

유형	피해사례	대처방법
<p>인터넷뱅킹을 이용한 장기카드대출(카드론) 및 예금 편취</p>	<ul style="list-style-type: none"> -충주에 사는 이모씨는 서울중앙지검 검사를 사칭한 사기범으로부터 사기사건에 연루됐다는 전화를 받고, 사기범이 알려준 가짜 금감원 홈페이지에 접속하여 자신의 개인정보를 입력함. -사기범은 이씨가 가지고 있던 공인인증서를 폐기하고 ㄱ은행에서 이씨 명의의 새 범용공인인증서를 재발급 받음. -이후 사기범은 ㄱ은행에서 이씨의 예금 200 만원을 인출하고, 이후 저축은행에서 500 만원, 대부업체에서 100 만원 대출을 받음. <ul style="list-style-type: none"> -성동구에 사는 A 씨는 “KB 국민은행입니다. 포털사이트 정보유출로 보안등급 후 이용해 주세요 www.card-kr.com”라는 문자 메시지를 받음. -이에 A 씨는 사기범이 보낸 국민은행 피싱사이트에 접속하여 통장계좌번호, 비밀번호, 인터넷뱅킹 ID 등 금융거래 정보를 입력함. -사기범은 입력받은 정보로 공인인증서를 재발급받아 인터넷뱅킹을 통해 피해자의 계좌에서 예금, 마이너스통장 및 적금담보 대출 등 총 4,700 만원을 사기계좌로 이체하여 편취함. 	<ul style="list-style-type: none"> -금융기관 등의 인터넷 홈페이지 접속 시 반드시 포털사이트 등을 통해 인터넷 주소를 확인하고 접속
<p>수사 · 공공기관 사칭</p>	<ul style="list-style-type: none"> -경기 수원 거주 김모씨는 경찰청 직원을 사칭한 사기범의 전화를 받음. -“당신의 모든 금융거래정보(비밀번호, 신용카드번호 등)가 해킹되어 금융자산 보호조치가 필요하니, 금감원이 관리하는 안전계좌로 모든 예금과 장기카드대출(카드론)을 받아 이체시켜야 한다”고 하여, -피해자 명의로 받은 장기카드대출(카드론) 대출금 2,000 만원과 보유예금 58 만원등 총 2,058 만원을 사기범이 불러주는 4 개의 계좌로 이체하여 피해를 봄. 	<ul style="list-style-type: none"> -전화를 통해 카드번호, 주민등록번호 등 개인정보 요구 시 일체 대응 금지 -사기범들 계좌에 자금을 이체했을 경우 즉시 ☎112 에 지급 정지 신청
<p>자녀납치 및 사고빙자</p>	<ul style="list-style-type: none"> -서울에 사는 회사원 박모씨는 휴대전화에 딸 번호가 떠 반갑게 받았지만, 40 대로 추정되는 남성이 	<ul style="list-style-type: none"> -위급시 자녀의 안부를 문의할 수 있는 자녀의 친구, 선생님

유형	피해사례	대처방법
	<p>"딸을 데리고 있다"고 협박함. 박씨가 "딸을 바꿔달라"고 하자, 전화기에선 "아빠 아저씨들이 때려요"라는 딸의 음성이 들림.</p> <ul style="list-style-type: none"> -다시 전화를 받은 남성은 "돈을 부치지 않으면 딸을 죽이겠다"고 400 만원을 요구하며, "입금할 때까지 이 전화를 끊지 말고 은행으로 가라"고 함. -박모씨는 곧장 은행으로 향했고, 그사이 회사 동료들이 딸의 행방을 수소문해 박씨가 돈을 입금하기 직전, 딸이 학교에 있다는 사실을 확인함. 	<p>등의 연락처 1 개 이상을 미리 소지</p> <ul style="list-style-type: none"> -최대한 침착함을 유지하면서 주위 사람에게 자녀의 안부전화 부탁 -특히 계좌송금 요구 시 절대 자금 먼저 이체 금지
메신저 피싱	<ul style="list-style-type: none"> -자영업을 하는 장씨는 친구로부터 카카오톡을 통해 돈을 빌려달라는 메시지를 받고 알려진 계좌로 600 만원을 입금함. -그러나 몇 시간 뒤 친구의 이름과 사진이 바뀌었고, 친구에 확인한 결과 사기임을 알게 됨. 	<ul style="list-style-type: none"> -금전을 요구하는 문자 수신 시 반드시 사실관계 확인 필요
ARS 를 이용한 장기카드대출 (카드론) 대금편취	<ul style="list-style-type: none"> -정모씨는 검사를 사칭한 사기범으로부터 "대포통장 사기사건 관련 출석을 하지않아 출국이 금지됐다"는 전화를 받고 사기범에게 카드번호, 통장 계좌번호 등을 알려줌. -이후 사기범은 정모씨 명의 신용카드를 대출을 실행해 정모씨 통장으로 입금시킨 후 "범죄자금이니 국고에 환수시켜야 한다" 며 현금을 이체 받아 가로챈. 	<ul style="list-style-type: none"> -전화를 통해 카드번호, 주민등록번호 등 개인정보 요구 시 일체 대응 금지 -사기범들 계좌에 자금을 이체했을 경우 즉시 ☎112 에 지급 정지 신청
대출사기	<ul style="list-style-type: none"> -급전이 필요했던 이모씨는 당일 대출이 가능하다는 △스캐피탈의 문자메시지를 받고, 대출금의 10%인 수수료 100 만원을 먼저 입금해야 대출할 수 있다는 업체 상담원의 요구에 따라 업체가 제시한 계좌로 돈을 송금함. -다음날 이모씨는 "100 만원을 더 입금하면 2000 만원을 대출해 주겠다"는 상담 직원의 전화를 받고 다시 송금함. -하지만 일주일쯤 넘게 기다려도 업체로부터 입금되지 않자 이를 확인하기 위해 대부업체에 전화했으나 이후 통화가 되지 않음. 	<ul style="list-style-type: none"> -대출신청 시 해당 금융업협회 홈페이지를 통해 업체 및 대출 모집인의 등록 여부 확인 <p>여신금융협회(www.crefia.or.kr) 은행연합회(www.kfb.or.kr) 저축은행중앙회(www.fsb.or.kr) 생명보험협회(www.klia.or.kr) 손해보험협회(www.knia.or.kr)</p> <ul style="list-style-type: none"> -불법 대출모집 광고 발견 시 금감원에 신고 -홈페이지(www.fss.or.kr) 참여마당→금융범죄 비리신고 →사이버 불법 금융행위 제보 전화(국번없이 1332→3→1)로 신고
	<ul style="list-style-type: none"> -A 씨는 '11.12 월 휴대폰 문자메시지를 보낸 업체에게 대출 	

유형	피해사례	대처방법
	<p>관련 서류를 송부하고 대출을 신청하였으나, 동 업체로부터 A 씨의 신용조회건수가 너무 많아 대출이 어렵다는 통보를 받음.</p> <ul style="list-style-type: none"> -며칠 후 A 씨는 “△△캐피탈”로부터 전화를 받았는데, 담당자로부터 신용정보 조회건수 과다는 전산처리할 수 있으므로 대출가능하다는 설명을 들음. -이에 A 씨는 △△캐피탈 대표번호로 전화하여 담당자의 재직여부를 확인하고 대출 500 만원을 신청하였는데, 담당자는 세 차례에 걸쳐 신용정보조회 삭제비용 20 만원, 3 년간 보증보험료 72 만원(36 개월×2 만원), 1 년간 이자 120 만원을 입금할 것을 요구하여 A 씨는 대출을 받기 위해 어쩔 수 없이 총 212 만원을 입금. -이후 담당자의 전화가 수신거부 상태이고 며칠이 지나도 연락이 없자 A 씨는 결국 사기를 당했다고 생각함. 	
특이형태의 기망	<ul style="list-style-type: none"> -올 대학수학능력시험을 치른 고 3 김모(19)군은 이달 초 수시모집에 지원한 대학 중 한 곳의 번호로 전화를 받음. -발신자는 “K 대학교 입학처”라며 “수시모집에 추가 합격했으니 불러주는 계좌번호로 등록금을 입금하라”고 함. 이에 김군이 “수시합격자 발표조차 아직 나지 않았는데 추가 모집 합격자가 벌써 발표됐느냐”고 문자 전화는 뚝 끊김. -수상하게 여긴 김군이 K 대에 문의하니 “그런 전화를 건 사실이 없다”는 답변이 돌아옴. 	<ul style="list-style-type: none"> -전화를 통해 금전을 요구하는 경우 반드시 사실관계 확인 필요
상황극 연출	카드	<ul style="list-style-type: none"> -김금융씨는 ARS 전화목소리로 신용카드연체 안내전화를 받음. 해당 신용카드 사에서 카드를 발급 받은 적이 없지만 불안감에 전화안내에 따라 직원을 연결함. -사기범이 본인확인을 한다며 김금융씨의 이름과 주민번호를 묻고, 김금융씨는 무의식적으로 개인정보(이름, 주민번호 등)를 사기범에게 알려줌. <p>• -전화를 통해 카드번호, 주민등록 번호 등 개인정보 요구 시 일체 대응 금지</p> <p>• -사기범에게 금융거래정보를 알려준 경우 ☎112 에 신고하고 비밀번호와 보안카드 변경</p>
		<ul style="list-style-type: none"> -“안녕하세요. 00 카드입니다. 금일 고객님의서 롯데백화점에서 198 만원을 사용 하였습니다.

유형	피해사례	대처방법
은행	<p>반복청취는 1 번, 상담원 연결은 9 번을 눌러 주세요.”</p> <ul style="list-style-type: none"> -A 씨는 국민은행 상담원의 전화를 받음. “A 씨 인가요? 여기 국민은행 00 지점인데요. B 씨란 분에게 통장과 도장을 맡겨 돈 찾아오라고 하셨나요? 주민등록번호가 000 맞지요? 사실이 아니면 경찰을 불러 드릴게요.” -A 씨가 그런 사실이 없다고 하자 경찰이라 하며 사기범을 바꿔줌. 사기범은 “지구대에서 나온 순경 김 00 입니다. 증거확보를 위해 녹음을 하겠습니다. 주민등록번호와 도용당한 통장번호, 비밀번호를 얘기해 주세요.” 	
보험	<ul style="list-style-type: none"> -A 씨는 국민은행 상담원의 전화를 받음. “A 씨 인가요? 여기 국민은행 00 지점 인데요. B 씨란 분에게 통장과 도장을 맡겨 돈 찾아오라고 하셨나요? 주민등록번호가 000 맞지요? 사실이 아니면 경찰을 불러 드릴게요.” -A 씨가 그런 사실이 없다고 하자 경찰이라 하며 사기범을 바꿔줌. 사기범은 “지구대에서 나온 순경 김 00 입니다. 증거확보를 위해 녹음을 하겠습니다. 주민등록번호와 도용당한 통장번호, 비밀번호를 얘기해 주세요.” 	<ul style="list-style-type: none"> - 전화를 통해 카드번호, 주민등록번호 등 개인정보 요구 시 일체 대응 금지 - 사기범에게 금융거래정보를 알려준 경우 ☎112 에 신고하고 비밀번호와 보안카드 변경
마트등 가맹점	<ul style="list-style-type: none"> -사기범은 마트에서 피해자 명의의 신용카드를 구매하려는 손님이 있다며 피해자에게 전화를 함. “강 00 씨예요? 00 마트인데요. 강 00 씨 신용카드를 물건을 구매하는 손님이 있는데수상해서 전화했어요. 서둘러야 해요, 현금인출도 하려하네요.” -피해자가 신용카드 도난 사실이 없다고 하자 “도용해서 사용하는 겁니다. 마침 경찰관이 왔어요.”하며 사기범을 바꿔줌. -사기범은 경찰을 사칭하며 사건 수사를 위해 신용카드 번호와 주민번호를 확인함. 	
우체국	<ul style="list-style-type: none"> -“우체국입니다. 수취인 부재로 우편물이 반송 예정입니다. 확인하시려면 0 번을 눌러주세요” 	

유형		피해사례	대처방법
		<ul style="list-style-type: none"> -0 번을 누르면 집배원을 가장한 사기범이 집배원의 실명을 밝혀 안심시킨 후 주소, 전화번호, 주민등록 번호, 계좌번호, 신용카드 번호 등을 물어봄 	
사이트	쇼핑몰	<ul style="list-style-type: none"> -김민지씨는 육아용품 전문 사이트 '오케이마망'에서 특정 상품을 다른 곳보다 훨씬 저렴하게 판매하자 해당 사이트에서 물품 구매 후 결제를 시도했지만 "안심클릭"*창에 신용카드 정보를 입력하면 번번이 결제오류가 나타남. -*신용카드 온라인 결제시스템으로 카드 결제 시 카드번호, 유효기간, 카드 비밀번호 2 자리, CVC 입력(BC 카드 이외 모든 카드 동 결제시스템 사용) -사이트에 문의한 결과 일시적인 오류 발생이라며 현금결제를 유도하여 현금으로 결제를 마침. -그러나, 이 과정에서 김씨의 카드정보와 주민번호 등이 유출됐고 범인들은 이를 이용해 상품권과 게임머니 등을 구매함. 	<ul style="list-style-type: none"> -신용카드 결제 오류가 발생했을 경우 소비자가 사용한 카드사로 연락하여 신용카드 이용내역 확인 -추가적인 도용 방지를 위해 신용카드 결제 알림서비스(SMS) 신청 - 기 신청자도 신청여부 확인 필요 -피싱사이트로 인한 피해 발생 시 금융감독원(☎1332) 또는 인터넷진흥원(☎118)에 신고
	SNS	<ul style="list-style-type: none"> -트위터 등에서 'Did you see this crazy tweet about you?' 등 사용자가 호기심을 가질만한 내용으로 위장한 단축 URL 을 클릭하면, 트위터 사용자 로그인 페이지와 유사한 웹 사이트로 연결됨. -그러나 실제 해당 웹 사이트는 트위터 사용자 계정과 로그인 암호를 수집하기 위해 정교하게 제작된 피싱 웹 페이지임. 	

(출처: 여신금융협회)