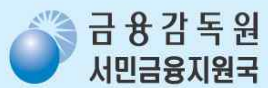

보이스피싱 피해예방 길라잡이

알기쉬운 보이스피싱 이야기

2012. 7



목 차

I . 보이스피싱의 정의	1
II . 보이스피싱의 특징	3
III . 보이스피싱 피해현황 및 피해유형	6
IV . 보이스피싱 피해예방 요령	8
V . 전기통신금융사기 피해금 환급제도	13
VI . 보이스피싱 예방관련 주요 제도	15
VII . 보이스피싱 피해사례	17

I 보이스피싱의 정의

- 보이스피싱*이란 ①기망행위로 타인의 재산을 편취하는 사기범죄의 하나로, 특히 ②전기통신수단을 이용한 비대면거래를 통해 ③금융분야에서 발생하는 일종의 특수사기범죄입니다

* 보이스피싱(Voice Phishing)이란 ‘전화를 통해 개인정보를 낚아 올린다’는 뜻으로 음성(Voice)+개인정보(Private data)+낚시(Fishing)를 합성한 신조어

보이스피싱의 법정 명칭은 전기통신금융사기이나, 본 안내책자에서는 독자의 이해를 돕기 위해 보이스피싱으로 표현

- 2000년대 초반에 대만에서 시작되어 이후 중국, 일본, 한국, 싱가포르 등 주로 아시아 지역으로 확산되었으며
- 해외에 본부와 콜센터를 두고, 국내에 인출팀, 환전·송금팀, 계좌모집팀 등을 두는 등 네트워크를 이루어 움직이는 조직형·지능형 범죄입니다



< 보이스피싱 사기과정 >

① 사기이용계좌 확보

예금통장 매입,
대출 등 미끼로 편취

▶ 신용불량자, 노숙자 등을 이용하여 통장 (대포통장)을 개설매입하거나 대출 또는 취업을 미끼로 예금통장을 편취

② 전화·문자 메시지 시도

해외(중국 등)콜센터에서
국내로 전화

▶ 해외(중국 등)에 본부를 둔 사기단이 금융 기관 및 검찰, 경찰, 금융감독원 등 공공 기관의 대표전화로 발신자번호를 조작 하여 무작위로 국내에 전화

③ 기망·공갈

개인정보유출, 범죄사건
연루 등으로 기망

▶ 금융기관 및 검찰, 경찰, 금융감독원 등 공공기관을 사칭하는 자가 개인 정보유출, 범죄사건 연루 등의 명목으로 기망하여 피해자의 개인정보 또는 금융 거래정보를 탈취

④ 계좌이체

송금·이체유도 또는
사기범이 직접 이체

▶ 계좌보호 조치 또는 범죄혐의 탈피 등 명분하에 사기계좌로 이체를 유도하거나 피해자로부터 편취한 정보로 공인 인증서를 재발급 받아 사기범이 직접 이체

⑤ 인출·송금

현금인출책·송금책을
통해 해외송금

▶ 점조직으로 이루어진 현금인출책이 송금책의 계좌로 입금하면 송금책이 환치기 등의 방법으로 범죄집단 본부로 송금 (글로벌 체크카드 이용 시 해외에서 직접 출금)

II 보이스피싱의 특징

보이스피싱은 다음과 같은 주요 특징들을 갖고 있습니다.

[첫째] 공공기관 및 금융기관을 사칭

- 사기범이 **검찰, 경찰, 금융감독원 등 공공기관 및 금융기관을 변갈아 사칭**하고 있습니다. 한명의 피해자에게 3~4명이 교대로 공신력 있는 여러 기관을 사칭하고 사전 각본에 의해 전화할 경우 피해자가 쉽게 속는 점을 이용하는 것입니다.



- 과거에는 사기범이 국세청 등을 사칭하여 세금환급 등 금전적 이득을 제공하는 수법을 사용하였으나
- 최근에는 **개인정보노출로 명의를 도용되어 피해자 계좌에서 예금인출이 되었다고 하거나, 범죄사건 연루, 자녀 납치 등 거짓사실로 피해자를 심리적으로 압박**하는 수법을 주로 이용하고 있습니다.

[셋째] 발신번호 조작을 통한 피해자 혼란 가중

- 초기에 발생한 보이스피싱은 피해자의 휴대전화 발신번호창에 **해외전화번호**가 표시되어 비교적 인지하기 용이하였으나
- 최근에는 사기범이 검찰, 경찰, 금융감독원 등 **공공기관 및 금융기관의 전화번호가 발신번호창에 나타나도록 조작**함에 따라 피해자들을 더욱 혼란스럽게 만들고 있습니다.

[넷째] 유창한 한국어 구사를 통한 피해자 공략

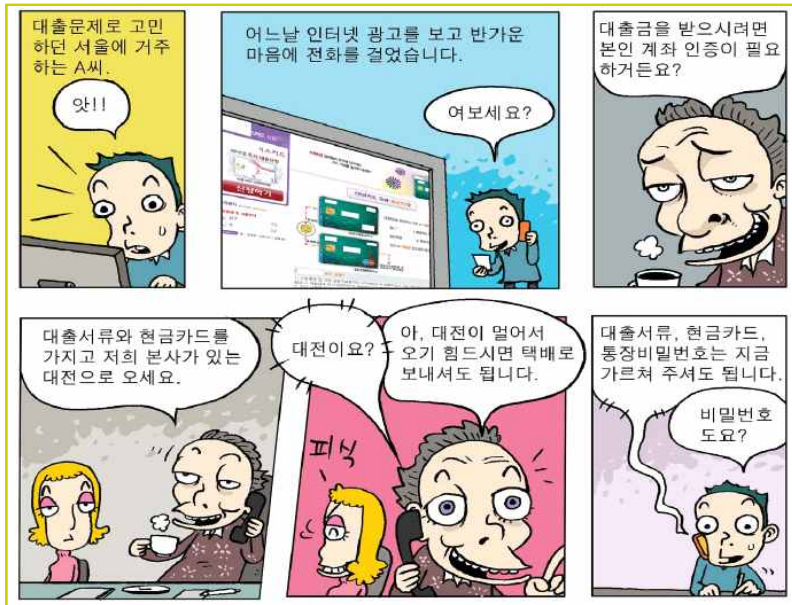
- 과거에는 사기범이 다소 어눌한 조선족 말투를 쓰고 조목조목 되묻거나 강경하게 대처하면 전화를 도중에 끊었으나
- 최근에는 **유창한 한국어를 구사**하고 집요하게 피해자를 공략하고 있습니다.

[다섯째] 피해자의 금융거래정보 편취를 통한 직접 인출

- 과거에는 사기범이 피해자를 속여 자금을 송금하게 하거나 CD기 또는 ATM기를 조작하게 하여 자금을 편취하였으나
- 최근에는 **피싱사이트 등에 금융거래정보(계좌번호, 카드번호, 인터넷뱅킹 정보 등)를 입력**하게 한 후 이를 이용하여 사기범이 피해자 모르게 대출을 받거나 예금 등을 직접 인출해 가는 수법을 주로 사용하고 있습니다.

[여섯째] 최근에는 대출 등을 미끼로 획득한 통장을 사기에 이용

- 과거에는 신용불량자, 노숙자 등을 이용하여 개설한 대포 통장을 보이스피싱 범죄에 이용하였으나
- 최근에는 **대출이나 취업 등을 미끼로 획득한 예금통장을** 사기에 이용하고 있습니다.



사기범은 일정기간동안 특정기관을 집중적으로 사칭하다가 국민들에게 노출이 많이 되면 사칭기관이나 유인방법들을 바꿔가면서 범행하는 등 사기수법을 계속 진화시키고 있어 금융업무에 어두운 시골 노인층은 물론 공무원, 의사, 변호사, 대기업 간부 등도 적지 않게 피해를 보고 있는 실정입니다.

Ⅲ 보이스피싱 피해현황 및 피해유형

1 피해 현황

- 보이스피싱이 처음 등장한 '06년 6월부터 '12년 5월까지 **총 37,459건**, 금액으로는 **3,953억원**의 피해가 발생하였습니다.
- '06년 이후 피해현황이 매년 증가하였으나 금융당국과 금융회사의 피해예방대책 시행에 힘입어 '09년부터 감소세로 전환되다가 **최근 카드로 보이스피싱, 공공기관 피싱사이트 등의 출현으로 다시 증가되는 양상**을 보이고 있습니다.
- 초기에는 금융지식이 부족하거나 정보력이 취약한 계층에서 많은 피해를 입었으나, 사기수법이 날로 진화하면서 **연령, 계층과 상관없이 무차별적으로 발생**하고 있습니다.
- 최근에는 이름, 주민번호, 주소 등 **개인신상정보를 미리 알려주면서 정보유출 또는 해킹사고 등 사회적 이슈사건 등과 연계**하여 치밀하게 접근하기 때문에 누구도 전화금융사기로부터 자유로울 수 없는 상황이 되고 있습니다.

전화금융사기 발생 현황



* 자료 : 경찰청

2 피해 유형

사기범이 피해자를 유인하는 방식은 크게 5가지 유형으로 집약됩니다.

[첫째, 보호형] 검찰, 경찰, 금융감독원 등 공공기관 및 금융기관을 사칭하며 개인정보 또는 **금융정보유출이나 범죄 사건 연루 등으로부터 피해자를 보호**해 주겠다고 유인하는 방식입니다. 가장 흔한 보이스피싱 유형입니다.

[둘째, 협박형] 피해자의 자녀를 납치하여 데리고 있다고 속이는 방식입니다. **자녀나 부모의 신상정보를 미리 파악하여 접근**하기 때문에 사기성공율이 높은 편에 속합니다.

[셋째, 지인사칭형] **가족, 친구, 직장동료 등 지인을 사칭하며 급전, 교통사고 합의금 등 긴급자금을 요구**하는 방식입니다. 메신저 또는 문자메시지로 이미 등록되어 있는 지인의 아이디나 전화번호로 접근하기 때문에 속기 쉬운 유형입니다.

[넷째, 보상제공형] 초과 납부한 **연금, 보험금, 세금 등을 환급해 준다거나 경품 등에 당첨**되었다고 피해자를 유인하는 방식입니다. 초기에 노인층을 대상으로 많이 발생했던 유형입니다.

[다섯째, 의무부과형] 동창회, 대학 등을 사칭하며 회비를 요구하거나 대학추가합격 등록금 납부를 요구하는 방식입니다. 동 유형도 **동창회 명부, 대학 지원현황자료 등을 미리 확보하여 접근**하기 때문에 피해자가 속기 쉬운 유형입니다.

IV 보이스피싱 피해예방 요령

1 금융거래정보 요구는 일절 응대하지 말 것

- 전화로 개인정보 유출, 범죄사건 연루 등을 이유로 계좌번호, 카드번호, 인터넷뱅킹 정보를 묻거나 인터넷 사이트에 입력을 요구하는 경우 절대 응하지 마시기 바랍니다.

공공기관 사칭 금융사기



정보유출, 범죄연루 보호조치 믿으면 안돼요!

경찰청, 경찰청, 금융감독원 등 공공기관은 전화로 개인정보나 금융거래정보를 묻지 않아요. 믿으면 안돼요.

피싱사이트 금융사기



안돼요. 믿으면 안돼요. 아무리 홈페이지가 똑같아도 공공기관은 홈페이지를 통해 금융거래정보를 묻지 않아요.

* 피싱사이트의 특징은 go.kr/or.kr 등의 공공기관 주소가 아닌 net/com 등의 주소를 쓰고 개인정보 또는 금융정보를 입력하도록 유인하는 특정 코너 이외의 다른 코너는 대부분 활성화되지 않는 경우가 많습니다.

→ 사기범이 불러주는 전화번호나 인터넷 주소를 통하지 말고, 반드시 **114 또는 포털사이트 등을 통해 확인**한 전화번호나 홈페이지 통해 접속하시기 바랍니다.

2 현금지급기로 유인하면 100% 보이스피싱

- 현금지급기를 이용하여 세금, 보험료 등을 환급해 준다거나 계좌안전조치를 취해주겠다면서 현금지급기로 유인하는 경우 절대로 응하지 마시기 바랍니다.

계좌이체 유도 금융사기



예금보호조치, 믿으면 안돼요♪

♪ 경찰도 은행도 금융감독원도 현금인출기로 예금보호조치를 하지 않아요. 믿으면 안돼요. ♫ 전화 끊으세요.

3

자녀납치 보이스피싱에 미리 대비

- 자녀납치 보이스피싱 대비를 위해 평소 자녀의 친구, 선생님, 인척 등의 연락처를 미리 확보해 두시기 바랍니다.

자녀납치 사기전화



자녀납치, 주변 지인 도움 요청하세요♪

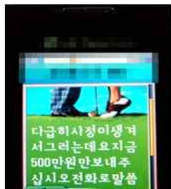
♪ 자녀납치 전화를 받은 경우 침착히 대응하면서 **지인** 등을 통해 **자녀안전 여부**를 확인하세요.

4

개인·금융거래정보를 미리 알고 접근하는 경우에도 내용의 진위를 확인

- 최근 개인·금융거래정보를 미리 알고 접근하는 경우가 많으므로 전화, 문자메시지, 인터넷메신저 내용의 진위를 반드시 확인하시기 바랍니다.

메신저, 문자메시지 사기



전화 또는 문자메시지, 진위여부 확인하세요♪

♪ 동창회, 친구, 대학입시처, 거래처 등을 가장하여 메신저 또는 문자메시지로 계좌번호를 알려주며 송금을 요구하거나 물품대금 송금 오류로 반환을 요구하는 경우 **사실관계나 입금내역**을 확인하세요.

5 피해를 당한 경우 신속히 지급정지를 요청

- ☐ 보이스피싱을 당한 경우 경찰청 112콜센터 또는 금융회사 콜센터를 통해 신속히 사기계좌에 대해 지급정지를 요청하시기 바랍니다.

계좌이체 시 대응요령



전화사기범들 계좌에 **자금을 이체**한 경우

➡ 신속히 **1 1 2** 로 지급정지 요청하세요!

6 유출된 금융거래정보는 즉시 폐기

- ☐ 유출된 금융거래정보는 즉시 해지하거나 폐기하시기 바랍니다.

유출 금융정보 폐기



유출된 금융거래정보, 신속히 해지 또는 폐기하세요!

개인정보를 악용한 추가적인 피해가 우려되는 경우 가까운 은행에 방문하여 “**개인정보노출자 사고예방시스템**”에 등록하세요.

- 통장이나 현금(체크)카드 양도 시 범죄에 이용되므로 어떠한 경우에도 타인에게 양도하시면 안됩니다.
- 통장이나 현금(체크)카드 양도는 전자금융거래법 위반으로 형사처벌을 받을 수 있는 범죄입니다.(3년 이하의 징역 또는 2천만원 이하의 벌금)

예금통장 양도 금지



예금통장양도, 절대 안돼요♪

♪ 예금통장 매매는 불법 행위로 형사처벌을 받을 수 있습니다.
 ♪ 대출, 취업 등을 미끼로 통장이나 카드를 양도하는 경우에도 형사처벌을 받을 수 있으며 비대면 인출 거래제한 등 큰 불편을 초래하므로 절대 안돼요.

☎ 전화금융사기 피해신고 및 피해상담 안내

피해신고 및 상담내용	피해신고 및 상담기관
① 지급정지 요청	경찰청 (☎ 112콜센터), 금융회사 (☎ 각 콜센터)
② 피해구제신청서 제출	금융회사 (본점 또는 영업점)
③ 피싱사이트 신고	한국인터넷진흥원 (☎ 118) 금융감독원 (☎ 1332)
④ 피해상담 및 환급제도 안내	금융감독원 (☎ 1332)

V 전기통신금융사기 피해금 환급제도

◇ 2011.9.30일부터 「전기통신금융사기 피해금 환급에 관한 특별법」이 시행됨에 따라 보이스피싱으로 지급정지된 피해금을 소송절차 없이 환급받을 수 있게 되었습니다.

- 피해자의 피해구제신청으로 지급정지된 사기이용계좌에 인출되지 않고 남아 있는 금액이 있는 경우 그 범위내에서 2개월간의 채권소멸절차를 거쳐 신속하게 돌려드립니다.
(총 3개월정도 소요)

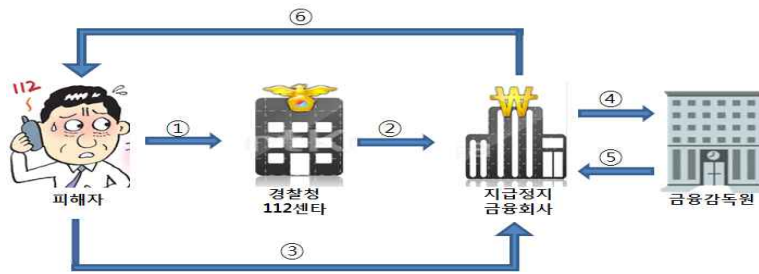
☞ **(피해구제신청 방법)** 전화로 사기범계좌에 대해 신속히 지급정지를 신청한 후 신청일부터 3일 이내에 신분증과 경찰서로부터 발부받은 피해신고확인서(사건사고사실확인서)를 지참하여 거래은행 또는 사기이용계좌 개설 은행에 피해구제신청서를 제출하시면 됩니다.

<유의 사항>

※ 피해금을 반환받기 위해서는 사기이용계좌에 잔액이 남아 있어야 하므로 피해자가 가장 먼저 취할 조치는 112콜센터를 통해 신속하게 지급정지를 요청하는 것임을 명심하여야 합니다.

‘12.2월부터는「전기통신 금융사기 피해금 환급제도」적용 대상에서 제외된 대출사기 건에 대해서도 지급정지가 가능하오니 사기 피해 발생 즉시 각 은행 콜센터를 통해 지급정지를 요청하시기 바랍니다.

< 보이스피싱 피해신고 및 피해금 환급절차 >



- ① **(보이스피싱 피해자)** 경찰청 112센터에 보이스피싱 피해 신고
 - ② **(경찰청)** 피해자의 신고전화를 사기범계좌 보유 금융회사에 연결(경찰청과 금융회사간 핫라인 이용), 금융회사는 즉시 지급정지 조치
 - ③ **(보이스피싱 피해자)** 지급정지 금융회사에 "피해구제 신청서" 제출
 - ④ **(금융회사)** 금융감독원에 사기범계좌에 대한 채권소멸절차 개시공고 요청
 - ⑤ **(금융감독원)** 홈페이지에 2개월간 채권소멸절차 개시공고 후 피해자별 피해환급금을 결정하여 금융회사에 통보
 - ⑥ **(금융회사)** 피해자에게 피해금 환급(피해자 계좌에 입금)
- 피해구제신청서 제출이후 3개월 이내 피해금 지급 완료

VI 보이스피싱 예방관련 주요 제도

1 이미 실행중인 제도

1 단기간내 다수의 예금통장을 개설하고자 하는 경우 거래목적을 명확히 소명하여야 합니다.

- 최근 1개월내 2개 이상의 요구불 예금통장을 개설하는 경우 은행에서 구체적인 거래목적을 확인하게 되며 거래 목적이 불분명한 경우 계좌개설을 거절할 수 있습니다.

2 예금통장이 보이스피싱에 이용되어 지급정지되는 경우 그 명의인은 정상적인 금융거래가 어려워집니다.

- 전화금융사기로 지급정지된 계좌의 명의인은 국내 다른 모든 계좌에 대해서도 CD기 인출, 인터넷뱅킹 등 비대면 인출거래가 제한됩니다.
- * 수사기관의 최종 처분결과서를 사기이용계좌 개설은행에 제출 하는 경우 비대면인출거래 제한조치는 해제됩니다.

3 장기간 계좌이체 실적이 없는 경우 CD/ATM를 통한 고객의 이체한도가 축소됩니다.

- 최근 1년간 이체실적이 없는 계좌의 CD/ATM의 1일 및 1회 이체한도가 70만원으로 축소됩니다.
- * 이체한도 복원을 위해서는 본인이 별도로 해당 금융회사에 한도 상향조정을 요청하여야 됩니다.

2 2012년 시행(예정) 제도

- 1 300만원 이상의 현금 입금액을 자동화기기를 통해 인출할 경우에는 입금된지 10분후에 인출이 허용됩니다.

→ '12.6.26일 시행

- 2 300만원 이상의 카드로 대출은 카드로 승인사실 안내 후 2시간 후에 입금이 되며, 통장 거래내역에 카드로임을 알 수 있도록 표시됩니다.

→ '12.5.17(일부 21)일 시행

- 3 공인인증서의 재발급 및 사용절차가 강화 됩니다.

→ '12.3분기 중 시범실시 및 추후 확대시행 예정

- 4 대포통장으로 의심되는 계좌명의인(예금통장 양도 계좌주) 정보를 은행연합회에 집중하여 상당기간 관리하며, 계좌주는 금융거래 시 불이익을 받을 수도 있습니다.

→ '12.4분기 시행 예정

- 5 금융회사들의 보이스피싱 혐의계좌에 대한 정보공유 등의 방법을 통해 모니터링이 더욱 강화 됩니다.

→ '12.4분기 시행 예정

VII 보이스피싱 피해사례

1 과거에 주로 발생한 사례

1 피해자를 기망하여 자동화기기로 유인 편취 (피해자는 이체사실을 모름)

<사기수법>

- ☐ 수사기관 직원을 사칭하는 자가 피해자에게 전화를 하여 피해자의 계좌가 사건(범죄)에 연루되어 피해자명의 계좌의 안전조치가 필요하다고 기망하여 현금지급기로 유인, 기기를 조작하게 하여 자금을 편취
- ☐ 국세청, 건강보험공단, 국민연금관리공단 직원 등을 사칭하는 자가 피해자에게 전화하여 세금, 보험료, 연금 등이 과다 또는 오류 징수되어 환급하여 주겠다고 자동화기기로 유인, 기기를 조작하게 하여 자금을 편취

<피해사례>

(사례 1)

- ☐ A씨(60대, 남)는 검찰수사관을 사칭하는 자로부터 “사기범을 검거했는데 A씨 명의의 계좌를 사용하고 있어 금감원 직원이 계좌안전조치를 해줄 것이니 현금지급기로 가서 기다리라”는

전화를 받고 현금지급기로 가서 기다리던 중 금감원 직원을 사칭하는 자가 전화로 현금지급기를 조작토록 유도하여 1,300만원의 피해를 봄

(사례 2)

- H씨(40대, 여)는 우체국직원을 사칭하는 자로부터 ARS로 “안녕하십니까, 우체국직원 000입니다. 고객님의게 발송된 택배가 반송되었습니다. 상담을 원하시면 9번을 누르세요”라는 전화를 받고 상담을 받았는데,
 - 우체국직원을 사칭하는 자가 “개인정보가 노출되었으니 신고해 주겠다”고 한 후 전화를 끊고, 잠시후 경찰을 사칭하는 자가 전화를 걸어 “피해접수를 해주겠다. 금융거래 안전을 위해 계좌안전조치가 필요하니 현금지급기로 가라”고 하면서 기기를 조작케 유도하여 730만원의 피해를 봄

(사례 3)

- D씨(40대, 남)는 건강보험공단 직원을 사칭하는 자로부터 “의료보험료가 많이 걸렸으니 과납된 보험료 50만원을 주겠다. 불러주는 환급등록번호를 가지고 CD기 앞으로 가라”는 전화를 받고 CD기로 가서 기다리던 중, 건강보험공단 직원을 사칭하는 자가 전화로 자동화기기를 조작토록 유도하여 600만원의 피해를 봄

**2 피해자를 기망하여 피해자에게 자금을 이체토록하여 편취
(피해자는 이체사실을 알고 있음)**

<사기수법>

- ☐ 검찰, 경찰, 금융감독원 등 공공기관 및 금융기관을 사칭하는 자가 누군가 피해자를 사칭하여 예금인출을 시도한다고 기망한 후 거래내역 추적을 위해 필요하다면서 사기범이 불러주는 계좌로 이체토록한 후 편취
- ☐ 사기범들이 학생의 대학지원 명세를 빼내 실제 대학교의 전화번호로 변조하여 학부모 및 학생에게 전화해서 사기범 계좌로 등록금 납부를 요구하여 편취

<피해사례>

(사례 1)

- ☐ H씨(30대, 남)는 ○○은행 직원이라는 자로부터 “누군가 당신의 신분증을 가지고 돈을 찾아가려고 한다. 경찰에 신고 해주겠다”는 전화를 받았는데,
 - 잠시후 경찰을 사칭하는 자가 다시 전화를 걸어 “내가 시키는 대로 해라. 당신 통장 계좌에 있는 거래내역을 추적해야 하니 내가 불러주는 계좌로 돈을 이체시켜라”는 말에 속아 5개 계좌에 3,000만원을 이체하여 피해를 봄

(사례 2)

- ☐ 대학 지원자인 G씨(20대, 여)는 오후 1시경 대학교 교직원을 사칭하는 자로부터 “지원한 대학에 추가합격하였으니 금일

오후 4시까지 등록금 530만원을 입금하여야만 등록처리 된다”는 전화를 받고 부모에게 연락하여 사기범이 불러주는 계좌로 동액을 입금하여 피해를 봄

3 자녀납치 및 사고 빙자 편취

<사기수법>

- ☐ 자녀와 부모의 전화번호 등을 사전에 알고 있는 사기범이 자녀의 전화번호로 발신자번호를 변조,
 - 부모에게 마치 자녀가 사고 또는 납치 상태인 것처럼 가장하여 부모로부터 자금을 편취하는 수법으로, 학교에 간 자녀 납치 빙자, 군대에 간 아들 사고 빙자, 유학중인 자녀 납치 또는 사고 빙자 등의 유형이 있음

<피해사례>

(사례 1)

- ☐ Y씨(40대, 여)는 오후 1시경 자녀의 이름과 학교를 대면서 “지금 당신 아이를 납치하였다. 허튼 수작하면 죽어버린다. 1,000만원을 불러주는 계좌로 송금해라”는 전화를 받고 보유하고 있던 300만원을 사기범 계좌로 이체하여 피해를 봄

(사례 2)

- ☐ K씨(50대, 여)는 오전에 사기범으로부터 “학교 행정실인데 아이가 머리를 다쳐서 치료를 해야 하니 1,000만원을 입금하라”는 전화를 받고 800만원을 입금하여 피해를 봄. 사기범은 자녀 이름, 휴대전화 번호, 학교이름을 정확히 알고 있었음

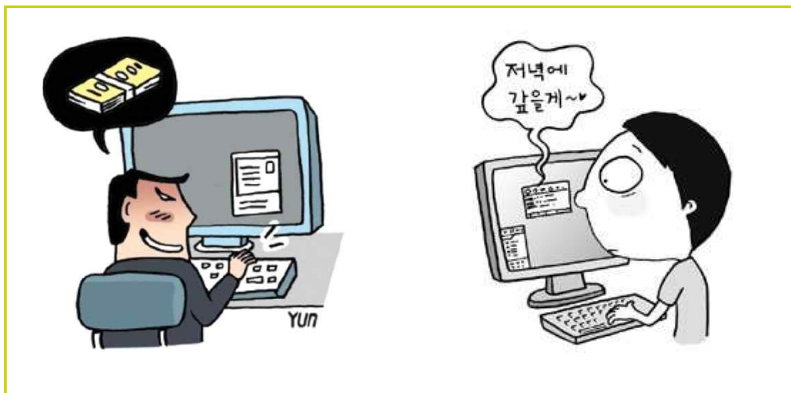
4 메신저 피싱

<사기수법>

- 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
- 메신저피싱 역시 해외에 서버를 두고 해킹하는 경우가 많고 대포통장을 이용하기 때문에 범인검거가 쉽지 않음

<피해사례>

- 회사원 E씨(28세, 여)는 오후 4시경 친언니의 네이트온 아이디를 도용한 사기범으로부터 “급하게 송금해줘야 할 데가 있으니 000명의 계좌로 270만원을 송금해주면 저녁에 주겠다”는 메시지를 받고 송금하여 피해를 봄



2 최근에 주로 발생하는 사례

1 ARS를 이용한 카드론 대금 편취 (전화를 통해 금융거래정보 획득)

<사기수법>

- 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

<피해사례>

- P씨(60대, 남)는 경찰청 수사관을 사칭하는 자로부터 “당신의 예금계좌가 범죄에 연루되었으니 신용카드번호와 비밀번호 등을 알려달라”는 전화를 받고 신용카드정보를 알려주었는데,
 - 이후 사기범이 동 정보를 이용하여 피해자 명의의 신용카드(4장)로 피해자 명의의 카드론 4,800만 원을 받은 후 다시 피해자에게 전화를 해서,
 - 당신의 통장에 범죄자금 4,800만 원이 입금되었으니 국가안 전계좌로 이체하라고 요구, 피해자는 사기범이 불러주는 계좌로 4,800만 원을 이체하여 피해를 봄

■ 인터넷 뱅킹을 이용해 카드론 대금 및 예금 등 편취 (피싱사이트를 통해 금융거래정보 획득)

<사기수법>

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

<피해사례>

- L씨(20대, 여)는 오후 1시경 경찰청 수사관을 사칭하는 자로부터 “최근 사기범을 검거하였는데 당신 명의의 통장이 범죄에 이용되고 있다”는 전화를 받고 그러한 사실이 없다고 하자,
 - 사기범이 “개인정보가 유출되어 명의가 도용된 것 같다. 신속히 경찰청 홈페이지에 접속하여 개인정보 침해신고를 해야 한다”고 강요하여
 - 피해자는 사기범이 알려준 경찰청 홈페이지를 가장한 피싱 사이트에 접속하여 거래은행명, 계좌번호 및 계좌비밀 번호, 이체비밀번호, 보안카드번호, 신용카드(3장) 번호 및 비밀번호, CVC번호 등을 입력하였음

- 그러자 사기범은 피해자가 입력한 금융거래정보 등을 이용하여 공인인증서를 재발급 받고, 피해자 명의로 카드로 2,000만원을 받은 후 인터넷뱅킹을 이용해 카드로 대금 2,000만원과 피해자 명의의 마이너스통장에서 1,300만원 등 합계 3,300만원을 사기범계좌로 이체하여 편취

■ 3 상황극 연출에 의한 피해자 기망 편취

<사기수법>

- 은행직원, 경찰·검찰 수사관을 사칭한 사기범들이 은행 객장과 경찰서, 검찰청 등의 사무실에서 실제로 일어나는 상황 연출로 피해자를 기망하여 금전 편취

<피해사례>

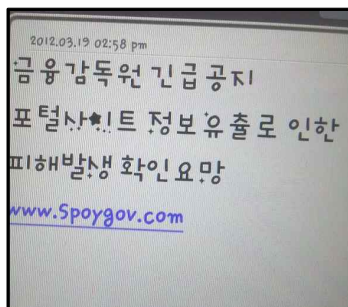
- J씨(50대, 남)는 은행의 객장을 연상케하는 소리(도장찍는 소리, 고객을 부르는 소리 등)가 들려오는 상황에서 은행 직원을 사칭하는 자로부터 “누군가 당신의 신분증을 가지고 돈을 찾아가려고 한다. 경찰에 신고해 주겠다”는 전화를 받았는데,
- 이후 경찰서 사무실을 연상케하는 소리(타이핑 소리, 동료 형사를 부르는 소리 등)가 들려오는 상황에서 수사관을 사칭하는 자로부터 “내가 시키는 대로 해라, 당신 통장 계좌에 있는 거래내역을 추적해야 하니 내가 불러주는 계좌로 돈을 이체시켜라”는 전화를 받고 사기범이 불러주는 계좌로 1,250만원을 이체하여 피해를 봄

**4 금융회사, 금감원 명의의 허위 긴급공지 문자메시지로
기망, 피싱사이트로 유도하여 예금 등 편취**

<사기수법>

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

<금융감독원 사칭 문자메시지>



<금융회사 사칭 문자메시지>



<피해사례>

- D씨(40대, 여)는 국민은행 명의의 보안승급 안내 문자메시지를
받고 아무런 의심 없이 문자메시지에 안내된 사이트에 접속하여
카드번호, 계좌번호 및 공인인증서 정보를 입력하였는데,
 - 이후 예금인출 500만원 및 대출 1,000만원 등이 실행된
것을 확인하고 은행에 문의한 결과 보안승급 자체가 없다는
말을 듣고 지급정지를 요청하였으나 이미 전액 출금된
상태였음

5 물품대금 오류송금 빙자로 피해자를 기망하여 편취

<사기수법>

- 사기범이 문자메시지 또는 전화로 물품대금, 숙박비 등을 송금하였다고 연락한 후, 잠시후 실수로 잘못 송금하였다는 면서 반환 또는 차액을 요구하여 편취

<피해사례>

- 사기범 P씨는 피해자 L씨로부터 고구마 10박스를 45만원에 구입하기로 하고, 마치 450만원으로 입금한 것처럼 피해자에게 문자 메시지(발송자 명의를 농협으로 조작)를 전송하였음
 - 이후 피해자 L씨(50대, 남)는 OO농협 365코너에서 P씨와 핸드폰으로 통화하는 과정에서 P씨로부터 “고구마 대금 10박스 45만원을 입금하면서 텔레뱅킹을 하다보니 실수로 0을 더 눌러 450만원을 입금하였다”는 말을 듣고 그 차액인 405만원을 사기범에게 이체하여 피해를 봄