전자금융범죄



법제처
찾기 쉬운 생활법령

이 정보는 2026년 10월 15일 기준으로 작성된 것입니다.

찾기 쉬운 생활법령은 국민이 실생활에 필요한 법령을 쉽게 찾아보고 이해할 수 있도록 관련 법령정보를 국민의 생활중심으로 재분류하여 제공하고 있습니다. 따라서 제공된 법령정보는 법적 효력을 갖는 유권해석(결정, 판단)의 근거가 되지 않고, 각종 신고, 불복 청구 등의 증거자료로서의 효력은 없습니다. 구체적인 법령에 대한 질의는 담당기관이나 국민 신문고에 문의하시기 바랍니다.

공공데이터 정책에 따라 '찾기 쉬운 생활법령'에서 제공하는 생활법령은 누구에게나 개방되어 있으며, 영리 목적의 이용을 포함하여 자유로운 활용이 보장됩니다. 이 경우 출처가 법제처 찾기 쉬운 생활법령(http://www.easylaw.go.kr)임을 명시해 주시고, 단순 인용이 아닌 영리목적의 이용이거나 자료의 상당 부분을 이용하는 경우에는 해당 사항을 법제처 법제정보담당관(044-200-6900)으로 통지하여 주시기 바랍니다.

※ 다만, '찾기 쉬운 생활법령'에서 제공하는 생활법령 중 제3자가 저작권을 갖는 저작물의 경우에는 원 저작자의 저작권 정책 및 「저작권법」에 따릅니다.

찾기 쉬운 생활법령에서 제공하는 자료를 위조 · 변조하거나 생활법령에 포함된 제3자의 저작권을 침해하는 경우에는 관련 법령(「저작권법」 제136조부터 제138조까지)에 따라 처벌을 받을 수 있으니 유의하시기 바랍니다.

[전자금융범죄]

끊임없이 진화하며 지능화, 고도화되고 있는 보이스피싱, 스미싱, 파밍, 메모리해킹 등의 전자금융범죄들의 피해사례 및 구제방법에 대해 구체적으로 제시하여 전자금융범죄 피해를 예방하고, 피해발생시 즉각 대처할 수 있도록 법령정보를 제공하고 있습니다.

전자금융범죄 1
1. 전자금융범죄 알아보기 4
1.1. 전자금융범죄의 유형 및 현황 4
1.1.1. 전자금융범죄의 개념, 유형 및 현황 4
2. 전자금융범죄 유형별 피해사례 및 대처방안 7
2.1. 피싱(Phishing) 7
2.1.1. 피해사례 7
2.1.2. 대처방안 13
2.2. 스미싱(Smishing) 17
2.2.1. 피해사례 17
2.2.2. 대처방안 18
2.3. 파밍(Pharming) 21
2.3.1. 피해사례 21
2.3.2. 대처방안 27
2.4. 메모리해킹(Memory Hacking) 31
2.4.1. 피해사례 31
3. 전자금융범죄 피해구제 33
3.1. 피해금 환급 33
3.1.1. 피해구제 신청 33
3.1.2. 지급정지 35
3.1.3. 채권소멸 36
3.1.4. 피해환급금 결정·지급 및 소멸채권 환급 청구 38
3.2. 손해배상 40
3.2.1. 금융회사 등에 대한 손해배상 청구 41
3.2.2. 가해자 등에 대한 손해배상 청구 43
3.3. 피해자 지원 45
3.3.1. 피해자 긴급자금 금융지원 45
4. 전자금융범죄 피해 예방 48
4.1. 전자금융범죄 피해 예방 제도 48
4.1.1. 전자금융사기 예방 서비스 48
4.1.2. 지연인출·이체제도 50
4.1.3. 개인정보보호 관련 예방제도 52
4.2. 전자금융범죄 피해 예방 요령 56
4.2.1. 전자금융범죄 유형별 피해 예방 요령 56

1. 전자금융범죄 알아보기

1.1. 전자금융범죄의 유형 및 현황

1.1.1. 전자금융범죄의 개념, 유형 및 현황

“전자금융범죄”의 개념 및 특징

“전기통신금융사기”의 개념

▪ "전기통신금융사기"란 전기통신을 이용하여 타인을 기망(欺罔)·공갈(恐喝)함으로써 자금 또는 재산상의 이익을 취하거나 제3자에게 자금 또는 재산상의 이익을 취하게 하는 다음의 행위를 말합니다. 다만, 재화의 공급 또는 용역의 제공 등을 가장한 행위는 제외하되, 대출의 제공·알선·중개를 가장한 행위는 포함됩니다(「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법」 제2조제2호).

- 자금을 송금·이체하도록 하거나 「가상자산 이용자 보호 등에 관한 법률」 제2조제1호에 따른 가상자산을 이전하도록 하는 행위
- 개인정보를 알아내어 자금을 송금·이체하거나 가상자산을 이전하는 행위
- 자금 또는 가상자산이 저장된 수단을 교부받거나 교부하도록 하는 행위
- 자금을 출금하거나 출금하도록 하는 행위

> ※ “전기통신”이란 유선·무선·광선 및 그 밖의 전자적 방식에 의하여 부호·문언·음향 또는 영상을 송신하거나 수신하는 것을 말합니다(「전기통신기본법」 제2조제1호).

▪ “전자금융거래등”이란 금융회사등이 전자적 장치를 통해 금융상품 및 서비스 또는 「가상자산 이용자 보호 등에 관한 법률」 제2조제2호 각 목의 행위를 통한 서비스를 제공하고, 이용자가 금융회사등의 종사자와 직접 대면하거나 의사소통을 하지 않고 자동화된 방식으로 이를 이용하는 거래를 말합니다(「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법」 제2조제2호의2).

> ※ 본 콘텐츠에서는 보이스피싱 등 전기통신금융사기와 전자금융거래시에 발생하는 금융 범죄 등을 **“전자금융범죄”**로 통일하여 작성하였습니다.

전자금융범죄의 특징



전자금융범죄의 유형 및 현황

전자금융범죄의 주요 유형

- 자녀납치 및 사고 빙자 편취

  - 자녀와 부모의 전화번호 등을 사전에 알고 있는 사기범이 자녀의 전화번호로 발신자번호를 변조, 부모에게 마치 자녀가 사고 또는 납치 상태인 것처럼 가장하여 부모로부터 자금을 편취하는 수법(학교에 간 자녀 납치 빙자, 군대에 간 아들 사고 빙자, 유학 중인 자녀 납치 또는 사고 빙자 등)

- 메신저상에서 지인을 사칭하여 송금을 요구

  - 타인의 인터넷 메신저 아이디와 비밀번호를 해킹하여 로그인한 후 이미 등록되어 있는 가족, 친구 등 지인에게 1:1 대화 또는 쪽지 등을 통해 금전, 교통사고 합의금 등 긴급자금을 요청하고 피해자가 속아 송금하면 이를 편취

- 인터넷 뱅킹을 이용해 카드론 대금 및 예금 등 편취

  - 명의도용, 정보유출, 범죄사건 연루 등 명목으로 피해자를 현혹하여 피싱사이트를 통해 신용카드정보(카드번호, 비밀번호, CVC번호) 및 인터넷뱅킹정보(인터넷뱅킹 ID, 비밀번호, 계좌번호, 공인인증서비밀번호, 보안카드번호 등)를 알아낸 후, 사기범이 ARS 또는 인터넷으로 피해자명의로 카드론을 받고 사기범이 공인인증서 재발급을 통해 인터넷뱅킹으로 카드론 대금 등을 사기범계좌로 이체하여 편취

- 금융회사, 금융감독원 명의의 허위 긴급공지 문자메시지로 기망, 피싱사이트로 유도하여 예금 등 편취

  - 금융회사 또는 금융감독원에서 보내는 공지사항(보안승급, 정보유출 피해확인 등)인 것처럼 문자메시지를 발송하여 피싱사이트로 유도한 후 금융거래정보를 입력하게 하고 동 정보로 피해자 명의의 대출 등을 받아 편취

- 전화 통화를 통해 텔레뱅킹 이용정보를 알아내어 금전 편취

  - 50~70대 고령층을 대상으로 전화통화를 통해 텔레뱅킹 가입 사실을 확인하거나 가입하게 한 후, 명의도용, 정보유출, 범죄사건 연루 등 명목으로 피해자를 현혹하여 텔레뱅킹에 필요한 정보(주민등록번호, 이체비밀번호, 통장비밀번호, 보안카드일련번호, 보안카드코드 등)를 알아내어 피해자 계좌에서 금전을 사기범계좌로 이체하여 편취

- 피해자를 기망하여 자동화기기로 유인 편취

  - 국세청, 건강보험공단, 국민연금공단 직원 등을 사칭하는 자가 피해자에게 전화하여 세금, 보험료, 연금 등이 과다 또는 오류 징수되어 환급하여 주겠다며 자동화기기로 유인, 기기를 조작하게 하여 자금을 편취

- 피해자를 기망하여 피해자에게 자금을 이체하도록 해 편취

▹ 경찰, 금융감독원 등 공공기관 및 금융기관을 사칭하는 자가 누군가 피해자를 사칭하여 예금인출을 시도한다고 기망한 후 거래내역 추적을 위해 필요하다면서 사기범이 불러주는 계좌로 이체한 후 편취

▹ 사기범들이 학생의 대학지원 명세를 빼내 실제 대학교의 전화번호로 변조하여 학부모 및 학생에게 전화해서 사기범계좌로 등록금 납부를 요구하여 편취

▪ 신용카드정보 취득 후 ARS를 이용한 카드론 대금 편취

▹ 명의도용, 정보유출, 범죄사건 연루 등 명목으로 피해자를 현혹하여 신용카드정보(카드번호, 비밀번호, CVC번호)를 알아낸 후, 사기범이 ARS를 통해 피해자 명의로 카드론을 받음과 동시에 피해자에게 다시 전화를 걸어 허위로 범죄자금 입금사실을 알리고 피해자에게 사기범계좌로 이체토록 유도하여 편취

▪ 상황극 연출에 의한 피해자 기망 편취

▹ 은행직원이나 경찰 등 수사기관의 수사관을 사칭한 사기범들이 은행객장과 경찰서 등에서 실제로 일어나는 상황 연출로 피해자를 기망하여 금전 편취

▪ 물품대금 오류송금 빙자로 피해자를 기망하여 편취

▹ 사기범이 문자메시지 또는 전화로 물품대금, 숙박비 등을 송금하였다고 연락한 후, 잠시 후 실수로 잘못 송금하였다면서 반환 또는 차액을 요구하여 편취

<출처 : 금융감독원, 민원·신고-보이스피싱 지킴이-보이스피싱 한 눈에-주요 사기유형-피싱사기-주요유형 참조>

전자금융범죄의 현황

▪ 보이스피싱 피해 현황

(단위 : 억원, 명, %, %p)

구 분	'19년	'20년	'21년	'22년	'23년	전년대비 증감(률)
피해금액[1]	6,720	2,353	1,682	1,451	1,965	(35.4)
환급액	1,915	1,141	603	379	652	(72.0)
환급률	28.5	48.5	35.9	26.1	33.2	(7.1)
피해자수	50,372	18,265	13,213	12,816	11,503	(△10.2)

주1) 피해구제신청접수(1차 계좌) 기준 (이하 동일)

<출처 : 금융감독원,민원·신고-보이스피싱 지킴이-보이스피싱 한 눈에-보도자료-작년 보이스피싱 피해자 1인당 1,700만원 피해, 전년比 1.5배↑ 2023년 보이스피싱 피해현황 분석 2024. 3. 8. p.2>

2. 전자금융범죄 유형별 피해사례 및 대처방안

2.1. 피싱(Phishing)

2.1.1. 피해사례

피싱(Phishing)의 개념

피싱(Phishing)의 유형

▪ “피싱(Phishing)”이란 ‘개인정보(Private data)를 낚는다(Fishing)’라는 의미의 합성어로, 전화·문자·메신저·가짜사이트 등 전기통신수단을 이용하여 피해자를 기망·공갈함으로써 이용자의 개인정보나 금융정보를 빼낸 후 금품을 갈취하는 사기 수법을 말합니다(KISA 보호나라& KrCERT/CC, 알림마당-자세히 알아보기-피싱 예방 가이드 정의 참조).

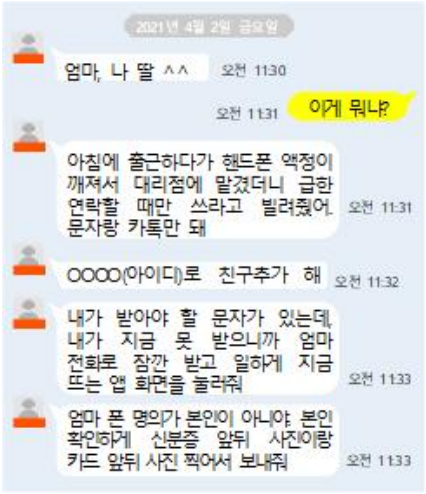
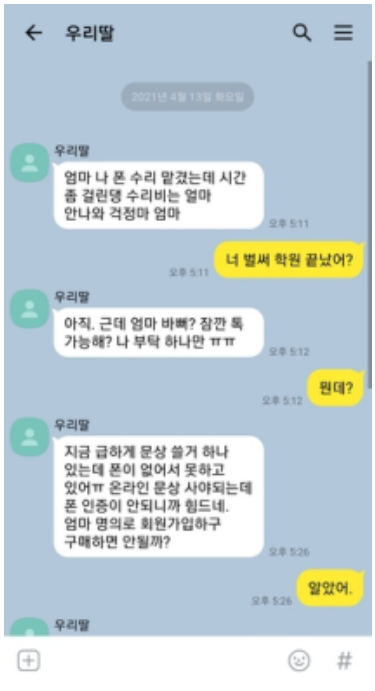
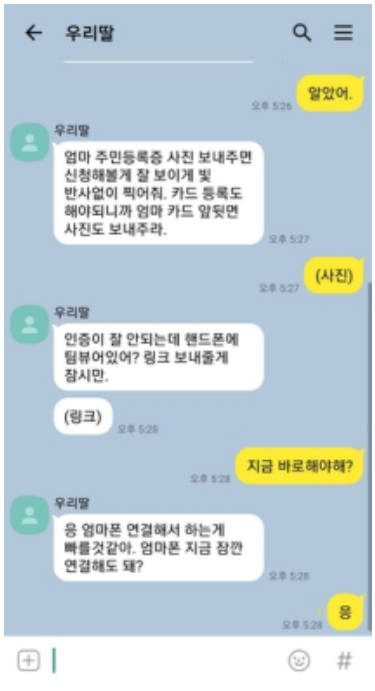
▪ 피싱 사기는 전화뿐만 아니라 문자, 메신저, 인터넷 사이트 등 다양한 전기통신수단을 통해 이루어지고 있습니다.

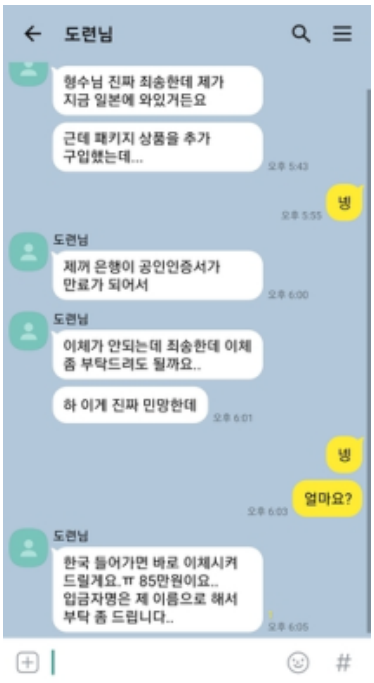
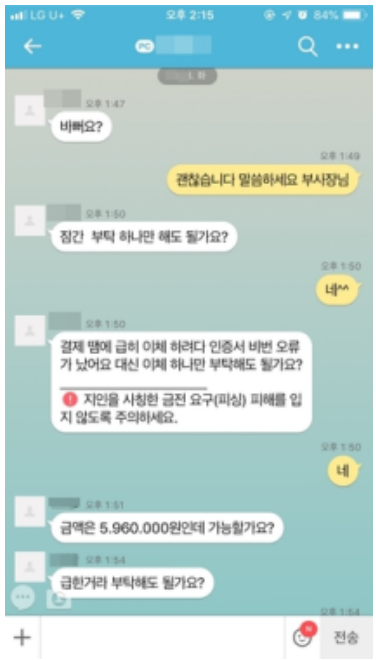
구분	내용
보이스피싱	유선전화 발신번호를 수사기관 등으로 조작하여 해당기관을 사칭하면서 금품을 편취하거나 자녀납치, 사고빙자 등 이용자 환경의 약점을 노려 금품을 편취하는 수법
메신저피싱	SNS, 모바일(또는 PC) 기반 메신저 등 신규인터넷 서비스의 친구추가 기능을 악용하여 친구나 지인의 계정으로 접속한 후 금전 차용 등을 요구하는 수법
피싱사이트	불특정 다수에게 문자, 이메일 등을 보내 정상 홈페이지와 유사한 가짜 홈페이지로 접속을 유도하여 개인정보 및 금융정보를 편취하는 수법
몸캠피싱	스카이프 등 스마트폰 채팅 어플을 통해 음란 화상 채팅(몸캠피싱)을 하자고 접근하여 상대방의 음란한 행위를 녹화한 후 피해자의 스마트폰에 악성코드를 심어 피해자 지인의 연락처를 탈취한 다음 지인들에게 녹화해둔 영상(사진)을 유포하겠다고 협박하여 금전을 갈취하는 범죄 수법
스피어 피싱	고위 공직자, 유명인 등 특정 개인 및 회사를 대상으로 개인정보를 캐내거나 특정 정보 탈취 목적으로 하는 피싱 공격 수법
큐싱	출처가 불분명한 ‘QR코드’를 스마트폰으로 찍을 경우, 악성 앱을 내려 받도록 유도하거나 악성프로그램을 설치하게 하는 금융사기 수법 -QR코드 + phishing의 합성어로, 스미싱에서 한 단계 더 진화된 신종 금융사기 수법
로맨스스캠	SNS 및 이메일 등 온라인상으로 접근하여 호감을 표시한 뒤 재력, 외모 등으로 신뢰를 형성한 후 각종 이유로 금전을 요구하는 방법의 사기

<출처 : 경찰청 사이버수사국, 사이버범죄예방홍보물 및 방송통신위원회 와이즈유저, 피해예방 교육-피해사례별 예방법 참조>

피싱(Phishing) 주요 피해사례

주요 피싱 피해사례

구분	내용
(지인사칭) 자녀를 사칭하며 접근하여 친구 추가 및 앱 설치 요구	 -결제 또는 회원인증을 한다며 피해자의 신분증(촬영본), 계좌번호 및 비밀번호, 신용카드번호 등을 요구하여 탈취, 탈취한 신분증과 개인정보를 활용하여 피해자 명의로 핸드폰과 비대면 계좌를 개설한 후, 피해자 명의로 은행대출, 카드론 및 약관대출 등을 받아 편취하는 방식 <출처 : 금융감독원, 민원·신고-보이스피싱-보이스피싱 한 눈에 보이는-보도자료-'20년 보이스피싱 피해 현황 분석 참조>
(지인사칭) 휴대폰 고장을 핑계로 신분정보 탈취 및 악성앱 설치 유도	  <출처 : 금융감독원, 민원·신고-보이스피싱-보이스피싱 사전예방-피해사례-2021년 최신 메신저피싱 수법 사례 참조>

(지인사칭)마스크하고 손소독제 구매자금 부족을 사유로 지인에게 자금 이체를 요구	보이스피싱 사기범은 카카오톡을 통해 피해자에게 친언니를 사칭하여 접근, “동생, 마스크하고 손소독제를 싸게 대량으로 살 수 있는데, 내가 지금 돈이 없어서... 지금 알려주는 계좌로 90만원 정도 보내줄 수 있니?” 라고 피해자를 기망하여 90만원을 편취 -이체 요청금액을 100만원 이하 금액을 요청하여 피해자의 자금부담을 줄이고, 실제 물품구매 목적인 것으로 오인시키고자 개인명의가 아닌 법인계좌로 이체토록 유도 <출처 : 금융감독원, 민원·신고-보이스피싱-보이스피싱 한 눈에 보이는-보도자료-‘코로나19관련 마스크 손 소독제 물품구매를 사칭한 보이스피싱 피해사례 발생 참조>
(기관사칭) 제가 범죄사건에 연루되었다고요	① ‘18.7월 E씨(34세, 직장인)는 서울OO지검 수사관을 사칭한 사기범으로부터 “국제마약 사건에 연루되었으니 내일 검찰로 출두하라”고 요구하였고 E씨가 보이스피싱을 의심하자 “내 말을 못 믿겠으면 대검찰청 홈페이지를 알려 줄테니 영장을 확인하라”며 피해자를 기망 ② 사기범이 불러주는 인터넷사이트에서 자신의 성명과 주민등록번호를 입력한 후 본인에게 발부된 (가짜) 영장을 확인한 E씨는 사기범의 말을 신뢰하고 수사에 협조하기 위해 사기범이 자금이체를 요구하며 알려준 금감원 F팀장의 계좌로 전 재산 *억원을 이체 ③ 자금출처를 확인한 후 곧 환급될 것이라는 말과 달리 며칠이 지나도록 연락이 없자 E씨는 금감원에 문의하는 과정에서 보이스피싱임을 알아차리고 지급정지 하였으나 이미 전액 현금으로 인출 <출처 : 금융감독원, 민원·신고-보이스피싱-보이스피싱 한 눈에 보이는-보도자료-‘20년 보이스피싱 피해 현황 참조>
호칭을 특정하기 쉬운 사람에게 접근하여 송금불가를 핑계로 금전 편취	  <출처 : 금융감독원, 민원·신고-보이스피싱-보이스피싱 사전예방-피해사례-2021년 최신 메신저피싱 수법 사례 참조>
	[Web발신] (광고)“『ㅇㅇ』는 고객님의 만족을 위해 더 나은 품질의 서비스로 정성을 다하겠습니다.” 고객님께 4차 추가경정예산 지원금

재난지원금 지급 및 백신 접종을 빙자한 보이스피싱 경보

대출 관련하여 다음과 같이 시행됨을 안내 드립니다.

[신청기간]

·지원시기: 2021. 03. 02 ~ 15일 (월요일) 마감.

·4차 지원금소진시 까지 금융지원 (최대 8조원 이상 피해계층 긴급지원)

[상품안내]

·시행금융기관: 제 1금융권 (ㅇㅇ은행)

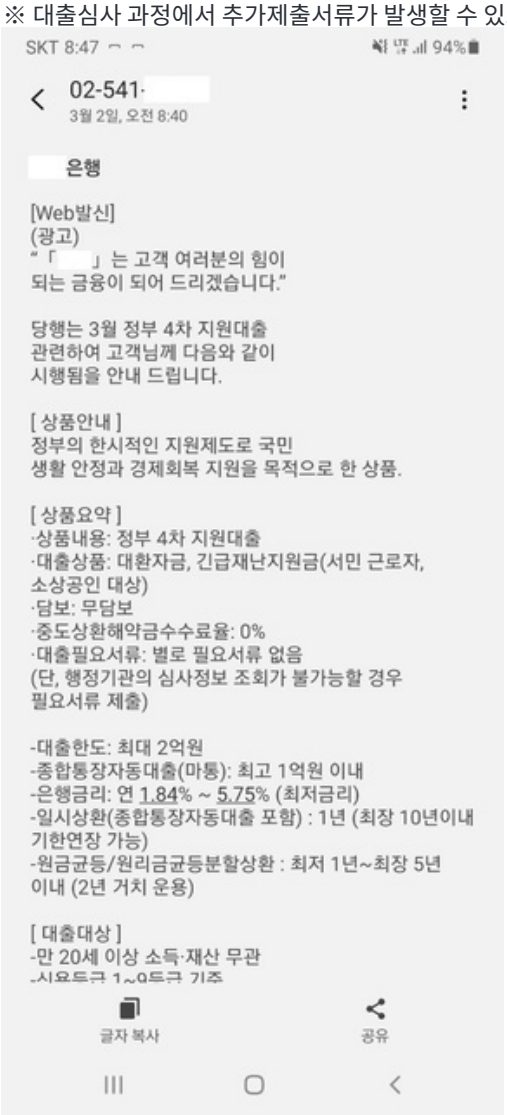
·지원대출상품: 고용안전지원금, 생계지원금, 대환자금대출

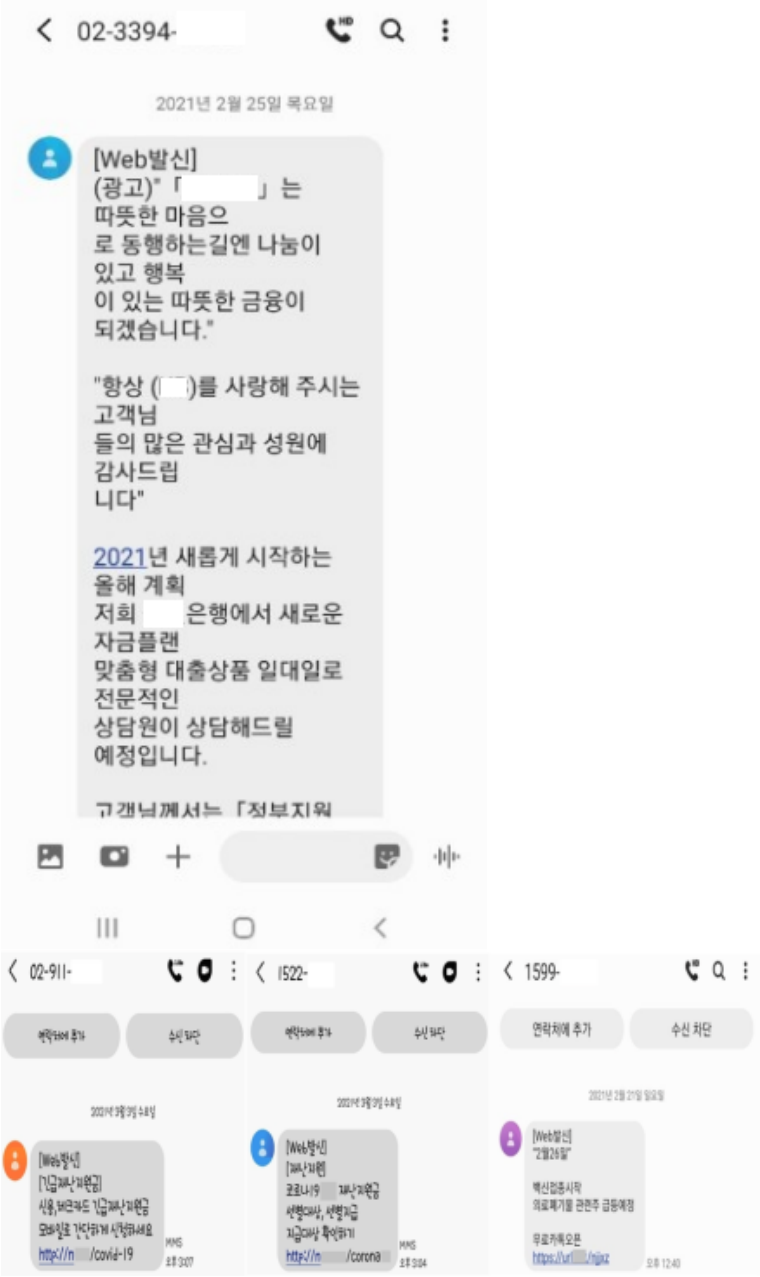
·담보: 무보증

·대출필요서류: 별로 준비서류 없음

※ 대출 이용 중 또는 중도상환 시 고객이 부담해야 하는 비용은 없습니다.

※ 대출심사 과정에서 추가제출서류가 발생할 수 있으며 추가제출서류 필요





<출처 : 금융감독원, 민원·신고-보이스피싱-보이스피싱 한 눈에 보이는-보도자료-재난지원금 백신 등 빙자 보이스피싱 경보 참조>

몸캠피싱을 당했어요	① 타인 사진을 도용하여 여성으로 가장한 범죄자가 「랜덤 채팅」 어플 또는 「모바일 메신저」 채팅방 등을 통해 남성 피해자에게 접근합니다. ② 협박에 필요한 피해자의 음란 동영상을 확보하기 위해, "오빠, 야하게 놀래" 등으로 유혹하며, 「skype」 등으로 이동하여 화상채팅할 것을 피해자에게 제의하는 방식입니다. ③ 미리 준비해 둔 여성 동영상을 보여주며, 상대방도 함께 음란행위를 하도록 유도하면서, 협박할 때 유용하게 사용하기 위해 피해자에게 얼굴과 중요 부위가 함께 화면에 나타나도록 요구합니다. ④ 화상채팅에 필요한 어플이라거나, 화상채팅 중 상대방의 목소리가 들리지 않아 '음성지원용'으로 필요하다며 특정한 파일(*.apk)을 스마트폰에 설치해 달라고 피해자에게 요구합니다. ⑤ 피해자에게 피해자 지인들의 명단과 연락처를 보여주면서 동영상을 유포하겠다는 협박과 함께 돈을 요구하면서, 연락처가 유출되지 않았더라도 "각종 게시판에 올리겠다"며 협박하는 경우도 있습니다. <출처 : 경찰청 사이버수사국, 사이버범죄예방홍보물 참조>
인터넷뱅킹으로 자금이체 중 추가인증이 필요하다며 QR코드를 이용한 앱설치를 요구	인터넷 뱅킹으로 자금이체 중 추가인증이 필요하다며 QR코드를 이용한 앱 설치를 요구하였고, 앱설치 후 카메라 화면을 통해 보안카드 인식을 요구해 이상했으나 보안카드를 찍은 후 곧바로 35만원이 결제된 상황 <출처 : 방송통신위원회 와이즈유저, 피해예방 교육-피해사례별 예방법 참조>
온라인상으로 접근하여 호감 표시한 뒤 신뢰 형성 후 각종 이유로 금전 요구	1) 해외 파병 나간 군인으로 대화상대 필요하다며 접근, 다른 나라 정부로부터 고가의 물품을 선물 받아 보관의뢰에 필요하다며 배송비용 등 명목으로 금전을 요구하여 편취한 사례 2) 미혼이라 소개하며 거액을 상속 받을 예정으로 상속세 내야 하는데 빌려 달라며 기망하여 금원 편취한 사례 <출처 : 경찰청 사이버수사국, 사이버범죄예방홍보물-예방수칙 참조>
'전화 가로채기 앱' 활용 수법	① '18.9월 B씨(52세, 자영업)는 성명불상자로부터 "00저축은행 박00 대리입니다. 고객님은 저금리 대환대출이 가능하십니다. 대출전용 애플리케이션을 설치하여 모바일로 신청"하라는 안내 문자메시지를 받고 메시지에 첨부된 링크를 눌러 00저축은행 앱을 설치하고 대출을 신청 ② 잠시 후 박00 대리라며 대출상담원을 가장한 사기범이 전화상으로 "기존 대출상환을 위해 알려주는 계좌로 0천만원을 입금하라"고 하자 대출사기가 의심스러워 일단 전화를 끊고 해당 저축은행으로 전화하였으나 방금 통화한 박00이 다시 전화를 받자 안심하고 기존 대출상환 자금을 알려준 계좌로 송금 ③ 사기범은 "며칠 안으로 대출승인 연락이 갈 것"이라며 B씨를 안심시켰으나, 일주일이 지나도 연락이 없자 대출사기임을 깨닫고 뒤늦게 지급정지하였으나, 이미 사기범은 이를 인출하여 잠적 <출처 : 금융감독원, 민원·신고-보이스피싱지킴이-참여마당-FAQ-금융감독원 불법금융신고센터의 불법사금융 대응요령 및 상담사례집 2019. 10. p.91 참조>

‘아르바이트 모집’에 응했다가 인출책으로 이용	① '18.10월 K씨(37세, 주부)는 불상자로부터 "당사는 병행수입업체인데, 누진세 부과를 피하기 위해 개인판매인 것처럼 위장하여 물품 판매대금을 대신 받아 전달해줄 사람을 모집한다"는 문자를 받고 문자에 기재된 연락처로 연락하여 정00 부장이라는 불상자가 요구하는 대로 자신의 은행 계좌번호를 알려줌 ② K씨는 자신의 계좌에 입금된 1,000만원 중 알바수당 10만원을 제외한 990만원을 지정한 계좌로 송금하거나 현금으로 인출하여 사기범 일당에게 전달 ③ 다음날 K씨는 은행으로부터 "보이스피싱 사기에 이용되어 계좌가 지급정지되었다"는 문자를 받고 사기에 연루되었음을 깨달았으나, 경찰로부터 사기 가담여부에 대해 수사를 받고 있으며, 피해자로부터 손해배상소송을 당해 재판 중 <출처 : 금융감독원, 민원·신고-보이스피싱지킴이-참여마당-FAQ-금융감독원 불법금융신고센터의 불법사금융 대응요령 및 상담사례집 2019. 10. p.92 참조>
상품권 구매 대행아르바이트를 했으나 자금세탁에 이용	① '18.12월 A씨(25세, 직장인)는 "대행알바"라는 카카오톡 대화명을 쓰는 성명불상자가 "계좌로 100만원을 입금해줄테니 뽑기사이트에서 상품권을 구매하여 카카오톡으로 상품권 핀번호를 알려주면 알바비 3만원을 주겠다"는 문자를 보고 자신의 계좌번호를 알려주고 상품권 구매를 대행해 주고 아르바이트비 9만원 수취 ② 다음날 은행으로부터 “지급정지" 문자를 받은 후에야 자신이 보이스피싱 자금세탁에 이용된 사실을 깨달았으나 피해자로부터 형사고발을 당해 사기방조 혐의로 경찰에서 수사를 받음 <출처 : 금융감독원, 민원·신고-보이스피싱지킴이-참여마당-FAQ-금융감독원 불법금융신고센터의 불법사금융 대응요령 및 상담사례집 2019. 10. p.92 참조>

2.1.2. 대처방안

피싱(Phishing) 피해 대처방법

보이스피싱 피해 시 대처방법



<출처 : 금융감독원, 민원·신고-보이스피싱지킴이-보이스피싱을 당했다면 어떻게?-보이스피싱 피해 시 대처방법 참조>

피싱 피해시 주요 연락처



<출처 : 금융감독원, 민원·신고-보이스피싱지킴이-보이스피싱을 당했다면 어떻게?-피싱피해 시 주요 연락처 참조>

피싱사이트 신고하기

▪ 대검찰청, 경찰청, 인터넷진흥원, 금융기관, 택배 등을 사칭하는 피싱사이트, 스미싱 문자로 인한 금전적 피해가 발생하고 있습니다. 사이트 접속 시 바로 개인정보를 입력하지 말고 먼저 사이트 주소를 확인하시기 바랍니다.

▪ 금융거래정보를 빼내기 위해 은행 등의 홈페이지를 모방하여 만든 가짜 홈페이지 즉, 피싱사이트로 의심되거나 확인된 경우에는 해당 사이트를 신고하여 추가적인 피해를 예방해야 합니다.

> ※ **피싱사이트 신고방법**
>
> - KISA 보호나라&KrCERT/CC(www.krcert.or.kr)의 <침해사고 신고>를 통해 신고하기
>
> - 한국인터넷진흥원 상담센터 국번없이 ☎118

피싱(Phishing) 관련 처벌

사기죄에 따른 처벌

▪ 전자금융범죄는 타인을 속여서 획득한 개인정보 및 금융거래정보를 이용하여 재산상 이익을 취득하는 범죄행위로서 「형법」 상 사기죄에 따라 처벌받을 수 있습니다. 사람을 기망하여 재물의 교부를 받거나 재산상의 이익을 취득하거나 제3자에게 취득하게 해서는 안 됩니다(「형법」 제347조제1항 및 제2항).

> ※ 사기죄 성립 요건에 관한 판례
>
> - 사기죄는 타인을 기망하여 착오에 빠뜨리게 하고 그 처분행위를 유발하여 재물, 재산상의 이익을 얻음으로써 성립하고, 여기서 처분행위라 함은 범인 등에게 재물을 교부하거나 재산상의 이익을 부여하는 재산적 처분행위를 의미하며, 그것은 피기망자가 처분의사를 가지고 그 의사에 지배된 행위를 하여야 하고, 피기망자는 재물 또는 재산상의 이익에 대한 처분행위를 할 권한이 있는 자여야 한다고 한 사례(대법원 2012. 6. 28 선고 2012도4773 판결 참조).

▪ 통장 및 현금카드 등이 사기범행에 사용될 것을 알고도 이를 양도한 경우에는 「전자금융거래법」 위반죄와는 별도로 「형법」 상 사기방조죄에 따른 처벌을 받을 수 있습니다.

> ※ 사기방조죄 성립에 관한 판례
>
> - 피고인은 사기 범행에 이용되리라는 사정을 알고서도 자신의 명의로 은행 예금계좌를 개설하여 계좌의 통장, 현금카드, 비밀번호를 甲에게 양도함으로써 甲이 乙을 속여 乙로 하여금 현금을 위 계좌로 송금하게 한 사건에서 피고인은 사기 범행을 방조하였다고 본 사례(대법원 2010. 12. 9, 선고 2010도6256 판결 참조)

▪ 이를 위반하면 20년 이하의 징역 또는 5천만원 이하의 벌금에 처해집니다(「형법」 제347조제1항 및 제2항).

▪ 상습으로 사기죄를 범한 자는 정한 형의 2분의 1까지 가중할 수 있으며(「형법」 제351조), 타인의 사기죄를 방조한 자는 종범으로 처벌하며, 종범의 형은 정범의 형보다 감경합니다(「형법」 제32조).

컴퓨터 등 사용 사기죄에 따른 처벌

▪ 전자금융범죄는 명의를 도용하여 공동인증서 등을 발급받거나 타인의 보안카드번호를 편취하여 예금을 이체하는 행위 또는 악성프로그램을 유포하는 등 권한없는 자에 의한 정보처리 업무를 통해 재산상 이익을 취득하는 범죄행위에 해당하므로

「형법」 상 컴퓨터사용사기죄로 처벌받을 수 있습니다.

▪ 컴퓨터 등 정보처리장치에 허위의 정보 또는 부정한 명령을 입력하거나 권한 없이 정보를 입력·변경해서 정보처리를 하게 함으로써 재산상의 이익을 취득하거나 제3자에게 취득하게 해서는 안 됩니다(「형법」 제347조의2).

▪ 이를 위반하면 20년 이하의 징역 또는 5천만원 이하의 벌금에 처해집니다(「형법」 제347조의2).

공갈죄에 따른 처벌

▪ 전자금융범죄는 피해자에게 "아들을 납치했다" 또는 "개인정보가 유출됐다" 등의 말로 공포를 느끼게 하여 피해자의 재산을 편취하는 범죄행위로서 「형법」 상 공갈죄로 처벌받을 수 있습니다.

▪ 사람을 공갈(恐喝)하여 재물의 교부를 받거나 재산상의 이익을 취득하거나 제3자에게 재물의 교부를 받게 하거나 재산상의 이익을 취득하게 해서는 안 됩니다(「형법」 제350조제1항 및 제2항).

※ 공갈죄 성립 요건에 관한 판례

- 공갈죄는 다른 사람을 공갈하여 그로 인한 하자 있는 의사에 기하여 자기 또는 제3자에게 재물을 교부하게 하거나 재산상 이익을 취득하게 함으로써 성립되는 범죄로서, 공갈의 상대방이 재산상의 피해자와 같아야 할 필요는 없고, 피공갈자의 하자 있는 의사에 기하여 이루어지는 재물의 교부 자체가 공갈죄에서의 재산상 손해에 해당하므로, 반드시 피해자의 전체 재산의 감소가 요구되는 것도 아닙니다(대법원 2013. 4. 11, 선고, 2010도13774 판결 참조).

※ "공갈"이란 재물을 교부받을 목적으로 타인에게 폭행 또는 협박을 수단으로 일정한 해악을 가할 것을 통고(通告)하여 상대방으로 하여금 공포심을 일으키게 함을 말합니다<출처 : 국가법령정보센터(www.law.go.kr)-법령용어 검색 참조>.

▪ 이를 위반하면 10년 이하의 징역 또는 2천만원 이하의 벌금에 처해집니다(「형법」 제350조제1항 및 제2항).

▪ 상습으로 공갈죄를 범한 자는 정한 형의 2분의 1까지 가중할 수 있습니다(「형법」 제351조).

범죄단체조직

▪ 보이스피싱 조직은 형법상의 범죄단체에 해당하고, 조직의 업무를 수행한 피고인들에게 범죄단체 가입 및 활동에 대한 고의가 인정되며 사기범죄 행위가 범죄단체 활동에 해당하면 「형법」 상 범죄단체 등의 조직죄로 처벌받을 수 있습니다(「형법」 제114조).

※ 범죄단체 등의 조직죄 성립 요건에 관한 판례

- 불특정 다수의 피해자들에게 전화하여 금융기관 등을 사칭하면서 신용등급을 올려 낮은 이자로 대출을 해주겠다고 속여 신용관리비용 명목의 돈을 송금받아 편취할 목적으로 보이스피싱 사기 조직을 구성하고 이에 가담하여 조직원으로 활동함으로써 범죄단체를 조직하거나 이에 가입·활동한 사실이 인정되면, 위 보이스피싱 조직은 보이스피싱이라는 사기범죄를 목적으로 구성된 다수인의 계속적인 결합체로서 총책을 중심으로 간부급 조직원들과 상담원들, 현금인출책 등으로 구성되어 내부의 위계질서가 유지되고 조직원의 역할 분담이 이루어지는 최소한의 통솔체계를 갖춘 형법상의 범죄단체에 해당하고, 보이스피싱 조직의 업무를 수행한 피고인들에게 범죄단체 가입 및 활동에 대한 고의가 인정되며, 피고인들의 보이스피싱 조직에 의한 사기범죄 행위가 범죄단체 활동에 해당합니다(대법원 2017. 10. 26. 선고 2017도8600 판결 참조).

2.2. 스미싱(Smishing)

2.2.1. 피해사례

스미싱(Smishing)의 개념

스미싱(Smishing)의 수법 진화

▪ “스미싱(Smishing)” 이란 문자 메시지(SMS)와 피싱(phishing)의 합성어로 2012년도에 국내에 처음 등장한 신종 금융사기입니다. 그 수법은 문자 메시지를 이용하여 악성 앱이나 악성코드를 휴대전화에 유포한 후 휴대전화 소액결제 관련 정보를 가로챕니다. 이후 게임 사이트에서 아이템 구매 등을 하여 소액결제 피해를 입힙니다. 최근에는 파밍·피싱사이트 수법과 결합한 스미싱 수법이 등장하는 등 그 수법이 점차 진화하고 있습니다.

<출처 : 금융감독원, 업무자료-공통-조사연구자료-금융감독제도일반-알아두면 든든한 금융사기 예방법 2014. 12. p.46~49 참조>

스미싱(Smishing) 최신 피해사례

신종 코로나 바이러스 문자 관련 스미싱주의



<출처 : 금융감독원, 민원·신고-보이스피싱 지킴이-보이스피싱 한 눈에-보도자료-신종 코로나 바이러스 문자 관련 보이스피싱 주의 2020. 1. 31. 배포 참조>

코로나로 자택에서 온라인 연수를 진행한다며 구직자 명의로 비대면 대출 진행

▪ 2030 세대에 친숙한 비대면 면접, 재택근무, 유튜브 연수 등을 활용한 신종 스미싱 사기가 발생하고 있습니다. ① 취업사이트를 통해 광고회사에 지원하여 합격 연락을 받았는데, ② 코로나로 자택에서 온라인 연수를 진행한다며 수일간 업무 동영상 등을 청취하고 과제를 제출하면 연수비를 입금하는 등 구직자가 취업한 것으로 착각하게 한 후 입사지원서의 위변조를 확인한다며 신분증 사진 및 신용도 조회 캡쳐화면 등을 SNS로 전송토록 유도하고, ③업무용 휴대폰을 보낼테니 민원인 명의로 개통하여 택배로 보내면 보안팀에서 회사 보안앱을 설치하여 다시 배송한다고 기망한 후 구직자 명의로 비대면 대출을 실행된 사례(금융감독원, 민원·신고-보이스피싱 지킴이-보이스피싱 한 눈에-보도자료-2030 대상 취업 미끼 비대면 대출 사기, “소비자경보” 발령. 21. 7. 28. 배포 참조).

인터넷주소

▪ 스미싱은 악성코드에 감염된 스마트폰을 이용한 사이버사기 수법으로 악성앱을 설치하기 위한 인터넷주소가 문자메시지에 포함되어 있습니다. 이러한 인터넷 주소(URL)는 단축 서비스를 사용하여 이용자가 웹사이트 정보를 알기 어렵고, 정상적인 사이트와 매우 유사하게 모방하여 제작된 가짜사이트인 피싱사이트로 연결됩니다. 최근에는 정상적인 사이트와 유사한 일반적인 인터넷주소를 사용하는 경우도 있으므로 주의해야 합니다.



< 단축 URL 사용 예시 > < 일반 도메인 악용 예시 >

<출처 : KISA 보호나라 & KrCERT/CC, 알림마당-자세히 알아보기-스미싱 참조>

악성앱

▪ 휴대전화에 일반적으로 많이 설치된 정상앱(예: 크롬, Play 스토어, 공공기관에서 사용하는 정부24, 유명 모바일 백신 등)을 사칭하여 악성앱 설치를 유도합니다. 전화, 문자메시지 관리, 개인정보 조회, 저장소 조회, 위치정보, 기기관리자 권한 요구 등 정상앱 보다 과도한 권한을 포함하고 있으므로 앱 설치 단계에서 주의해야 합니다. 또한 악성앱이 악성행위를 직접 수행하기도 하지만 별도의 악성앱을 설치하도록 유도하는 기능이 탑재된 경우도 있습니다. 크롬, 뱅킹, 백신 등 특정 애플리케이션이 실행될 경우 '업데이트 파일입니다'라는 형태로 업데이트를 안내하여 이용자들이 악성앱을 다운로드하도록 유도하고 있습니다.

<출처 : KISA 보호나라 & KrCERT/CC, 알림마당-자세히 알아보기-스미싱 참조>

관심을 유도하는 문자메시지



<출처 : KISA 보호나라 & KrCERT/CC, 알림마당-자세히 알아보기-스미싱 참조>

2.2.2. 대처방안

스미싱(Smishing) 피해 대처방법

통신과금서비스 이용의 정정 요구

▪ 통신과금서비스이용자는 통신과금서비스가 자신의 의사에 반하여 제공되었음을 안 때에는 통신과금서비스제공자에게 이에 대한 정정을 요구할 수 있으며(통신과금서비스이용자의 고의 또는 중과실이 있는 경우는 제외함), 통신과금서비스제공자는 이용자의 정정요구가 이유 있을 경우 판매자에 대한 이용대금의 지급을 유보하고 그 정정 요구를 받은 날부터 2주 이내에 처리 결과를 알려 주어야 합니다(「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제58조제3항).

> ※ "통신과금서비스"란 정보통신서비스로서 다음의 업무를 말합니다(「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제10호).
>
> 타인이 판매·제공하는 재화 또는 용역(이하 "재화 등"이라 함)의 대가를 자신이 제공하는 전기통신역무의 요금과 함께 청구·징수하는 업무
>
> 타인이 판매·제공하는 재화 등의 대가가 위의 업무를 제공하는 자의 전기통신역무의 요금과 함께 청구·징수되도록 거래정보를 전자적으로 송수신하는 것 또는 그 대가의 정산을 대행하거나 매개하는 업무
>
> ※ "통신과금서비스제공자"란 통신과금서비스제공자로 등록을 하고 통신과금서비스를 제공하는 자를 말합니다(「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제11호).
>
> ※ "통신과금서비스이용자"란 통신과금서비스제공자로부터 통신과금서비스를 이용하여 재화 등을 구입·이용하는 자를 말합니다(「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제12호).

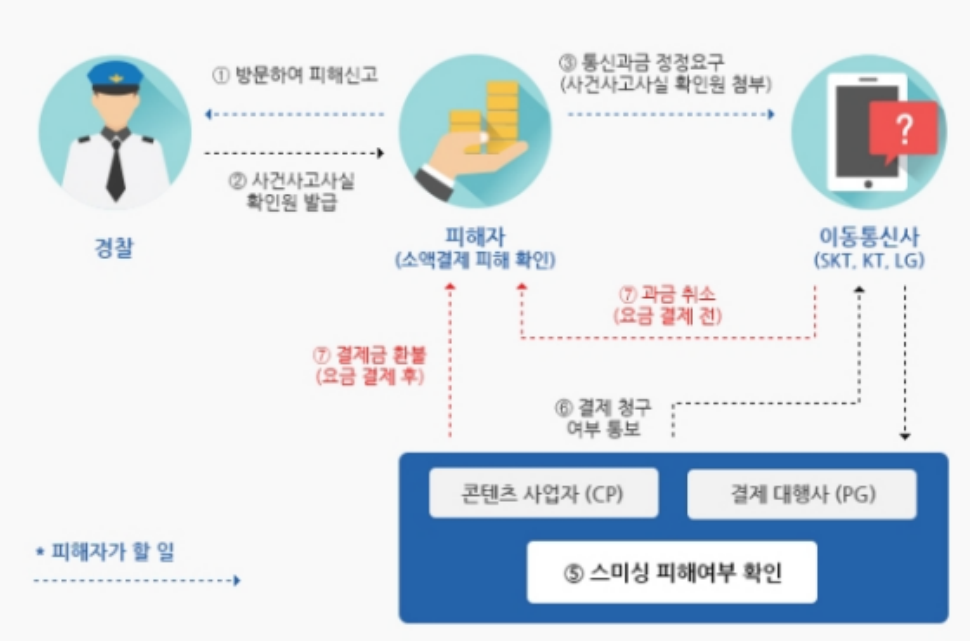
▪ 이를 위반하여 통신과금서비스이용자의 요청에 대한 처리 결과를 통신과금서비스이용자에게 알려 주지 않거나 통신과금서비스에 관한 기록을 보존하지 않은 경우에는 1천만원 이하의 과태료가 부과됩니다(「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제76조제4항제19호 및 제20호).

휴대폰 소액결제 피해 구제 방법

▪ 스미싱으로 의심되는 문자를 받았다면

▹ 경찰청 사이버범죄 신고시스템(ECRM)(https://ecrm.cyber.go.kr / ☎182)로 신고하고, 해당 이동통신사의 고객센터(☎114)에 소액결제서비스 차단을 신청하여 본인도 모르게 소액결제가 되지 않도록 해야 합니다.

▪ 소액결제 피해가 발생했다면



<출처 : 사이버범죄 신고시스템(ECRM), 피해자 구제 제도-스미싱 피해 구제 절차 참조>

▹ 모바일 결제 확인 및 취소하기

※ 스미싱 악성앱에 감염되면 모바일 결제 피해가 발생할 수 있습니다. 따라서 이동통신사에 모바일 결제 내역이 있는지 확인해야 합니다.

① 통신사 고객센터를 통하여 최근 모바일 결제 내역 확인

② 모바일 결제 피해가 확인되면 피해가 의심되는 스미싱 문자 캡쳐

③ 통신사 고객센터를 통해 스미싱 피해 신고 및 '소액결제확인서' 발급

④ 소액결제확인서를 지참하여 관할 경찰서 사이버수사대 또는 민원실을 방문하여 사고 내역 신고

⑤ 사고 내역을 확인받고 '사건사고 사실 확인서' 발급

⑥ 사건사고 사실 확인서 등 필요서류를 지참하여 통신사 고객센터 방문 또는 팩스나 전자우편 발송

⑦ 통신사나 결제대행 업체에 사실 및 피해 내역 확인 후 피해보상 요구

<출처 : KISA 인터넷보호나라 & KrCERT, 사이버위협-스미싱 참조>

▹ 피해사실 신고하기

√ 경찰서에서 발급받은 '사건사고 사실확인원'을 이동통신사, 게임사, 결제대행사 등 관련 사업자에게 제출하고 피해사실을 신고해야 합니다.

▹ 악성파일 삭제하기

√ 스마트폰 내 '다운로드' 앱을 실행하여 ① 문자를 클릭한 시점 이후에 확장자명이 'apk'인 파일 저장여부를 확인하고, ② 해당 'apk'파일을 삭제합니다.

√ 악성파일이 삭제되지 않는 경우에는 ① 휴대전화 서비스센터에 방문하거나 ② 스마트폰을 초기화해야 합니다.

▹ 공동인증서[(구)공인인증서] 폐기 및 재발급하기

√ 악성앱에 감염되었던 스마트폰으로 모바일 금융서비스를 이용했다면 공동인증서, 보안카드 등 금융거래에 필요한 정보가 유출되었을 가능성이 존재합니다. 따라서 해당 정보를 폐기하고 재발급을 받아야 유출된 금융 정보로 인한 2차 피해가 발생하는 것을 예방할 수 있습니다. 스마트폰에 보안카드 등 금융 거래에 필요한 정보를 사진첩, 메모장에 기록했다면 폐기처분하고 재발급을 받아야 합니다.

※ 더 자세한 피해구제 방법은『휴대전화 이용자』콘텐츠의 (휴대전화의 이용-소액결제-소액결제 이용 및 피해구제)에서 확인할 수 있습니다.

스미싱(Smishing) 관련 처벌

컴퓨터등 사용사기죄에 따른 처벌

▪ 명의를 도용하여 공동인증서를 발급받거나 타인의 보안카드번호를 편취하여 예금을 이체하는 행위 또는 악성프로그램을 유포하는 등 권한 없는 자에 의한 정보처리 업무를 통해 재산상 이익을 취득하는 범죄행위는 「형법」상 컴퓨터등 사용사기죄로 처벌받을 수 있습니다.

▪ 컴퓨터 등 정보처리장치에 허위의 정보 또는 부정한 명령을 입력하거나 권한 없이 정보를 입력·변경해서 정보처리를 하게 함으로써 재산상의 이익을 취득하거나 제3자에게 취득하게 해서는 안 됩니다(「형법」 제347조의2).

※ 컴퓨터등 사용사기죄를 인정한 판례

A가 권한 없이 주식회사 B의 아이디와 패스워드를 입력하여 인터넷뱅킹에 접속한 다음 위 B회사의 예금계좌로부터 자신의 예금계좌로 예금을 이체하는 내용의 정보를 입력하여 자신의 예금액을 증액시킨 경우에는 컴퓨터등 사용사기죄가 성립합니다(대법원 2004. 4. 16. 선고 2004도353 판결 참조).

타인의 명의를 도용하여 발급받은 신용카드 번호와 그 비밀번호를 이용하여 ARS전화서비스나 인터넷 등을 통해 신용대출을 받는 방법으로 재산상 이익을 취득하는 행위 역시 미리 포괄적으로 허용된 행위가 아닌 이상, 컴퓨터 등 정보처리장치에 권한 없이 정보를 입력해서 정보처리를 하게 함으로써 재산상 이익을 취득하는 행위로서 컴퓨터등사용사기죄에 해당합니다(대법원 2006. 7. 27. 선고 2006도3126 판결 참조).

▪ 이를 위반하면 20년 이하의 징역 또는 5천만원 이하의 벌금에 처해집니다(「형법」 제347조의2).

※ 그 밖에 스미싱 관련 처벌에 대한 자세한 내용은 이 콘텐츠의 <전자금융범죄 유형별 피해사례 및 대처방안-피싱(Phishing)-대처방안>에서 확인할 수 있습니다.

2.3. 파밍(Pharming)

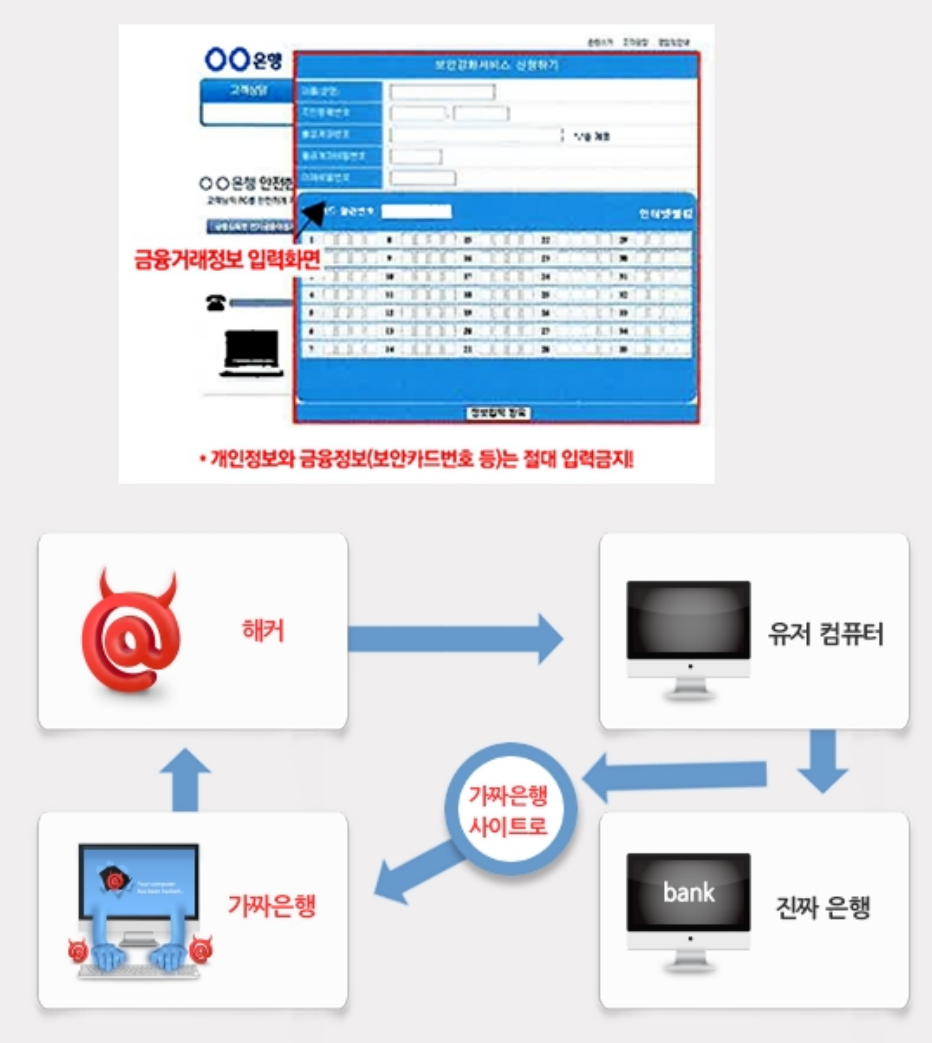
2.3.1. 피해사례

파밍(Pharming)의 개념

피싱(가짜)사이트로 유도

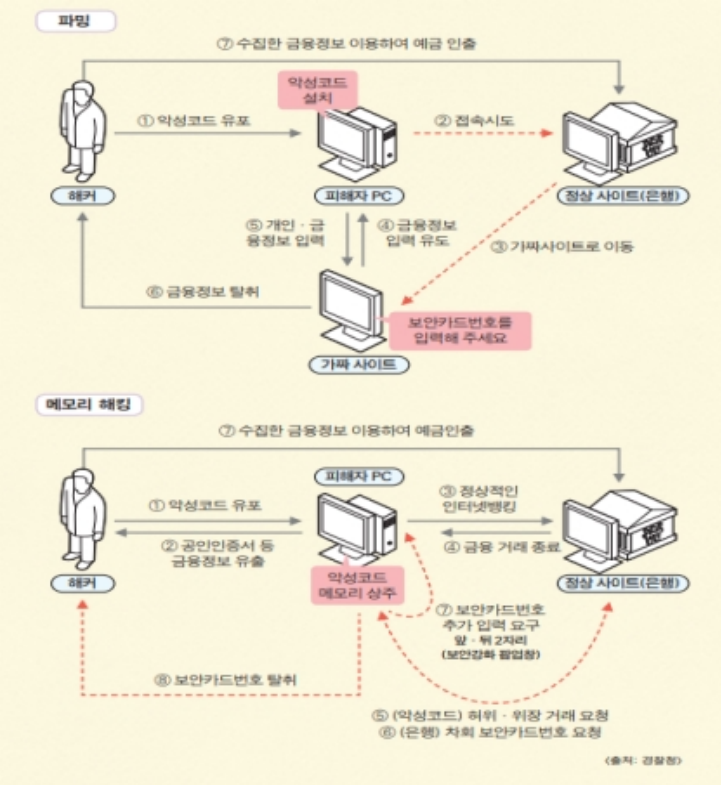
▪ “파밍(Pharming)”이란 악성코드에 감염된 PC를 조작해, 이용자가 인터넷 ‘즐겨찾기’ 또는 포털사이트를 통해 금융회사 홈페이지에 접속하여도 피싱(가짜)사이트로 유도되어 금융정보를 탈취한 후, 탈취한 정보를 이용하여 예금을 인출하는 방식을 뜻합니다.

▪ 파밍에 의해 유도된 피싱사이트



<출처 : 경찰청 사이버수사국, 사이버범죄예방홍보물-예방수칙-파밍 참조>

파밍과 메모리해킹 비교



<출처 : 금융감독원, 업무자료-공통-조사연구자료-금융감독제도 일반 참조>

파밍(Pharming) 주요 피해사례

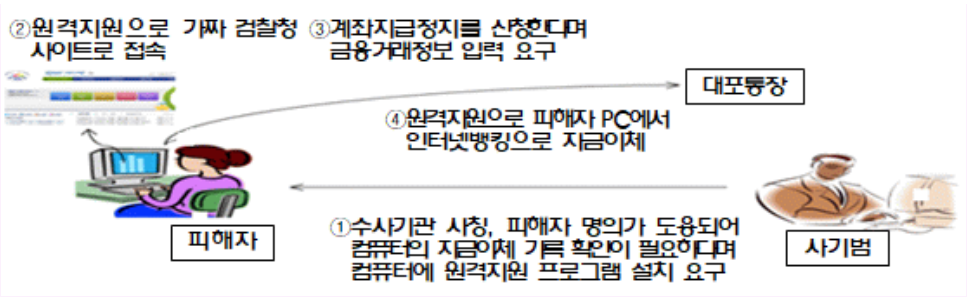
사기범이 원격지원으로 피해자 PC에 접속하여 직접 자금 이체한 사례

사례1) ① 사기범은 검찰 사이버수사팀 수사관을 사칭하면서 피해자 A씨에게 접근하여, A씨 명의 계좌가 대포통장으로 사용되었으니 A씨가 명의도용된 피해자인지 여부를 확인하기 위해서는 컴퓨터에서 자금이체기록 등을 확인해야 한다고 하면서 컴퓨터를 켜게 한 후 '팀뷰어'라는 원격제어 프로그램을 설치토록 유도 ② 이후 사기범은 가짜 검찰청사이트로 접속하여 사건 조회 검색을 통해 실제 사건임을 믿게 한 후, 계좌 안전조치를 취하기 위해서 계좌 지급정지 및 금융보호서비스를 신청해야 한다며 비밀번호, 공인인증서 번호 등 금융정보를 입력하게 하여 금융정보를 탈취 ③ 이어서 사기범은 A씨에게 잠시 기다리라고 한 후, 원격제어를 통해 A씨 컴퓨터 화면을 보이지 않게 만든 후 인터넷뱅킹을 통해 사기범의 계좌(대포통장)로 4,140만원을 이체한 후 잠적

사례2) ① 사기범은 서초경찰서 지능범죄수사과 김태진 수사관을 사칭하면서 피해자 B씨에게 접근하여, 피해자의 계좌가 범죄에 연루되어 2, 3차 피해를 막기 위해서 보안강화를 위해 '팀뷰어' 프로그램을 설치토록 유도 ② 이후 사기범은 B씨의 컴퓨터에서 가짜 검찰청 사이트로 접속하여 B씨에게 은행 계좌번호, 비밀번호 등을 입력하게 하는 방법으로 B씨의 개인금융정보를 탈취한 후, 보안강화작업을 진행하려고 하니 컴퓨터 모니터를 꺼두라고 지시 ③ B씨가 컴퓨터 모니터를 끄자 사기범은 피해자의 컴퓨터에서 인터넷뱅킹을 통해 사기범의 계좌(대포통장)로 총 1,855만원을 이체한 후 잠적

<출처 : 금융감독원, 알림·소식-보도자료-원격으로 피해자 PC에 접속하여 자금을 이체하는 신종 파밍 주의 16.10.14. 보도 참조>

원격지원 프로그램을 악용한 신종 파밍 수법



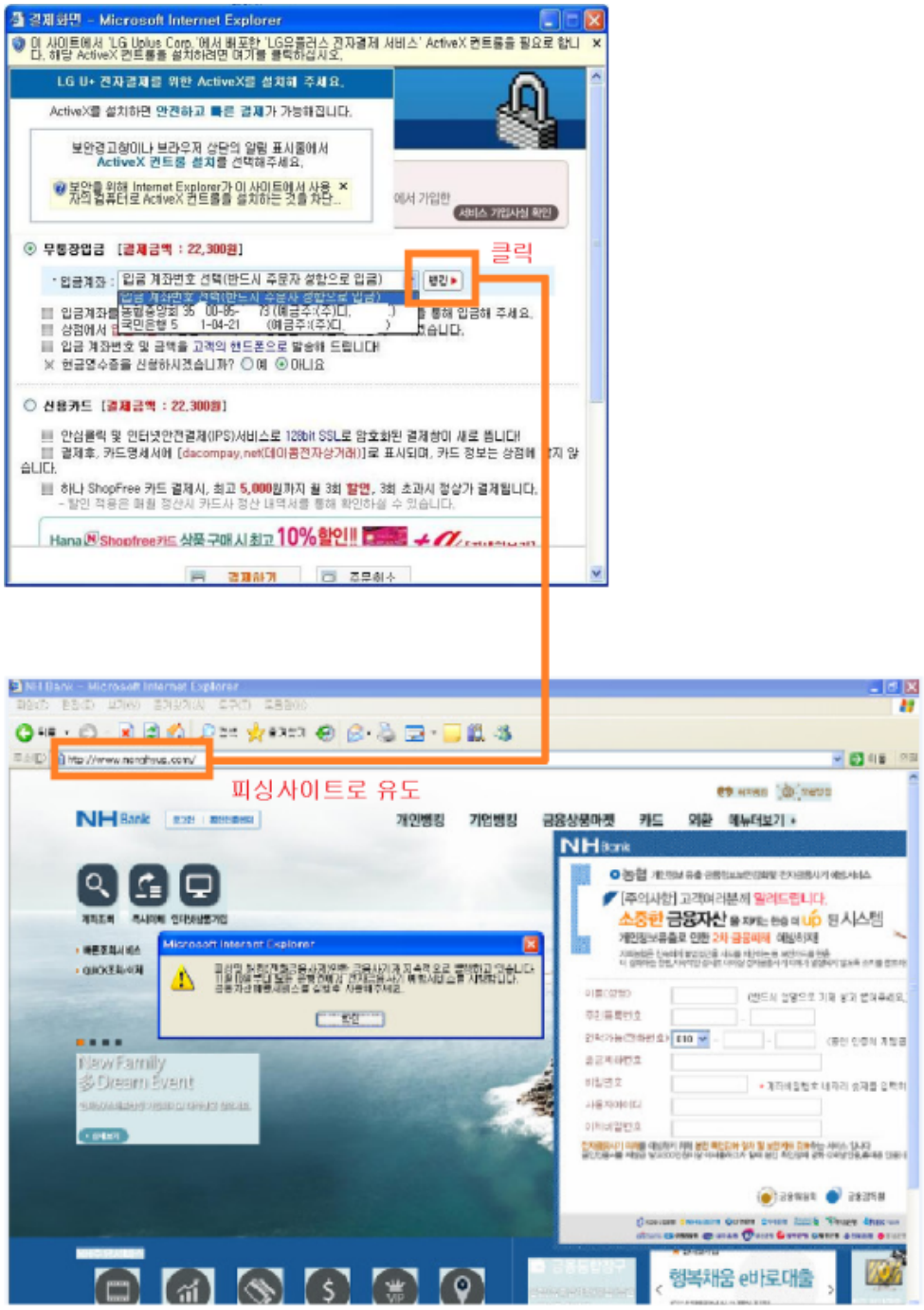
<출처 : 금융감독원,민원·신고-보이스피싱 지킴이-보이스피싱 한 눈에-보도자료-원격으로 피해자 PC에 접속하여 자금을 이체하는 신종 파밍 주의 16.10.14 보도 참조>

가짜 쇼핑몰 결제 팝업창

▪ ① 제주시 거주 강모씨(20대, 여)는 '13.3.27일 오후 4시경 인터넷쇼핑몰인 "△△감성"사이트에서 옷을 구매하면서 결제수단 중 실시간 계좌이체를 선택

② 인터넷뱅킹으로 계좌이체를 하기 위해 결제창 內 "뱅킹"버튼을 선택하였는데 악성코드에 감염된 PC로 인하여 N은행 피싱사이트로 유도되어 보안카드 코드번호 전체와 계좌비밀번호, 인터넷뱅킹아이디 등의 금융거래정보를 입력

③ 이후 피해자의 금융거래정보를 알아낸 사기범이 공인인증서를 재발급 받아 3.28일 새벽 1시경 피해자 명의의 인터넷뱅킹을 통해 258만원을 사기범계좌로 이체하여 편취



<출처 : 금융감독원, 민원·신고-보이스피싱 지킴이-보이스피싱 한 눈에-보도자료-쇼핑몰 무통장입금 결제창을 통한 파밍주의 13. 4. 5. 배포 참조>

금융감독원을 사칭하는 가짜 팝업창을 열게 되어 감염

▪ ① 금융사기범은 금융감독원을 사칭하여 스마트폰 팝업창 이용 개인정보 유출 여부를 확인하라는 팝업창을 발송하여 개인신용정보 탈취 피싱사이트로 유도

② 확인을 누르면 금융감독원 사칭 홈페이지로 이동

③ 금융감독원 사칭 도메인 주소와 정보를 정확히 입력하라는 안내창이 나타남 ④ 본인확인창에 카드번호, 카드유효기간, CVC번호, 비밀번호, 공동인증서 비밀번호, 이름, 주민등록번호 입력하라는 화면으로 이동





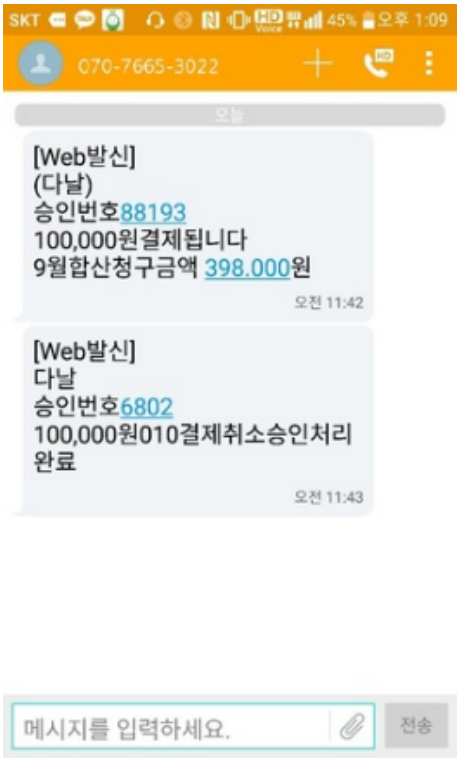
<출처 : 금융감독원, 민원·신고-보이스피싱 지킴이-보이스피싱 한 눈에-보도자료-금융감독원을 사칭한 개인정보 탈취 사기문자 소비자경보 발령 21. 8. 13. 배포 참조>

금융감독원 금융민원센터 사이트를 위조한 피싱사이트 이용 사례

▪ ① 피해자 C씨는 '카메라 구입 398,000원 지불' 이라는 문자메시지를 받고, 해당 업체로 전화하여 물건을 구매한 사실이 없다고 하자, 결제를 취소해주겠다고 하여 전화를 끊음

② 이후 사이버경찰청 최영호 팀장이라며 전화가 와서 C씨가 금융사기 피해를 당한 사실이 확인되었으니 통장 안전조치를 위해 금융감독원 e-민원센터 홈페이지로 접속하여 주민등록번호, 카드번호, 통장번호, 비밀번호, 공인인증번호를 입력하라고 지시

③ 사기범은 탈취한 금융정보를 이용해 C씨의 계좌에서 사기범의 계좌로 총 4,578만원을 이체

사기범이 다날 업체를 사칭하여 피해자에게 보낸 문자 내역	금융감독원 e-금융민원센터 사칭 홈페이지
	

<출처 : 금융감독원, 민원·신고-보이스피싱 지킴이-보이스피싱 한 눈에-보도자료-원격으로 피해자 PC에 접속하여 자금을

이체하는 신종 파밍 주의 16. 10. 14. 보도 참조>

신용카드 이메일 명세서를 이용하여 악성코드를 유포

▪ 신용카드 이메일 명세서를 이용하여 악성코드를 유포하는 사례가 발견되어 이용자의 각별한 주의가 요망됩니다. 해커 또는 사기범이 고객에게 '3월 카드 거래내역'이란 제목으로 이메일을 발송한 후, 고객이 파일을 열면 주민등록번호를 입력하도록 하는 등 개인정보 탈취를 시도하거나 PC가 다운되는 현상 발생

▪ 이용자 유의사항

- 금융회사에 신청한 메일 주소와 상이한 이메일로 명세서가 올 경우, 열지 말고 즉시 삭제
- 금융회사의 경우 전체 보안카드 번호 등 사용자 정보의 입력을 요구하지 않고 있어, 절대로 사용자 정보를 입력하지 않기
- 금융회사 홈페이지 등에 접속하여 PC백신프로그램 등을 이용하여 악성코드 탐지 및 제거
- 정보유출 및 예금인출 사고를 당한 경우 즉시, 해당 금융회사에 신고하고 지급정지 요청하기 등

<출처 : 금융감독원, 민원·신고-보이스피싱 지킴이-보이스피싱 한 눈에-보도자료-신용카드 이메일 명세서를 이용한 '피싱'피해 예방 당부 13. 4. 1. 배포 참조>

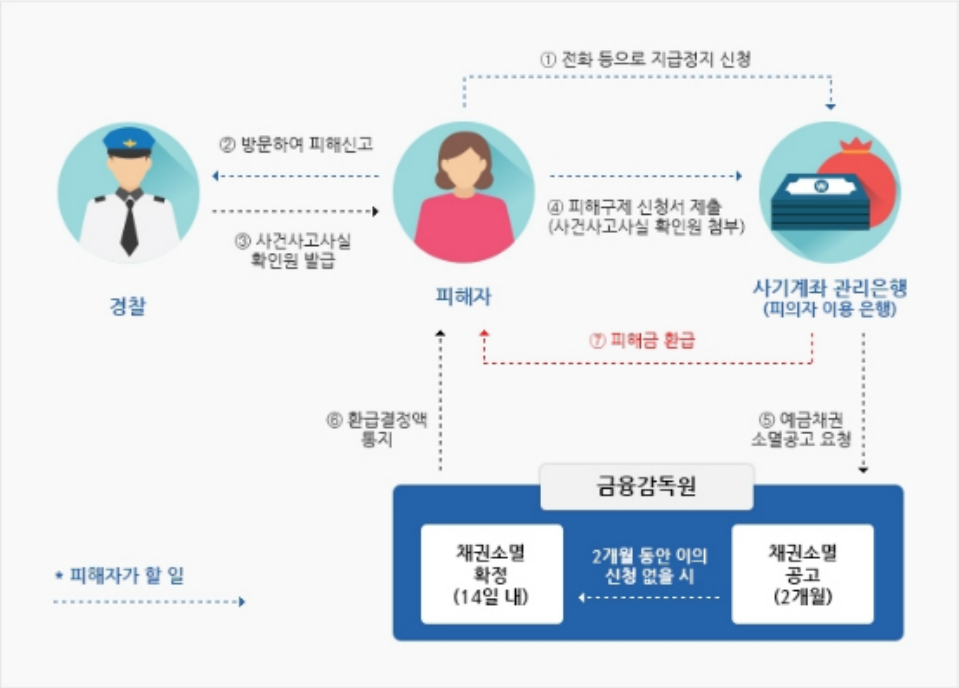
2.3.2. 대처방안

파밍(Pharming) 피해 대처방법

지급정지 및 피해금 환급 신청

▪ 파밍 사기로 인해 금전적인 피해가 발생한 피해자는 다음과 같이 지급정지 및 환급신청을 합니다[「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법」 제3조 및 사이버범죄 신고시스템(https://ecrm.police.go.kr/)-기타 안내-피해자 구제 제도 참조].

1. 피해자는 범죄에 이용된 계좌를 관리하는 금융회사에 전화로 지급정지를 신청합니다. 전화로 하는 경우 3일 이내에 지급정지에 필요한 서류(사건사고사실확인원, 피해구제신청서)를 제출해야 합니다.
2. 피해자는 거주지 관할경찰서(사이버수사팀)에 방문하여 피해사실을 신고하고 신고를 접수한 경찰관에게 요청하여 '사건사고사실확인원'을 발급받습니다.
3. 피해자는 지급정지를 신청한 금융회사를 방문하여 '피해구제신청서'를 작성해서 '사건사고사실확인원'과 함께 제출합니다.
4. 금융회사는 신청된 계좌에 대하여 지급정지 조치를 취하고 금융감독원에 예금채권 소멸공고를 요청합니다.
5. 금융감독원은 2개월간 채권소멸공고를 하고 이 기간 내에 이의신청이 없으면 채권소멸을 확정하고 환급결정액을 금융회사에 통지합니다.
6. 위 환급결정액이 금융회사에 통지되면 금융회사에서는 피해자에게 해당 금액을 환급하여 주게 됩니다(통상 2~3일 소요).



<출처: 사이버범죄 신고시스템(https://ecrm.police.go.kr/)-기타 안내-피해자 구제 제도>

※ 지급정지·피해신고

경찰청 국번없이 ☎112 / 금융회사 콜센터

※ 피해상담 및 피해금 환급안내

금융감독원 국번없이 ☎1332

악성프로그램에 감염된 PC치료

▪ 은행 등 금융회사 홈페이지 접속 시 다음과 같은 증상이 나타나면 이용 중인 PC가 악성프로그램에 감염되었을 가능성이 있으므로 PC를 치료해야 합니다.

※ 악성프로그램에 감염된 예시

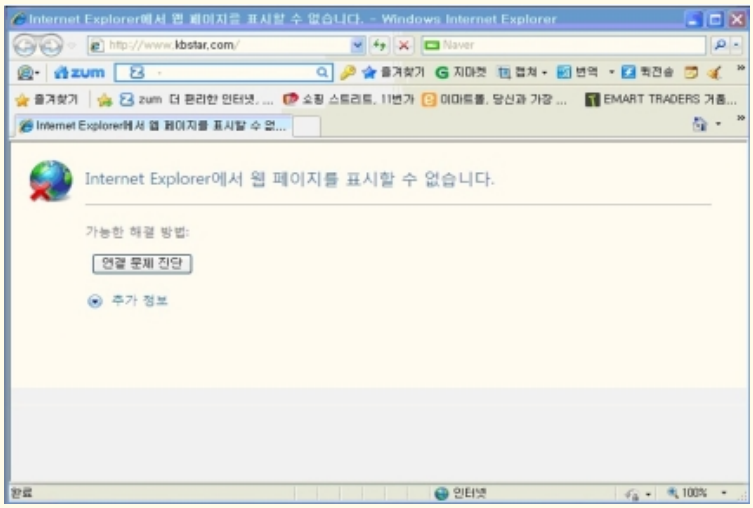
- 금융회사 홈페이지와 유사한 모습의 피싱사이트로 연결되어 보안카드번호 등의 금융거래정보를 입력하도록 유도하는 경우



- 파밍사이트 차단 안내 페이지로 연결되는 경우



- 웹페이지 연결 실패 오류가 뜨는 경우



<출처 : 한국인터넷진흥원 보호나라(www.boho.or.kr), 자료실-공지사항 참조>

파밍(Pharming) 피해 관련 처벌

전자거래에서의 전자적 침해행위에 대한 처벌

▪ 누구든지 다음의 어느 하나에 해당하는 행위를 하여서는 안 됩니다(「전자금융거래법」 제21조의4).

▹ 접근권한을 가지지 않은 자가 전자금융기반시설에 접근하거나 접근권한을 가진 자가 그 권한을 넘어 저장된 데이터를 조작·파괴·은닉 또는 유출하는 행위

▹ 전자금융기반시설에 대하여 데이터를 파괴하거나 전자금융기반시설의 운영을 방해할 목적으로 컴퓨터 바이러스, 논리폭탄 또는 메일폭탄 등의 프로그램을 투입하는 행위

▹ 전자금융기반시설의 안정적 운영을 방해할 목적으로 일시에 대량의 신호, 고출력 전자기파 또는 데이터를 보내거나 부정한 명령을 처리하도록 하는 등의 방법으로 전자금융기반시설에 오류 또는 장애를 발생하게 하는 행위

※ "전자금융기반시설"이란 전자금융거래에 이용되는 정보처리시스템 및 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제1호에 따른 정보통신망을 말합니다(「전자금융거래법」 제2조제21호).

※ "전자적 침해행위"란 해킹, 컴퓨터 바이러스, 논리폭탄, 메일폭탄, 서비스 거부 또는 고출력 전자기파 등의 방법으로 전자금융기반시설을 공격하는 행위를 말합니다(「전자금융거래법」 제2조제22호).

※ "정보통신망"이란 「전기통신사업법」 제2조제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체제를 말합니다(「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제1호).

▪ 이를 위반하여 전자적 침해행위를 한 자는 10년 이하의 징역 또는 1억원 이하의 벌금에 처해집니다(「전자금융거래법」 제49조제1항).

정보통신망 침입에 대한 처벌

▪ 누구든지 정당한 접근권한 없이 또는 허용된 접근권한을 넘어 정보통신망에 침입해서는 안 됩니다(「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제48조제1항).

※ 정당한 접근권한 없이 정보통신망에 침입한 행위에 관한 판례

A 회사가 운영하는 웹사이트에서 무료프로그램을 다운로드받을 경우 악성프로그램이 숨겨진 특정프로그램을 필수적으로 컴퓨터 내에 설치하도록 유도하는 방법으로 정당한 접근권한 없이 또는 허용된 접근권한을 초과하여 악성프로그램이 설치된 것은 컴퓨터 사용자들이 사용하는 정보통신망에 침입한 행위에 해당합니다(대법원 2013. 3. 28. 선고 2010도14607 판결 참조).

▪ 이를 위반하여 정보통신망에 침입한 경우는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처해집니다(「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제71조제1항제11호).

악성프로그램 유포에 대한 처벌

▪ 누구든지 정당한 사유 없이 정보통신시스템, 데이터 또는 프로그램 등을 훼손·멸실·변경·위조하거나 그 운용을 방해할 수 있는 프로그램을 전달 또는 유포해서는 안 됩니다(「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제48조제2항).

▪ 이를 위반하여 악성프로그램을 전달 또는 유포한 경우는 7년 이하의 징역 또는 7천만원 이하의 벌금에

처해집니다(「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제70조의2).

해킹을 통한 정보 등의 훼손 및 누설금지

▪ 누구든지 정보통신망에 의해 처리·보관 또는 전송되는 타인의 정보를 훼손하거나 타인의 비밀을 침해·도용 또는 누설해서는 안 됩니다(「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제49조).

▪ 이를 위반하여 타인의 정보를 훼손하거나 타인의 비밀을 침해·도용 또는 누설한 경우는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처해집니다(「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제71조제1항제14호).

2.4. 메모리해킹(Memory Hacking)

2.4.1. 피해사례

메모리해킹(Memory Hacking) 피해 대처방법

지급정지 신청

▪ 메모리해킹 사기로 인해 금전적인 피해가 발생한 피해자는 신속히 경찰서나 금융회사 콜센터를 통해 지급정지 요청을 해야 합니다(「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법」 제3조 참조).

> ※ **지급정지·피해신고**
>
> 경찰청 국번 없이 ☎112 / 금융회사 콜센터
>
> ※ **피해상담**
>
> 금융감독원 국번없이 ☎1332

악성프로그램에 감염된 PC 치료

▪ 은행 등 금융회사 홈페이지 접속 시 이상 증상이 나타나면 이용 중인 PC가 악성프로그램에 감염되었을 가능성이 있으므로 PC를 치료해야 합니다.

금융회사 등의 해킹에 따른 피해 보상

▪ 금융회사 또는 전자금융업자는 전자금융거래를 위한 전자적 장치 또는 정보통신망(「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제1호)에 침입하여 거짓이나 그 밖의 부정한 방법으로 획득한 접근매체의 이용으로 발생한 사고로 인해 이용자에게 손해가 발생한 경우 그 손해를 배상할 책임이 있습니다. 다만, 이용자의 고의나 중대한 과실이 있는 경우로서 그 책임의 전부 또는 일부를 이용자가 부담하도록 하는 취지의 약정을 미리 체결한 경우 등에는 책임의 전부 또는 일부를 이용자가 부담하게 할 수 있습니다(「전자금융거래법」 제9조제1항제3호 및 제2항 참조).

메모리해킹 피해 관련 처벌

악성프로그램 유포에 대한 처벌

▪ 누구든지 정당한 사유 없이 정보통신시스템, 데이터 또는 프로그램 등을 훼손·멸실·변경·위조하거나 그 운용을 방해할 수 있는 프로그램을 전달 또는 유포해서는 안 됩니다(「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제48조제2항).

▪ 이를 위반하여 악성프로그램을 전달 또는 유포한 경우는 7년 이하의 징역 또는 7천만원 이하의 벌금에

처해집니다(「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제70조의2).

해킹을 통한 정보 등의 훼손 및 누설 금지

▪ 누구든지 정보통신망에 의해 처리·보관 또는 전송되는 타인의 정보를 훼손하거나 타인의 비밀을 침해·도용 또는 누설해서는 안 됩니다(「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제49조).

▪ 이를 위반하여 타인의 정보를 훼손하거나 타인의 비밀을 침해·도용 또는 누설한 경우는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처해집니다(「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제71조제1항제14호).

> ※ 더 자세한 피해구제 방법은 이 콘텐츠의 <전자금융범죄 유형별 피해사례 및 대처방안-파밍(Pharming)-대처방안>에서 확인할 수 있습니다.

3. 전자금융범죄 피해구제

3.1. 피해금 환급

3.1.1. 피해구제 신청

피해구제 신청 방법

피해자의 구제신청

▪ 피해자는 전기통신금융사기로 인하여 재산상의 피해를 입은 자로서(이하 “피해자”라 함), 피해자산을 송금·이체 또는 이전한 계좌등을 관리하는 금융회사등 또는 사기이용계좌등을 관리하는 금융회사등에 대하여 사기이용계좌등의 지급정지 등 전기통신금융사기의 피해구제를 신청할 수 있습니다(「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법」 제2조제3호 및 제3조제1항).

※ “금융회사등”이란 다음의 어느 하나에 해당하는 기관을 말합니다. 다만, 15. 기관은 「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법」 제2조의4제1항제1호·제2항, 제13조의4, 제18조제1항제2호 및 「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법 시행령」 제11조의2제2항을 적용하는 경우로 한정하며, 16. 기관은 「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법」 제2조의4제1항제1호·제2항, 제18조제1항제2호 및 「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법 시행령」 제11조의2제2항을 적용하는 경우로 한정합니다.(「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법」 제2조제1호 및 「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법 시행령」 제2조).

1. 「은행법」에 따른 은행
2. 「한국산업은행법」에 따른 한국산업은행
3. 「중소기업은행법」에 따른 중소기업은행
4. 「한국수출입은행법」에 따른 한국수출입은행
5. 「자본시장과 금융투자업에 관한 법률」에 따른 투자매매업자·투자중개업자·집합투자업자·신탁업자·증권금융회사·종합금융회사 및 명의개서대행회사
6. 「상호저축은행법」에 따른 상호저축은행과 그 중앙회
7. 「농업협동조합법」에 따른 농업협동조합과 그 중앙회
8. 「수산업협동조합법」에 따른 수산업협동조합과 그 중앙회
9. 「신용협동조합법」에 따른 신용협동조합과 그 중앙회
10. 「새마을금고법」에 따른 금고와 그 중앙회
11. 「보험업법」에 따른 보험회사
12. 「우체국예금·보험에 관한 법률」에 따른 체신관서
13. 「농업협동조합법」에 따른 축산업협동조합
14. 「산림조합법」에 따른 산림조합과 그 중앙회
15. 「여신전문금융업법」에 따른 여신전문금융회사(신기술사업금융전문회사는 제외함)
16. 「대부업 등의 등록 및 금융이용자 보호에 관한 법률」 제3조제2항제5호에 따라 등록한 대부업자 중 직전

사업연도말 기준으로 500억원 이상인 자(「대부업 등의 등록 및 금융이용자 보호에 관한 법률 시행령」 제6조의6제1항제2호)

17. 「가상자산 이용자 보호 등에 관한 법률」 제2조제4호의 가상자산시장을 개설·운영하는 같은 조 제2호의 가상자산사업자

18. 그 밖에 「가상자산 이용자 보호 등에 관한 법률」 제2조제2호의 가상자산사업자로서 「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법 시행령」으로 정하는 기관

※ "사기이용계좌등"이란 전기통신금융사기에 이용된 다음의 어느 하나에 해당하는 계좌 또는 계정(가상자산거래소가 가상자산의 거래·보관 등의 서비스 제공을 위해 「가상자산 이용자 보호 등에 관한 법률」 제2조제3호의 이용자에게 부여한 고유식별번호를 말함)을 말합니다(「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법」 제2조제4호).

가. 피해자의 자금이 송금·이체된 계좌

나. 피해자가 교부했거나 피해자의 계좌에서 출금된 자금이 입금된 계좌

다. 피해자의 가상자산이 이전된 계정

라. 가.부터 다.까지의 계좌 또는 계정으로부터 자금 또는 가상자산의 이전에 이용된 계좌 또는 계정

※ "피해자산"이란 전기통신금융사기로 인하여 피해자의 계좌 또는 계정(이하 "계좌등"이라 함)에서 사기이용계좌등으로 송금·이체·이전된 금전 또는 가상자산, 피해자가 교부한 금전, 피해자가 가상자산이 저장된 수단을 교부한 경우에는 그 가상자산 또는 피해자의 계좌에서 출금된 금전을 말합니다(「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법」 제2조제5호).

피해구제 신청 절차

피해구제 신청서 등의 제출

▪ 피해구제를 신청하려는 피해자는 피해구제신청서(「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법 시행령」 별지 제1호서식)에 피해자의 신분증 사본을 첨부하여 해당 금융회사등에 제출하여야 합니다(「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법」 제3조제5항 및 「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법 시행령」 제3조제1항 본문).

▪ 다만, 긴급하거나 부득이한 사유가 있는 경우에는 전화 또는 구술로 신청할 수 있습니다(「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법 시행령」 제3조제1항 단서).

▹ 이에 따라 피해구제의 신청을 받은 금융회사등은 피해자의 인적사항, 피해내역 및 신청사유 등을 확인하여야 합니다. 이 경우 피해구제를 신청한 피해자는 그 신청한 날부터 3일 이내에 피해구제신청서(「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법 시행령」 별지 제1호서식)를 해당 금융회사등에 제출하여야 합니다(「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법 시행령」 제3조제2항).

▪ 피해구제의 신청을 받은 금융회사등은 필요하다고 인정하는 경우에는 피해자에게 수사기관의 피해신고확인서 등 관련 자료의 제출을 요청할 수 있습니다(「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법 시행령」 제3조제3항).

지급정지의 요청

▪ 피해구제의 신청 및 지급정지의 요청을 받은 금융회사등은 다른 금융회사등의 사기이용계좌등으로 피해자산이 송금·이체 또는 이전된 경우 해당 금융회사등에 대하여 필요한 정보를 제공하고 지급정지를

요청하여야 합니다(「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법」 제3조제4항).

위반 시 제재

▪ 거짓으로 피해구제를 신청하거나 지급정지를 요청한 경우는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처해집니다(「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법」 제16조제1호 및 제2호).

3.1.2. 지급정지

지급정지 조치

금융회사의 지급정지 조치

▪ 금융회사는 다음의 어느 하나에 해당하는 경우 거래내역 등의 확인을 통하여 전기통신금융사기의 사기이용계좌로 의심할 만한 사정이 있다고 인정되면 해당 사기이용계좌의 전부에 대하여 지급정지 조치를 하여야 합니다(「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법」 제4조제1항).

- 피해구제 신청 또는 지급정지 요청이 있는 경우
- 수사기관 또는 금융감독원 등으로부터 사기이용계좌로 의심된다는 정보제공이 있는 경우
- 피해의심거래계좌에 대한 본인확인조치 결과 사기이용계좌로 추정되는 경우
- 「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법」 제15조제3항에 따라 사기이용계좌에 관한 정보를 제공받은 경우

> ※ “금융회사”란 「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법」 제2조제1호의 어느 하나에 해당하는 기관을 말합니다.
>
> ※ “사기이용계좌”란 전기통신금융사기로 인하여 피해자의 자금이 송금·이체된 계좌, 피해자가 교부하였거나 피해자의 계좌에서 출금된 자금이 입금된 계좌 및 해당 계좌로부터 자금의 이전에 이용된 계좌를 말합니다(「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법」 제2조제4호).

금융회사의 지급정지 조치에 대한 통지 및 공시

▪ 금융회사는 지급정지 조치를 한 경우 지체 없이 다음의 사항을 통지 및 공시(14일 이상)하여야 합니다(「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법 시행령」 제5조제2항).

- 지급정지의 일시, 사유 및 금액 등에 관한 사항
- 지급정지와 관련된 점포, 예금종별 및 계좌번호 등 지급정지 된 사기이용계좌에 관한 사항
- 지급정지를 요청한 금융회사에 관한 사항
- 사기이용계좌의 잔액이 1만원 금액 이하인 경우라도 피해자가 지급정지의 통지를 받은 날부터 30일 이내에 금융회사에 채권소멸절차의 개시를 요청한 경우

▪ 금융회사는 지급정지 조치를 한 경우 지체 없이 다음의 자에게 해당 지급정지 조치에 관한 사항을 통지하여야 합니다. 다만, 지급정지된 사기이용계좌의 명의인(이하 “명의인”이라 함)의 소재를 알 수 없는 경우에는 금융회사의 인터넷 홈페이지 등에 지급정지 조치에 관한 사실을 공시하여야 합니다(「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법」 제4조제2항).

- 명의인
- 피해구제신청을 한 피해자
- 「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법」 제3조제3항 또는 제6조제2항에 따라 금융회사에 통지된 피해자(수사기관의 통지가 있는 때에 통지)
- 피해금을 송금·이체한 계좌를 관리하는 금융회사
- 금융감독원
- 수사기관(정보제공을 한 경우, 지급정지를 요청한 경우만 해당)

> ※ "피해금"이란 전기통신금융사기로 인하여 피해자의 계좌에서 사기이용계좌로 송금·이체된 금전, 피해자가 교부한 금전 또는 피해자의 계좌에서 출금된 금전을 말합니다(「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법」 제2조제5호).

지급정지 이후 압류 금지

▪ 누구든지 지급정지가 된 사기이용계좌의 채권 전부 또는 일부와 관련하여 손해배상·부당이득반환청구소송 등의 제기, 민사집행법에 따른 압류·가압류 또는 가처분의 신청, 국세징수법에 따른 체납절차의 개시 및 질권(質權)의 설정 행위를 할 수 없습니다(「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법」 제4조의2제1항 본문).

3.1.3. 채권소멸

채권소멸 개시

채권소멸절차의 개시 공고의 요청

▪ 금융회사등은 지급정지 조치를 행한 경우 지체 없이 금융감독원에 명의인의 채권이 소멸되는 절차(이하 "채권소멸절차"라 함)를 개시하기 위한 공고를 요청하여야 합니다. 다만, 명의인의 채권 전부 또는 일부가 다음의 어느 하나에 해당하는 경우에는 그렇지 않으며, 「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법」 제3조제2항에 따른 지급정지 요청에 따라 지급정지 조치를 행한 경우에는 「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법」 제3조제3항에 따른 통지가 있는 때에 공고를 요청해야 합니다(「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법」 제5조제1항 및 「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법 시행령」 제6조제2항).

- 지급정지 조치를 하기 전에 손해배상·부당이득반환 등의 청구소송이 제기되어 법원에 계속(係屬) 중인 경우
- 지급정지 조치를 하기 전에 「민사집행법」에 따른 압류·가압류 또는 가처분의 명령이 집행된 경우
- 지급정지 조치를 하기 전에 「국세징수법」에 따른 체납절차가 개시된 경우
- 지급정지 조치를 하기 전에 질권(質權)이 설정된 경우
- 지급정지된 후에 명의인과 피해자 간 채무부존재확인·부당이득반환청구 소송 등이 제기되어 법원에 계속 중인 경우
- 지급정지가 이루어진 사기이용계좌등의 잔액이 계좌의 경우 1만원 이하이거나, 계정의 경우 해당 계정에 존재하는 가상자산의 종류별 환산금액의 합계액이 1만원 이하인 경우(다만, 피해자가 지급정지의 통지를 받은 날부터 30일 이내에 금융회사에 채권소멸절차의 개시를 요청한 경우에는 그렇지 않음)

채권소멸절차 개시 공고 요청시 제출서류

▪ 금융회사가 채권소멸절차의 개시공고를 요청하는 경우에는 채권소멸절차 개시공고요청서(「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법 시행령」 별지 제3호서식)에 다음의 구분에 따른 서류를 첨부하여 금융감독원에 제출해야 합니다(「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법」 제5조제1항 본문 및 「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법 시행령」 제6조제1항).

- 피해구제 신청에 따라 지급정지 조치를 한 경우
  - √ 피해자의 피해구제 신청서류 사본
  - √ 금융회사등의 지급정지 요청서류 사본
  - √ 금융회사등의 통지 또는 공시 관련 서류 사본
- 지급정지 요청에 따라 지급정지 조치를 한 경우
  - √ 수사기관의 지급정지 요청서류 사본
  - √ 수사기관의 피해자·피해자산 통지 서류 사본 통지 서류 사본
  - √ 금융회사등의 지급정지 요청서류 사본
  - √ 금융회사등의 통지 또는 공시 관련 서류 사본
- 채권소멸절차 개시의 공고 요청(「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법」 제5조제2항)에 따른 통지 또는 공시 관련 서류의 사본

채권소멸절차 개시 공고 및 통지

▪ 금융감독원은 채권소멸절차 개시의 공고 요청을 받은 경우 지체 없이 금융감독원의 인터넷 홈페이지에 2개월간 다음의 사항을 공고하여야 합니다(「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법」 제5조제2항 및 「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법 시행령」 제6조제3항).

- 전기통신금융사기와 관련하여 채권소멸절차가 개시되었다는 취지
- 사기이용계좌등과 관련된 금융회사등, 점포 및 예금 등의 종별, 계좌번호 및 계정정보
- 명의인의 성명 또는 명칭
- 공고 전 피해구제 신청에 따라 채권소멸대상에 해당하는 채권의 금액 또는 가상자산의 종류 및 수량
- 채권소멸절차 개시 이후의 피해구제 신청의 방법 및 절차
- 명의인의 이의제기 방법 및 절차
- 전자금융거래제한대상자로 지정되었다는 취지와 이의제기 방법 및 절차

▪ 금융감독원은 채권소멸절차의 개시에 관한 공고를 한 경우 지체 없이 명의인에게 채권소멸절차의 개시에 관한 사실을 통지해야 합니다. 다만, 명의인의 소재를 알 수 없는 경우에는 채권소멸절차의 개시 공고로 명의인에 대한 통지가 이루어진 것으로 봅니다(「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법」 제5조제3항).

채권소멸절차 개시 이후의 피해구제 신청

※ 채권소멸절차 개시 이후에 피해구제를 신청할 수 없나요

Q. 저는 보이스피싱 사기를 당한 피해자인데요. 피해구제 신청을 하려고 보니까 이미 해당 계좌의 채권소멸절차개시가 공고 중이더라고요. 이런 경우 저는 피해자로 인정도 못 받고 피해금을 환급받지 못하는 건가요

A. 채권소멸절차 개시 공고 이후라도 피해구제신청을 할 수 있습니다.

채권소멸절차 개시의 공고가 이루어진 사기이용계좌등의 피해자로서 채권소멸절차 개시의 공고 전에 피해구제를 신청하지 않은 경우에도 해당 금융회사등에 피해구제 신청을 할 수 있습니다. 이때, 피해구제신청은 이미 진행 중인 채권소멸절차 개시의 공고일부터 2개월 이내에 하면 됩니다(「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법」 제6조제1항).

수사기관은 채권소멸절차 개시의 공고가 이루어진 사기이용계좌등과 관련한 추가 피해자와 피해자산을 공고일로부터 2개월 이내에 금융회사등에 통지할 수 있습니다(「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법」 제6조제2항).

금융회사등은 피해구제 신청에 대하여 해당 거래내역 등을 확인하여 피해자로 인정된다고 판단하는 경우 또는 수사기관의 통지가 있는 경우에는 금융감독원에 해당 피해자산에 대한 채권소멸절차의 개시 공고를 요청해야 하고 금융감독원은 지체 없이 해당 사항을 공고해야 합니다(「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법」 제6조제3항 및 제4항).

만약, 거짓으로 피해구제를 신청하면 3년 이하의 징역 또는 3천만원 이하의 벌금에 처해질 수 있으니(「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법」 제16조제3호) 유의하세요!

채권의 소멸

채권소멸의 효력

▪ 명의인의 채권(채권소멸절차 개시 공고가 이루어진 금액등으로 한정함)은 최초의 채권소멸절차 개시의 공고일부터 2개월이 경과하면 소멸합니다(「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법」 제9조제1항).

채권소멸의 통지

▪ 금융감독원은 명의인의 채권이 소멸된 경우 다음의 사항을 해당 명의인, 피해구제를 신청한 피해자(「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법」 제3조 및 제6조) 및 관련 금융회사등에게 통지하여야 합니다. 다만, 명의인의 소재를 알 수 없는 경우에는 금융감독원 및 해당 금융회사등의 인터넷 홈페이지 등에 해당 사실을 공시하여야 합니다(「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법」 제9조제2항).

- 해당 명의인의 채권이 소멸되었다는 사실
- 소멸되는 채권의 금액등
- 그 밖에 「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법 시행령」으로 정하는 사항

3.1.4. 피해환급금 결정·지급 및 소멸채권 환급 청구

피해환급자산 결정·지급

피해환급자산 결정

▪ 피해환급자산은 총피해금액등이 소멸채권 금액등을 초과하는 경우 소멸채권 금액등에 각 피해자의 피해금액등의 총피해금액등에 대한 비율을 곱한 금액등으로 하며, 그 외의 경우에는 해당 피해금액등으로 합니다(「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법」 제10조제2항).

※ “피해환급자산” 이란 피해자산을 환급하기 위하여 소멸된 채권을 기초로 하여 피해환급자산의 결정·지급에 따라 산정되어 금융회사등이 피해자에게 지급하는 금전 또는 가상자산을 말한다(「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법」 제2조제6호).

▪ 금융감독원은 피해환급자산의 결정을 위하여 금융회사등에 필요한 자료의 제출을 요구할 수 있습니다(「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법」 제10조제3항).

피해환급자산 지급

▪ 금융감독원은 채권이 소멸된 날부터 14일 이내에 피해환급자산을 지급받을 자 및 그 금액등을 결정하여 그 내역을 피해구제를 신청한 피해자 및 금융회사등에 통지하여야 하고, 통지를 받은 금융회사등은 지체 없이 피해환급자산을 피해자에게 지급하여야 합니다(「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법」 제10조제1항).

▪ 위에도 불구하고 위에 따라 피해환급자산이 가상자산이고 피해자가 요청하는 경우에는 가상자산거래소가 해당 가상자산을 매도한 후 그 대금을 피해자에게 금전으로 지급할 수 있습니다(「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법」 제10조제4항 본문).

※ 이 경우 가상자산거래소는 가상자산 이용자 보호업무를 수행할 수 있는 「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법 시행령」으로 정하는 기관에 해당 가상자산의 매도를 요청할 수 있습니다(「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법」 제10조제4항 단서).

▪ 금융회사등이 피해환급자산을 지급하는 경우에는 피해자가 지정하는 금융회사등의 계좌로 입금하여야 합니다(「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법」 제10조제1항 및 「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법 시행령」 제9조제1항).

▪ 피해환급자산을 지급한 금융회사등은 그 지급한 날부터 3일 이내에 해당 지급 사실을 금융감독원에 알려야 합니다(「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법 시행령」 제9조제4항).

피해환급자산을 지급받을 수 없는 자

▪ 다음의 어느 하나에 해당하는 자는 피해환급자산을 지급받을 수 없습니다(「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법」 제11조).

- 해당 전기통신금융사기로 인한 피해자산의 전부 배상이 이루어진 경우의 피해자 및 그 승계인
- 해당 전기통신금융사기 등과 관련하여 부당이득을 취한 자
- 해당 전기통신금융사기 등에 공범으로 가담하였거나 자신에게 불법원인이 있는 자
- 그 밖에 「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법 시행령」으로 정하는 자

※ 피해환급자산을 지급받고도 사기이용계좌등의 명의인을 상대로 손해배상을 청구할 수 있나요

Q. 저는 파밍 사기를 당한 후, 피해구제를 신청하여 금융회사등으로부터 피해환급자산을 지급받았습니다. 그런데 이번 사기 범행에 사기이용계좌 즉, 대포통장이 이용된 것으로 밝혀졌는데요. 다른 사람에게 통장 및 현금카드 등을 양도하는 것은 「전자금융거래법」을 위반한 행위로서 이에 따라 사기이용계좌의 주인에게도 불법행위에 따른 책임이 있다고

생각합니다. 이처럼 피해금을 환급받는 것과는 별도로 사기이용계좌 명의인에게 손해배상을 청구할 수 있을까요?

A. 「전자금융거래법」 제6조에 따라 통장, 현금카드 등과 같은 접근매체의 양도·양수하는 행위 등은 금지하고 있으며 이를 위반한 경우에는 5년 이하의 징역 또는 3천만원 이하의 벌금에 처해집니다(「전자금융거래법」 제49조제4항).

"접근매체"란 전자식 카드 및 이에 준하는 전자적 정보(비밀번호 포함), 전자서명생성정보 및 인증서(비밀번호 포함), 금융회사 또는 전자금융업자에 등록된 이용자번호, 이용자의 생체정보를 말합니다(「전자금융거래법」 제2조제10호). 여기서 말하는 '양도'에는 단순히 접근매체를 빌려주거나 일시적으로 사용하게 하는 행위는 포함되지 않지만 여러 사정을 종합적으로 고려하여 구체적 사건에 따라 개별적으로 판단됩니다.

피해자가 「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법」에 따라 금융회사등으로부터 피해환급자산을 지급받은 경우 해당 전기통신금융사기로 발생한 손해배상청구권 및 그 밖의 청구권은 환급을 받은 한도에서 소멸됩니다(「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법」 제12조).

따라서 전기통신금융사기로 인한 손해 중 「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법」에 따라 피해환급자산으로 환급받은 범위를 제외한 나머지 손해에 대해서는 손해배상을 청구할 수 있습니다

수수료의 징수

▪ 금융감독원장은 피해환급자산을 지급받은 피해자에 대하여 수수료를 받을 수 있습니다(「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법」 제14조).

▪ 수수료는 채권소멸절차 개시의 통지, 채권소멸의 통지 및 피해환급자산 지급의 통지 및 사기이용계좌의 명의인에 대한 전자금융거래 제한에 사용된 실비의 범위에서 부과됩니다(「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법」 제14조 및 「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법 시행령」 제11조제1항 본문).

▹ 다만, 피해환급자산의 규모 및 피해자의 부담능력 등을 고려하여 필요하다고 인정하는 경우에는 부과하지 않을 수 있습니다(「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법 시행령」 제11조제1항 단서).

▹ 수수료는 현금, 전자화폐 및 전자결제 등의 방법으로 납부할 수 있습니다(「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법 시행령」 제11조제2항).

소멸채권 환급

소멸채권의 환급청구

▪ 채권이 소멸된 명의인이 다음의 요건을 모두 갖춘 경우에는 금융감독원에 소멸된 채권의 환급을 청구할 수 있습니다(「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법」 제13조제1항).

▹ 해당 계좌등이 사기이용계좌등이 아니라는 사실을 소명하는 경우, 소멸될 채권의 전부 또는 일부를 명의인이 재화 또는 용역의 공급에 대한 대가로 받았거나 그 밖에 정당한 권원에 의하여 취득한 것임을 객관적인 자료로 소명하는 경우, 또는 해당 계좌등이 피해자산 편취를 위하여 이용된 계좌등이 아니라는 사실을 객관적인 자료로 소명하는 경우(「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법」 제7조제1항제1호·제2호 및 제3호)

▹ 지급정지 및 채권소멸절차에 대해 이의제기(「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법」 제7조제1항)를 하지 못한 정당한 사유가 있는 경우

3.2. 손해배상

3.2.1. 금융회사 등에 대한 손해배상 청구

금융회사 등의 손해배상 책임

손해배상 책임의 범위와 대상자

▪ 금융회사 또는 전자금융업자는 다음 어느 하나에 해당하는 사고로 인하여 이용자에게 손해가 발생한 경우에는 그 손해를 배상할 책임이 있습니다(「전자금융거래법」 제9조제1항).

1. 접근매체의 위조나 변조로 발생한 사고
2. 계약체결 또는 거래지시의 전자적 전송이나 처리 과정에서 발생한 사고
3. 전자금융거래를 위한 전자적 장치 또는 정보통신망에 침입하여 거짓이나 그 밖의 부정한 방법으로 획득한 접근매체의 이용으로 발생한 사고

※ “금융회사”란 은행, 증권금융회사, 보험회사, 상호저축은행, 농협, 수협 및 그 밖에 금융업 및 금융관련 업무를 행하는 기관이나 단체 또는 사업자 등을 뜻합니다(「전자금융거래법」 제2조제3호 및 「전자금융거래법 시행령」 제2조)

※ “전자금융업자”란 「전자금융거래법」 제28조에 따라 허가를 받거나 등록을 한 자(금융회사는 제외)를 말합니다(「전자금융거래법」 제2조제4호).

※ 보이스피싱 관련 ‘이용자의 고의나 중대한 과실’판단기준

- 「전자금융거래법」 제9조, 「전자금융거래법 시행령」 제8조 등에서 정하는 ‘고의 또는 중대한 과실’이 있는지 여부는 접근매체의 위조 등 금융사고가 일어난 구체적인 경위, 그 위조 등 수법의 내용 및 그 수법에 대한 일반인의 인식 정도, 금융거래 이용자의 직업 및 금융거래 이용경력 기타 제반 사정을 고려하여 판단해야 합니다.

- A씨는 금융기관인 B 주식회사 등에서 예금계좌를 개설하여 금융거래를 하면서 인터넷뱅킹서비스를 이용하여 왔는데, C는 전화금융사기(이른바 보이스피싱)를 통해 A에게서 취득한 금융거래정보를 이용하여 A씨 명의의 공인인증서를 재발급받아 다른 금융기관들로부터 대출서비스 등을 받은 사안에서, A가 제3자에게 접근매체인 공인인증서 발급에 필수적인 계좌번호, 계좌비밀번호, 주민등록번호, 보안카드번호, 보안카드비밀번호를 모두 알려준 점 등 제반 사정에 비추어, A의 금융거래정보 노출행위가 전자금융거래법 등에서 정한 금융사고의 발생에 이용자의 ‘중대한 과실’이 인정됩니다(대법원 2014. 1. 29. 선고 2013다86489 판결 참조)

※ 금융기관 또는 전자금융업자가 손해배상책임을 부담하는 “사고”의 의미

직접 대면하거나 의사소통을 하지 않고 전자적 장치를 통해 자동화된 방식으로 이루어지는 전자금융거래의 특성을 고려하여 일반적인 대면 거래라면 발생하지 않았을 권한 없는 제3자에 의한 거래나 이용자의 거래지시와 거래의 이행 결과 사이의 불일치로 인하여 이용자에게 손해가 발생한 경우에는 원칙적으로 금융기관 또는 전자금융업자로 하여금 손해배상책임을 지도록 하되, 예외적으로 이용자가 거래지시나 이용자 및 거래내용의 진실성과 정확성을 확보하기 위해 사용되는 접근매체를 대여하거나 누설하는 등의 경우 및 이용자가 법인인 경우로 금융기관 또는 전자금융업자가 보안절차의 수립과 준수 등 충분한 주의의무를 다한 경우에 한정하여 이용자가 책임의 전부 또는 일부를 부담하게 할 수 있도록 함으로써 전자금융거래의 안전성과 신뢰성을 확보함과 아울러 이용자를 보호하려는 데 취지가 있습니다.

따라서, 금융기관 또는 전자금융업자가 손해배상책임을 부담하는 ‘사고’는 권한 없는 제3자에 의하여 전자금융거래가 이행되거나 이용자의 거래지시가 없었음에도 전자금융거래가 이행되거나 이용자의 거래지시가 있었으나 그에 따라 전자금융거래가 이행되지 않은 경우 등을 의미합니다(대법원 2015. 5. 14. 선고 2013다69989 판결

참조).

▪ 분쟁조정 결정 사례

▹ 휴대폰 소액결제로 인한 손해배상 요구

※ 스미싱 소액결제 사기 피해를 당한 경우에는 누구에게 손해배상을 청구해야 하나요?

Q. A씨는 성명불상자로부터 '결제 인증번호와 청구금액'이 기재된 휴대폰 문자를 받고, 문자를 발신한 번호로 전화하였더니 성명불상자가 인증번호를 알려주면 결제취소 해주겠다고 하여 인증번호를 알려주었어요. 이후 게임회사에서 30만원 상당의 게임 아이템을 구입하였다며 이동통신사가 요금을 청구하여 납부하게 되면서 스미싱 사기 피해를 당했는데요. A씨는 콘텐츠 제공업자, 이동통신사와 결제대행업자에게 손해배상 청구를 하려고 하는데, 가능할까요?

A. 스미싱 사기로 모바일 결제 대금을 낸 A씨에 대해 콘텐츠 제공업자, 이동통신사와 결제대행업자 모두 손해배상을 해야 합니다.

우선, 콘텐츠 제공업자는 게임 아이템 거래 시 본인확인의무를 가지고 건전한 게임서비스 문화를 조성할 책임이 있는데, 게임 아이템을 무작위로 구매하는 불법행위를 방지할 제반 조치를 취하지 않은 데에 책임이 있으므로 공동불법행위자로서 손해배상책임이 있습니다.

또한, 이동통신사와 결제대행업자는 소비자에게 통신과금서비스를 제공하고 그에 따른 수익을 얻고 있으므로 모바일 결제에서 일어날 수 있는 사고 예방 및 차단을 위한 제반 조치를 할 책임이 있으며, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제60조 제1항 "통신과금서비스제공자는 통신과금서비스를 제공함에 있어서 통신과금서비스이용자에게 손해가 발생한 경우에 그 손해를 배상해야 한다"는 규정에 따라 이동통신사와 결제대행업자는 A씨에게 손해배상책임을 부담합니다.

<출처 : 한국소비자원, 소비자뉴스-보도자료-소비자분쟁조정위원회, 보이스피싱 모바일 소액결제 피해 배상결정 2013. 7. 15. 보도 참조>

금융회사 등의 손해배상책임 면책

이용자가 부담하는 경우

▪ 「전자금융거래법」 제9조제1항에도 불구하고 금융회사 또는 전자금융업자는 다음의 어느 하나에 해당하는 경우에는 그 책임의 전부 또는 일부를 이용자가 부담하게 할 수 있습니다(「전자금융거래법」 제9조제2항).

▹ 사고 발생에 있어서 이용자의 고의나 중대한 과실이 있는 경우로서 그 책임의 전부 또는 일부를 이용자의 부담으로 할 수 있다는 취지의 약정을 미리 이용자와 체결한 경우

▹ 법인(「중소기업기본법」 제2조제2항에 의한 소기업을 제외함)인 이용자에게 손해가 발생한 경우로 금융회사 또는 전자금융업자가 사고를 방지하기 위하여 보안절차를 수립하고 이를 철저히 준수하는 등 합리적으로 요구되는 충분한 주의의무를 다한 경우

이용자의 고의나 중대한 과실의 범위

▪ 이용자의 고의나 중대한 과실은 다음의 범위에서 전자금융거래에 관한 약관에 기재된 것에 한정합니다(「전자금융거래법」 제9조제3항 및 「전자금융거래법 시행령」 제8조).

1. 이용자가 접근매체를 제3자에게 대여하거나 그 사용을 위임한 경우 또는 양도나 담보의 목적으로 제공한 경우(선불전자지급수단이나 전자화폐를 양도하거나 담보로 제공한 경우는 제외함)

2. 제3자가 권한 없이 이용자의 접근매체를 이용하여 전자금융거래를 할 수 있음을 알았거나 쉽게 알 수 있었음에도 불구하고 접근매체를 누설하거나 노출 또는 방치한 경우

3. 금융회사 또는 전자금융업자가 「전자금융거래법」 제6조제1항에 따른 확인 외에 보안강화를 위해 전자금융거래 시 요구하는 추가적인 보안조치를 이용자가 정당한 사유 없이 거부하여 「전자금융거래법」 제9조제1항제3호에 따른 사고가 발생한 경우

4. 이용자가 위 3.에 따른 추가적인 보안조치에 사용되는 매체·수단 또는 정보에 대해 다음의 어느 하나에 해당하는 행위를 하여 「전자금융거래법」 제9조제1항제3호에 따른 사고가 발생한 경우

√ 누설·노출 또는 방치한 행위

√ 제3자에게 대여하거나 그 사용을 위임한 행위 또는 양도나 담보의 목적으로 제공한 행위

3.2.2. 가해자 등에 대한 손해배상 청구

가해자 등에 대한 손해배상 책임

민사상 손해배상 청구

▪ 전자금융범죄로 인해 피해를 입은 피해자는 가해자의 고의 또는 과실로 인한 위법행위로 손해를 입은 경우 그 불법행위를 원인으로 민사상 손해배상을 청구할 수 있습니다(「민법」 제750조 참조).

▪ 민사소송은 일반적으로 '소장의 제출 → 소장부본의 송달과 답변서의 제출 → 변론준비절차 → 변론준비기일 → 변론기일 → 판결'의 순서로 진행됩니다(「민사소송법」 제248조, 제255조, 제256조, 제280조부터 제284조까지 및 제287조).

> ※ 민사소송절차에 대한 자세한 내용은 이 사이트의 『나홀로 민사소송』에서 확인할 수 있습니다.

사기이용계좌 명의인에 대한 피해구제 신청

▪ 부당이득반환청구

▹ 전자금융범죄의 피해자는 범행에 이용된 계좌의 명의인에게 「민법」 제741조를 근거로 법률상 원인없이 타인의 재화나 노무로부터 얻은 이익, 즉 부당이득의 반환을 청구할 수 있습니다.

> ※ 명의인의 예금채권 부당이득에 대한 판단
>
> 통상의 자금이체에서 송금의뢰인과 수취인 사이에 계좌이체의 원인인 법률관계가 존재하는지 여부에 관계없이 수취인과 수취은행 사이에는 계좌이체금액 상당의 예금계약이 성립하고, 수취인이 수취은행에 대하여 계좌이체에 따른 금액 상당의 예금채권을 취득하므로, 지급인과 수취인 사이에 원인이 되는 법률관계가 존재하지 않음에도 불구하고 계좌이체에 의하여 수취인이 계좌이체금액 상당의 예금채권을 취득한 경우에는 송금의뢰인은 수취인에 대하여 위 금액 상당의 부당이득반환청구권을 가지게 되지만, 수취은행은 이익을 얻은 것이 없으므로 수취은행에 대하여는 부당이득반환청구권을 취득하지 않는다고 한 사례(대법원 2007. 11. 29. 선고 2007다51239 판결 참조)

▪ 공동불법행위에 따른 손해배상 청구

▹ 전자금융범죄에는 소위 말하는 '대포통장'을 통해 피해자의 예금을 이체받는 등의 방식으로 범행이 이루어지고

있습니다.

이와 같이 통장, 현금카드 등의 전자매체를 양도·대여하는 행위는 「전자금융거래법」 제6조제3항에서 금지하고 있는 행위로서 전자금융범죄의 피해자는 사기이용계좌 명의인에게 「전자금융거래법」을 위반하여 전자금융범죄를 용이하게 한 점을 근거로 하여 「민법」 제760조에 따른 공동불법행위책임을 청구할 수 있습니다.

※ 공동불법행위의 성립

수인이 공동하여 타인에게 손해를 가하는 「민법」 제760조의 공동불법행위에 있어서 행위자 상호간의 공모는 물론 공동의 인식을 필요로 하지 아니하고, 다만 객관적으로 그 공동행위가 관련 공동되어 있으면 족하고 그 관련 공동성 있는 행위에 의하여 손해가 발생함으로써 그에 대한 배상책임을 지는 공동불법행위가 성립한다. 공동불법행위에 있어 방조라 함은 불법행위를 용이하게 하는 직접·간접의 모든 행위를 가리키는 것으로서 형법과 달리 손해의 전보를 목적으로 하여 과실을 원칙적으로 고의와 동일시하는 민법의 해석으로서는 과실에 의한 방조도 가능하다고 할 것이며, 이 경우의 과실의 내용은 불법행위에 도움을 주지 않아야 할 주의의무가 있음을 전제로 하여 이 의무에 위반하는 것을 말합니다(대법원 2009. 4. 23. 선고 2009다1313 판결 참조).

※ 공동불법행위에 따른 손해배상청구

A씨는 성명불상자에게 A씨의 명의로 개설된 통장을 양도할 당시 그 통장이 B씨와 같은 불특정 다수인들을 기망한 다음 그들로부터 입금을 하게 하여 그 돈을 편취하는 이른바 '보이스피싱'에 사용될 수 있음을 충분히 예견할 수 있었다고 보이고, 비록 A씨가 '보이스피싱'의 범죄행위에 적극적으로 가담하지 않았다고 하더라도 적어도 A씨는 통장을 양도함으로써 위와 같은 범죄행위를 용이하게 하여 이를 도운 것이므로, A씨는 「민법」 제760조에 따라 공동불법행위자로서 그 손해를 배상할 책임이 있습니다(서울동부지법 2011.3.28. 선고 2010가단50237 판결 참조).

형사상 손해배상 청구

▪ 전자금융범죄로 인해 피해를 입은 피해자는 별도로 민사소송상 손해배상 청구를 하지 않더라도 해당 사건의 사기와 공갈의 죄에 대한 형사공판 절차에서 피고인에 대해 유죄판결이 선고될 경우 배상명령을 신청하여 피고인으로부터 범죄행위로 인하여 발생한 손해를 배상받을 수 있습니다(「형법」 제39장 참조).

※ 제1심 또는 제2심의 형사공판 절차에서 사기와 공갈의 죄로 유죄판결을 선고할 경우에 법원은 직권으로 또는 피해자나 그 상속인의 신청에 의해 피고사건의 범죄행위로 인해 발생한 직접적인 물적(物的) 피해, 치료비 손해 및 위자료의 배상을 명할 수 있는데 이를 "배상명령"이라고 합니다(「소송촉진 등에 관한 특례법」 제25조제1항).

※ 배상명령제도에 관한 자세한 내용은 이 사이트 『범죄피해자』 콘텐츠의 <형사절차에서 보호배상배상명령>에서 확인할 수 있습니다.

※ 보이스피싱에 사용된 통장명의자의 법적 책임 유무

A씨가 성명불상자의 말에 속아 본인 명의의 통장사본, 현금카드 및 비밀번호를 건네주었는데, 성명불상자가 위

접근매체를 전화금융사기 범행에 사용한 사안에서, 전화금융사기 범행에 대한 상당인과관계를 인정하여 A에게 과실에 의한 방조책임을 지우기 위해서는, A가 접근매체를 성명불상자에게 넘겨주었다는 사정만으로는 부족하고, A씨가 성명불상자에게 접근매체를 넘겨줄 때 이를 통하여 위 범행과 같은 불법행위에 해당하는 거래가 이루어지며 접근매체가 불법행위를 용이하게 한다는 점에 관하여 예견할 수 있었다는 사정이 인정되어야 합니다(대법원 2014. 12. 24. 선고 2013다98222 판결 참조).

※ 은행이 공인인증서 재발급에 있어 이용자에게 통지할 주의의무 유무

A씨가 금융기관인 B 주식회사 등에서 예금계좌를 개설하여 금융거래를 하면서 인터넷뱅킹서비스를 이용하여 왔는데, C가 전화금융사기(이른바 보이스피싱)를 통하여 A에게서 취득한 금융거래정보를 이용하여 A 명의의 공인인증서를 재발급받아 다른 금융기관들로부터 대출서비스 등을 받은 사안에서, A가 제3자에게 접근매체인 공인인증서 발급에 필수적인 계좌번호, 계좌비밀번호, 주민등록번호, 보안카드번호, 보안카드비밀번호를 모두 알려준 점 등 제반 사정에 비추어, A의 금융거래정보 노출행위가 전자금융거래법 등에서 정한 금융사고의 발생에 이용자의 '중대한 과실'이 있는 경우라 인정됩니다.

B 은행에게 공인인증서의 재발급에 있어서 A에게 이를 문자메시지 등을 이용하여 통지할 주의의무가 있다고 할 수 없고 오히려 문자메시지 등을 이용한 통지는 B 은행이 이용자의 요청에 따라 제공하는 서비스로 보이는데 A는 인터넷뱅킹서비스 신청 당시 보안 SMS 신청을 하지 아니하였으며, 설령 B은행에게 그러한 주의의무가 있다고 하더라도 이를 이행하지 아니함으로써 이 사건 금융사고가 발생하였다고 할 수 없다고 봅니다(대법원 2014. 1. 29. 선고 2013다86489 판결 참조).

3.3. 피해자 지원

3.3.1. 피해자 긴급자금 금융지원

보이스피싱 등에 의한 금융피해를 입은 취약계층은 긴급자금을 대출받을 수 있습니다.

새희망힐링론

▪ 신용회복위원회는 금융회사, 금융업협회 및 금융감독원의 법인카드 포인트로 마련한 사회 공헌기금을 기부 받아 금융 관련 피해로 인해 생계유지가 어려운 서민·취약계층에게 긴급자금을 대출하여 생활안정을 돕기 위한 프로그램인 "새희망힐링론"을 운영하고 있습니다(신용회복위원회, 금융과 생활-소액금융-소액대출-상품안내-특별대출-새희망 힐링론 참조)

보이스피싱 등에 의한 금융피해를 입은 취약계층으로서 다음 요건에 해당하는 사람

▪ 연소득 4천만원 이하로서 개인신용평점이 하위 100분의 20 이하인 사람(연소득 2천만원 이하인 경우 신용평점 무관)

▪ 금융피해자 : 보이스피싱, 불법사금융, 저축은행 후순위채권, 무인가 투자자문 및 선물업자 관련, 펀드 불완전판매 관련 피해자 및 보험사고 사망자 유자녀

<출처 : 신용회복위원회, 금융과 생활-소액금융-소액대출-상품안내-특별대출-새희망 힐링론 참조>

구분	조건
지원한도	금융피해 범위 내에서 최대 5백만원
대출내용	생활안정자금, 학자금
상환방법	2년 거치 3년 원리금균등 분할상환(최장 5년)
금 리	연3%(원리금 24개월 이상 성실납부 시 2%) ※ 다만, 금융사기피해 취약계층(다문화가족, 북한이탈주민) 지원시 우대금리(연 3%→연 2.5%) 적용

<출처 : 신용회복위원회, 금융과 생활-소액금융-소액대출-상품안내-특별대출-새희망 힐링론 참조>

새희망힐링론 신청

- 새희망힐링론을 신청할 때에는 다음의 서류를 제출해야 합니다.
  - 주민등록등본(최근 2개월 이내 발급분), 신분증
  - 소득증빙서류
    1. 급여명세서(3개월분) 또는 통장사본
    2. 근로소득원천징수영수증 또는 근로계약서
    3. 소득확인서(사업주확인용)
  - 금융피해내용 및 입증서류

구분	금융피해내용	증빙서류	발급기관
보이스피싱 피해자	전기통신금융사기로 인한 개인정보유출 등으로 자금을 송금·이체하여 발생한 피해	피해신고확인서 사건사고접수 확인원 법원 판결문 중 택1	경찰청 법원
불법사금융 피해자	대부업체의 불법추심·법정금리 초과 부당 등으로 발생한 피해	피해신고확인서 사건사고접수 확인원 법원 판결문 중 택1	경찰청 법원
저축은행 후순위채 피해자	저축은행 후순위 채권을 매입·투자하였으나 해당 금융회사의 영업정지·파산등으로 발생한 피해	피해신고확인서 사건사고접수 확인원 법원 판결문 중 택1	해당기관 법원
펀드 불완전판매 피해자	펀드 불완전 판매로 입은 피해	분쟁중임을 확인할 수 있는 서류 법원 판결문 중 택1	금감원 또는 한국소비자원 법원 등
무인가투자 자문 및 선물업자 관련 피해자	무인가 또는 허가 받지 않은 자를 통한 투자 등 유사수신 행위 등으로 발생한 피해	피해신고확인서 사건사고접수 확인원 법원 판결문 중 택1	경찰청 법원
보험사고 사망자 유자녀	부모의 재해사망 보험 사고로 인해 생활, 학업 등을 계속하기 어려운 경우 (단, 재해보험금 수령액이 1억원 이하인 경우에 한함)	보험회사 확인서 및 사망확인서류	해당기관

<출처 : 신용회복위원회, 금융과 생활-소액금융-소액대출-상품안내-특별대출-새희망 힐링론 참조>

- 새희망힐링론을 신청하려는 보이스피싱 금융피해자는 신용회복위원회의 전국 지부상담소에서 상담 및 신청접수(☎1600-5500)를 할 수 있습니다.

※ 신용회복위원회 전국 지부상담소에 대한 정보는 <신용회복위원회(www.ccrs.or.kr), 위원회 소개-지부위치 안내>에서 확인할 수 있습니다.

4. 전자금융범죄 피해 예방

4.1. 전자금융범죄 피해 예방 제도

4.1.1. 전자금융사기 예방 서비스

전자금융사기 예방 서비스 제도

전자금융사기 예방서비스

▪ “전자금융사기 예방서비스”는 사기범이 고객정보를 불법으로 획득한 후 타인명의 인증서를 부정 발급받아 금융자산을 편취해가는 사기수법 등을 예방하기 위해 도입되었습니다(금융감독원, 민원·신고-보이스피싱 지킴이-보이스피싱 한눈에-주요제도안내-전자금융사기 예방서비스 참조).

▹ (이용대상) 인터넷 뱅킹 개인고객

▹ (신청방법) 거래금융회사 인터넷 뱅킹 ´인증/보안´ 메뉴에서 가능(금융사마다 메뉴명이 다를 수 있음)

전자금융사기예방 서비스 종류



<출처 : 금융감독원,민원·신고-보이스피싱 지킴이-보이스피싱 한눈에-주요제도안내-전자금융사기 예방서비스 참조>

전자금융거래등 제한 제도

전자금융거래등 제한

▪ 전기통신금융사기로 인한 피해확산을 방지하기 위해 금융감독원은 지급정지 조치에 관한 사항을 통지받거나 지급정지 조치를 받은 적이 있는 명의인이 다음의 어느 하나에 해당하는 사실을 확인한 경우 해당 명의인을 전자금융거래등제한대상자로 지정해야 합니다(「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법」 제13조의2제1항).

▹ 「전자금융거래법」 제49조제4항제1호부터 제3호까지의 어느 하나에 해당(전기통신금융사기와 관련된 경우에 한정)하면서 접근매체를 양도하거나 대여한 자 또는 접근매체에 대한 질권설정자로서 벌금형을 선고받은 날부터 3년이 경과하지 않거나 징역형(집행유예를 포함)을 선고받은 날부터 5년이 경과하지 않은것으로 확인된 경우

▹ 「전자금융거래법」 제49조제4항제5호에 해당(전기통신금융사기와 관련된 경우에 한정)하면서 계좌와 관련된 정보를 제공한 자로서 벌금형을 선고받은 날부터 3년이 경과하지 않거나 징역형(집행유예를 포함)을 선고받은 날부터 5년이 경과하지 않은 것으로 확인된 경우

▹ 그 밖에 전기통신금융사기를 목적으로 한 범죄로 벌금형을 선고받은 날부터 3년이 경과하지 않거나 징역형(집행유예를

포함)을 선고받은 날부터 5년이 경과하지 않은 것으로 확인된 경우

> ※ “전자금융거래등”이란 금융회사등이 전자적 장치를 통해 금융상품 및 서비스 또는 「가상자산 이용자 보호 등에 관한 법률」 제2조제2호 각 목의 행위를 통한 서비스를 제공하고, 이용자가 금융회사등의 종사자와 직접 대면하거나 의사소통을 하지 않고 자동화된 방식으로 이를 이용하는 거래를 말합니다(「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법」 제2조제2호의2).

▪ 금융감독원은 명의인을 전자금융거래등제한대상자로 지정한 경우 지체 없이 금융회사등 및 명의인에게 이를 통지해야 합니다(「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법」 제13조의2제2항 본문).

전자금융거래등 제한 종료

▪ 금융회사등 및 금융감독원은 다음의 어느 하나에 해당하는 경우 사기이용계좌등의 전부 또는 일부에 대하여 이 법에 따른 지급정지·채권소멸절차 및 명의인에 대한 전자금융거래 제한을 종료해야 합니다(「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법」 제8조제1항 본문).

1. 손해배상·부당이득반환 등의 청구소송이 제기되어 법원에 계속(係屬) 중인 경우, 압류·가압류 또는 가처분의 명령이 집행된 경우 등처럼 「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법」 제5조제1항제1호부터 제4호까지의 어느 하나에 해당하는 사유가 발생한 경우
2. 지급정지된 후에 명의인과 피해자 간 채무부존재확인·부당이득반환청구 소송 등이 제기되어 법원에 계속 중인 경우
3. 해당 계좌등이 사기이용계좌등이 아니라는 사실을 소명한 경우
4. 소멸될 채권의 전부 또는 일부를 명의인이 재화 또는 용역의 공급에 대한 대가로 받았거나 그밖에 정당한 권원에 의하여 취득한 것임을 객관적인 자료로 소명하는 경우(다만, 해당 계좌등이 전기통신금융사기에 이용된 사실을 사기이용계좌등으로 이용된 경위, 거래행태, 거래내역 등의 확인을 통하여 명의인이 알았거나 중대한 과실로 알지 못하였다고 인정되는 경우는 제외)
5. 해당 계좌등이 피해자산 편취를 위해 이용된 계좌등이 아니라는 사실을 객관적인 자료로 소명하는 경우(해당 사기이용계좌등에 예치된 금액등 중 전기통신금융사기 피해자산을 제외한 금액등에 한정)
6. 금융감독원 또는 수사기관이 해당 계좌등이 사기이용계좌등이 아니라고 인정하는 경우
7. 피해환급자산 지급이 종료된 경우
8. 그밖에 피해구제를 신청한 모든 피해자가 그 신청을 취소하는 경우 등(「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법 시행령」 제8조)로 정하는 경우

▪ 다만, 위 1. 및 전기통신금융사기와 관련된 경우 접근매체를 양도하거나 대여한 자 또는 접근매체에 대한 질권설정자로서 벌금형을 선고받은 날부터 3년이 경과하지 아니하거나 징역형을 선고받은 날부터 5년이 경과하지 아니한 것으로 확인한 경우 등(「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법」 제13조의2제1항제1호부터 제3호)에 해당하는 경우에는 전자금융거래 제한을 종료하지 아니합니다(「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법」 제8조제1항 단서).

전자금융거래등의 제한 해제 통보

▪ 금융감독원은 전자금융거래등제한대상자로 지정된 자가 전자금융거래등의 제한이 해제된 때에는

전자금융거래등제한대상자의 지정을 취소하고 이를 금융회사등 및 명의인에게 통보해야 합니다(「전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법」 제13조의2제4항).

4.1.2. 지연인출·이체제도

지연인출제도 및 지연이체서비스

지연인출제도

▪ "지연인출제도"란 1회에 100만원 이상 금액이 송금·이체되어 입금된 경우 입금된 때부터 해당금액 상당액 범위에서 30분간 자동화기기(CD/ATM기 등)를 통한 인출·이체가 지연되는 제도를 말합니다. 다만, 금융회사 창구에서는 즉시 인출·이체가 가능합니다(금융감독원, 민원·신고-보이스피싱 지킴이-보이스피싱 한눈에-주요제도안내-지연인출제도-ATM 지연인출제도 참조).

구분	내용
적용 거래	√ 수취계좌(입금계좌) 기준 1회 100만원 이상 현금 입금된 건에 대해 카드 등으로 자동화기기에서 출금·이체할 경우
지연 방법	√ 1회 100만원 이상이 입금된 후 이체 등으로 잔액이 변동되어도 입금된 금액을 한도로 30분간 인출 지연
참여 기관	√ 입출금이 자유로운 예금(요구불예금) 취급기관[은행, 우체국, 농·수·축협 및 산림조합, 신협, 새마을금고, 저축은행, 금융투자회사(증권사) 일부 등]

<출처 : 금융감독원, 민원·신고-보이스피싱 지킴이-보이스피싱 한눈에-주요제도안내-지연인출제도-ATM 지연인출제도 참조>

지연이체서비스

▪ "지연이체서비스"란 이체 시 수취인 계좌에 일정시간(최소 3시간) 경과 후 입금되도록 하는 서비스를 말하며, 이체신청 후 일정 시간 내(최종 이체처리시간 30분 전까지)에는 취소가 가능합니다. 다만, 금융회사 창구 거래에는 적용되지 않습니다(금융감독원, 민원·신고-보이스피싱 지킴이-보이스피싱 한눈에-주요제도안내-지연인출제도-지연이체서비스 참조).

▪ 지연이체서비스는 해당 금융회사 인터넷(스마트) 뱅킹, 영업점 방문을 통해 신청할 수 있으며, 은행마다 서비스 내용에 차이가 있을 수 있습니다.

▪ 지연이체서비스 내용

- 이체 지연 시간은 최소 3시간 이상 일정 시간 단위로 선택 가능
- 지연이체서비스를 이용하더라도 본인이 별도로 건별한도(최대100만원)를 설정하여 즉시이체 서비스도 이용가능
- 해당 은행 본인계좌간 송금, 사전 등록된 계좌간 이체 등 일정한 경우 즉시 이체 가능

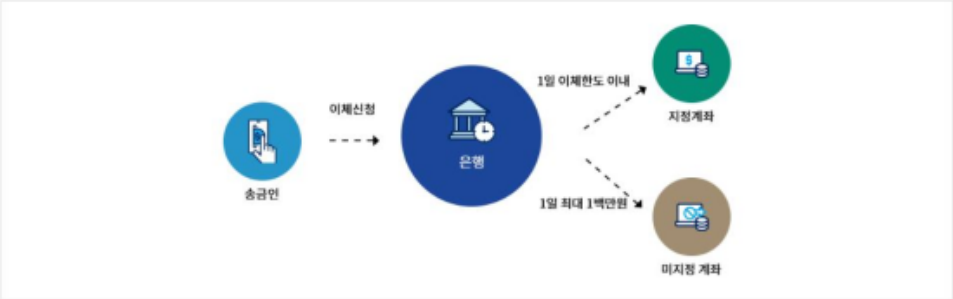


<출처 : 금융감독원, 민원·신고-보이스피싱 지킴이-보이스피싱 한눈에-주요제도안내-지연인출제도-지연이체서비스 참조>

입금계좌지정서비스

▪ “입금계좌지정서비스”란 본인이 미리 지정한 계좌로는 본인의 전자금융 이체 한도 내에서 자유롭게 송금이 가능하지만, 지정하지 않은 계좌로는 소액 송금만 가능(1일 1백만원 이내 이체한도 설정)한 서비스를 말합니다. 다만, 금융회사 창구 거래는 적용되지 않습니다(금융감독원, 민원·신고-보이스피싱 지킴이-보이스피싱 한눈에-주요제도안내-지연인출제도-입금계좌 지정서비스 참조)

▪ 입금계좌지정서비스는 해당 금융회사 인터넷(스마트) 뱅킹, 영업점 방문을 통해 신청할 수 있으며, 은행마다 서비스 내용에 차이가 있을 수 있습니다.

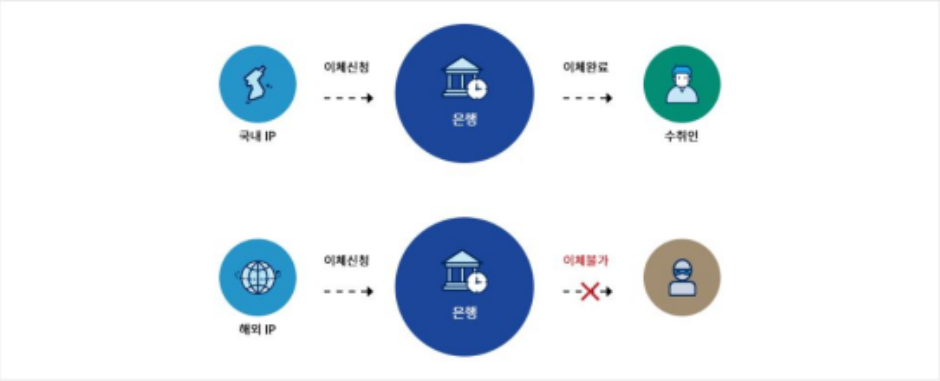


<출처 : 금융감독원, 민원·신고-보이스피싱 지킴이-보이스피싱 한눈에-주요제도안내-지연인출제도-입금계좌 지정서비스 참조>

해외 IP 차단 서비스

▪ “해외 IP 차단 서비스”란 국내 사용 IP대역이 아닌 경우 이체거래를 할 수 없도록 차단하는 서비스로, 정보유출 또는 해킹 등으로 취득한 정보를 이용하여 해외에서 시도하는 금전 인출을 방지하고자 합니다(금융감독원, 민원·신고-보이스피싱 지킴이-보이스피싱 한눈에-주요제도안내-지연인출제도-해외 IP 차단 서비스 참조).

▪ 해외 IP 차단 서비스는 해당 금융회사 인터넷(스마트) 뱅킹, 영업점 방문을 통해 신청할 수 있으며, 은행에 따라 이용되지 않는 은행이 있거나 서비스 내용에 차이가 있을 수 있습니다.



<출처 : 금융감독원, 민원·신고-보이스피싱 지킴이-보이스피싱 한눈에-주요제도안내-지연인출제도-해외 IP 차단 서비스 참조>

카드론 지연 입금제도

카드론 지연 입금제도

▪ “카드론 지연 입금제도”란 카드론 최초 이용자가 300만원 이상 카드론을 신청한 경우 승인 후에 2시간 지연하여 입금시키는 제도입니다.

▪ 최초로 카드론을 이용하여 300만원 이상 대출받는 경우(이용금액이 3백만원 미만이거나 과거에 해당 카드사에서 카드론을 이용한 적이 있으면 지연입금 대상에서 제외함)

▪ 300만원 이상 카드론 신청을 하고 승인을 받은 후에 2시간 지연 입금

<출처 : 금융감독원, 민원·신고-보이스피싱 지킴이-보이스피싱 한 눈에-보도자료-“카드론 지연입금 시행”, 2012. 5. 15. 참조>

4.1.3. 개인정보보호 관련 예방제도

개인정보노출자 사고 예방시스템

본인확인절차 강화

▪ “개인정보노출자 사고 예방시스템”이란 주민등록증, 운전면허증 분실 등 개인정보가 노출된 금융소비자가 개인정보 노출사실을 개인정보노출자 사고 예방시스템에 등록하면 신청인의 개인정보(성명, 주민등록번호 등)를 금융회사와 공유함으로써 금융회사로 하여금 당해 신청인 명의의 특정 금융거래(신용카드 발급, 예금계좌 개설 등)시 본인확인절차를 강화하도록 하는 시스템입니다(금융감독원 금융소비자 정보포털 FINE, 금융용어사전 참조).

구분	내용
신청 대상자	√ 신분증(주민등록증, 운전면허증 등) 분실자, 기타 개인정보노출 피해자
이용 방법	√ ① 금융이용자가 신분증 분실 등으로 개인정보 노출 우려 시 금융감독원 금융소비자포털 '파인(FINE)'에 등록하여 명의도용을 예방하는 시스템으로 개인업무를 취급하는 전체 금융회사와 연결 √ ② 개인정보 노출사실이 등록되면, 해당 정보가 실시간 금융회사에 전달되어 금융회사 영업점 단말기에 '본인확인 주의' 문구가 게시되고, 금융회사 영업점 직원은 통상 이상의 주의를 기울여 본인 확인을 하고, 명의도용 의심 시 거래제한 조치 등 실시 √ ③ 금융이용자는 PC 또는 휴대폰을 이용해 해당 시스템에 온라인으로 접속해 자신의 개인정보 노출사실을 한 번에 등록(또는 해제)할 수 있으며, 온라인 이용이 어려울 경우 은행 등 영업점을 통해서도 등록(또는 해제) 가능

<출처 : 금융감독원 보도자료, [금융꿀팁200선] 개인정보노출자 사고예방시스템 안내, 2022.05.12. 7면 참조>

명의도용 방지 서비스

명의도용 피해 예방

▪ 신규로 각종 통신서비스(이동전화, 무선인터넷[WiBro], 유선전화, 초고속인터넷, 인터넷전화[VoIP], 유료방송 등)에 가입하거나 명의변경을 통해 양도받을 경우 그 사실을 본인 명의로 사용하고 있는 이동전화 회선을 통해 SMS로 알려주는 서비스를 말합니다. 또한, 홈페이지(www.msafer.or.kr)에서는 가입사실현황조회 서비스, 가입제한 서비스, 이메일안내 서비스 등의 부가 서비스를 제공하고 있으며, 본 서비스는 명의도용 피해를 예방하고자 제공하는 대국민 무료 서비스입니다(「전기통신사업법」 제32조의6 참조).

구분	내용
명의도용방지 서비스	√ 본인 명의로 각종 통신서비스(이동전화, 무선인터넷[WIBro], 유선전화[VOIP], 유료방송 등)에 신규로 가입하거나 번호이동 또는 명의변경을 통해 양도 받을 경우 그 사실을 가입자 본인 명의로 사용하고 있는 이동전화 회선을 통해 SMS로 알려주는 서비스
가입사실현황조회 서비스	√ 조회일자 기준, 본인 명의로 가입된 이동전화, 무선인터넷[WIBro], 유선전화[VOIP] 및 유료방송 등의 통신서비스를 확인할 수 있는 서비스
가입제한 서비스	√ 이동전화의 신규가입·번호이동·기기변경·명의변경을 사전에 차단하는 서비스 ※ 엠세이퍼 홈페이지, PASS앱 & 카카오뱅크앱 또는 각 통신사 직영점에서 신청 가능
이메일안내 서비스	√ 본인 명의로 각종 통신서비스(이동전화, 무선인터넷[WIBro], 유선전화[VOIP] 및 유료방송 등)에 신규로 가입하거나 번호이동 또는 명의변경을 통해 양도받을 경우 그 사실을 e-mail로 알려주는 서비스
서비스 대상사업자	√ 이동통신, 유선전화, 인터넷전화, 무선인터넷, 종합유료방송



<출처 : 한국정보통신진흥협회 홈페이지(www.kait.or.kr), 주요사업-통신 서비스 기반조성-명의도용방지>

개인정보침해신고센터

개인정보 관련 침해 신고 및 상담

▪ '한국인터넷진흥원 개인정보침해 신고센터(https://privacy.kisa.or.kr)'는 「개인정보 보호법」에 설립 근거를 두고 개인 및 공공기관, 사업자의 개인정보 관련 침해 신고 및 상담의 처리를 하고 있습니다.

구분	내용
① 신청 대상	·개인정보침해 신고센터에 신고·상담 신청을 할 수 있는 대상은 개인정보처리자로부터 개인정보에 관한 권리 또는 이익을 침해받은 당사자 또는 법정대리인입니다.
② 신청 방법	·신고·상담 신청은 개인정보침해 신고센터 웹사이트를 통한 인터넷 신청(http://privacy.kisa.or.kr)을 원칙으로 하고 있으며, 이용자의 편의를 위해 팩스, 우편도 가능합니다. √ 인 터 넷 : https://privacy.kisa.or.kr(개인정보침해 신고센터) √ 우편 : (58324) 전라남도 나주시 진흥길 9(빛가람동) 개인정보침해 신고센터
③ 처리 절차	·상담 : 인터넷, 전자우편 등을 통해 접수된 상담은 담당자가 내용을 확인 후 원칙적으로 14일 이내에 답변합니다. 침해 상담으로 처리될 경우, 연락처를 통해 문자 접수증을 발부하나 접수번호가 생성되지 않습니다. 답변은 신고인의 전자우편으로 발송하는 것을 원칙으로 하며, 전화를 통하여 추가내용을 안내하는 경우도 있습니다. 전화로 접수된 상담은 그 즉시 상담원이 관련 내용을 안내하고 종결합니다. ·행정지도 : 행정지도는 접수일로부터 60일 이내에 완료하는 것을 원칙으로 하고 있습니다. 개인정보처리자(공공기관, 법인, 단체, 개인 등)의 「개인정보 보호법」 위반사항에 대한 신속한 시정 유도로 신고인의 침해받은 개인정보 권리 및 이익을 구제하고 종결할 수 있습니다. 행정지도는 신고인의 개인정보침해에 대한 정확한 사실관계 서술 및 증거자료 제출이 요구됩니다. 따라서 서면 접수가 원칙이며, 사실관계 서술이 모호한 경우, 증거자료를 갖추지 못하는 경우, 침해 내용이 신고인의 일방적 주장에 그치는 경우 등에는 사실관계 확인이 어려워 행정지도가 불가할 수 있습니다. 행정지도 결과를 통지 받은 신고인은 통지를 받은 날부터 14일 이내에 이의제기 신청서를 작성하여 재신고의 방식으로 이의제기를 할 수 있습니다. ·행정조사 : 행정조사는 행정지도에서 전환된 날짜로부터 120일 이내에 완료하는 것을 원칙으로 합니다. 행정지도 과정에서 고충 해결 및 「개인정보 보호법」 위반사항이 시정되지 않았을 경우 행정조사로 전환할 수 있습니다. 행정조사는 「개인정보 보호법」 및 「행정조사기본법」 등 관계 법령에 따라 비공개로 추진되며, 중립적·객관적인 입장에서 자료제출 요구 또는 검사 등의 조사를 수행합니다. 이에 따른 행정조사 결과는 개인정보보호위원회로 통보하고 종결할 수 있습니다. 행정조사 결과를 통지 받은 조사대상자는 이의제기 신청서를 작성하여 이의제기를 할 수 있습니다.

<출처 : KISA 개인정보침해신고센터, 이용안내-이용방법 참조>

정보주체 권리행사 서비스

소중한 내 개인정보 지키기

▪ "정보주체 권리행사 서비스(https://www.privacy.go.kr)"는 "본인확인 내역 조회, 웹사이트 회원 탈퇴, 개인정보 열람 등 신청"의 서비스를 제공합니다.



<출처 : 개인정보 포털-개인서비스-서비스 소개 참조>

4.2. 전자금융범죄 피해 예방 요령

4.2.1. 전자금융범죄 유형별 피해 예방 요령

전자금융범죄의 일반 예방 요령

- 공통 예방 요령

구분	내용
이메일 이용시 주의점	1. 출처가 불분명한 이메일이나 첨부파일은 열지 말고 삭제한다. 2. 첨부파일 열람 및 저장 전에는 반드시 백신으로 검사한다. 3. 메일을 통해 개인정보제공을 요구하는 서비스의 경우 가급적 이용을 자제한다. 4. 만약 이용할 경우 반드시 해당 업체 홈페이지에 직접 접속하여 꼼꼼히 확인한 후 이용한다. 5. 날마다 메일을 체크하고 중요하지 않은 메일은 즉시 지운다. 6. 이메일프로그램 또는 이메일제공서비스의 다양한 차단기능을 살펴보고 활용한다. 7. 인터넷 게시판 등에 이메일 주소를 남길 때 신중히 한다. 8. 인터넷 서비스 가입시 광고메일 수신 여부를 반드시 확인한다.
온라인 금융거래 주의점	1. 은행, 신용카드 등 금융기관 사이트는 즐겨찾기를 이용하거나, 주소를 정확하게 입력하고 이용한다. 2. 금융기관 등에서는 전화나 메일로 개인정보를 확인하는 경우는 없으므로 정보를 요청하는 메일은 일단 의심한다. 3. 인증서는 안전하게 관리하고, 타인에게 노출되지 않도록 주의한다. 4. 보안카드는 반드시 본인이 소지하고, 온라인 다른 곳에 기재해 두지 않는다. 5. 온라인 금융거래 이용 후, 이를 알려주는 휴대폰 문자서비스를 이용한다. 6. 시간이 걸리더라도 금융기관에서 제공하는 보안프로그램은 반드시 설치한다. 7. 금융기관 이용 비밀번호 등은 기타 다른 사이트의 비밀번호와는 다르게 설정한다. 8. 공공장소 PC는 보안에 취약하므로 온라인 금융거래 이용을 자제한다.
가족의 안전한 사이버 생활	1. 컴퓨터를 개방된 공간에 두고 가족들이 공유할 수 있도록 한다. 2. 자녀가 가입한 사이트, 카페 및 자녀의 ID가 무엇인지 알아둔다. 3. 자녀가 사이버상에서 하는 활동에 대해 항상 대화한다. 4. 온라인 게임은 규칙을 정해서 이용하도록 하고, 아이템이나 계정 거래 등에 대해 알아둔다. 5. 부모의 주민번호, 신용카드번호 및 기타 비밀번호를 공개하지 않는다. 6. 자녀에게 다음의 인터넷 수칙을 알려준다. -인터넷 채팅의 익명성을 알려주고 이름, 주소, 학교 등 신상정보를 알려주지 않도록 한다. -부모의 허락없이 인터넷을 통해 직접 사람을 만나지 않도록 한다. -부모의 허락없이 부가적인 요금을 내야하는 정보나 게임 등을 이용하지 않도록 한다. -인터넷 게시판에 글을 쓸 때는 에티켓을 갖추어야 한다. -저작자의 허락없이 저작물을 인터넷에 올려 저작권을 침해하지 않도록 한다.

<출처 : 경찰청 사이버수사국, 사이버범죄예방홍보물-예방수칙 참조>

계좌정보통합관리서비스

▪ "계좌정보통합관리서비스(https://www.payinfo.or.kr)"는 다음 서비스를 제공 합니다.

① 계좌조회:고객이 계좌통합관리서비스(Account Info) 홈페이지 및 은행창구를 통해 모든 은행에 개설된 본인명의 계좌정보를 일괄 조회할 수 있는 서비스입니다.

② 잔고이전 및 해지: 고객이 계좌통합관리서비스(Account Info) 홈페이지를 통해 소액 비활동성계좌를 해지하고 잔고를 본인명의 계좌로 이전하거나 서민금융진흥원에 기부할 수 있는 서비스입니다.

③ 휴면예금·보험금 조회 및 지급: 소멸시효가 완성되어 서민금융진흥원에 출연된 휴면예금 및 보험금을 조회하고, 휴면예금 및 보험금을 본인 계좌로 지급신청하거나 서민금융진흥원에 기부할 수 있는 서비스 입니다.

<출처 : 계좌정보통합관리서비스, 서비스안내-서비스소개 참조>

피싱 피해 예방 요령

피싱 피해를 예방하기 위한 기본 요령

① 가족을 사칭하며 문자로 개인(신용)정보 등 요구하는 경우

가족의 연락처로 전화하여 반드시 직접 확인해야 하며, 조금이라도 의심스러운 경우 자녀 등 가족이라 하더라도 신분증 사진, 신용카드 및 계좌 번호 등을 제공해서는 안됩니다.

또한, 자녀가 핸드폰 파손・고장 등의 사유로 전화통화가 안된다고 하면서, 전혀 모르는 번호를 카톡에 추가해 달라고 해도 무조건 거절해야 합니다.

② 출처가 불분명한 악성앱 등 설치 요구하는 경우

악성앱·팀뷰어 등 설치시 개인(신용)정보가 전부 유출되므로 절대 설치해서는 안되며, 필요시 가족 등 지인의 전화기로 해당 금융회사 또는 금융감독원(☎1332)에 사실 여부를 확인해야 합니다.

악성 앱이 설치된 본인 전화기로 금융회사, 금감원, 경찰 등에 전화할 경우, 사기범이 중간에서 전화를 모두 가로채므로 전화가 보이스피싱범에게 연결되므로 주의하세요.

악성앱을 이미 설치했다면 모바일 백신앱(최신 버전 업데이트)으로 검사후 삭제, 데이터 백업 후 휴대폰 초기화, 지인이나 휴대폰 서비스센터에 도움 요청 등 필요한 경우 금융회사의 보안강화 서비스에 반드시 가입합니다.

③ 보이스피싱 피해를 입은 경우

금융회사 콜센터 또는 금융감독원 콜센터(☎1332)에 전화하여 해당 계좌 지급정지를 요청하고 피해구제를 신청하고 개인정보 유출에 따른 추가 피해를 막기 위하여 금융감독원 금융소비자 정보포털, '파인'의 개인정보노출자 사고예방시스템을 적극 활용

"계좌정보 통합관리서비스"(www.payinfo.or.kr)를 활용하여 본인 모르게 개설된 계좌 또는 대출을 한눈에 확인

본인 모르게 휴대폰이 개통되지 않도록 한국정보통신진흥협회의 명의도용 방지서비스(www.msafer.or.kr)를 통해 가입사실 현황조회 서비스 및 가입제한 서비스 등 활용

④ 명절 허위 결제・택배 문자를 받은 경우

문자 내용에 포함된 URL주소를 클릭하거나 전화번호로 통화하지 말고 즉시 삭제

<출처 : 금융감독원, 알림·소식 참조>

피싱예방 어떻게 하나요?

1. 출처가 불분명한 이메일, 문자메시지, 블로그 등에 포함된 URL에 접근하지 않기
2. 개인정보(로그인), 금융정보(보안카드 등)에 대한 입력을 진행할 때 홈페이지 주소의 자물쇠 그림 또는 도메인 주소의 철자 확인하기

3. 경품 이벤트 등 무분별한 인터넷 이벤트 참여를 통해 개인정보 입력하지 않기

4. 안전한 비밀번호를 사용하고 주기적으로 변경하기

5.공유기 보안설정 강화하기

<출처 : KISA 인터넷보호나라 & KrCERT, 알림마당-자세히 알아보기-피싱 예방 가이드 참조>

몸캠피싱 예방 요령

▪ 스마트폰의 ´환경설정-보안´ 메뉴에서 스마트폰의 보안설정을 강화시키세요. 특히, 출처 불명의 실행파일(*.apk)을 스마트폰에 다운받은 후 이를 스마트폰에 설치하는 행위는 절대 하지 마세요.

> ※ “출처 불명”이란 공식 ‘앱 스토어’(구글 플레이 스토어, 삼성스토어 등)가 아닌, 문자·모바일 채팅 등을 통해 URL에 접속해서 내려받는 경우를 말합니다.
>
> <출처 : 경찰청 사이버수사국, 사이버범죄예방홍보물-예방수칙-몸캠피싱 참조>

▪ “랜덤 채팅”에서 낯선 미모의 여성과 대화할 때, 언제든지 이러한 범죄의 표적이 될 수 있음을 유의하셔야 합니다. 또한 익명성 보장을 이유로 개인 정보와 채팅 내용을 저장하지 않으므로, 몸캠피싱 외에 ´조건 만남 계약금 사기´등 여러 가지 범죄의 시발점이 됩니다. 따라서 그 전에 ´음란 채팅´을 하지 않는 것이 가장 중요 하겠습니다(경찰청 사이버수사국, 사이버범죄예방홍보물-예방수칙-몸캠피싱 참조).

그 밖의 전자금융범죄 예방 요령

구분	예방 요령
스피어 피싱	1. 이메일 발신자 정보 면밀히 확인 (아이디, 도메인 등) 예) 경찰청 도메인 : or.kr(×)/ go.kr( ) 2. 메일 내 확인 되지 않은 첨부파일 다운로드 금지 예) 해커들이 주로 PDF파일 안에 악성 파일을 숨기는 방법 자주 사용 3. 이중 확장자로 된 파일(예-doc.lnk 등)은 사기 가능성이 매우 크므로 열람 금지 4. 메일 본문 중 링크된 사이트 연결 지양 5. 개인정보 및 특정 정보 회신 요구하는 경우 반드시 해당 담당자와 전화통화 확인 6. 온라인 상에 자신의 개인정보 노출 최소화 7. 주로 쓰는 문서 프로그램이나 윈도우 등 운영체제(OS) 등의 최신 보안패치 설치 <경찰청 사이버수사국, 사이버범죄예방홍보물-예방수칙-스피어 피싱 참조>
디도스(DDoS) 공격	1. 윈도우 등 운영체제 및 소프트웨어의 최신 보안 패치 설치 및 버전 업그레이드 2. 바이러스 백신 설치 및 실시간 감시 기능 활성화 3. 신뢰할 수 있는 웹사이트에서만 액티브 X 설치 4. 출처가 불분명한 이메일 확인 및 첨부 파일 클릭 금지 5. 불법 콘텐츠 공유 사이트 접속 지양 및 불법 파일 다운로드 금지 6. 정품 소프트웨어 사용 7. 컴퓨터에 반드시 암호 설정 <출처 : 경찰청 사이버수사국, 사이버범죄예방홍보물-예방수칙-디도스(DDos)공격 참조>

로맨스스캠	1. SNS에서 무분별한 친구 추가 자제 및 인터넷상에서 교제는 신중히 고려 2. 해외 교포, 낯선 외국인과의 인터넷상에서 교제는 신중히 고려 3. 인터넷상만으로 교제(연락)하는 경우, 부탁을 가장한 요구에 입금 금지 4. 상대방이 선물 발송 빙자로 인한 배송 업체 사이트 URL에 접속 지양 <출처 : 경찰청 사이버수사국, 사이버범죄예방홍보물-예방수칙-로맨스스캠 참조>
스미싱	1. 모바일 백신 설치 및 실시간 감시 기능 설정 2. 스마트폰 운영 체제 최신 업데이트 3. 문자메시지 내 포함된 인터넷 주소(URL) 절대 클릭 금지 4. 스마트폰 기본 운영 체제 변경 지양 5. 스미싱 차단앱 설치 6. 비밀번호 설정되지 않는 무선 공유기(WiFi)에 접속 지양 7. 앱 다운로드시, 공식 애플리케이션 마켓 이용 <출처 : 경찰청 사이버수사국, 사이버범죄예방홍보물-예방수칙-스미싱 참조>
파밍	1. 사이트 주소가 정상인지 확인하고, 보안카드번호 전부는 절대 입력하지마세요. 2. 보안카드 사진등을 컴퓨터나 이메일에 저장하지 마세요. 3. OTP(일회성 비밀번호생성기),보안토큰(비밀번호 복사방지)등을 사용하기를 권장하며, '전자금융사기 예방서비스'에 가입하세요. 4. 스마트폰 문자메시지에 포함된 인터넷주소 클릭하지 마세요. 5. 무료 다운로드 사이트의 이용을 자제하시고,출처가 정확하지 않은 파일이나 이메일은 즉시 삭제하세요. 6. 윈도우,백신프로그램 등을 최신상태로 유지하세요 7. 파밍 등이 의심될때에는 신속히 경찰청 112센터나 금융기관 콜센터를 통해 지급정지를 요청하세요 <출처 :경찰청 사이버수사국, 사이버범죄예방홍보물-예방수칙-파밍 참조>
메모리해킹	1. 윈도우,백신프로그램을 최신상태로 업데이트하시고, 실시간 감시상태 유지하세요. 2. 영화.음란물 등 무료다운로드 사이트 이용을 자제 하시고 ,출처가 확인되지 않은 파일이나 이메일은 열람하지 말고 즉시 삭제 하세요. 3. 컴퓨터. 보안카드 사진, 비밀번호는 저장하지 마시고,OTP(일회성 비밀번호생성기),보안토큰(비밀번호 복사방지) 등을 사용하세요. 4. 전자금융사기 예방서비스에 가입하세요. <출처 : 경찰청 사이버수사국, 사이버범죄예방홍보물-예방수칙-메모리해킹 참조>