겠다'고 속이는 방식

▸**스마트폰에 '원격제어 어플'을 설치하도록 유도**

- 스마트폰 사용이 익숙하지 않은 피해자에게 '팀뷰어' 등 원격제어 어플을 설치토록 유도한 후 해당 휴대폰을 직접 제어하거나 개인정보를 탈취해 온라인 결제 등을 통해 금전을 편취하는 방식

▸**신용카드의 사진과 비밀번호 전송 요구**

- 스마트폰 계좌이체나 온라인 상품권 구매 등에 익숙하지 않은 중장년층을 주된 타겟으로 삼는 수법으로, 카드 정보와 비밀번호를 요구한 후 이를 이용해 범인이 직접 상품권 등을 구매하는 방식

한편, 가족·지인을 사칭하는 경우뿐 아니라 정부기관이나 기업 등을 사칭하는 경우도 꾸준히 발생하고 있어 주의가 필요하다.(붙임2 참고)

경찰청은 올해 말까지 메신저 피싱 등 서민경제 침해사범에 대한 집중단속을 추진하고 있다.

▸**「서민경제 침해사범 집중단속」 중점 단속대상**

△ 피싱사기(보이스 피싱, 메신저 피싱), △ 생활사기(불법사금융, 보험·취업·전세사기), △ 사이버사기(직거래 사기·쇼핑몰사기, 게임사기 등)

또한, ‘사이버 캅’ 앱을 통해 메신저 피싱 피해사례, 범행 수법, 피해 예방수칙 등을 알리는 피해경보를 발령하고, 전국 경찰관서 및 관계기관(업체)의 홈페이지와 SNS를 통해 메신저 피싱 예방 콘텐츠를 전파하는 등 예방을 위한 홍보 활동도 집중 추진할 예정이다.

방송통신위원회는 한국정보통신진흥협회(KAIT), 이동통신사업자와 협력하여 7월 초 이동통신3사 가입자에게 「지인을 사칭한 메신저 피싱 주의」 문자메시지를 발송하고, 알뜰 통신 가입자에게는 요금 고지서(우편, 이메일)로 피해 예방 정보를 안내할 계획이다

▸ **문자메시지 내용**

- 메신저로 지인이 송금, 상품권번호 요청 시 사기일 수 있으니 주의하세요!

금융위원회는 6. 24. 금융·통신·수사의 협업을 통해 반사회적 민생침해 범죄인 보이스피싱을 척결하는 방안을 발표하며, 통신당국 등 관계부처 협업을 통해 메신저 피싱에 악용될 수 있는 다양한 전기통신수단을 신속하게 차단해 나가는 한편, 통신당국, 수사당국 등과 협업을 강화하여 메신저 피싱에 대한 홍보도 강화해 나갈 방침이다.

금융감독원은 메신저 피싱은 피해 예방이 무엇보다 중요한 만큼 가족·지인 외의 타인 계좌로 송금하지 말고, 출처가 불분명한 이메일·문자·URL 주소는 삭제하고 앱 설치를 차단(스마트폰 보안설정 강화)하는 한편, 메신저 비밀번호를 정기적으로 변경하는 등 각별한 주의를 당부하였다.

▸ **메신저 피싱 예방 수칙**

- 실제 가족, 지인이 맞는지 반드시 직접 전화통화로 확인
- 긴급한 상황을 연출하더라도, 전화로 확인 전에는 절대 송금 금지
- 가족.지인 본인이 아닌 타인의 계좌로 송금요청시 일단 의심

메신저 피싱 등으로 피해를 당한 경우 즉시 112에 신고하고, 공인인증서가 노출된 경우 한국인터넷진흥원(KISA) 118 ARS (4번→1번)을 통해 공인인증서 분실 및 긴급 폐기를 요청할 수 있다.

아울러, 피해자의 명의가 도용당한 경우에는 한국정보통신진흥협회(KAIT)에서 운영하는 명의도용방지서비스(msafer.or.kr)에 접속하여 휴대전화 가입현황 등을 조회하거나

개인정보(성명, 전화번호, 주민번호)가 노출된 경우 금융감독원 소비자 정보포털 '파인'에 접속하여 명의도용 금융거래사고 예방을 위해 운영되고 있는 '개인정보 노출 등록·해제' 메뉴를 이용하여 개인정보 노출을 등록함으로써 추가적인 피해 발생을 예방할 필요가 있다.

▸ **명의도용방지서비스(msafer)**

- 국민의 명의도용 피해를 예방하고자 ▵가입사실현황조회, ▵가입제한, ▵SMS 및 이메일 안내 서비스 제공
- 가입사실현황조회 : 피해자 명의로 가입된 휴대전화, 초고속인터넷 등의 통신서비스 가입현황을 조회일자 기준으로 확인할 수 있는 서비스

▸ **개인정보 노출자 사고예방시스템(금융감독원 소비자 정보포털 '파인')**

- 명의도용 금융거래사고를 예방하기 위해 운영되고 있으며, 등록된 개인정보는 금융회사에 공유되어 노출자 명의의 거래가 시도될 경우 일부 금융거래(신규계좌 개설, 신용카드 발급, 휴대폰 할부 구입시 보증보험 가입 등)가 제한 될 수 있음

각 부처 관계자는 "메신저 피싱 예방에 무엇보다 중요한 것은 누구나 피해자가 될 수 있다는 사실을 명심하는 것이다. SNS 등으로 개인정보나 금품 등을 요구받으면 상대가 누구든지 확인하고 또 확인해 보는 습관이 필요하다."라고 강조했다.

OPEN 공공누리 공공저작물 자유이용허락

이 보도 자료와 관련하여 보다 자세한 내용이나 취재를 원하시면 경찰청 사이버수사과 경정 이명원(☎ 02-3150-0235)에게 연락주시기 바랍니다.

[붙임1-1] 가족·지인 사칭 메신저피싱 주요 수법

1 **가족.지인을 사칭하며, 피해자 상태를 파악하기 위해 질문***
* 엄마, 지금 뭐해?, 많이 바빠? 바쁜거 아니면 톡 해줘

2 **핸드폰 고장*으로 수리중이고, PC로 메신저(카톡 등)를 보낸다고 함**
* 액정파손, 충전단자 파손, 공인인증서오류 등

3 **지금 당장 급히 돈이 필요*하다며 다급한 상황을 연출**
* 긴급한 송금, 선배에게 빌린 돈 상환, 대출금 상환, 친구 사정으로 대신 입금

4 **직접 통화하자는 요청을 여러 변명을 대면서 회피***
* 전화기 고장나서 지금은 안돼, 좀 있다 오후에 전화하면 안돼?

5 **본인이 아닌 다른 사람의 계좌*로 송금할 것을 요청**
* 선배 계좌번호, 대출 담당자 계좌번호, 부동산 계좌번호

6 **송금 요청 후에도 계속 독촉***
* 아직도 안보냈어?, 언제쯤 보낼거야?, 보내고 바로 알려줘, 영수증 보내줘

7 **좀 있다 계좌오류 해결후 돈 보내준다며 회유*하고 자금 인출 후 잠적**
* 수수료 때문에 그래?, 수수료도 돈 보낼 때 같이 보내줄게

[붙임1-2] 피해 예방 수칙

☑ **실제 가족, 지인이 맞는지 반드시 직접 전화통화로 확인**
* 납치·협박·부상 등 전화를 받은 경우 가족 등의 안전을 직접 전화해서 확인

☑ **긴급한 상황을 연출하더라도, 전화로 확인 전에는 절대 송금 금지**
* 지금 당장 송금하지 않으면 안된다고 독촉하더라도 전화 확인이 우선

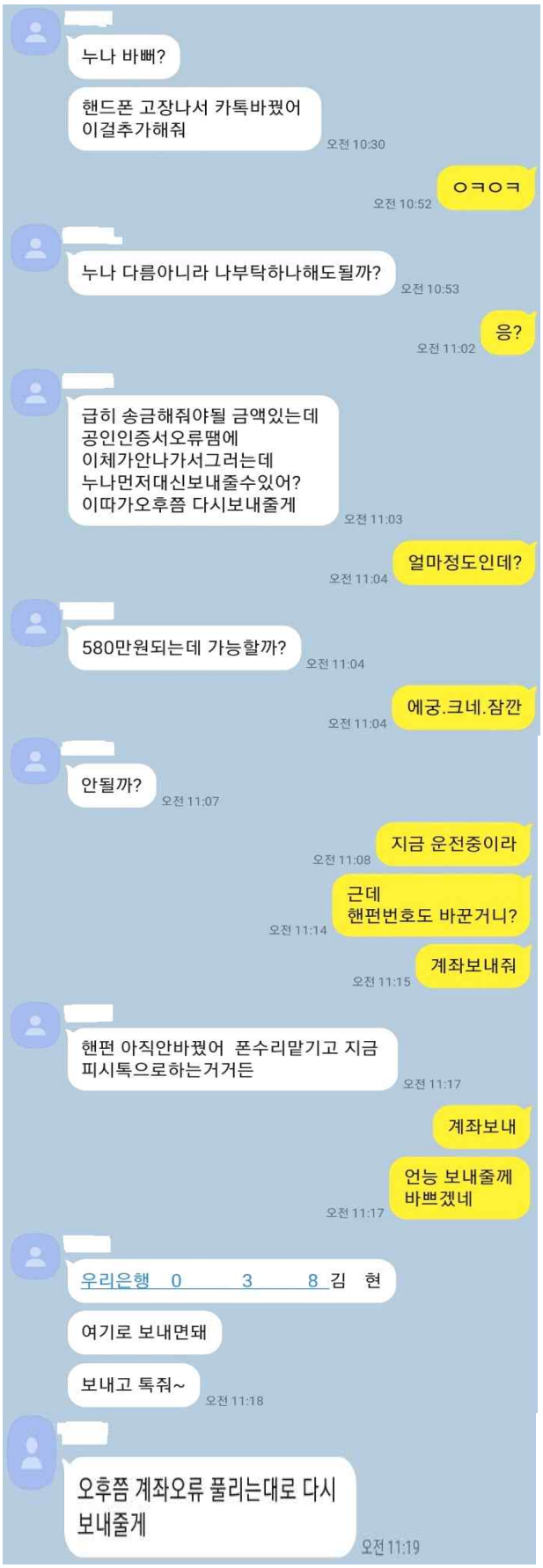
☑ **가족.지인 본인이 아닌 타인의 계좌로 송금요청시 일단 의심**
* 가족 등의 본인의 계좌번호를 알려줄 것을 요구하고, 타인계좌로 송금 금지

◈ 불가피하게 **메신저피싱 피해**가 발생한 경우, **즉시 신고***하여 송금·이체한 계좌의 **지급정지를 요청**하세요

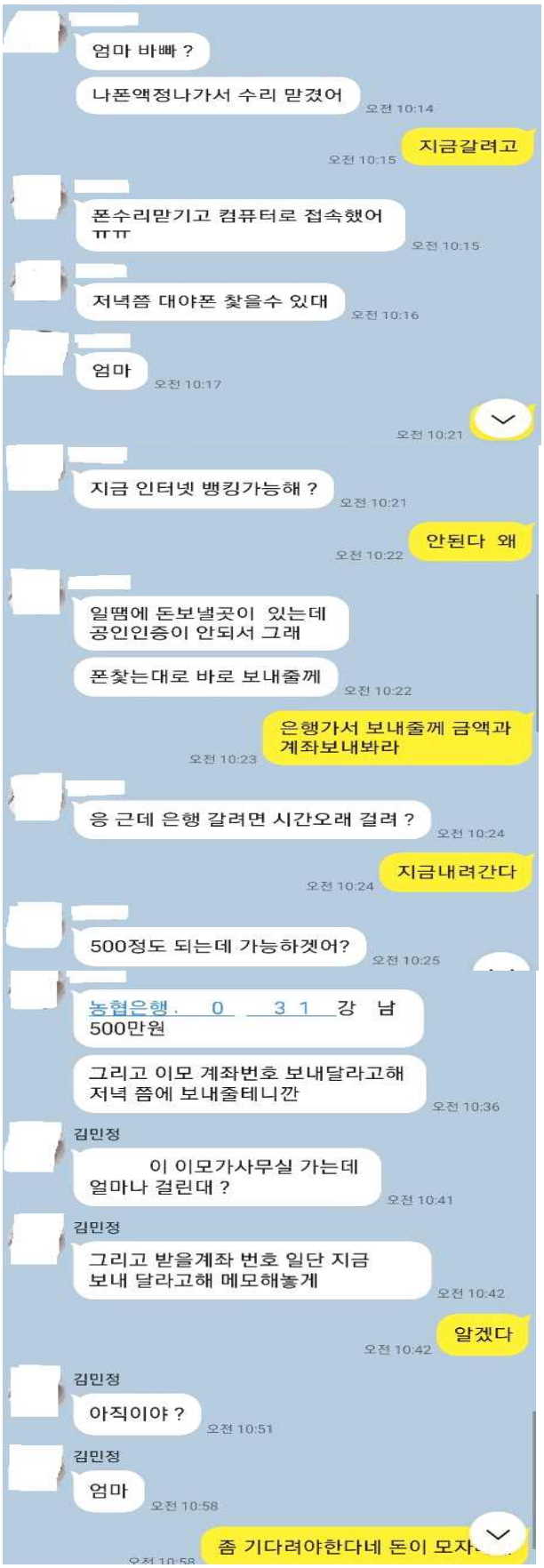
*** 은행(고객센터), 경찰(☎112, 182), 금융감독원(☎1332)**

[붙임1-3] 메신저피싱 사기범의 실제 대화 내용

1. 폰고장, 공인인증서 오류, 남동생 빙자



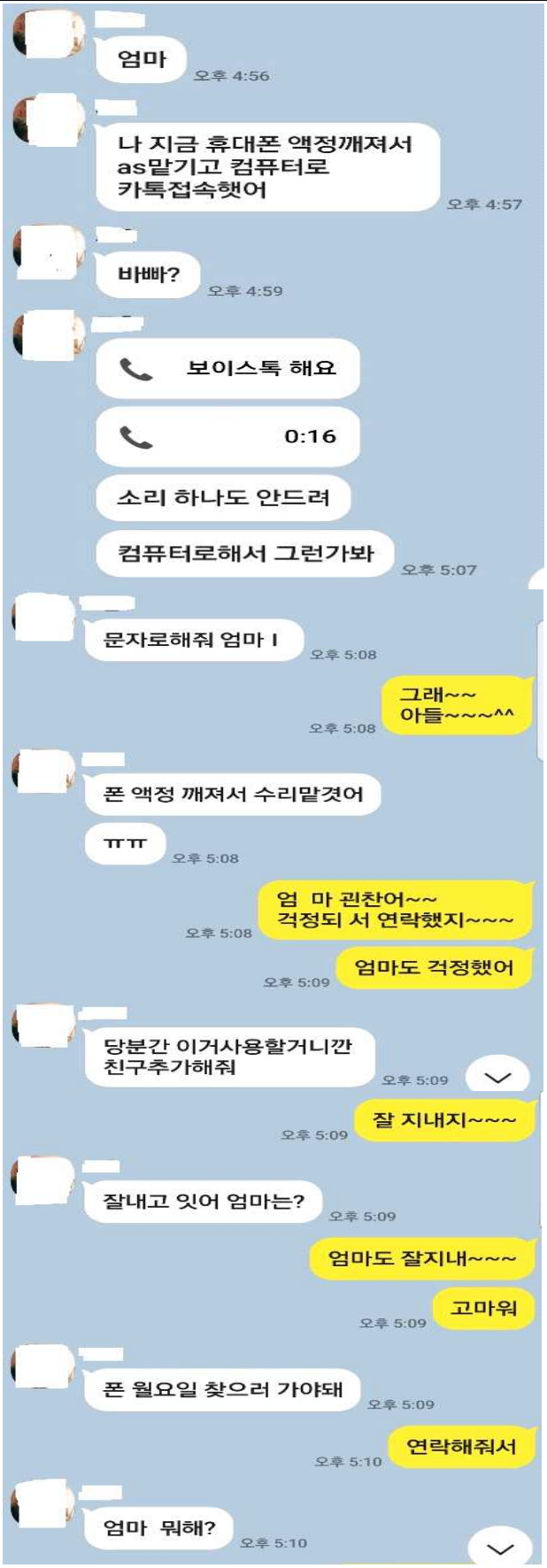
2. 액정파손, 공인인증서 오류, 자녀 빙자



3. 충전단자 파손, 대출상환, 자녀 빙자

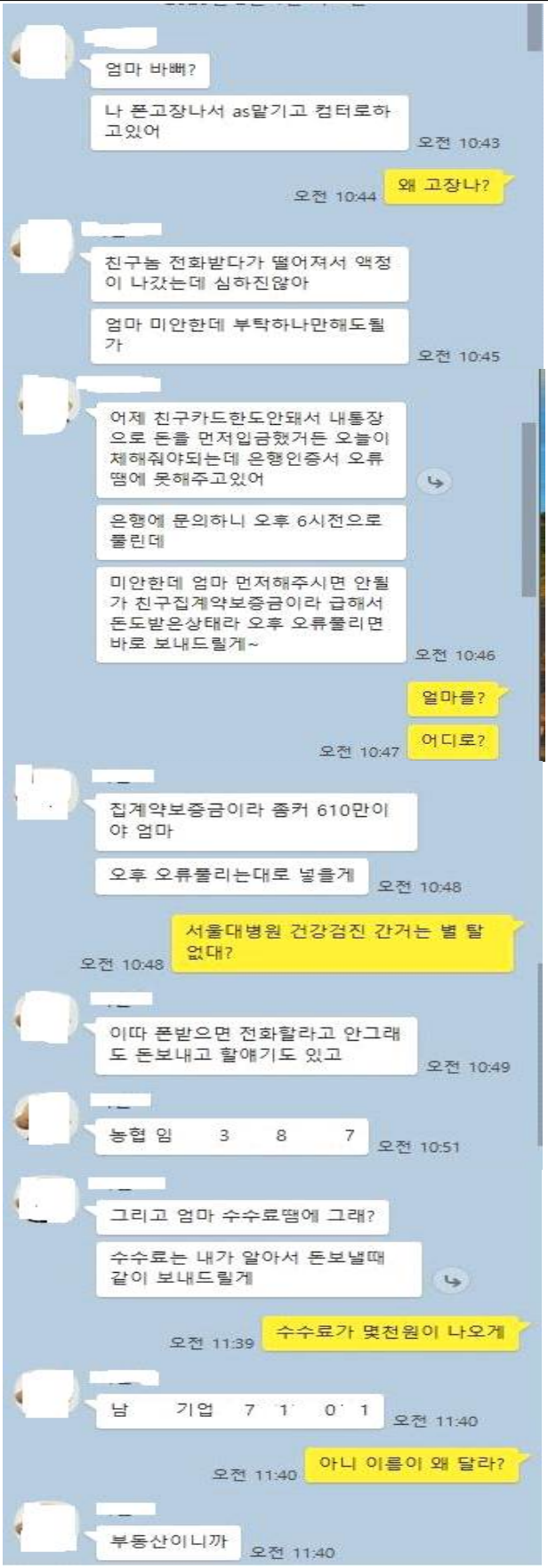


4. 액정파손, 원룸 보증금 상환, 자녀 빙자

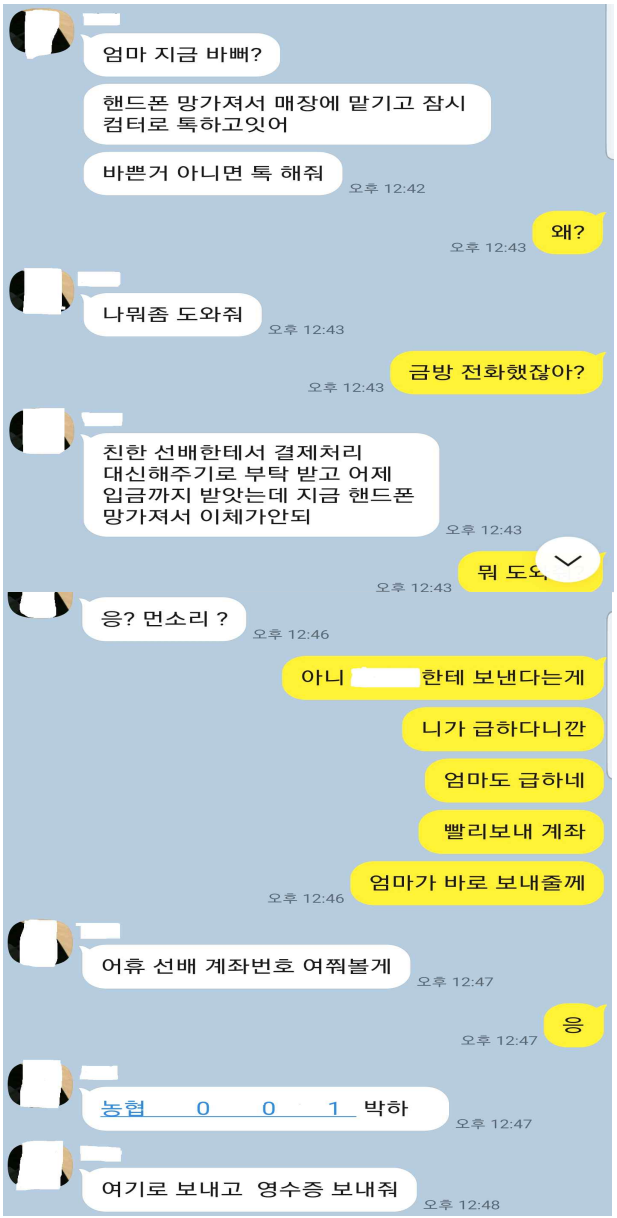




5. 액정파손, 부동산보증금, 자녀 빙자



6. 휴대폰 수리, 지인자금상환, 자녀 빙자



[붙임2-1] 정부·공공기관 사칭(스미싱) 주요 수법

1 **긴급생활비 신청 접수, 긴급재난자금 상품권 도착 등 정부 지원사업 사칭**

2 **교통위반 단속, 민원유발 접수 등 공공기관 사칭**

3 **택배반송, 배송지연 등 택배회사 사칭**

4 **상품권, 쿠폰 당첨 등 쇼핑몰 사칭**

5 **물품대금 결제 등 카드사 사칭**

[붙임2-2] 피해 예방 수칙

☑ **출처가 불분명한 문자메시지, 앱, URL 주소 등 절대 클릭 금지**
* 악성 앱 설치, 불법 사이트 접속시 계좌번호, 개인정보 유출 우려

☑ **실수로 앱 설치시 즉시 앱을 삭제하고, 비밀번호 등 개인정보 입력 금지**

☑ **스마트폰 보안설정 강화**
* 스마트폰 '설정'에서 「알 수 없는 출처의 앱 설치 차단」 클릭

☑ **의심스런 문자는 해당 업체 콜센터 등에 전화로 직접 확인**
* 미신청 긴급지원금 수령, 미주문 택배 배송 지연, 미사용 카드 결제 안내 등

[붙임2-3] 공공기관 등 사칭 실제 사례

< 허위 긴급 생활비, 재난자금 지원 >

[Web발신]
긴급생활비 지원사업이
집수되었습니다 다시한번 확인
부탁드립니다 www.

[Web발신]
[긴급재난자금]
상품권이
도착했읍니다.확인해
주세요. https://
bit.

< 허위 교통단속, 민원 >

[도로공사] 님차량
불법단속대상 적발!
확인 후 빠른처리 요망!
http .com

[생활불편신고] 귀하에게
민원이 접수되어 통보드립니다.
민원확인
http://

< 허위 택배 배송 >

[OO택배] 추석배송 물량증가로
배송이 지연되고 있습니다.
배송일정 확인하세요
http://

< 허위 카드결제 >

[Web발신]
(주)
주문하신 안마의자
57만3000원 결제되
였습니다
문의번호:
02-

< 허위 상품권, 쿠폰 당첨 >

추석선물 도착 전 상품 무료
배송! 할인쿠폰 지급완료!
즉시 사용가능!
확인 http://