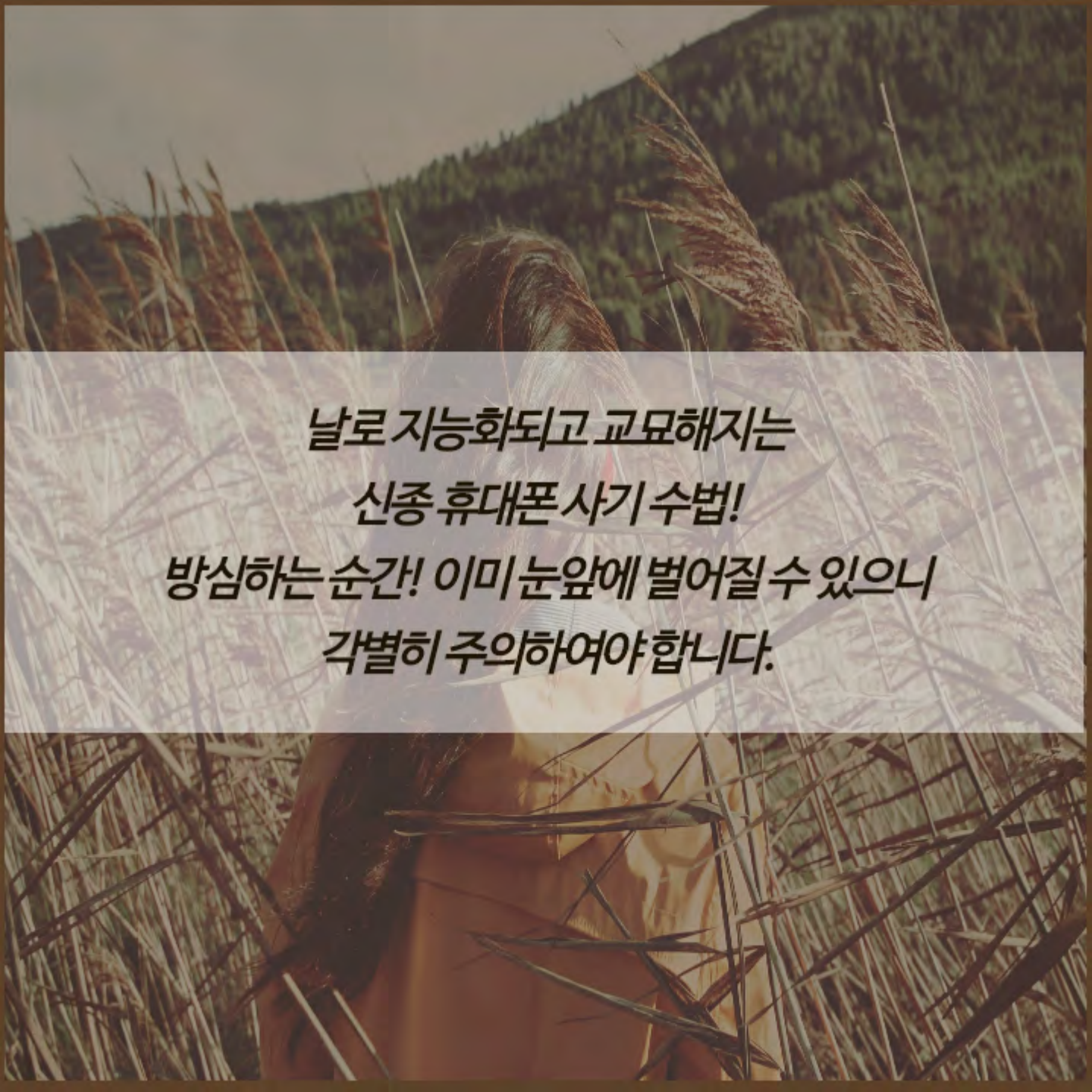
통신관련 소비자 교육 콘텐츠 제14탄

통신가이드

휴대폰 사기예방


날로 지능화되고 교묘해지는
신종 휴대폰 사기 수법!
방심하는 순간! 이미 눈앞에 벌어질 수 있으니
각별히 주의하여야 합니다.

스미싱, 파밍, 큐싱?

스미싱 Smishing

출처가 불분명한 문자메시지에 포함된 인터넷 주소에 접속할 경우, 악성코드가 스마트폰에 설치되어 개인정보, 금융정보 유출, 소액결제 피해 등을 일으키는 사기 수법

파밍 Pharming

사용자의 PC 나 휴대폰을 악성코드로 감염시켜 금융정보를 빼내는 수법

큐싱 Qshing

출처가 불분명한 'QR 코드'를 스마트폰으로 찍을 경우, 악성 앱을 내려받도록 유도하거나 악성 프로그램을 설치하게 하는 금융사기 수법

사례1. 휴대폰 대출 관련 사기

서울 중랑경찰서는 핸드폰을 개통해 보내주면 저금리로 대출해주겠다고 속여 1400만원상당의 신형 핸드폰을 가로챈 혐의(사기)로 국내 관리책 조모(32)씨를 구속했습니다.

이들은 캐피털 상담원을 사칭해 무작위로 '통신사 제휴 대출상품이 한시적으로 개발됐으니 핸드폰을 개통해 보내주면 6.2%의 저금리로 대출해 주겠다' 고 문자를 발송한 후 이를 보고 전화한 피해자들에게 개통된 갤럭시S5 핸드폰을 보내주면 대출해주겠다고 속였다고 합니다.

98만원 상당의 갤럭시 신형 핸드폰을 받아 챙기는 등 4일간 총 9명으로부터 1400만원 상당의 핸드폰을 가로챘습니다.

사례2. 잠시 빌린 휴대폰으로 주인몰래 결제

경기 의정부경찰서에서는 주로 노년층이 운영하는 작은 규모의 상가에서 가게 주인이 한눈을 팔 때 휴대전화를 잠시 훔치거나 빌린다며 가져간 뒤 한 번에 20~30만원 상당의 문화상품권을 결제한 후 교통카드를 충전하고 환불받는 방식으로 현금화시켜 1300여만원을 가로챈 심모씨(22)를 붙잡았다고 합니다.

이 과정에서 심씨는 특정버튼을 눌러 휴대전화를 초기화하여, 피해자들이 걸어놓았던 잠금 패턴도 금방 풀어버렸는데 피해자들이 주로 노년층이다 보니 초기화 된 사실을 알아차리지 못하였고, 결제 내역까지 지워버려 요금 명세서를 받고 나서야 피해 사실을 알 수 있었습니다.

심씨는 휴대전화 대리점에서 두 달 간 근무하며 휴대전화 초기화 방법과 모바일 결제의 취약점을 악혀 범죄에 악용한 것으로 드러났습니다.

사례3. 보이스피싱의 진화

보이스피싱 조직원이 A씨의 집으로 전화해 "아들이 3,000만원의 빚보증을 서 붙잡아 두고 있으니 돈을 보내지 않으면 장기를 팔아버리겠다"고 협박하였고, 피해자 A씨는 아들과 실제로 연락이 닿지 않자 적금을 해약해 2,000만원을 준비했습니다.

결국 경찰에 의해 보이스피싱 조직원들은 모두 붙잡혔지만 특이한 것은 이들 조직이 피해자에게 전화하기 전 아들의 휴대전화를 일시 정지시키는 신종 수법을 이용했다는 점이었습니다.

보이스피싱 수법이 많이 알려져 자녀의 안전이 바로 확인돼 미수에 그치는 경우가 많아지자 범죄조직이 자녀의 안전을 확인할 수 없도록 범행 대상의 주민번호 등 개인정보를 이용, 통신사 콜센터에 전화해 휴대전화 분실 등을 이유로 일시정지를 신청한 것이었습니다. 콜센터의 신원확인 절차가 복잡하지 않다는 점을 이용한 신종 수법이었습니다.

사례4. 택배 등을사칭한 스미싱

B씨에게 며칠 전 핸드폰 문자로 '택배반송'이라는 문자를 받고 반송된 주소를 확인하고자 무심코 문자메세지에 첨부된 인터넷 주소를 열어봤다고 합니다. 그러자 자동으로 'XX통운'이라는 애플리케이션이 설치가 되었고 B씨의 스마트폰에 모르는 번호로 100여통이 넘는 전화와 문자메세지가 쏟아졌는데 '왜 나에게 스미싱 메세지를 보내느냐'는 항의내용이었습니다. 애플리케이션이 설치되면서 B씨의 번호가 스미싱 메세지 발신번호로 도용이 된 것이었습니다.

※ 주의해야 할 스미싱 문자 유형 ※

→ ○○고객님 크리스마스 선물 택배 주소지 확인

→ ○○제과 크리스마스 파티 초대

→ ○○님 신년연하장이 도착했습니다

→ 크리스마스 이벤트, ○○마켓 쿠폰 확인

→ 송년회 참석 여부 투표

→ ○○대학 합격자 알려 드립니다 등

스미싱, 파밍, 큐싱의 예방!

- 출처가 확인되지 않은 문자메시지의 인터넷 주소 클릭 주의
- 지인에게서 온 문자도 인터넷 주소가 포함돼 있으면 주의
- 전자금융사기 예방 서비스 이용, 공인인증서 PC 지정 및 추가 인증
- 백신 프로그램 설치 업데이트, 실시간 감시상태 유지
- 소액결제 차단 또는 결제금액 제한
- 보안 강화·업데이트 명목의 금융정보 요구 시 입력 금지
- 스마트폰 보안설정 강화

스미싱, 파밍, 큐싱의 피해구제 방법

▷ 스미싱, 파밍 : 피해 발생 시 신속히 경찰서나 금융기관 콜센터에 신고하고 경찰서에서 '사건사고 사실 확인원'을 발급받아 해당 스미싱의 경우 관련 사업자(이통사, 게임사, 결제대행사 등), 파밍의 경우 은행에 제출하여 피해금 환급 신청

▷ 큐싱 : 큐싱 피해발생 시 경찰서에 피해 내용을 신고 또는 국번 없이 118 (보호나라 , www.boho.or.kr) 신고

휴대폰 사기 예방

서울특별시
SEOUL METROPOLITAN GOVERNMENT

사단법인 소비자공익네트워크
CONSUMER NETWORK FOR PUBLIC INTEREST