



통신서비스 피해예방 매뉴얼





목 차

1. 온라인 메신저를 이용한 피싱	2
2. 대출 또는 현금지급 조건 휴대폰 개통사기	3
3. 불법메시지를 이용한 스미싱	4
4. 송금오류를 빙자한 금전요구	9
5. 불법사이트(악성코드)를 이용한 파밍	10
6. 상황극 연출에 의한 보이스피싱	12
7. 인증절차 없이 이루어지는 앱 결제시의 피해	13
8. 무료 콘텐츠 사이트 가입 유도 후 이용시 결제 피해	14
9. 유료방송 무료이벤트 후 자동 유료전환 및 요금청구	16
10. 유료방송 계약시 미고지한 수신기 대금 청구	18
참고 : 방송통신서비스 관련 민원기관	19





1 온라인 메신저를 이용한 피싱

수 법

- 다른 사람의 개인정보(아이디(ID), 비밀번호 등)를 도용하여 인터넷 메신저에 로그인한 후 등록되어 있는 친구, 가족 등에게 1:1 채팅 또는 메시지를 보내 급히 돈이 필요하니 보내달라고 요청
 - ※ 메신저 : 인터넷을 통해 실시간으로 메시지와 데이터를 무료로 주고 받을 수 있는 컴퓨터 프로그램.
예) 네이트온, 카카오톡 등
 - ※ 피싱(Phishing) : 개인정보와 낚시의 합성어로 전화, 이메일, 인터넷 사이트를 통해 금융 정보를 몰래 빼가는 수법

피해사례

- 대학생 A씨(24세, 여)는 친한 언니의 네이트온 아이디를 도용한 사기범으로부터 "급하게 송금해줘야 할 데가 있는데 보안카드를 안가지고 나와서 돈을 송금할 수 없으니 000명의 계좌로 30만원을 송금해주면 저녁에 주겠다"는 메시지를 받고 송금하여 피해 발생



예 방법

- 메신저 비밀번호는 주기적으로 변경하고 사용하지 않는 메신저 아이디는 삭제
- 각 메신저별 아이디와 비밀번호는 가급적 다르게 설정
- 메신저나 SNS의 개인정보 공개 설정 범위를 직접 확인하고 필요한 만큼만 공개

구제

- 메신저 피싱이 의심될 경우 피해자는 피해금을 송금·이체한 계좌의 금융회사에 지급정지 및 경찰서(신고전화 112)를 통해 피해 내용 신고

2 대출 또는 현금지급 조건 휴대폰 개통사기

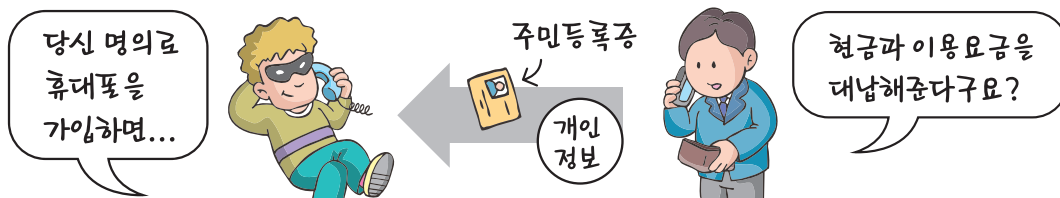


수 법

- 휴대폰 문자메시지, 지하철 쪽지 광고를 통해 "신용등급이 낮아도 소액대출이 가능합니다."라는 문자를 보내 대출문의가 들어오면 서류(신분증, 인감증명서 등)를 요청하여 신청된 서류를 활용해 휴대폰 개통

피해사례

- 주부 K씨(34세, 여)는 대출을 받기 위해 대출업자에게 본인의 개인정보(주민등록사본, 인적사항 및 신용카드 번호 등)를 보낸 이후 대출이 불가능하다는 사유로 서류는 반송 받았으나 본인도 모르는 사이에 휴대폰 개통되어 단말기 대금 및 이용요금 발생
- 회사원 B씨(25세, 남)는 휴대폰 광고전화를 받고, 본인 명의로 가입하여 휴대폰을 킷서비스 및 택배 등으로 보내주면 현금 40만원과 단말기 대금 및 이용요금을 대납해준다고 하여 휴대폰을 제공하였으나 현금지급 조건이 이행되지 않아 단말기 대금 및 이용요금 발생



예 방법

- 휴대전화를 개통하여 타인에게 제공하거나 개통에 필요한 서류를 넘겨주는 일이 없어야 함
- 불법대출업체에 신분증 및 신용카드 등 개인정보를 제공한 경우에는 신분증 재발급 및 해당 신용카드 해지 등을 통해 피해 방지
- 대출 또는 현금지급 조건 휴대폰 개통을 시도한 경우 관련 각 통신사 또는 명의도용방지서비스(www.msafar.or.kr)에서 본인명의로의 휴대폰 개통 여부 확인 필요

피해구제

- 피해를 입은 경우, 통신사업자(이동전화 114)에게 즉시 신고하며 해결이 되지 않을 경우 통신민원조정센터(080-3472-119)와 경찰서(신고전화 112)에 신고하여 도움 요청
- ※ 한국정보통신진흥협회의 명의도용방지서비스(www.msafar.or.kr)를 이용하여 본인 명의로 개통된 통신서비스 확인 및 이동전화 가입제한 서비스(무료)를 통해 불법개통을 사전에 차단 가능



3 불법메시지를 이용한 스미싱

① 할인쿠폰 문자 메시지를 이용한 스미싱

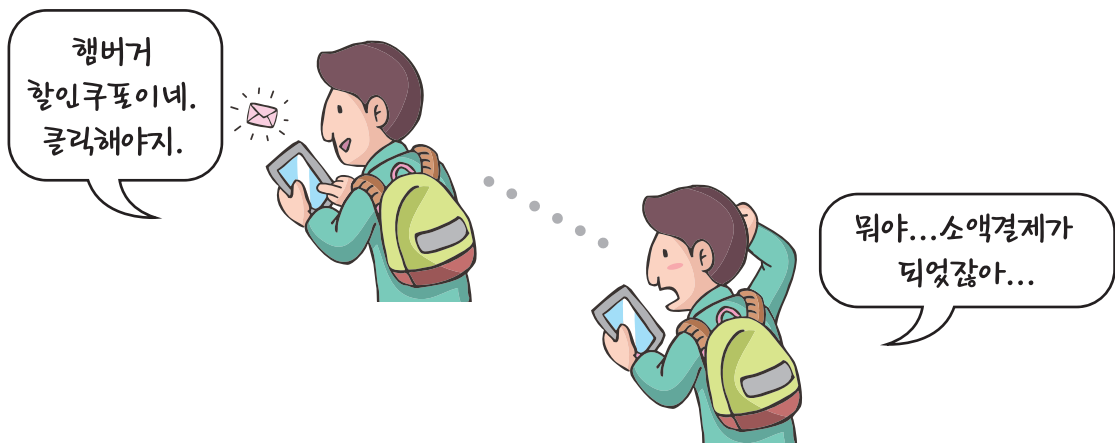
수 법

- 유명 패스트푸드, 외식업체 등에서 무료쿠폰 또는 할인쿠폰을 제공한다는 문자 메시지를 보내 링크된 사이트에 접속하도록 유도한 후 이용자가 문자 메시지에 링크된 사이트를 접속하였을 경우 게임 사이트 등에서 소액결제 발생

※ 스미싱(Smishing) : 문자메시지와 피싱의 합성어로 피해자가 모르는 사이에 소액결제 피해 발생 또는 개인·금융정보를 탈취하는 수법

피해사례

- 대학생 H씨(21세, 남)의 휴대폰으로 "[OOOO] 불고기버거세트 50%할인쿠폰 2매(전매장사용가능) http://tiny.cc/h*****we"라는 문자가 도착하여 확인을 위해 링크된 사이트를 클릭하는 순간 악성코드가 휴대폰에 설치되어 소액결제 피해 발생



※ 예방법과 피해구제법은 7페이지 참고



② 초대문자 메시지를 이용한 스미싱

수 법

- 돌잔치, 모바일 청첩장 등 지인의 초대문자로 오인하게 만들어 해당 문자 메시지에 링크된 사이트를 접속하게 되면 소액결제 발생

피해사례

- 회사원 A씨(35세, 남)는 "모바일 돌잔치 초대장을 보내드렸습니다. 참석하여 주시기 바랍니다. 돌잔치 오시는길 <http://oa.to/pJaZv>"라는 문자를 받고 하단의 인터넷 주소를 무심코 눌러 인터넷에 연결되고, 한 달 뒤 소액결제 피해 발생



※ 예방법과 피해구제법은 7페이지 참고



3 불법메시지를 이용한 스미싱

③ 무료증정 문자메시지를 이용한 스미싱

수 법

- 온라인 게임에서 사용되는 게임머니나 캐쉬 등을 무료로 증정하겠다는 문자를 받고 앱을 다운로드 할 시 악성코드가 설치되어 소액결제 발생

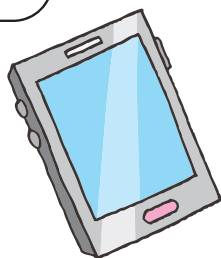
※ 스미싱 피해단계

- ①피해자가 문자메시지 인터넷주소 클릭 → ②스마트폰에 악성코드 설치 → ③범인에게 소액결제 인증번호 전송 → ④범죄자는 게임 아이템 또는 사이버머니 구입 → ⑤소액결제(30만원 이하) 대금 청구

피해사례

- 회원 L씨(32세, 남)는 "000게임머니 무료 증정! 지금 즉시 받아주세요! <http://od.fjd/Kgds>"라는 문자를 받고 평소 즐기던 게임이라 의심없이 인터넷 주소에 접속하였고, 그 후 휴대폰 인증을 통한 사이버머니 35,000원이 결제되는 피해 발생

게임머니 무료 증정!
<http://od.fjd/Kgds>



클릭





예 방법

- 소액결제 이용이 없는 이용자는 해당 통신사로 휴대전화 소액결제 차단을 요청하거나, 이용 패턴에 맞게 결제 금액 제한 신청

〈통신사별 소액결제 차단·제한방법〉

통신사	소액 결제 차단·제한 방법
SKT	자신의 스마트폰으로 114를 눌러 SK텔레콤고객센터 연결 → 상담원과 연결 → 소액 결제 모두 차단 또는 제한
KT	자신의 스마트폰으로 114를 눌러 KT모바일고객센터로 연결 → 상담원과 연결 → 소액 결제 모두 차단 또는 제한 (오프라인 결제·무선결제·청구대행·본인인증차단 등 선택)
LGU+	자신의 휴대폰으로 114를 눌러 LGU+ 고객센터로 연결 → 상담원과 연결 → 소액 결제 모두 차단 또는 제한

- 백신프로그램 설치 및 주기적인 업데이트, 실시간 감시상태 유지
- 앱스토어, 플레이스토어, T스토어, 올레마켓, U+앱마켓 등 공인된 오픈마켓을 통해 앱 설치
- 알 수 없는 출처의 앱 설치 제한
 - ※ 스마트폰의 보안설정 강화방법
: 환경설정 > 보안 > 디바이스관리 > '알 수 없는 출처'에 √체크 해제
- 스마트기기의 앱 설치시 "앱 권한" 화면에서 앱의 원래 목적·기능과 무관한 권한이 주어지는지 확인 후 의심 가는 경우 설치 중지
- 인터넷상에서 다운받은 안드로이드, 아이폰용 파일은 스마트기기에 저장 및 설치 금지

피해구제

- 경찰서(신고전화 112)에 스미싱 피해 내용을 신고하여 '사건사고 사실확인원' 발급 후 통신사업자, 게임사, 결제대행사 등 관련 사업자에게 제출



3 불법메시지를 이용한 스미싱

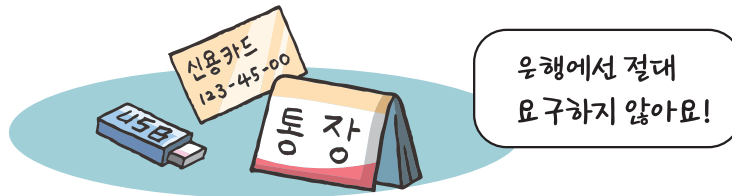
④ 금융권 명의 사칭 메시지로 인한 스미싱

수 법

- 은행, 금융회사, 국정원, 경찰 등에서 보내는 안내문자인 것처럼 문자메시지를 발송하여 인터넷 주소를 통해 접속하게 되면 가짜사이트로 유도하여 금융거래 정보를 입력하게 한 후 그 정보를 이용하여 계좌의 돈을 빼가거나 온라인 대출 신청

피해사례

- 회사원 Y씨(31세, 남)는 평소 자신이 이용하던 은행명의로 "[OO은행] OO사이트 정보유출로 인한 피해 발생. 보안승급 후 이용해주세요. bank.ohd" 라는 문자를 받고 안내된 사이트로 접속하여 보안승급을 위해 계좌번호, 공인인증서 정보를 입력하였고, 이후 계좌에 있던 320만원 인출과 온라인 대출 2,000만원 등 피해 발생



※ 은행, 금융회사, 국정원, 경찰 등에서는 금융정보를 묻거나 홈페이지에 개인정보 입력을 요구하지 않음

예 방법

- 문자메시지로 제공된 인터넷 주소 접속 금지 및 포털사이트 검색 등을 통해 확인 후 접속
- 공공기관 및 금융회사의 일반적인 인터넷 주소 체계도
 - 검찰, 경찰 등 국가기관 : www.△△△.go.kr
 - 금감원 등 공공기관 : www.△△△.or.kr
 - 은행 등 금융회사 : www.△△△.com 또는 △△△.co.kr

피해구제

- 피해를 당한 경우 경찰서(신고전화 112) 혹은 금융회사 콜센터를 통해 신속한 지급 정지 요청 필요

4 송금오류를 빙자한 금전요구

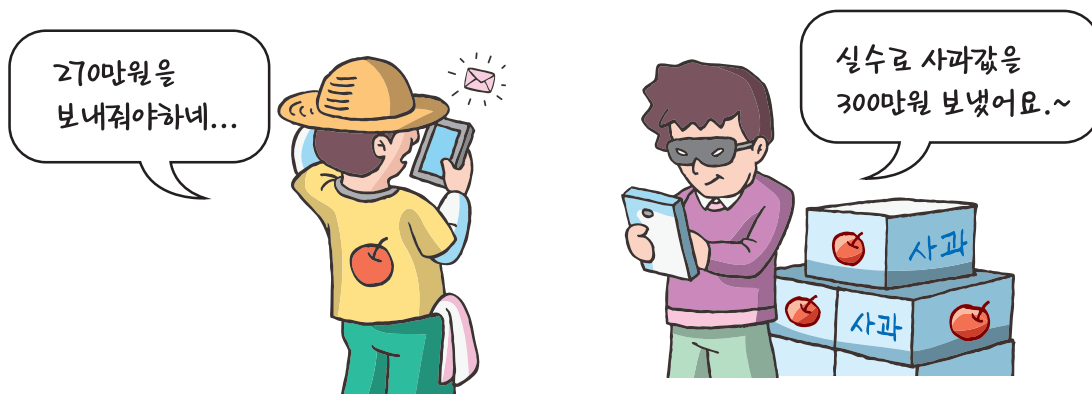


수 법

- 온·오프라인에서 물건을 구매 후 문자 또는 전화로 결제대금을 실수로 잘못 송금하였다며, 구매가격의 차액 반환 요구

피해사례

- 농산물판매직 L씨(45세, 남)는 온라인매장에서 한 구매자에게 사과 5박스를 30만원에 판매를 하였고, 이후 결제대금을 실수로 300만원으로 입금하였다는 문자를 받아 30만원을 제외한 270만원을 구매자에게 송금하여 피해를 발생



예 방법

- 메시지를 통한 금전 요청 시, 즉시 판매자 계좌에 결제대금이 제대로 이체 되었는지 확인 후, 구매자를 상대로 본인여부를 확인하고 타인 명의의 통장으로는 송금금지

피해구제

- 송금오류를 빙자해 금전요구 시 이체한 경우 피해자는 피해금을 송금·이체한 계좌를 관리하는 금융회사에 지급정지 신청 및 경찰서(신고전화 112)



5 불법사이트(악성코드)를 이용한 파밍

① 은행사이트 팝업창을 이용한 파밍

수 법

- 금융기관의 명칭 및 로고까지 동일한 사이트를 개설하고 이용자로 하여금 계좌 번호와 비밀번호, 보안카드번호를 입력하게 하여, 이 자료를 이용하여 공인 인증서 재발급, 계좌 잔액 인출, 카드론 대출, 마이너스통장 개설, 적금 해지 신청

※ 파밍(Pharming) : 악성코드에 감염된 PC를 조작해 정상적인 홈페이지 주소로 접속하여도 피싱(가짜) 사이트로 유도되어 개인 금융 정보 등을 몰래 빼가는 수법

피해사례

- J씨(37대, 남)는 인터넷뱅킹을 하기 위해서 사무실 컴퓨터를 통해 은행사이트로 접속하자 금융감독원을 사칭한 보안인증 팝업창이 뜨는 것을 확인하고, 파밍 사이트에 접속하여 개인금융거래정보를 입력하라는 내용을 보고, 의심없이 관련 정보를 일체 입력 하였고, 이후 약 한 시간 동안 총 20회에 걸쳐 5,200만원 상당의 금전 피해 발생



② 온라인 쇼핑몰 결제를 이용한 파밍

수 법

- 악성코드에 감염된 PC로 온라인 매장에서 물건을 구매하고 결제할 경우, 피싱 사이트로 접속하게 한 후 개인금융정보를 빼내어 계좌의 돈을 빼가거나 온라인 대출 신청



피해사례

- D씨(28세, 여)는 최근 온라인 쇼핑몰 매장에서 옷, 악세사리 등을 구매하였고, 결제 수단으로 실시간 계좌이체를 선택하여, 결제창에 바로가기를 클릭하였으나, 이미 악성코드에 감염된 PC로 인해 피싱사이트로 유도된 사실을 모른 채 금융거래정보를 입력하였고, 이때 유출된 정보로 피해자 명의의 인터넷뱅킹을 통해 168만원이 이체되어 피해 발생



예방법

- 공인인증서는 하드디스크가 아닌 USB 등 보조기억매체에 별도 보관
- 백신/보안프로그램 최신버전 유지 및 정기적인 검사를 실시
 - ※ 사이버경찰청, 네탄(Netan) 등에 게시되어 있는 '파밍캡' 활용
- 사이트 주소 정상여부 확인 및 출금 계좌번호 마우스 입력 활용
 - ※ 정상적인 금융사이트 주소일 경우 주소창의 배경색이 흰색에서 초록색으로 변경되며 자물쇠 아이콘이 생성됨
- 보안등급 등을 이유로 보안카드 번호를 입력하도록 요구하는 경우는 파밍사이트 이므로 주의 필요
- 출처가 불분명한 파일이나 이메일은 즉시 삭제 및 무료다운로드 사이트 이용 자제
- OTP(일회성 비밀번호), 보안토큰 사용 권장
- 인터넷 이용 중 발견한 파밍사이트는 은행과 금융감독원에 신고

피해구제

- 피해를 당한 경우 경찰서(신고전화 112) 혹은 금융회사 콜센터를 통해 신속한 지급정지 요청이 필요함



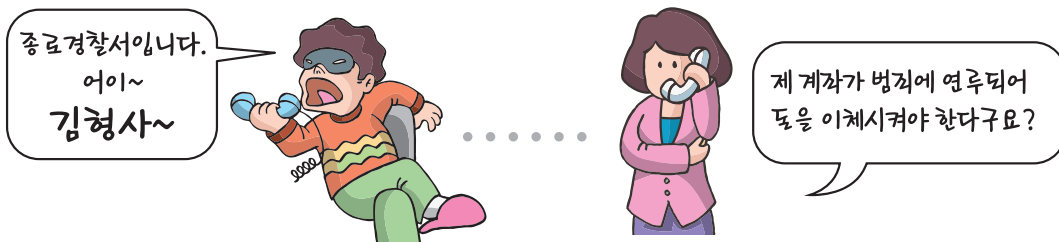
6 상황극 연출에 의한 보이스피싱

수 법

- 금융 및 공공기관의 직원을 사칭하여 실제로 긴급한 상황을 연출(통화중 경찰을 부르는 상황으로 경찰서인 것처럼 위장 등)하여 이용자에게 접근 후 송금, 인출, 계좌이체 등을 유도

피해사례

- J씨(45세, 여)는 경찰서 사무실로 오인할 수 있도록 동료 형사를 부르는 소리가 들려 오는 상황에서 경찰관을 사칭하는 자로부터 "당신 통장 계좌에서 범죄에 연루된 정황을 찾았으니, 그 계좌의 거래내역을 추적해야 합니다. 지금부터 내가 불러주는 계좌로 돈을 이체시켜 주시길 바랍니다."라는 전화를 받고 사기범이 불러주는 계좌로 500만원을 이체하여 피해 발생



예방법

- 금융 및 공공기관에서는 개인정보를 수집하지 않으므로, 해당기관에 직접 연락하여 확인 필요
 - ※ 114 전화번호 안내를 통해 전화번호 확인
- 노출된 계좌는 비밀번호를 변경 또는 계좌해지 조치 필요

피해구제

- 피해자는 피해금을 송금·이체한 금융회사에 피해구제를 신청
 - 금융회사는 보이스피싱 피해자의 요청이 있으면 입금내역 등을 확인하여 계좌 전체에 대하여 지급정지
 - 금감원은 채권소멸일로부터 14일 이내에 환급금액을 결정하게 되며 금융회사는 이를 지체 없이 피해자에게 환급
 - ※보이스피싱 피해신고(112), 금융감독원피해상담 및 환급(1332)

7 인증절차없이 이루어지는 앱 결제시의 피해

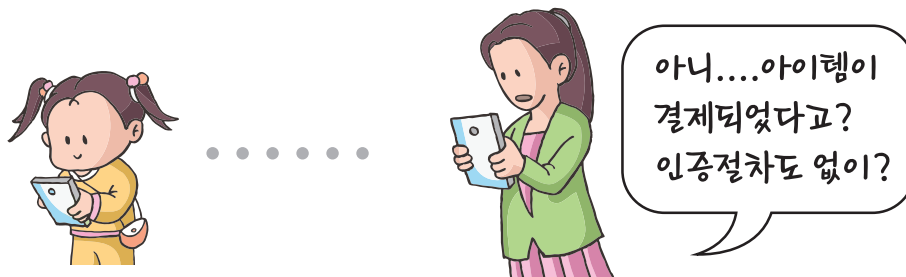


피해형태

- 타인이 휴대폰 이용 시 온라인 앱 마켓(앱스토어, 구글 플레이 스토어, 티스토어, 올레마켓, U+앱마켓 등)이나 앱 내에서 간단한 조작만으로 별도의 인증절차 없이 쉽게 유료 앱, 아이템, 사이버머니의 구입 및 결제가 가능하기 때문에 실수 또는 아이들의 조작미숙 등으로 본인도 모르게 소액결제 발생

피해사례

- 주부 J씨(34세, 여)의 6살 자녀가 자신의 휴대폰으로 온라인 마켓을 통해 앱을 다운 받아 사용하던 중 아무런 인증절차 없이 게임 내 아이템이 휴대폰 결제로 구매(54,000원)되어 피해 발생



예방방법

- 각 통신사 고객센터 및 홈페이지를 통해 소액 결제를 차단 하거나 결제금액 제한 신청
- 미성년자의 경우 앱 결제창이 뜨는 경우에는 부모의 동의 후 확인을 누를 수 있도록 주의 필요
- 휴대전화번호, 주민번호 등 개인정보를 입력할 경우에 '성인인증' 인지 '결제'인지 절차 확인 필요

피해구제

- 결제확인 알림 문자 수신 여부 확인 및 확인 시 해당 결제대행회사 고객센터로 결제 취소 요청
- 통신사업자와 결제대행회사에 이의제기
- 통신사업자 및 결제대행회사와 해결되지 않을 경우, 소액결제중재센터(www.spayment.org)를 통해 도움 요청



8 무료 콘텐츠사이트 가입 유도 후 이용시 결제 피해

피해형태

- 무료쿠폰이나 이벤트로 유인되어 콘텐츠 다운로드 사이트에서 회원가입 시 유료 결제를 인지 못하고 주민번호와 인증번호 등을 입력하였더니 소액결제가 이루어 지거나, 무료 이용기간 종료 후 자동으로 유료 전환되어 매월 요금 발생

피해사례

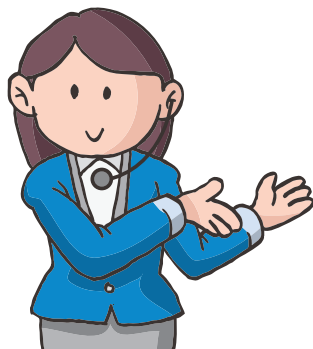
- 대학생 L씨(27세, 남)는 복권번호 추첨 사이트에서 1개월 무료 이벤트에 참여하여 몇 차례 복권번호를 수신하다가 잊고 지냈으나, 다음 달 무료 이벤트가 끝나고 자동으로 유료 전환되어 6개월간 총 65,300원이 결제되어 피해 발생
- 회사원 A씨(32세, 여)는 인터넷 상에서 "회원가입 및 다운로드 무료"라는 팝업창을 통해 영화 콘텐츠 다운로드 사이트에 접속하여 휴대폰 본인 인증을 거쳐 회원가입한 이후 요금청구에 해당사이트 회원가입시 결제 인증이 이루어져 25,000원의 소액결제 피해 발생





예 방법

- 콘텐츠 이용 사이트에 회원가입 시 약관이나 계약조건 등을 확인하고, "무료", "이벤트" 라는 문구 주의 필요(유료 회원가입 여부, 자동 연장결제 여부 등 체크)
- 콘텐츠 이용계약의 경우 매월 별도의 해지 신청이 없을 시 지속적으로 서비스가 제공되어 자동 결제가 되는지 확인 필요(요금고지서 등)
- 소액이라 무심코 지나치기 쉬우므로 매월 발송되는 요금청구서를 확인하여 본인이 모르는 결제내역이 있는지 확인 필요
- 주민번호, 휴대폰 번호, 인증번호 등은 결제에 이용될 수 있으므로 불필요한 정보를 요구하는 사이트는 이용 자제
- 각 통신사 고객센터 및 홈페이지를 통해 소액결제를 차단하거나 결제금액 제한 신청



✓ 이벤트에 현혹되지 말자

✓ 개인정보는 소중히!

✓ 요금고지서 확인

✓ 소액결제 차단신청

피해구제

- 결제확인 알림 문자 수신 여부 확인 및 결제 확인 시 해당 결제대행회사 고객센터로 결제 취소 요청
- 통신사업자와 결제대행회사에 이의제기
- 통신사업자 및 결제대행회사와 해결되지 않을 경우, 소액결제중재센터(www.spayment.org)를 통해 도움 요청



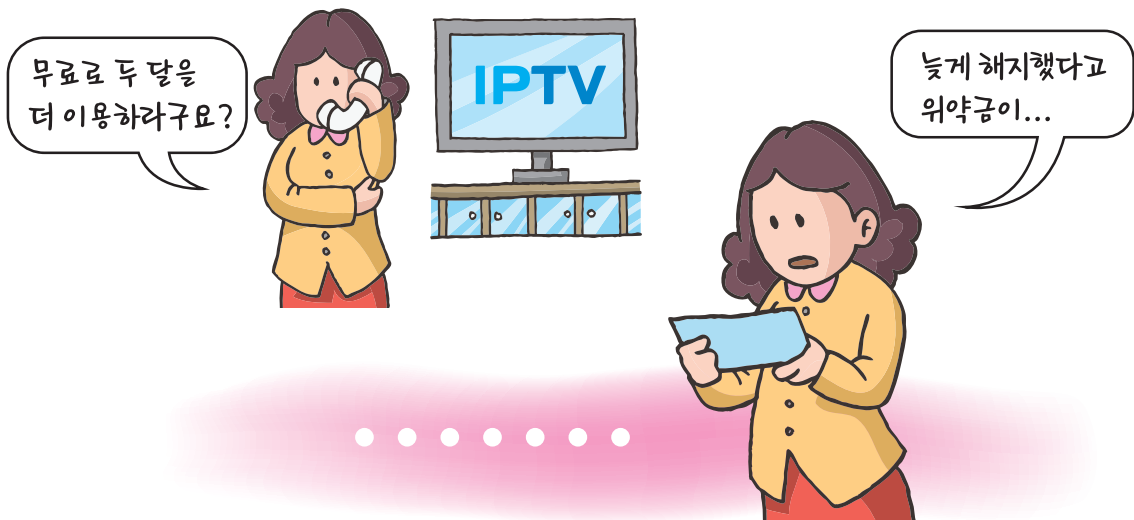
9 유료방송 무료이벤트 후 유료전환 및 요금청구

수 법

- 유료방송 사업자가 무료체험, 이벤트 또는 프로모션 등으로 유료방송 서비스를 1개월 동안 무료로 제공하기로 하고 제공된 무료서비스 기간 이후 이용자의 동의 없이 계약을 체결하여 요금을 부과하고, 이용자가 계약 해지를 요청할 경우 위약금 청구

피해사례

- 주부 K씨(38세, 여)는 유료방송서비스 한 달 무료체험 권유를 받아 이용 후 해지한 사실이 있으며, 그 이후 다른 직원으로부터 두 달 무료체험을 더 이용하라는 권유를 받아 동의하고 사용하던 중 무료체험 기간이 만료되었으나 미처 해지를 하지 못하였는데 사업자로부터 미납요금 청구를 받고 유료방송서비스 해지를 요구하니, 3년 약정이 체결되었다며 위약금 85,000원을 청구하여 피해 발생
 - 최초 무료체험 권유 시에는 3년 약정과 관련된 설명을 들었지만 이미 해지하였고, 두 번째 무료체험 권유 시에는 3년 약정에 대한 설명을 들은 바 없음





예 방법

- 서비스 계약 시 '요금·위약금, 채널·패키지 변경, 해지방법, 결합서비스, 월 이용 요금, 의무사용(약정) 기간' 등 약관상 중요사항에 대해서 사업자에게 설명 요구(가입계약서 보관 필요)
- 유료방송 서비스 계약 시 무료체험 서비스를 제공할 경우 무료서비스 기간과 자동 연장 등 확인 필요
 - 요금을 자동이체 한 경우라면 해당 은행 자동이체를 해지
- 유료방송 가입 후 약정기간 이내에 중도 해지 시 위약금이 부과될 수 있으므로 위약금에 대한 확인 필요
 - 수신기(셋탑박스)의 반환 및 수신기 대금 등 확인

피해구제

- 이용자의 해지 요구에도 불구하고, 고의로 해지 처리를 지연하는 등 과잉 해지 방어를 하는 사업자의 부당행위에 대해서는 방송통신 CS센터(국번없이 1335) 또는 소비자상담센터(국번없이 1372)를 통해 신고

유료방송서비스로
피해를 입으시면...



✓ 미래창조과학부(국번없이 1335)

✓ 소비자상담센터(국번없이 1372)



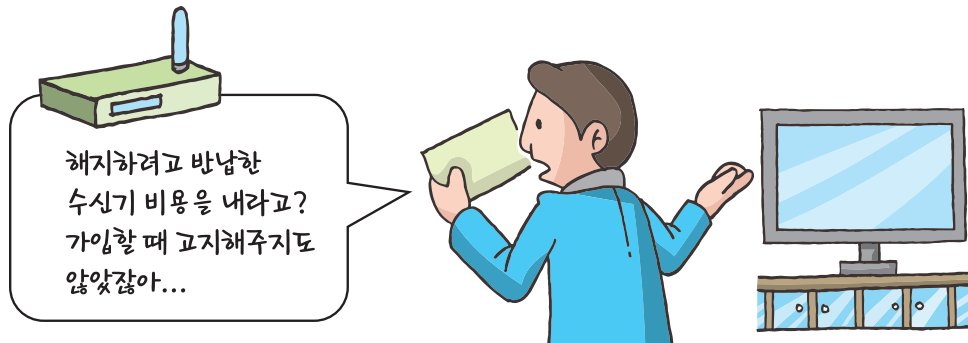
10 유료방송 계약시 미고지한 수신기대금 청구

수 법

- 유료방송 가입 시 수신기에 대한 비용을 미고지하고 이용자가 약정기간 이내에 해지 시에 수신기 대금 비용 청구

피해사례

- 회사원 M씨(33세, 남)는 종합유선방송사업자인 A사의 케이블TV를 3년간 이용하기로 계약을 한 후 수신기를 제공받아 사용해오던 중 계약기간 이내 해지를 위해 업체에 수신기를 반납하였고, 이때 가입 시 미고지되었던 수신기 비용으로 150,000원을 청구 받아 피해 발생



예 방법

- 가입계약서 상의 수신기 요금에 대한 부분이 명시되어 있는지 확인 필요(가입계약서 보관 필요)
- 유료방송 가입 후 약정기간 이내에 중도 해지 시 위약금이 부과될 수 있으므로 위약금에 대한 확인 필요
 - 수신기(셋탑박스)의 반환 및 수신기 대금 등 확인

피해구제

- 가입 시 고지 받지 못한 수신기 대금 청구의 피해가 발생하였을 경우 해당 사업자에게 미고지 사실 확인 필요
- 해당 사업자와 원만히 해결 되지 않을 경우 방송통신 CS센터(국번없이 1335) 또는 소비자상담센터(국번없이 1372)를 통해 신고

방송통신서비스 관련 민원기관 안내

- 방송통신 CS센터 : ☎ (국번없이)1335, www.msip.go.kr
 - 방송통신서비스 가입 및 해지, 부당요금, 통화품질 등의 피해
- 금융 민원상담 : ☎ (국번없이)1332, www.fcsc.kr
 - 금융피해와 관련된 모든 사항을 상담·처리
- 경찰서 : ☎ (국번없이)112, www.police.go.kr
 - 피싱, 스미싱, 금융사기, 휴대폰 개통사기 등 피해
- 국민신문고 : ☎ (국번없이)110, www.epeople.go.kr
 - 일반적인 권리침해에 대한 고발
- 소비자상담센터 : ☎ (국번없이)1372, www.ccn.go.kr
 - 소비 관련 상담신청, 피해처리신청, 피해구제신청 등
- 명의도용피해 : ☎ 080-3472-119, www.msafes.or.kr
 - 방송통신서비스 관련 명의도용 피해
- 소액결제중재센터 : ☎ 1644-2367, <http://www.spayment.org>
 - 앱 결제, 무료사이트 이용시 결제 등의 피해
- 한국인터넷진흥원 : ☎ (국번없이)118, www.kisa.or.kr
 - 스팸, 개인정보유출 및 수집 관련 피해, 해킹 등 인터넷 침해사고
- 방송통신심의위원회 : ☎ (국번없이)1377, www.kocsc.go.kr
 - 방송프로그램 내용(선정성, 폭력성 등)
 - 인터넷 등의 음란, 명예훼손, 사이버스토킹, 도박, 청소년유해정보 등

방송통신서비스 관련 민원기관 안내

- 불법·유해정보 신고 : ☎ 1566-8274, 스마트보안관.kr
 - 불법·청소년 유해정보 관련 앱 신고
- 분실단말기집중관리 : ☎ 02-3471-1155, www.handphone.or.kr
 - 분실 이동전화 단말기 관련 회수전달
- 통신 미환급액 정보조회서비스 : ☎ 02-2015-9181, www.smartchoice.or.kr
 - 이동통신서비스 이용자 미환급액 정보조회 및 환급신청
- 유료방송 미환급액 정보조회서비스 : ☎ 080-080-4278, www.kait-tvrefund.kr
 - 유료방송서비스 이용자 미환급액 정보조회 및 환급신청
- 오픈넷CS센터 : ☎ 1600-8272, www.opennetcs.or.kr
 - 이동통신 무선인터넷 서비스 관련 불만 및 피해사항
- 불법복제물 신고센터 : ☎ 02-2669-0074, copyright.moiba.or.kr
 - 저작권법에 따라 보호되는 권리를 침해하는 복제물 또는 정보 신고
- 이동통신서비스 불법 TM 신고센터 : ☎ 1661-9558, www.notm.or.kr
 - 통신사업자의 대리점 또는 판매점에서 불법적으로 수집한 개인정보를 활용한 텔레마케팅 행위 신고
- 이동통신사업자 민원센터 : ☎ (휴대전화) 114
 - SKT : 080-816-2000
 - K T : 080-080-1618
 - LGU+ : 080-019-7000

※ 본 매뉴얼의 내용과 관련된 문의사항은 해당기관으로 연락하여 주시기 바랍니다.

발행처 방송통신위원회
한국정보통신진흥협회

주소 서울시 서초구 서초동 1678-2번지

전화 02-580-0754

팩스 02-580-0769

홈페이지 <http://www.wiseuser.go.kr>

편집위원 방송통신위원회 이상목 사무관
한국정보통신진흥협회 이상민 대리

디자인 · 인쇄 예당문화

