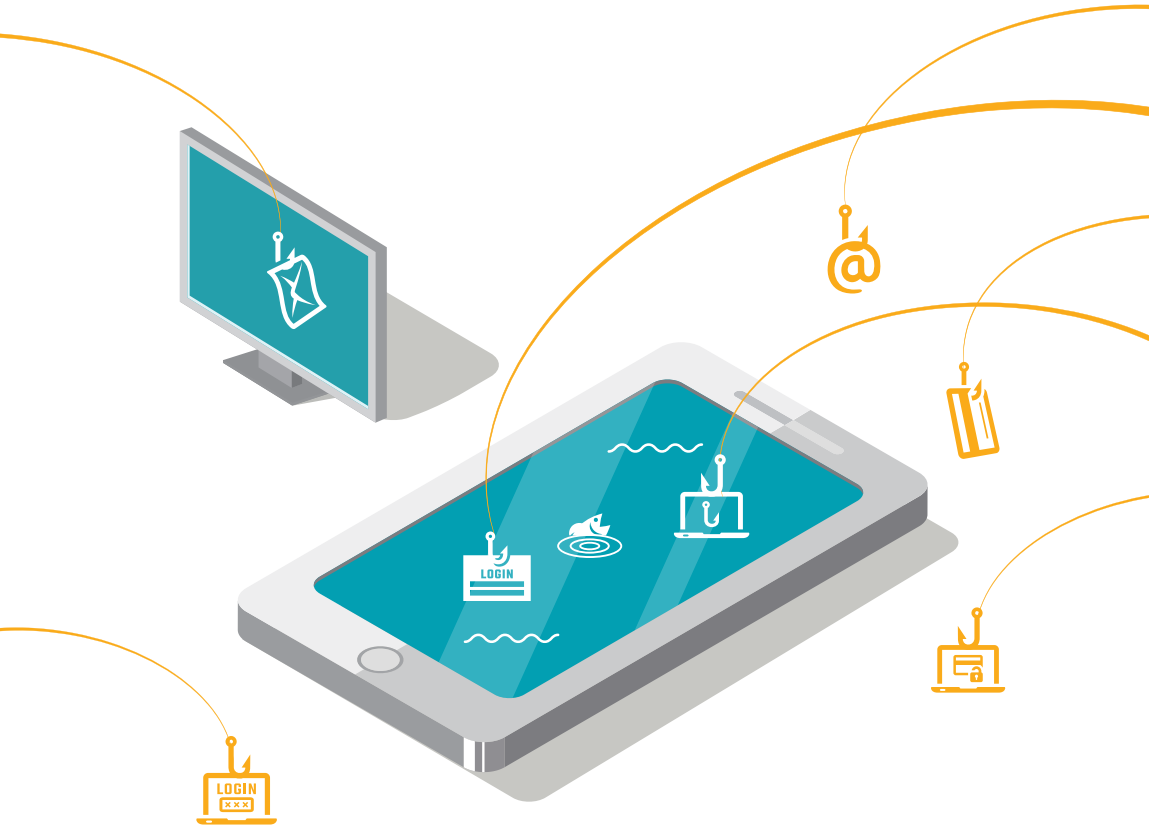
전기통신금융사기 사례로 배우는
안전한 금융생활 안내서

알아두면 든든한
금융사기 예방법



금융감독원

머리말

오늘날에는 거의 모든 사람들이 "금융" 생활을 하며 살아갑니다. 내 통장으로 용돈이나 월급이 입금되고, 내 집 마련을 위해 적금을 붓고, 휴대전화나 인터넷을 이용해서 공과금을 납부하기도 하며, 은행에서 돈을 빌리기도 합니다. 이렇듯 "금융"은 우리의 일상생활과 매우 밀접하게 연관되어 많은 편리함과 이로움을 가져다줍니다.

금융시장은 하루가 다르게 발전하며 일상생활에 큰 영향을 미치고 있습니다. 이에 따라 더 간편하고 신속하게 거래할 수 있는 전자적 방식의 금융 거래도 다양하게 등장하고 있습니다. 하지만 이러한 간편함과 신속함을 이용한 보이스피싱 등 전기통신금융사기 또한 증가하고 있습니다.

기존의 전기통신금융사기는 전화를 이용한 보이스피싱 정도였으나 오늘날에는 악성코드를 유포하여 실제와 유사한 금융회사의 인터넷뱅킹 사이트로 유인하는 피싱사이트 등 그 수법과 종류도 교묘하고 다양하게 진화하고 있습니다.

따라서 금융감독원에서는 금융사기를 뿌리뽑고 금융소비자를 보호하기 위해 그간 추진해 온 다양한 노력들 외에도 금융소비자들 스스로 금융사기 피해를 예방하고, 피해가 발생했을 때 신속하게 대처함으로써 피해를 최소화할 수 있도록 하기 위해 종합 안내서를 발간하게 되었습니다.

본 안내서에서는 전기통신금융사기의 유형 및 특징들을 살펴보고, 이를 예방할 수 있는 방법을 소개하며, 대포통장의 위험성, 안전한 금융생활 습관과 금융사기 피해 발생 시 대처 요령 등에 관한 내용을 수록하고 있습니다.

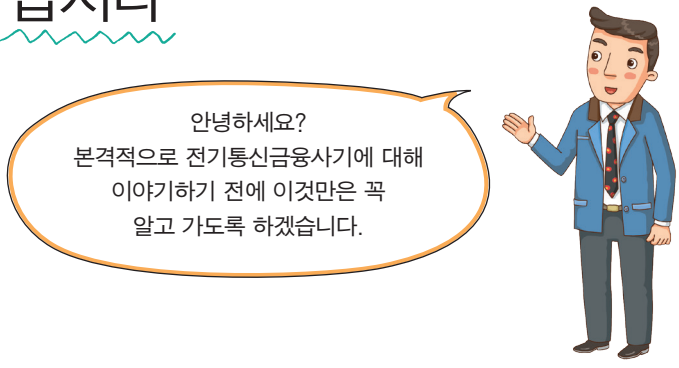
아무쪼록 이 책자가 널리 활용됨으로써 금융소비자 여러분의 소중한 재산을 더욱 안전하게 보호하여 행복하고 안정된 일상을 누리시는 데 도움이 되기를 바랍니다.

2014년 12월

금융감독원 서민금융지원국

차 례

금융사기, 이것만은 꼭! 알고 갑시다



▶ 보이스피싱과 피싱사기는 같은 말이다 (X)

보이스피싱을 피싱사기와 같은 뜻으로 사용하는 경우가 많습니다. 하지만 최근 들어 전화를 이용한 보이스피싱뿐만 아니라 실제와 유사한 가짜 사이트를 이용하는 피싱사이트, 악성코드를 이용한 파밍 등 다양한 신·변종 피싱사기 유형들이 나타나고 있습니다. 따라서 보이스피싱을 피싱사기의 전부라고 생각하면 안 됩니다.

피싱사기의 법적 명칭은 '전기통신금융사기'입니다. 따라서 전기통신금융사기라는 말은 피싱사기(보이스피싱 · 메신저피싱 · 파밍 · 피싱사이트)와 대출빙자사기를 포함하는 개념이며, 스미싱과 메모리 해킹은 제외됩니다.

이 책에서는 피싱사기로 분류되는 보이스피싱, 메신저피싱, 파밍 및 피싱사이트와 이 밖에 주의해야 할 금융사기인 대출빙자사기, 스미싱, 메모리 해킹을 구별해서 다룰 생각입니다.

▶ 공공기관이나 금융회사에서는 전화나 문자 메시지로 주민등록번호나 예금 계좌번호를 묻는 경우가 있다 (X)

금융감독원 · 경찰 · 검찰 등 공공기관이나 은행 · 캐피탈 등 금융회사에서는 전화나 문자 메시지 등을 이용해서 개인정보(주민등록번호, 주소 등)나 금융거래정보(은행명, 계좌 잔액, 예금 계좌번호, 보안카드번호 등)를 묻지 않습니다. 따라서 수사 협조나 보안강화 등을 명목으로 이들 정보를 물을 때에는 금융사기일 수 있으므로 절대로 응하지 말고 해당 기관에 사실 여부를 먼저 확인하시기 바랍니다.

▶ 피싱사기는 형법상 사기범죄에 해당한다 (O)

전기통신금융사기란 남을 속이거나 거짓말로 타인의 재산을 취득하는 사기범죄의 하나로서, 특히 전기통신수단을 이용하여 서로 얼굴을 마주하지 않은 상태로 이뤄지는 금융 거래에서 발생하는 특수사기범죄를 말합니다.

▶ 불법대출 중개수수료는 대출빙자사기와 다르다 (O)

대출빙자사기는 대출을 미끼로 하여 수수료 등의 명목으로 금전을 요구한다는 점에서 불법대출 중개수수료와 비슷해 보입니다. 하지만 불법대출 중개수수료는 대출을 성사시켜 주고 고객으로부터 그 대가를 받는 불법 행위인 반면, 대출빙자사기는 대출 자체가 이루어지지 않는 불법 행위라는 점에서 차이가 있습니다.

▶ 특별법에 의한 환급제도는 국가에서 피해금액을 대신 보상해 주는 제도이다 (X)

금융감독원에서는 특별법(2014. 7. 29. 개정 시행)에 의해 피싱사기 및 대출빙자사기 피해자들에 대한 피해금 환급제도를 시행하고 있습니다. 별도의 민사소송 등 복잡한 절차 없이 지급정지된 잔액 범위 내에서 2개월간의 채권 소멸기간을 거쳐 피해금액을 환급받을 수 있습니다. 잔액을 초과한 피해금액에 대해서는 민사소송 등으로 해결해야 합니다.

하지만 특별법에 의한 환급제도는 국가에서 범죄자 대신 피해자에게 보상해 주는 제도가 아닙니다. 피해환급금은 지급정지된 사기이용계좌의 잔액 범위 내에서 산정하며, 피해자가 여러 명인 경우 지급정지된 사기이용계좌의 잔액을 피해금액에 비례하여 피해자별로 환급합니다.

따라서 피해금 환급은 지급정지된 사기이용계좌에 금액이 남아 있는 경우에만 가능하므로 전기통신금융사기를 당했을 때에는 사기범이 돈을 인출해 가지 못하도록 신속히 지급정지 조치를 하는 것이 무엇보다 중요합니다.

▶ 해킹은 특별법에 의한 피해금 환급이 가능하다 (X)

개인정보와 금융거래정보를 빼내는 해킹사고는 피해자를 속여 재산상의 이익을 취한 것이 아니므로 특별법에 의한 피해구제 대상에 포함되지 않습니다.

피해금을 환급받을 수 있는 전기통신금융사기는 보이스피싱 · 메신저피싱 · 파밍 및 피싱사이트 · 대출빙자사기이며, 메모리 해킹과 스미싱,

일반 사기는 피해금을 환급받을 수 없습니다.

메모리 해킹의 경우는 각 금융회사를 통하여 별도의 피해구제 절차를 밟아야 하며, 스미싱에 의해 소액결제 피해를 입은 경우에는 해당 통신사를 통해 해결해야 합니다.

▶ 내 통장을 남에게 빌려주는 것만으로도 범죄자로 처벌받을 수 있다 (O)

통장을 남에게 빌려주거나 넘겨주는 행위는 3년 이하의 징역 또는 2천만 원 이하의 벌금에 처해질 수 있는 아주 위험한 불법행위입니다. 남의 통장을 빌려 달라고 하는 사람은 사기범일 가능성이 매우 높고, 실제로 타인에게 건네진 통장은 대부분 금융사기에 이용됩니다.

이렇게 통장이 금융사기에 이용되는 경우 통장의 명의인도 형사처벌과 함께 1년간 신규 예금계좌를 개설할 수 없고, 다른 은행 계좌에 대한 전자금융 거래 제한 등 금융 거래 시 많은 불이익을 당합니다. 따라서 통장을 빌려주거나 사고파는 행위를 절대 해서는 안 됩니다.

I 금융사기의 유형과 예방 요령, 알아두면 든든합니다

1. 보이스피싱과 메신저피싱
2. 파밍과 피싱사이트
3. 대출빙자사기
4. 스미싱
5. 메모리 해킹

초기에는 금융지식이 부족하거나 정보력이 취약한 계층에서 많은 피해를 입었으나, 사기수법이 날로 진화하면서 연령, 직업, 계층과 상관없이 광범위하게 피해가 발생하고 있습니다. 최근에는 사기범이 미리 확보한 이름, 주민등록번호, 주소 등을 언급하거나, 정보유출, 해킹사고 등 사회적 이슈를 내세우며 치밀하게 접근하기 때문에 피싱사기로 인한 피해 예방을 위해 각별한 주의가 필요합니다.

보이스피싱과 메신저피싱이란

보이스피싱이란 '음성(voice)'+'개인정보(private data)'+'낚시(fishing)'를 합성한 신조어로서 금융 분야에서 속임수나 거짓말로 타인의 재산을 자기 것으로 만드는 특수 사기범죄의 하나입니다. 전화를 통해 개인정보를 낚아 올린다는 의미에서 보이스피싱이란 명칭으로 사용됩니다.

보이스피싱 (voice phishing) = 음성 (voice) + 개인정보 (private data) + 낚시 (fishing)

보이스피싱은 2000년대 초반에 대만에서 시작되어 이후 중국, 일본, 한국, 싱가포르 등 주로 아시아 지역으로 확산되었습니다. 보이스피싱은 사기범 혼자서 저지르는 단독 범죄가 아니라 본부와 콜센터, 인출 팀, 환전·송금 팀, 계좌모집 팀 등의 네트워크를 이루어 움직이는 조직형·지능형 범죄입니다.

또한, 소셜네트워크(SNS)의 발달과 더불어 사기 과정이 보이스피싱과 유사하나 전화 대신 메신저를 이용해 피해자를 속이는 메신저피싱도 나타났습니다.

메신저피싱이란 다른 사람의 인터넷 메신저 아이디와 비밀번호를 이용하여 로그인한 후 이미 등록되어 있던 가족, 친구 등 지인에게 1:1 대화 또는 쪽지 등을 보내 치료비, 교통사고 합의금 등 긴급 자금을 요청하고, 이에 피해자가 속아 송금하면 이를 가로채는 사기 수법을 말합니다.

궁금해요

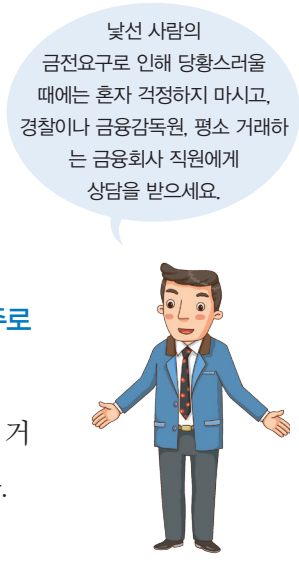
보이스피싱과 메신저피싱의 차이점은 무엇인가요?

보이스피싱이 전화를 이용하여 주로 경찰 · 검찰 등 공공기관을 사칭해서 접근하는 반면, 메신저피싱은 카카오톡 · 페이스북 등 메신저를 이용하여 주로 친척 · 친구 등 지인을 사칭해서 접근하는 차이가 있습니다.

보이스피싱의 특징은

■ **공공기관 및 금융회사를 사칭합니다.**

사기범이 검찰, 경찰, 금융감독원 등의 공공기관이나 은행, 캐피탈 등의 금융회사를 번갈아 가면서 사칭합니다.



■ **심리적으로 압박받을 수 있는 거짓 내용을 주로 사용합니다.**

개인정보 유출, 범죄사건 연루, 자녀 납치 등 거짓 내용으로 피해자를 심리적으로 압박합니다.

■ **발신번호를 조작하여 피해자를 현혹합니다.**

피해자가 보이스피싱임을 눈치챌 수 없게끔 발신번호창에 공공기관 및 금융회사의 전화번호가 나타나도록 조작하여 피해자를 현혹합니다.

■ **유창한 한국어를 구사합니다.**

사기범은 예전처럼 어눌한 우리말을 쓰지 않고, 유창한 우리말을 구사하면서 피해자를 공략합니다.

■ **조직적으로 역할을 분담하여 범행을 진행합니다.**

사기범들은 전화, 대포통장 획득, 피해금 이체 및 인출 등으로 각자의 역할을 분담하여 조직적으로 범죄를 진행합니다.

■ **신분 노출을 피하기 위해 주로 대포통장을 이용합니다.**

사기범들은 대출이나 취업 알선, 통장 양도 시 대가 지급 등을 미끼로 통장을 획득하여 자신들의 신분이 노출되지 않도록 이를 이용합니다.

메신저피싱의 특징은

■ 피싱사이트로 접속을 유도합니다.

메신저를 이용하는 다수에게 피싱사이트의 인터넷 주소가 포함된 허위정보를 전송하여 이를 클릭하도록 유도한 후 피싱사이트에 접속하면 금융거래정보를 입력하게 하여 금전적 피해를 입힙니다.

■ 다른 사람의 아이디와 패스워드로 로그인을 시도합니다.

보안이 취약한 웹사이트의 고객정보를 해킹한 후 아이디와 패스워드를 가로챈 후 메신저에 불법으로 로그인합니다.

■ 대화 상대방의 진위 확인이 어렵습니다.

사기범이 가로챈 아이디로 지인을 사칭하여 메시지를 보내는 경우 평소 알고 지내던 지인으로 착각하기 쉽습니다.

피해 사례

사례 1 검찰수사관 및 금융감독원 직원을 사칭한 사례

A씨(60대, 남)는 검찰수사관을 사칭하는 자로부터 "검거한 범인이 A씨 명의의 계좌를 대포통장으로 사용하고 있어 금융감독원 직원이 계좌 안전조치를 해 줄 것입니다. 그러니 가까운 현금지급기로 가서 기다리십시오."라는 전화를 받았습니다. 이를 믿은 A씨가 현금지급기로 가자 금융감독원 직원을 사칭하는 사기범으로부터 전화가 왔습니다. 사기범은 계좌 및 예금 안전조치를 위해서 금융감독원에서 관리하는 국가안전계좌라고 속인 대포통장으로 A씨의 예금을 입금하도록 지시했습니다. A씨는 예금 안전조치라는 사기범의 말을 믿고 지시대로 사기범들의 계좌로 예금액을 송금했습니다. 사기범들은 A씨가 예금액을 모두 송금할 때까지 통화를 계속 하며 A씨를 현혹했습니다.

A씨가 예금액 1,300만 원을 모두 송금하자 금융감독원 직원을 사칭한 사기범은 자신이 다시 연락할테니 먼저 연락하지 말고 기다리라고 했고, 사기범 일당은 A씨가 송금한 피해금 전액을 인출하여 잠적했습니다.

사례 2 수사관을 사칭하여 알아낸 정보로 카드론을 받아 가로챈 사례

P씨(60대, 남)는 경찰청 수사관을 사칭하는 자로부터 "당신의 예금계좌가 범죄에 연루되었습니다. 수사 협조와 보안등급 강화가 필요하니 당신의 계좌 비밀번호, 신용카드 정보 등을 알려주십시오. 만약 수사에 협조하지 않으면 법적 처벌을 받을 수 있습니다."라는 전화를 받았습니다. 이에 당황한 P씨는 황급히 금융거래정보를 알려주었습니다.

이후 사기범은 P씨가 알려준 정보를 이용하여 P씨 명의의 신용카드(4장)로 카드론 4,800만 원을 받은 후 다시 P씨에게 전화를 걸어 "당신의 통장으로 범죄 자금 4,800만 원이 입금되었으니 국가안전계좌로 이체하십시오."라고 요구했습니다. P씨는 사기범이 불러주는 계좌로 4,800만 원을 이체하여 피해를 보았습니다.

사례 3 대학교 교직원을 사칭하여 등록금을 가로챈 사례

○○대학교에 지원했던 G씨(20대, 여)는 대학교 교직원을 사칭하는 자로부터 "지원한 대학에 추가 합격했으니 금일 오후 4시까지 제가 불러 주는 계좌로 등록금 530만 원을 송금해야만 등록처리됩니다."라는 전화를 받았습니다. 이 말을 들은 G씨는 부모님께 연락하여 사기범이 불러 준 계좌로 돈을 송금하여 피해를 보았습니다.

사례 4 자녀 학교의 행정실 직원을 사칭한 사례

K씨(50대, 여)는 "학교 행정실입니다. 아이가 머리를 크게 다쳐서 당장 수술을 해야 하니 1,000만 원을 송금하세요."라는 전화를 받았습니다. 사기범이 자녀의 이름, 휴대전화 번호, 학교 이름까지 정확히 알고 있었기 때문에 의심없이 사실이라고 믿은 K씨는 당황하여 사기범이 불러주는 대포통장 계좌로 급히 800만 원을 송금했습니다.

이후 K씨가 해당 병원과 학교에 확인하여 보이스피싱임을 알아차렸을 때는 이미 사기범 일당이 피해금을 모두 인출해 간 뒤였습니다.

사례 5 ARS를 통한 전화요금 연체 안내를 사칭한 사례

K씨(70대, 남)는 집 전화로 "전화요금이 연체되어 오늘 전화가 끊어집니다. 상담을 원하시면 9번을 누르세요."라는 ARS 전화를 받았습니다. 당황한 K씨가 9번을 누르자 통신회사 직원을 사칭하는 자에게 연결되었고, 전화요금을 묻는 K씨에게 사기범은 "개인정보가 노출돼서 전화요금이 많이 나온것 같으니 경찰에 신고해 주겠다."라고 한 후 전화를 끊었습니다. 곧 경찰을 사칭하는 자가 전화를 걸어 K씨와 피해접수 상담 후 금융거래 안전을 위해 금융감독원을 연결해 주겠다며 전화를 종료했습니다. 그러자 금융감독원 직원을 사칭하는 자가 전화하여 개인정보 유출로 피해자 통장에서 예금이 모두 인출될 수 있으니 은행을 방문하여 폰뱅킹에 가입하고 예금을 피해자 명의의 한 계좌로 모으라고 지시했습니다. K씨는 지시대로 따랐고, 사기범은 피해자로부터 알아낸 폰뱅킹 정보를 이용하여 피해자의 예금 3,500만 원을 모두 대포통장으로 이체했습니다.

사례 6 친구를 사칭한 메신저피싱 사례

J씨(40대, 여)는 퇴근 후 휴식을 취하면서 스마트폰으로 메신저 메시지를 확인하던 중, 친구로부터 "갑자기 가족이 아파서 급전이 필요하니 100만 원을 잠시 빌려주면 1주일 후 갚아 주겠다."라는 메시지를 받았습니다. J씨가 아무 의심없이 친구에게 응답하자 친구는 고마움을 표하며 자신의 계좌번호를 메신저로 보내주었고, J씨는 돈을 송금했습니다.

J씨는 자신이 메신저피싱을 당했다는 사실을 뒤늦게야 알았습니다. 이는 사기범 일당이 J씨 친구의 메신저 아이디와 비밀번호를 알아내어 접속한 후, 친구인 척 행세하며 다수의 사람에게 급전을 미끼로 돈을 송금해줄 것을 요구한 메신저피싱이었습니다.

사례 7 직장 상사를 사칭한 메신저피싱 사례

L씨(30대, 남)는 퇴근 후 직장 상사로부터 "지금 급히 170만 원을 송금해야 하는데 인증서 오류로 인해 이체거래가 안된다. 그러니 대신 송금을 해 주면 내가 내일 수수료와 함께 돌려주겠다."라는 메신저 메시지를 받았습니다. L씨는 별다른 의심없이 직장 상사가 알려 준 계좌번호로 돈을 입금하였습니다.

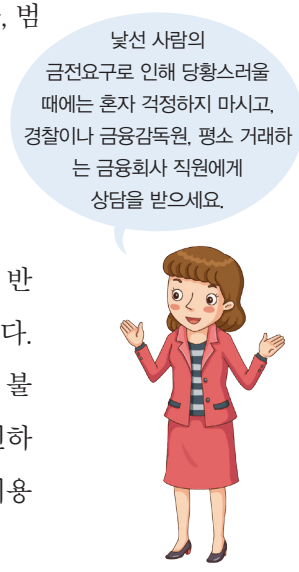
다음날 회사에 출근한 L씨는 사기범이 L씨의 직장 상사의 메신저 아이디와 비밀번호를 도용하여 로그인한 후, 지인들에게 급전을 요구했던 메신저피싱임을 알게 되었습니다.

보이스피싱, 이렇게 하면 예방할 수 있습니다

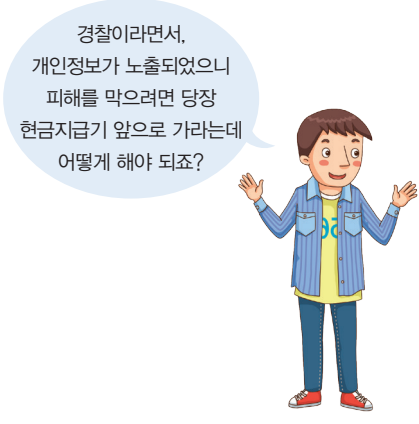
낯선 사람에게는 금융거래정보를 절대 알려 주면 안 됩니다.

금융회사 및 공공기관에서는 개인정보 유출, 범죄사건 연루 등과 관련하여 전화를 통해 계좌번호, 계좌 비밀번호, 보안카드번호 등을 묻거나 인터넷 사이트에 금융거래정보를 입력하도록 요구하지 않습니다.

낯선 전화를 받고 불안하거나 의심스러우면 반드시 해당 기관에 사실 여부를 확인해야 합니다. 이때 해당 기관의 연락처는 절대로 사기범이 불러 주는 전화번호나 인터넷 주소를 통해 확인하지 말고, 반드시 114 또는 포털사이트 등을 이용해 확인하시기 바랍니다.



현금지급기로 유인하면 100% 피싱사기입니다.



세금, 보험료 등을 환급해 준다거나 계좌 안전조치를 취해 주겠다면서 현금지급기로 유인하더라도 절대 응해서는 안됩니다. 경찰, 금융감독원, 은행 등 어느 기관에서도 현금지급기 등을 이용하여 입금하도록 요구하지 않습니다.

자녀 납치 보이스피싱에 미리 대비합니다.

평소 자녀의 친구, 선생님, 인척 등의 연락처를 미리 알아 두도록 합니다. 또한, 자녀가 다쳤다거나 납치되었다는 전화를 받았을 때에는 침착하게 대처해야 합니다. 사기범의 요구대로 금융거래정보를 알려 주거나 입금부터 하지 마시고, 평소 준비해 둔 지인들의 연락처를 이용해서 자녀가 안전한지부터 확인하기 바랍니다.

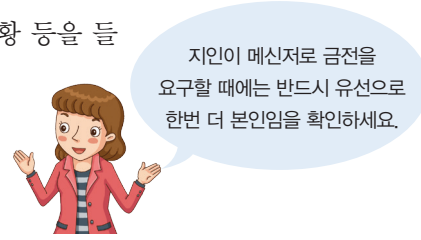
개인정보를 미리 알고 접근하는 경우에도 내용의 사실 여부를 반드시 확인해야 합니다.

최근 동창회, 친구, 대학 입학처, 거래처 등을 가장하여 전화로 계좌번호를 알려 주며 송금을 요구하는 경우가 많습니다. 주민등록번호, 가족 이름 등 개인정보를 알고 접근하는 경우가 많으므로 전화의 내용이 사실인지를 반드시 확인해야 합니다.

메신저피싱, 이렇게 하면 예방할 수 있습니다

메신저로 금전을 요구하는 경우 반드시 전화를 걸어 본인임을 확인하세요.

만약 상대방이 통화할 수 없는 상황 등을 들어 본인 확인을 회피하고자 한다면 직접 신분을 확인할 때까지 일체 요구에 응하지 말아야 합니다.



메신저 자체 보안 설정 및 보안 프로그램을 최신 버전으로 업데이트하세요.

보안 프로그램을 주기적으로 업데이트하여 최신 버전으로 유지하고, 이를 통해 새로운 유형의 피싱 범죄를 예방할 수 있도록 노력해야 합니다.

평소 메신저를 통해 개인정보를 주고받지 마세요.

지인의 아이디로 메신저에 접속한 사기범이 정보를 요구하는 경우에 별다른 의심없이 응할 수 있고, 메신저 대화 기록에 남아 있는 금융거래 정보가 유출될 수 있습니다.

정기적으로 메신저 비밀번호를 변경하세요.

메신저의 비밀번호는 다른 사이트의 비밀번호나 본인의 개인정보와 연관성이 없도록 설정하고, 정기적으로 변경해야 합니다.

메신저에 포함된 출처가 불분명한 파일이나 이메일, 인터넷 주소는 클릭하지 말고 바로 삭제하세요.

스마트폰이나 컴퓨터에서 출처가 불분명한 파일이나 이메일의 첨부 파일, 인터넷 주소 등을 클릭하면 해당 기기가 악성코드에 감염될 확률이 높습니다. 악성코드는 전자금융 거래 시 금융거래정보의 유출을 야기하는 주요 원인이 됩니다.

공공장소에 설치된 전자기기로 메신저 사용이나 인터넷뱅킹 등의 거래를 자제하세요.

PC방 등 공공장소에 설치된 컴퓨터 등은 많은 사람들이 다양한 웹 사이트에 접속하기 때문에 악성코드나 바이러스에 감염될 위험이 높습니다. 따라서 메신저 사용이나 인터넷뱅킹 거래 등을 통해 나의 개인 정보가 공공장소의 컴퓨터에 저장되지 않도록 주의하고, 사용 후에는 반드시 로그아웃해야 합니다.

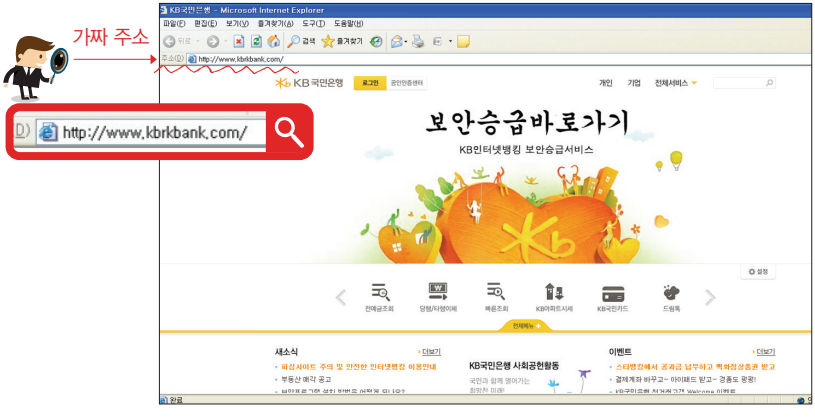
2 파밍(pharming)과 피싱사이트 (phishing site)

2011년부터 본격적으로 발생한 파밍과 피싱사이트는 보이스피싱과 더불어 큰 피해를 야기하고 있는 주요 피싱사기입니다. 2012년 들어 대폭 증가하였고, 특히 보안승급과 강화 등을 이유로 금융거래정보를 입력하도록 유도하는 피싱사이트가 급증하고 있습니다.

파밍과 피싱사이트란

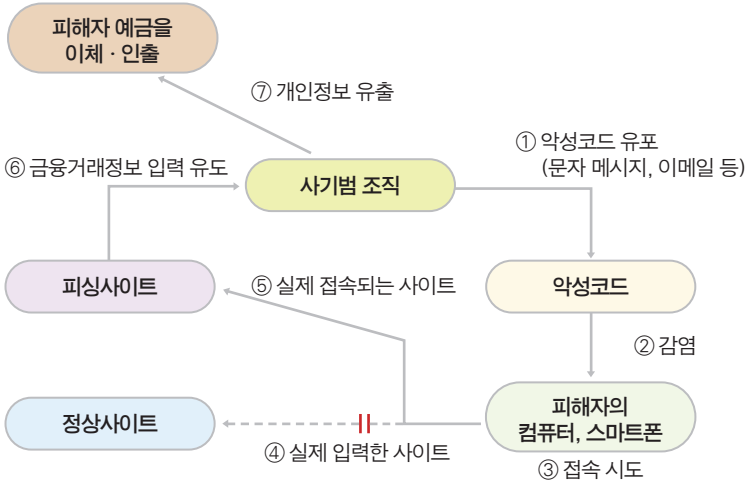
피싱사이트란 피싱(phishing)과 사이트(site)의 합성어로, 금융거래정보를 빼내기 위해 은행 등의 홈페이지와 매우 유사하게 모방하여 만든 가짜사이트를 말합니다. 사기범들은 피싱사이트를 이용하여 금융거래정보의 입력을 유도하고 있습니다.

❖ 은행을 사칭한 피싱사이트 사례



파밍의 경우에는, 사기범이 먼저 이용자의 컴퓨터를 악성코드에 감염시켜 호스트 파일이나 브라우저 메모리를 변조시킵니다. 이후 컴퓨터 이용자가 인터넷 '즐겨찾기'나 포털사이트 검색을 통해 정상적인 금융회사 홈페이지로 접속하더라도 피싱사이트로 연결되도록 하여 이용자의 금융거래정보(계좌 비밀번호, 보안카드번호 등)를 가로채는 피싱사기입니다.

❖ 파밍과 피싱사이트의 금융사기 과정



파밍과 피싱사이트에 의한 금융거래정보 유출 과정

1 단계

문자 메시지나 이메일 등을 이용해서 악성코드 유포

2 단계

악성코드에 감염된 컴퓨터나 스마트폰에서 인터넷 사용 시 가짜 포털사이트 화면이나 가짜 금융감독원 팝업창이 나타남.

※ 이런 화면이 보이는 경우, 반드시 악성코드 치료를 해야 정상적으로 컴퓨터 및 스마트폰을 사용할 수 있고 금융사기를 예방할 수 있음.

금융감독원 외에 경찰청, 한국인터넷진흥원(KISA)등을 모방한 팝업창이 나타나기도 합니다.

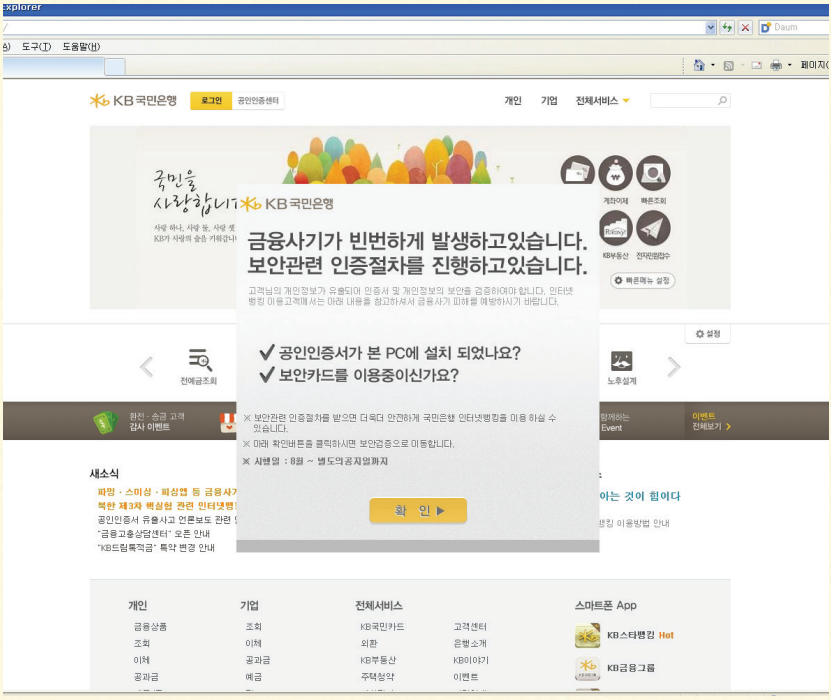
3 단계

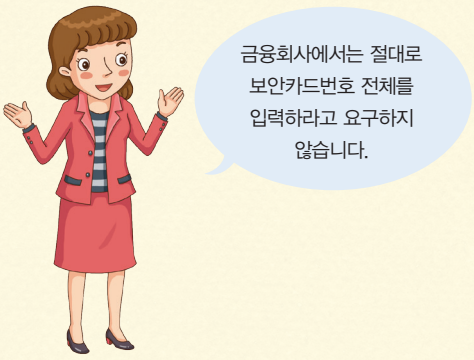
가짜 금융감독원 팝업창 클릭 시 금융감독원 홈페이지를 모방한 피싱사이트로 이동

정상 사이트와 다른 화면

4
단계

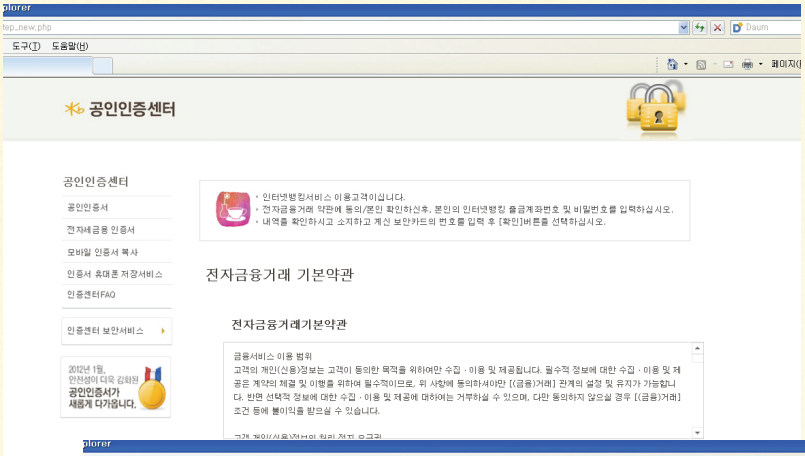
금융감독원 홈페이지를 모방한 피싱사이트 클릭 시 금융회사 홈페이지를 모방한 피싱사이트로 이동





5
단계

금융거래정보 입력 유도



파밍과 피싱사이트의 특징은

과도한 금융거래정보의 입력을 요구한다면 일단 피싱사이트를 의심해야 합니다.

■ 금융거래정보를 과도하게 요구합니다.

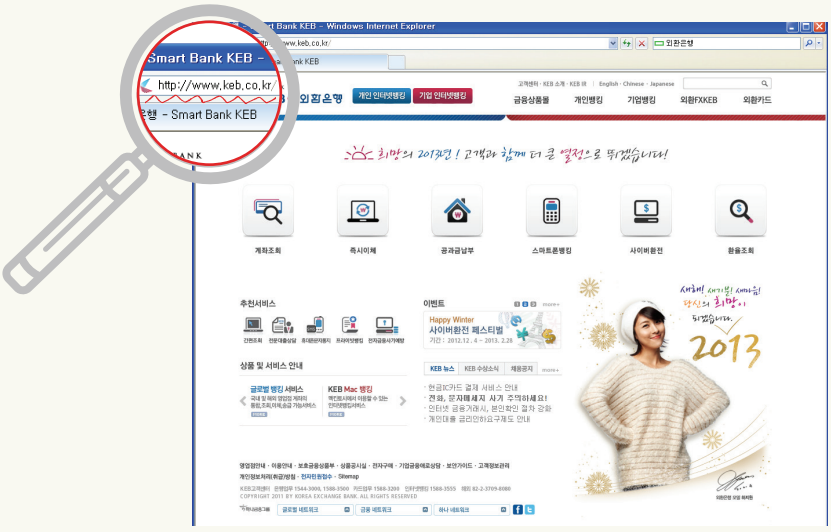
보안 인증 및 강화를 명분으로 이용자의 의사와 상관없이 팝업 창이나 피싱사이트 화면을 계속해서 컴퓨터 화면에 띄웁니다. 또한, 비밀번호, 보안카드번호 전체를 입력하라고 하는 등 과도한 금융거래정보를 요구합니다.

■ 악성코드는 다양한 방식으로 유포됩니다.

사기범들에 의해 유포된 악성코드는 SMS 문자 메시지나 메신저의 메시지에 포함된 인터넷 주소를 클릭하는 경우, 낯선 사람으로부터 온 이메일의 첨부파일을 여는 경우, 낯선 사이트에서 다운로드 받은 파일 등 다양한 방식으로 여러분의 컴퓨터나 스마트폰을 감염시킵니다.

정상 사이트와 파밍에 의한 피싱사이트 비교

정상 사이트 ▶



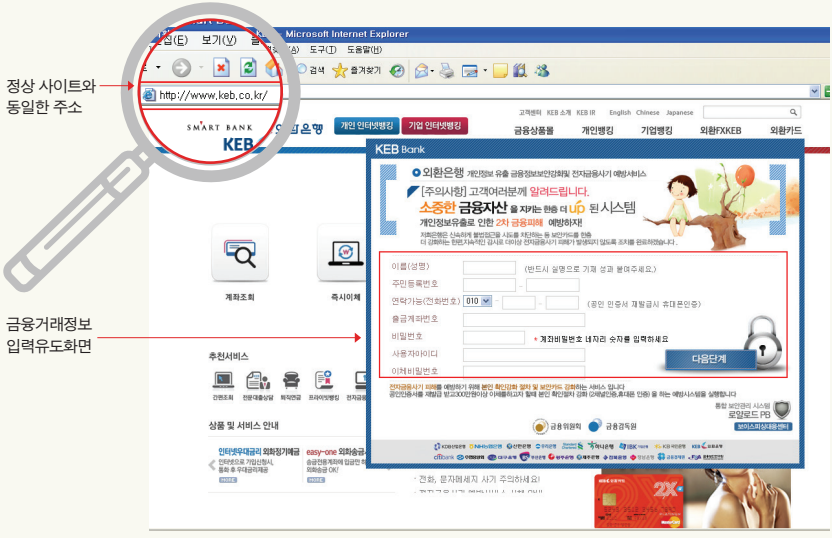
■ 정상 웹사이트와 구별하기 어려워 피싱사이트를 정상 웹사이트로 착각합니다.

파밍은 포털사이트 검색이나 인터넷 즐겨찾기 기능을 통해 정상적인 웹사이트에 접속하는 경우에도 악성코드에 의해 피싱사이트로 연결되므로 보이스피싱에 비해 피싱사기라는 것을 깨닫는 것이 어렵습니다. 따라서 피싱사기 피해를 알아차리고 지급정지 조치를 하기까지 시간이 늦어져 피해금액이 커지므로 각별한 주의가 필요합니다.

■ 공포 전술을 이용합니다.

악성코드에 의한 팝업창이나 피싱사이트 화면의 내용을 보면, 금융범죄 연루로 인한 예금자보호 조치나 신원정보 보호 등을 명분으로 즉각적인 조치가 필요하다고 긴장감과 공포감을 조장하여 거래은행명, 계좌번호 등의 금융거래정보 입력을 요구합니다.

파밍에 의해 유도된 피싱사이트 ▶



피해 사례

사례 1 인터넷 즐겨찾기 기능을 이용하다가 피싱사이트로 연결된 사례

K씨(40대, 여)는 인터넷뱅킹을 이용하기 위해 본인이 사용하는 컴퓨터에 저장해 놓은 인터넷 즐겨찾기를 통해서 ○○은행의 사이트에 접속했습니다. 그러나 접속된 사이트는 ○○은행 사이트와 유사하게 가장한 피싱사이트였습니다.

K씨는 평소와 다르게 주민등록번호와 계좌번호를 직접 입력하게 하고, 보안카드번호 전체를 입력하도록 요구하는 화면에 의아했으나, 평소 자신이 거래하던 ○○은행 사이트와 매우 유사했기 때문에 결국 피싱사이트에 속아 금융거래정보를 모두 입력했습니다.

사기범 일당은 피싱사이트를 통해 얻은 K씨의 정보를 이용하여 공인인증서를 재발급받았고, ○○은행에서 K씨 계좌의 이상거래를 발견하는 경우 본인확인을 할 수 없도록 연락처 등을 수정했습니다. 이들은 5일간 K씨 명의의 인터넷뱅킹을 통해 K씨의 은행 계좌에서 총 5회에 걸쳐 1,000만 원을 빼낸 후 잠적했습니다.

사례 2 금융감독원에 의한 보안강화를 내세운 피싱사이트 사례

Y씨(30대, 남)는 평소처럼 인터넷을 이용하려고 포털사이트에 접속했습니다. 포털사이트 화면에는 안전한 금융 거래를 위해 보안강화 인증 절차를 밟도록 안내하는 금융감독원 팝업창이 띄워져 있었습니다. 이는 악성코드 감염으로 인해 연결된 피싱사이트였습니다.

그러나 이를 알지 못한 Y씨는 금융감독원 팝업창을 없앤 후 인터넷을 이용하려고 했으나 팝업창은 없어지지 않았고, 팝업창을 클릭하지 않으면 인터넷 사용이 불가능했습니다. 결국 Y씨가 팝업창을 클릭하자 금융감독원 홈페이지를 모방한 피싱사이트에 연결되었고, 이 사이트를 클릭하자 ○○은행 홈페이지를 모방한 또 다른 피싱사이트로 연결되었습니다. 피싱사이트에서는 보안승급을 위해 주민등록번호, 거래 은행명, 계좌번호, 보안카드번호 전체, 계좌 비밀번호 등을 입력하도록 요구했고, 이에 속은 Y씨는 의심없이 정보를 모두 입력했습니다. 사기범 일당은 Y씨의 정보를 이용해서 공인인증서를 재발급 받고, 비밀번호를 변경한 후 3일에 걸쳐 1500만 원을 인출했습니다.

사례 3 보이스피싱과 피싱사이트를 동시에 이용한 피해 사례

J씨(50대, 남)는 검찰청 수사관을 사칭하는 자로부터 "검찰 수사 과정에서 범인들이 J씨의 계좌를 대상으로 범죄를 시도한 정황을 포착했습니다. 수사 협조와 본인 예금계좌에 대한 보안조치가 필요하니 적극 협조하십시오."라는 전화를 받았습니다. 위압적이고 그럴싸한 사기범의 말에 속은 J씨가 인터넷 주소창에 사기범이 알려준 홈페이지 주소를 입력하자 검찰청 홈페이지를 모방한 피싱사이트로 연결되었습니다. 사기범은 통화를 계속하며 범죄 수사를 위해 필요한 것처럼 속여 J씨의 금융거래정보 입력을 유도했습니다. 결국 J씨는 주민등록번호, 계좌 비밀번호, 보안카드번호 전체를 입력했고, 휴대전화로 수신된 인증번호 문자 메시지까지 사기범에게 알려주었습니다. 정보를 모두 알아낸 사기범은 3일 정도 기다리면 별도의 연락을 주겠다고 안심시켰고 J씨는 이를 믿었습니다.

이후 사기범 일당은 J씨 명의로 공인인증서를 재발급 받아 카드론 대출과 예금 인출 등 총 3,000만 원의 피해금을 가로챈 뒤 잠적했습니다.

사례 4 쇼핑몰 결제창을 통한 파밍 피해 사례

K씨(20대, 여)는 인터넷쇼핑몰인 "△△감성" 사이트에서 옷을 구매하기 위해 결제 방법을 실시간 계좌이체로 선택하고, 결제창의 "뱅킹" 버튼을 클릭했습니다. 그러나 이미 악성코드에 감염되어 있던 컴퓨터는 ○○은행 홈페이지를 모방한 피싱사이트로 연결되었습니다. K씨는 평소 거래할 때와 달리 보안카드번호 전체를 입력하도록 요구하는 것이 의아했지만, 계좌 비밀번호, 인터넷뱅킹 아이디 등 금융거래정보를 모두 입력했습니다.

K씨의 금융거래정보를 알아낸 사기범 일당은 공인인증서를 재발급 받아 인터넷뱅킹을 통해 258만 원을 K씨 통장에서 대포통장으로 이체한 뒤 전액 인출해 갔습니다.

사례 5 문자 메시지로 스마트폰의 악성코드 감염을 이용한 피해 사례

P씨(30대, 남)는 스마트폰으로 생일초대 문자 메시지를 받았습니다. 문자 메시지에는 생일파티 장소를 안내하는 인터넷 주소가 포함되어 있었으나, P씨가 인터넷 주소를 클릭했을 때 아무런 안내화면도 나타나지 않았습니다. P씨는 흔한 스팸 문자려니 생각하고 별다른 조치를 취하지 않았으나, P씨의 스마트폰은 이미 악성코드에 감염되었습니다. 이후 P씨가 스마트폰을 이용하여 ○○은행 어플을 실행하려고 하자 계속해서 보안인증 절차 강화를 위한 안내 화면(악성코드로 인해 연결되는 피싱사이트 화면)만 나타났습니다. P씨는 거래 은행명, 계좌 비밀번호, 보안카드번호 전체 등 금융거래정보를 모두 입력하였고, 이후 사기범은 이를 이용하여 P씨의 계좌에서 700만 원을 대포통장으로 이체하여 인출한 후 잠적했습니다.

파밍과 피싱사이트, 이렇게 하면 예방할 수 있습니다

공공기관 또는 금융회사를 사칭한 피싱사이트 유도에 주의하세요.

금융감독원에서는 해킹사고로 인한 정보유출을 이유로 보안관련 인증 절차를 진행하였거나 진행 중인 사실이 없습니다. 공공기관과 금융회사를 사칭하며 보안 인증·강화 절차를 진행하기 위해 특정 사이트로 접속하도록 유도할 경우나 보안카드번호 전체 등 과도하게 금융거래정보 입력을 유도하는 경우에는 100% 피싱사이트이므로 절대 응하면 안 됩니다.

금융회사의 보안강화 서비스에 가입하세요.

금융회사 홈페이지를 통해 '전자금융사기 예방서비스[1]'에 가입하면 금융사기로 인한 예금의 부정이체 등을 예방할 수 있습니다. 또한, 금융회사의 자체 보안강화 서비스 등을 적극적으로 활용하면 보다 안전한 금융생활이 가능합니다.

알아두세요

악성코드 치료 방법

- ▸ 컴 퓨 터: 한국인터넷진흥원(KISA)의 "보호나라" 사이트 → "알림마당" 메뉴 → 공지사항 108번 게시글 참고
  - 추가 문의는 한국인터넷진흥원(☎ 118)에서 가능
- ▸ 휴대전화: 휴대전화 A/S 센터를 방문하여 치료 의뢰

1) 공인인증서 (재)발급 및 인터넷뱅킹을 통한 300만 원 이상(1일 누적) 이체 시 SMS, 전화 등을 통해 본인 확인을 강화하여 피싱 · 파밍 등의 피해를 예방하는 제도

보안카드보다 안전성이 높은 보안매체를 적극 이용하세요.

금융 거래 시 OTP나 보안토큰 사용을 권장합니다. 만약 이런 보안매체를 사용하지 않는 경우 계좌 비밀번호 등 금융거래정보를 주기적으로 변경하여 금융생활의 안전성을 높이기 바랍니다.

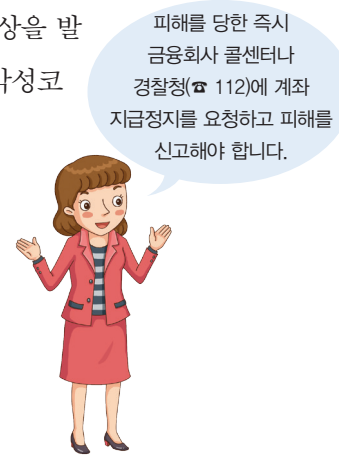
신 입금계좌지정제를 이용하세요.

고객이 사전에 지정한 계좌로는 고객의 전자금융 이체 한도 내에서 송금이 가능하고, 지정하지 않은 계좌로는 최대 100만 원(1일 누적 기준) 한도 내에서만 송금이 가능합니다. 일명 "안심통장서비스"라고 합니다.

평소 악성코드 탐지 및 제거를 생활화하세요.

컴퓨터가 악성코드에 감염됐거나 의심되는 증상을 발견하면 즉시 컴퓨터 백신프로그램을 이용하여 악성코드를 탐지하고 제거해야 합니다. 특히 금융회사의 인터넷뱅킹 사이트를 이용할 때에는 주기적으로 수행하는 등 컴퓨터 보안 점검을 생활화해야 합니다.

또한, 경찰청에서 개발하여 무료 배포 중인 파밍방지 프로그램인 '파밍캅(pharming cop)'을 이용합니다.



출처가 불분명한 파일이나 이메일은 클릭하지 마시고 바로 삭제하세요.

스마트폰이나 컴퓨터에서 출처가 불분명한 파일과 이메일, 인터넷 주소 등을 클릭하면 해당 전자기기가 악성코드에 감염될 확률이 높습니다. 만약 파일 등을 클릭하고자 한다면, 반드시 배포한 기관의 공신력 있는 전화번호, 홈페이지 등을 통해서 사실 여부부터 확인하기 바랍니다.

알아두세요

전기통신금융사기로 인한 피해 신고 및 상담 기관

- 금융회사 콜센터
- 경찰청(☎ 112)

• 금융거래정보의 노출로 피해가 걱정되는 내 계좌에 대한 지급정지 요청
• 내 피해금을 입금한 상대방 계좌(대포통장)에 대한 지급정지 요청

- 경찰청(☎ 112)

• 전기통신금융사기로 인한 피해 신고

- 금융회사(직접 방문)

- 금융감독원(☎ 1332)
- 금융회사 콜센터

• 금융감독원의 피해금 환급절차 신청

• 환급제도 안내 및 상담

- 한국인터넷진흥원(☎ 118)
- 금융감독원(☎ 1332)

- 한국인터넷진흥원(☎ 118)

• 피싱사이트 신고

• 스팸 전화나 문자 메시지의 신고

전화로 계좌의 지급정지 요청을 한 경우 3영업일 내에 금융회사를 방문해서 관련 서류를 제출해야 합니다.

3 대출빙자사기

사기범들이 다른 사람의 어려운 경제적 상황을 이용하여 대출을 빙자한 금융사기를 일으키므로, 금융소비자들은 더욱 큰 어려움을 겪지 않도록 각별한 주의를 기울여야 합니다.

대출빙자사기란

대출빙자사기란 얼굴을 대면하지 않는 전화나 문자 메시지 등의 통신수단을 통해 대출 상담, 대출 알선을 가장하여 접근한 후 신용등급 조정, 대출 수수료 등 각종 명목으로 금전을 요구하여 가로채는 사기수법입니다.

대출빙자사기의 특징은

■ 저금리로 대출을 알선해 주겠다고 미끼를 던집니다.

공신력 있는 제도권 금융회사의 직원을 사칭하여 저금리 대출로 대환해 주겠다며 접근합니다. 그런 후 대부업체 등의 고금리 대출을 받게하고, 대환대출[2] 명목으로 대출금을 입금하게 하여 돈을 가로챕니다. 또는 은행 등의 저금리 대출을 알선해 주겠다며 일정 기간 동안의 예치금 또는 공탁금 등의 명목으로 돈을 요구합니다.

2) 금융회사에서 대출을 받아 이전의 대출금이나 연체금을 갚는 제도.

■ **무작위로 SMS 문자 메시지를 발송하거나 스마트폰 악성 앱을 이용합니다.**

사기범들은 무작위로 저금리 대출을 해 줄 것처럼 문자 메시지를 보낸 후, 대출 상담 전화가 걸려오면 전화번호를 비롯한 개인정보들을 수집합니다. 또한, 사기범에게 대출을 필요로 하는 사람으로 한번 기록되면 반복해서 대출 알선 문자를 보내거나 전화를 합니다.

■ **신용등급 상향 조정을 미끼로 보증료 등을 요구합니다.**

신용등급이 낮아 대출 진행이 어려우므로 보증보험에 가입해야 한다고 하면서 보증료 납부를 요구하거나, 채무 이행 담보 명목으로 이자 선납 또는 신용불량 정보 삭제를 위한 전산비용 등을 요구합니다.

■ **공증료 등 법률비용 납부를 요구합니다.**

대출 실행 후에 발생할 수 있는 채무 불이행 또는 채권 추심 등에 대비한 공증료 등의 명목으로 금전을 요구합니다.

■ **통장 사본, 휴대전화 등 실물을 요구합니다.**

대출을 받기 위해서는 통장 또는 휴대전화 개설이 필요하다고 하면서 통장 사본, 체크(현금)카드, 휴대전화 등을 보내 달라고 요구 합니다. 피해자가 사기범의 요구대로 통장 사본, 휴대전화 등을 보내면 사기범은 이를 수령한 뒤 연락을 끊고 대포통장 또는 대포폰으로 악용합니다.

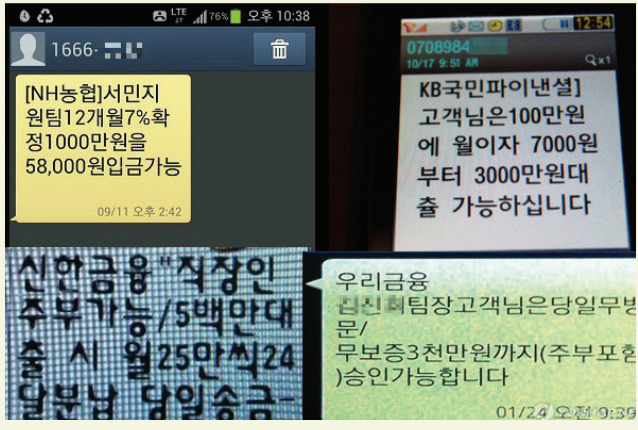
궁금해요

대출빙자사기는 불법대출 중개수수료와 어떻게 다른가요?

대출빙자사기는 대출을 미끼로 접근하여 수수료 등의 명목으로 금전을 요구하는 점에서 불법대출 중개수수료와 유사한 면이 있습니다. 하지만 불법대출 중개수수료는 대출을 성사시켜 주고 고객으로부터 그 대가를 받는 행위인 반면, 대출빙자사기는 대출 자체가 이루어지지 않는다는 점에서 차이가 있습니다.

그렇다면 피싱사기와는 어떻게 다른가요?

전화로 피해자를 속여 자금을 이체하도록 유인한다는 점에서는 보이스피싱과 유사한 면이 있습니다. 하지만 보이스피싱은 가족 납치를 빙자하거나 공공기관을 사칭하는 등의 방식으로 피해자를 속이는 반면, 대출빙자사기는 '대출이라는 용역의 제공'을 가장한 사기 수법이라는 점에서 차이가 있습니다.



피해 사례

사례 1 신용등급 상향을 미끼로 보증료 등을 요구한 사례

L씨(30대, 여)는 OO저축은행으로부터 저금리 대출이 가능하다는 문자 메시지를 받았습니다. 경제적으로 곤란한 상황에 처해있던 L씨는 이런 스팸 문자가 사기임을 의심하면서도, 혹시나 하는 마음에 전화를 걸었습니다. 전화는 OO저축은행 직원을 사칭한 사기범과 연결되었고, 사기범은 L씨가 거래하는 은행의 금융거래정보를 물으며 신용등급을 조회하는 듯한 상황을 연출했습니다. 그러고 나서 L씨에게 대출금 1,000만 원이 승인되었으나 신용등급이 낮기 때문에 신용보증을 위해서는 L씨의 통장에 300만 원이 잔액으로 있어야만 대출금이 지급된다고 말했습니다. 이에 L씨는 자신의 계좌에 300만 원을 입금했습니다. 사기범은 미리 알아낸 L씨의 금융거래정보로 텔레뱅킹을 이용하여 300만 원 전액을 대포통장으로 이체하여 인출한 뒤 잠적했습니다.

사례 2 저금리 대출로의 전환을 알선해 주겠다며 접근한 사례

K씨(40대, 남)는 ㅇㅇ은행의 직원을 사칭하는 사기범으로부터 고금리의 대출을 일정기간 사용하면 저금리 대출로 전환해 주겠다는 전화를 받았습니다. 전화 내용에 현혹된 K씨는 ㅁㅁ대부 및 ◇◇저축은행에 대출을 신청하여 총 1,350만 원의 대출을 받았고, 대환대출을 위해 필요하니 지정하는 계좌(대포통장)로 대출금을 입금하라는 사기범의 지시에 따랐습니다. 그러나 대환대출은 이뤄지지 않았고, 사기범들은 1,350만 원을 인출하여 잠적했습니다.

사례 3 공증료 등 법률비용 납부를 요구한 사례

P씨(50대, 남)는 ○○캐피탈 직원을 사칭하는 사기범으로부터 저금리로 1,500만 원까지 대출(마이너스 통장 개설)이 가능하다는 전화를 받았습니다. 사기범은 P씨의 현재 소득수준으로는 대출이 불가능하지만, 대출이 가능하도록 알선해줄테니 ○○은행에서 전화가 오면 P씨 본인이 ㈜ㅁㅁ공업 팀장으로 재직 중이라고 얘기하라면서 P씨를 현혹했습니다. 전화를 끊자 곧바로 ○○은행 직원을 사칭하는 자로부터 연락이 왔고, 채무 불이행 상황에 대비해 공증료 등 법률비용을 납부해야 한다며 380만 원을 세 개의 계좌(대포통장)로 분산 입금하라고 요구했습니다. 이를 믿은 P씨는 요구대로 입금했고, 사기범들은 이를 인출한 후 잠적했습니다.

사례 4 스마트폰 악성 앱을 이용한 대출사기 사례

J씨(30대, 여)는 ○○캐피탈 직원을 사칭하는 사기범으로부터 저금리 대출이 가능하다는 전화를 받았습니다. 사기범은 J씨의 현재 대출상황 등을 물어본 뒤 본인 인증 및 대출 가능 여부를 조회할 수 있다며 문자 메시지로 인터넷 주소를 보냈습니다. J씨가 해당 주소를 클릭하여 앱(악성 앱)을 설치하고 실행하자 여러 금융회사의 전화번호 목록이 나타났습니다. J씨는 사기범의 안내대로 본인 인증을 위해 성명, 주민등록번호 등을 입력했고, 대부업체의 기존 대출금을 상환해야 저금리 대출이 가능하다는 사기범의 말에 앱에 있는 통화연결 기능을 이용해서 ㅁㅁ대부의 전화번호로 연락했습니다. ㅁㅁ대부 직원을 가장한 또 다른 사기범에게 연결된 줄 몰랐던 J씨는 사기범이 알려준 계좌(대포통장)로 대출금을 상환하여 1,000만 원의 피해을 보았습니다.

대출빙자사기, 이렇게 하면 예방할 수 있습니다

전화 또는 문자 메시지를 이용한 대출광고는 절대 연락하지 마세요.

대출 여부는 대출 당시 고객의 신용등급, 채무내역, 연체이력 등을 고려하여 금융회사가 결정하는 것이므로 전화나 문자 메시지를 통한 대출 광고는 대출빙자사기일 가능성이 높습니다.

대출 실행과 관련해 금전을 요구할 때에는 대출 빙자 사기를 의심하세요.

정상적인 대출업체는 수수료나 선이자 등 어떠한 명목으로도 대출과 관련해 금전을 요구하지 않습니다.

타인에게 절대 개인정보와 통장 등을 넘겨주면 안 됩니다.

신분증, 보안카드번호, 문자 메시지 인증번호, 통장 사본 등 개인의 신용정보를 다른 사람에게 알려 주면 본인도 모르는 사이에 대출 거래나 자금 이체 승인 등 범죄에 이용될 가능성이 높습니다. 또한, 체크(현금)카드, 휴대전화 등을 대출권유 업체에게 넘겨주는 경우 대포통장이나 대포폰으로 이용되어 본인도 모르게 범죄에 연루될 수 있으므로 주의해야 합니다.

궁금해요

전기통신금융사기 피해자들에 대한 피해금 환급제도는 어떤 제도인가요?

「전기통신금융사기 피해 방지 및 피해금 환급에 관한 특별법」에 의거하여, 전기통신금융사기 피해자들의 피해금을 소송절차 없이 환급해 주는 제도입니다.

피해금 환급제도의 적용 대상은 어떻게 되나요?

환급의 대상이 되는 전기통신금융사기란 보이스피싱, 메신저피싱, 파밍과 피싱사이트, 대출빙자사기 등이며, 스미싱 및 메모리 해킹은 제외됩니다. 또한, 재화의 공급이나 용역의 제공 등을 가장한 행위 역시 제외됩니다.
피해금 환급은 지급정지를 신청한 사기이용계좌에 남아있는 피해금을 대상으로 진행되며, 계좌에 피해금이 없거나 남아있는 피해금을 초과한 금액에 대해서는 진행되지 않습니다.

❖ 전기통신금융사기 피해금 환급절차

- 지급정지 의뢰 및 피해 구제신청 — 피해자
- 지급정지
예금채권 소멸 공고요청 — 지급정지 은행
- 예금채권 소멸 공고(2개월)
피해자별 환급액 계산(14일 이내) — 금융감독원
- 피해환급금 지급 — 지급정지 은행

4 스미싱 (smishing)

스미싱은 휴대전화의 문자 메시지에 포함된 인터넷 주소를 클릭 시 악성코드에 감염되어 소액결제 피해를 일으킵니다. 최근에는 파밍 · 피싱사이트 수법과 결합한 스미싱 수법이 등장하는 등 그 수법이 점차 진화하고 있습니다.

스미싱이란

스미싱은 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 소액결제 피해뿐만 아니라 신·변종 스미싱 피해 사례들이 발생하고 있습니다. 문자 메시지의 인터넷 주소 등을 통해 금융회사를 가장한 악성 앱이나 악성코드를 설치하도록 유도하고, 앱에 표시된 번호로 전화를 걸면 사기범의 전화로 연결되어 다양한 명목으로 송금을 요구하거나 악성코드를 통해 피싱사이트로 연결하기도 합니다.

스미싱의 특징은

■ 문자 메시지를 클릭해서 악성 앱을 설치하도록 유도합니다.

악성코드나 악성 앱이 설치되도록 하는 인터넷 주소가 담긴 문자 메시지를 불특정 다수에게 발송하여 주로 휴대전화 소액결제 피해를 일으킵니다.

최근에는 문자 메시지의 인터넷 주소를 클릭하면 설치되는 악성 앱을 통해 금융거래정보를 손에 넣는 등 신종 수법들이 등장하고 있으므로 휴대전화 이용자들의 각별한 주의가 필요합니다.

■ 문자 메시지 내용이 매우 다양하고 교묘하게 진화하고 있습니다.

스미싱 문자 메시지 내용은 무료·할인 쿠폰, 돌잔치·결혼 청첩장, 경찰 출석 요구서, 교통범칙금 조회, 건강보험공단 무료 암 검진, 카드대금 조회 등 그 유형이 매우 다양합니다.

또한, 문자 메시지의 인터넷 주소 역시 '① 포털사이트 단축 URL(http://goo.gl/, http://me2.do/) → ② 무료 도메인 사이트(http://oa.to/, http://co1.kr/) → ③ 확장 URL(**.kr, **.net, **.com)'로 변화하는 등 그 수법이 교묘해지고 있습니다.

피해 사례

사례 1 대출금리 간편 비교 등 대출사기와 연결된 스미싱 사례

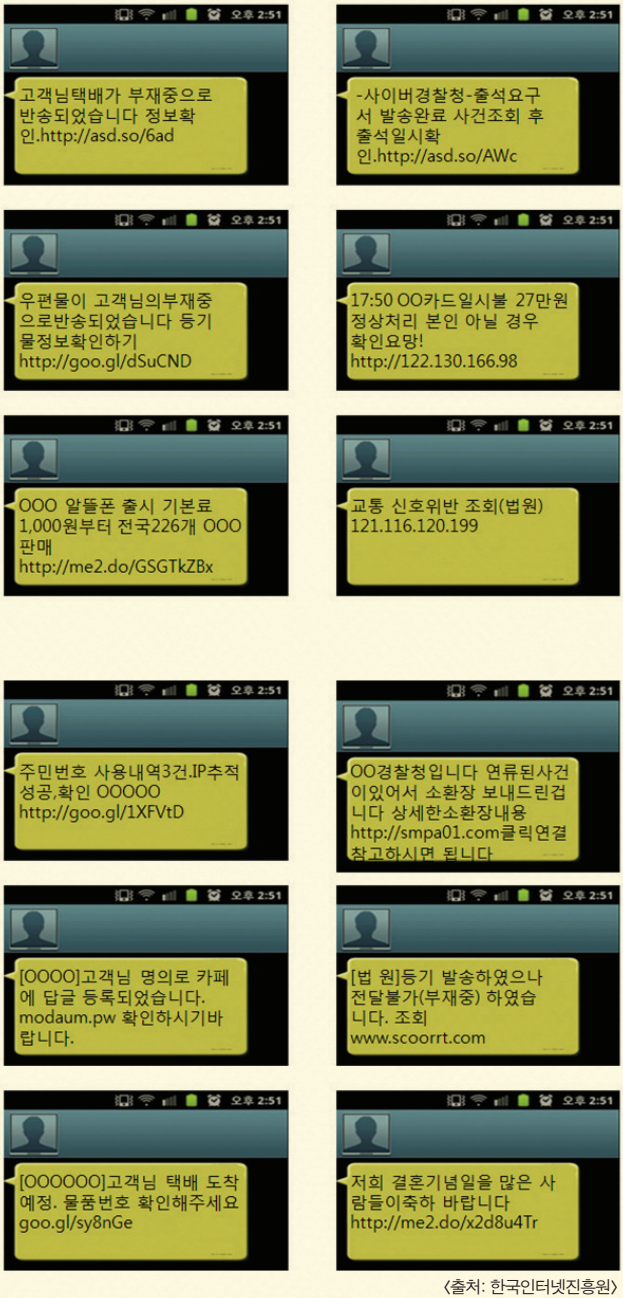
K씨(30대, 여)는 '대출금리 간편 비교'라는 문구와 인터넷 주소가 포함된 문자 메시지를 스마트폰으로 받았습니다. K씨는 문자 메시지에 적혀 있는 인터넷 주소를 클릭했고, 이로 인해 스마트폰에 악성 앱이 설치되었습니다. 악성 앱인지를 인식하지 못한 K씨가 앱을 실행하자 여러 금융회사의 전화번호 목록이 나타났고, K씨가 앱상의 통화연결 기능을 이용하여 전화를 걸자 사기범의 전화로 연결되었습니다. 사기범은 저금리로 대출을 해 주겠다고 속이며 보증료 명목으로 150만 원을 자신이 말하는 계좌(대포통장)로 입금할 것을 요구했습니다. 이에 K씨가 동 금액을 입금하자 사기범은 이를 인출하여 잠적했습니다.

사례 2 돌잔치 초대를 사칭한 스미싱 사례

L씨(40대, 남)는 직장 동료로부터 '돌잔치에 초대한다.'라는 내용이 담긴 문자 메시지를 받고, 링크된 인터넷 주소를 무심코 눌렀습니다. 그러자 본인도 모르게 전화번호부에 등록된 지인 전체에게 돌잔치 초대문자가 복사되어 발송되었습니다.

다행히 L씨는 휴대전화 소액결재 등 금전 피해를 입지는 않았지만, 본인의 스마트폰뿐만 아니라 많은 지인들의 스마트폰에 악성 앱이 설치되어 금융사기 위험에 노출되는 결과를 초래하였습니다.

스미싱 신고 사례

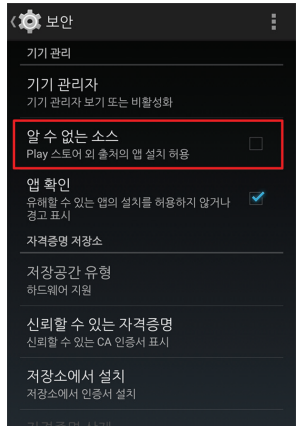


〈출처: 한국인터넷진흥원〉

스미싱, 이렇게 하면 예방할 수 있습니다

문자 메시지상의 알 수 없는 인터넷 주소를 클릭하거나 앱을 설치하지 마세요.

금융회사나 공공기관을 사칭하거나 각종 피싱사기 예방 등을 빙자하며 앱을 설치하도록 유도하더라도 반드시 해당 기관의 공신력 있는 전화번호로 사실 여부를 확인합니다. 스마트폰 설정 기능을 통해 '알 수 없는 소스'를 통한 앱 설치는 허용하지 않도록 설정합니다.



스미싱 방지용 앱을 적극 활용하세요.

한국인터넷진흥원(KISA)에서 배포한 스마트폰 보안점검 앱인 '폰키퍼(phone keeper)', 각 이동통신사나 보안업체에서 제공하는 다양한 백신프로그램들을 이용하면 이미 알려진 악성앱을 탐지하거나 치료할 수 있습니다. 따라서 이러한 보안 앱이나 백신프로그램을 설치하여 주기적으로 업데이트하고, 악성코드 감염 여부를 수시로 점검합니다.

휴대전화 소액결제 미이용 시 통신사 콜센터를 통해 서비스를 차단하세요.

평소 휴대전화 소액결제 서비스를 이용하지 않는다면 각 이동통신사의 콜센터로 전화해서 해당 서비스를 차단하도록 합니다.

알아두세요

스미싱 2차 피해(휴대전화에 설치된 악성 앱으로 인한 부작용)

- 피해자 본인의 휴대전화에서 다른 사람에게 유사한 내용의 스미싱 문자가 대량으로 발송되는 등 범행 도구로 사용될 수 있습니다.
- 악성 앱으로 인해 전화 수신이 불가능합니다.
- 피해자 본인의 휴대전화 연락처 목록이 유출되어, 사기범이 주소록에 등록된 피해자의 지인들에게 송금을 유인하는 협박성 문자 메시지나 전화를 할 수 있습니다.

〈출처: 경찰청〉

5 메모리 해킹 (memory hacking)

메모리 해킹은 악성코드를 이용해 정상적인 인터넷뱅킹 과정에서 입력한 금융거래정보를 가로채는 범죄로, 파밍 및 피싱사이트보다도 더욱 진화한 형태의 금융 범죄입니다.

메모리 해킹이란

이용자의 컴퓨터에 감염시킨 악성코드를 이용해서 정상적인 인터넷뱅킹 사이트에서 입력한 이용자의 금융거래정보(보안카드번호 2개, 계좌비밀번호 등)를 가로챕니다. 이후 획득한 금융거래정보를 이용하여 이용자의 계좌에서 무단으로 자금을 인출해 가는 금융범죄입니다.

메모리 해킹은 특별법에 의한 피해금 환급제도의 대상에서 제외되며, 각 금융회사 차원에서 피해 구제가 이뤄지고 있습니다.

메모리 해킹의 특징은

■ **악성코드를 이용해서 정상적인 인터넷뱅킹 사이트에서 입력한 금융거래정보를 가로챕니다.**

악성코드를 이용한다는 점에서는 파밍과 유사합니다. 그러나 피싱사이트로 유도하여 평상시보다 과도한 양의 금융거래정보를 입력하도록 하는 파밍과 달리, 메모리 해킹은 보안카드번호 2개 등 정상적인 거래를 할 때와 같은 양의 정보만을 입력하도록 합니다.

■ **인터넷뱅킹 오류로 인해 중도에 거래가 종료되거나, 거래 완료 이후 추가로 보안카드번호를 입력하도록 유도합니다.**

금융회사의 정상 사이트에서 인터넷뱅킹 중 오류로 인해 갑자기 거래가 종료되거나, 거래 완료 후에 보안강화 등을 이유로 보안카드번호를 추가로 입력하라고 요구하는 경우에는 메모리 해킹을 의심해야 합니다. 이런 경우 거래하는 금융회사로 즉시 연락해서 상담받고 적절한 조치를 취해야 합니다.

피해 사례

사례 1 정상적인 인터넷뱅킹 중 거래 오류로 진행이 중단된 사례

C씨(30대, 여)는 은행 홈페이지에 접속하여 자금을 이체하고자 공인인증서로 로그인하였습니다. 정상적으로 인터넷뱅킹을 진행하는 과정에서 계좌 비밀번호와 보안카드번호 앞뒤 2자리를 입력하였으나, 오류가 발생하여 더 이상 진행되지 않자 거래를 중단하였습니다. 그리고 당일 밤, 본인도 모르게 자신의 계좌에서 900만 원이 대포통장으로 이체되는 피해를 보았습니다.

사례 2 정상적인 인터넷뱅킹 후 정보 입력을 다시 요구한 사례

K씨(남, 50대)는 평소와 다름없이 OO은행의 인터넷뱅킹 사이트에 접속하여 정상적으로 이체 거래를 마쳤습니다. 거래 과정에서 금융거래정보 입력은 보안카드번호 2개, 공인인증서 비밀번호 등 평소와 다르지 않았습니다. 그런데 인터넷뱅킹을 마친 후 보안강화를 위한 인증 화면이 뜨면서 보안카드번호 2개를 추가로 입력하도록 유도하였습니다. K씨는 앞서 인터넷뱅킹 거래를 정상적으로 마쳤기 때문에 아무 의심없이 추가로 입력했습니다.

다음날 K씨가 또 다른 인터넷뱅킹을 하기 위해서 금융회사 사이트에 로그인하였으나 접속되지 않았습니다. 확인 결과 자신의 정보가 무단으로 변경되어 있었고, 최초의 이체 거래는 이뤄지지 않은 채 K씨의 예금계좌에서 엉뚱한 계좌(대포통장)로 700만 원이 이체되어 있었습니다. K씨는 메모리 해킹으로 인한 피해를 입었다는 사실을 알게 되었습니다.

알아두세요 메모리 해킹의 범죄 유형

▶ 수법1: 피해자 PC 악성코드 감염 → 정상적인 인터넷뱅킹 절차(보안카드번호 앞 · 뒤 2자리) 이행 후 이체 클릭 → 오류 발생 반복(이체정보 미전송) → 일정 시간 경과 후 범죄자가 동일한 보안카드번호 입력, 범행계좌로 이체

▶ 수법2: 피해자 PC 악성코드 감염 → 정상적인 계좌이체 종료 후, 보안강화 팝업창이 뜨면서 보안카드번호 앞 · 뒤 2자리 입력 요구 → 일정 시간 경과 후 범행계좌로 이체

※ 이럴 때 메모리 해킹을 의심하세요

- 인터넷뱅킹 이용 중 갑자기 컴퓨터가 꺼질 때
- 반복적으로 이체오류가 발생할 때
- 비밀번호 오류가 2회 연속 발생할 때
- 로그인이 안될 때

〈출처: 경찰청〉

메모리 해킹, 이렇게 하면 예방할 수 있습니다

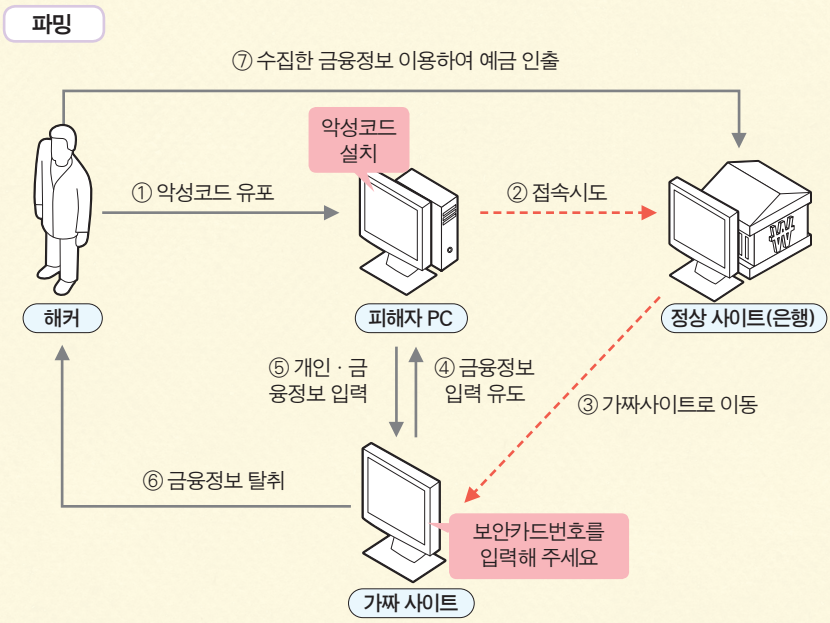
악성코드 탐지 및 제거 등 컴퓨터 보안 점검을 생활화하세요.

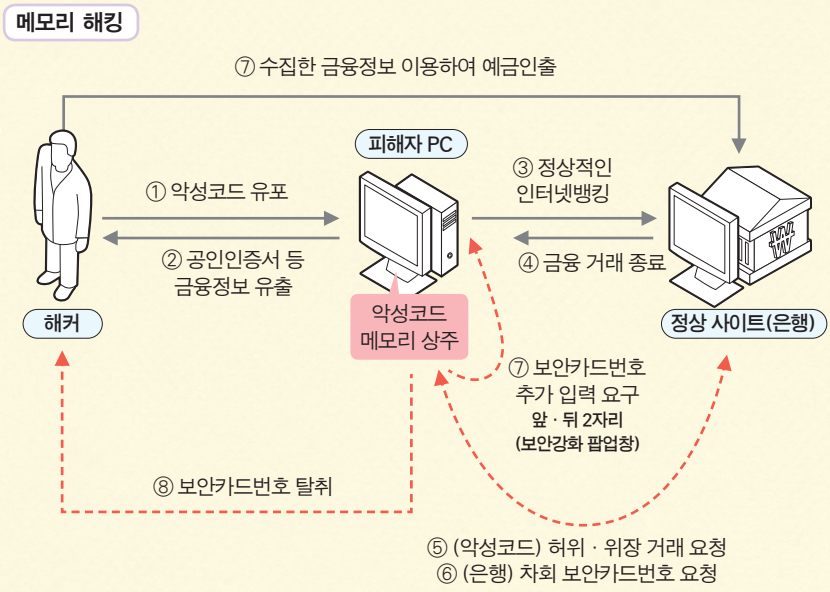
스마트폰, 컴퓨터 등의 보안 앱과 백신 프로그램을 항상 최신 상태로 업데이트하고, 악성코드 탐지 및 제거를 주기적으로 수행해야 합니다.

금융거래정보는 컴퓨터, 스마트폰에 사진이나 문서로 저장해 두지 마세요.

컴퓨터나 스마트폰에 통장이나 보안카드번호, 계좌 비밀번호, 공인인증서 비밀번호, 현금카드 등을 사진이나 문서로 저장해 두면 컴퓨터나 스마트폰이 악성코드에 감염되거나 해킹을 당하는 경우 금융범죄 피해로 이어질 수 있습니다.

파밍과 메모리 해킹의 비교





〈출처: 경찰청〉

Ⅱ 범죄의 온상인 대포통장, 위험합니다

1. 대포통장의 정의
2. 통장을 대여하거나 양도하는 행위의 위험성
3. 내 통장이 대포통장으로 범죄에 연루되는 것을 예방할 수 있는 방법

대포통장의 정의

보이스피싱, 대출빙자사기 등 모든 금융사기의 공통점이 무엇인지 아시나요? 바로 사기범들이 신분을 감추고, 피해금을 인출하기 위한 핵심 수단으로 '대포통장'을 이용한다는 점입니다. 여러분이 갖고 계신 평범한 통장도 다른 사람에게 대여되거나 양도되어 사용된다면 대포통장이 될 수 있습니다. 이 경우 통장 명의인인 여러분에게도 다양한 금융 거래 불이익이 따르게 되며 형사처벌까지 받을 수 있습니다.

대포통장이란

대포통장[1]이란 통장을 개설한 사람과 실제로 사용하는 사람이 다른 비정상적인 통장을 뜻합니다. 통장 명의자와 실사용자가 다르기 때문에 금융경로의 추적을 피할 수 있어 각종 범죄에서 사기 피해자금을 가로채는 수단으로 사용되고 있습니다. 특히 보이스피싱, 대출빙자사기 등 전기통신금융사기 범죄의 핵심적인 수단으로 이용됩니다. 따라서 각종 금융범죄의 예방을 위해서 대포통장은 반드시 근절되어야 합니다.

- 통장을 개설한 사람과 실제로 사용하는 사람이 다른 비정상적인 통장
- 금융경로의 추적을 피할 수 있어 보이스피싱 등 각종 범죄의 사기자금 수취 수단으로 사용

1) 대포통장에서 '통장'의 의미는 사전적 의미를 넘어 현금카드 등의 접근매체를 포함하는 넓은 의미로 사용되고 있습니다.

알아두세요 사기범이 대포통장을 획득하는 방법

▸ **통장 매입**

인터넷 게시판, 가출 카페 등에 '개인 · 법인통장 매매합니다.', '통장 사드립니다. 남녀노소 불문. 당일 입금'이라는 대포통장 매입 문구 등을 게시하여 각종 통장 및 체크(현금)카드 등을 매입

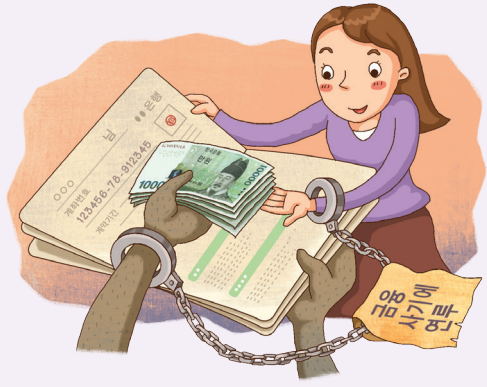
* 일부 인터넷 가출 카페의 경우 중개수수료를 받고 대포통장 매도자를 피싱사기 조직에 알선하는 경우도 있음.

▸ **통장 가로채기**

저리대출이나 취업 등을 빙자하여 '통장 및 체크(현금)카드를 보내면 당장 대출해 주겠다.', '우리회사에 취업을 하려면 본인의 금융 거래 확인이 필요하다.' 등의 이유를 내세우며 통장 및 체크(현금)카드를 가로챔.

▸ **개인정보 매매**

인터넷 카페, 블로그 게시판, 문자 메시지 등에 '각종 DB를 판매합니다.'라고 광고(개인신용정보 불법 판매)하는 곳에서 개인신용정보를 매입하고, 매입한 정보로 대포통장을 개설하거나 대출빙자사기 및 피싱사기 등 각종 범죄에 악용함.



2 통장을 대여하거나 양도하는 행위의 위험성

다른 사람에게 자신의 통장을 대여해 주거나 사고파는 행위는 명백한 불법행위입니다. 다른 사람의 통장을 필요로 하는 사람들은 사기범일 가능성이 높으며, 타인에게 넘겨진 대부분의 통장들은 대포통장으로 범죄에 이용됩니다. 이 경우 사기범에 대한 처벌과는 별도로 대포통장 명의인에게도 민 · 형사상 책임과 처벌, 다양한 금융 거래의 불이익이 따릅니다. 따라서 서랍 속의 평범한 내 통장을 다른 사람에게 건네는 순간, 나에게 범죄자 기록까지 남을 수 있음을 명심하고 통장 관리에 각별히 신경 써야 합니다.

대포통장 명의인의 민사책임

대포통장 거래 시 법원은 보이스피싱에 사용된 대포통장 명의인에 대하여 공동불법행위자로서 손해배상책임이 있다고 인정하고 있습니다. 따라서 대포통장 명의인은 피해자들에 대해 민사책임을 질 수 있습니다.

⊙ **판례** : 서울동부지법 2011.3.28. 선고, 사건 2010가단50237[부당 이득금]

⊙ **판결 요지** : 대포통장 명의인이 "보이스피싱"의 범죄 행위에 적극적으로 가담하지 않았다고 하더라도 적어도 해당 통장을 양도함으로써 그와 같은 범죄행위를 용이하게 한 것이므로, 대포통장 명의인은 민법 제760조에 따라 공동불법행위자로서 손해배상책임(70%)이 있다고 인정한 사례

대포통장 거래에 대한 형사처벌

대포통장 거래 시 전자금융거래법 제6조(접근매체의 선정과 사용 및 관리) 제3항 및 제49조(벌칙) 제4항에 근거하여 형사처벌을 합니다. 또한, 2015년 1월 20일에 전자금융거래법이 개정되면서 대가의 수수가 없더라도 대포통장 명의인에 대한 처벌이 가능해졌고, 대포통장을 보관 · 전달 · 유통하는 행위까지도 금지되었습니다.

⊙ **불법 행위** : 1. 통장을 양도하거나 양수하는 행위
2. 대가를 수수 · 요구 또는 약속하면서 통장을 대여받거나 대여하는 행위 또는 보관 · 전달 · 유통하는 행위
3. 범죄에 이용할 목적으로 또는 범죄에 이용될 것을 알면서 통장을 대여받거나 대여하는 행위 또는 보관 · 전달 · 유통하는 행위
4. 통장을 질권의 목적으로 하는 행위
5. 위 1~4번 행위를 알선하는 행위

⊙ **벌칙** : 3년 이하의 징역 또는 2천만 원 이하의 벌금에 처함.

대포통장 명의인에 대한 다양한 금융 거래 불이익

새로운 계좌개설의 제한

- 대포통장의 명의인으로 은행 전산망에 등록되는 경우, 원칙적으로 향후 1년간 전 금융회사에서 입출금이 자유로운 예금계좌 개설이 불가능
- 계좌 개설이 가능하다고 하더라도 금융 거래 목적 확인을 위한 객관적인 증명서 제출 등 추가적인 확인 절차를 거쳐야만 함.

대포통장 명의인을 전자금융 거래 제한 대상자로 지정

- 범죄에 이용된 계좌를 지급정지
- 대포통장 명의인은 전자금융 거래 제한 대상자로 지정
- 동 명의인의 다른 금융회사 계좌: 창구거래만 가능, 현금카드 · 이체 및 송금 · CD/ATM기 거래 등의 전자금융 거래 불가능

금융 거래 시 과거 대포통장 명의인 이력 반영

- 과거 대포통장 명의인 이력이 있는 경우 동 정보가 신용카드 발급 및 대출취급 심사 등의 과정에서 금융회사의 참고자료로 활용
- 금융생활을 영위함에 있어서 다양한 직 · 간접적인 불이익이 따름.

피해 사례

사례 1 대출을 미끼로 통장과 체크(현금)카드를 가로챈 사례

H씨(30대, 남)는 '○○금융' 팀장을 사칭하는 자로부터 대출광고 문자메시지를 받고 대출가능 여부를 문의했습니다. 사기범은 피해자의 신용등급이 낮고 대출건수가 많아 대출이 곤란하다며 사용하지 않는 통장과 체크카드를 보내주면 금융 거래 실적을 쌓아 대출이 가능하도록 조치하겠다고 현혹했습니다. H씨는 통장과 체크카드를 사기범에게 보낸 뒤 연락을 기다렸으나 사기범들은 잠적하였고, 이틀 후 본인의 다른 체크카드를 사용하려던 중 자신이 양도한 통장이 대출빙자사기에 이용되어 거래가 정지된 사실을 알게 되었습니다. H씨는 이후 전자금융 거래 제한 조치로 인해 금융생활에 큰 불편을 겪었고, 피해자들이 자신에게 제기한 대포통장 관련 민사소송 문제로 힘든 시간을 보내야 했습니다.

사례 2 아르바이트를 미끼로 통장과 체크(현금)카드를 가로챈 사례

B씨(20대, 남)는 군대를 전역해 직장을 구하던 중 아르바이트 사이트에서 한 건설회사의 전기보조 일을 찾게 되었습니다. 건설회사 과장은 "중간부터 일을 해도 월급이 다 나가 회사가 손해를 볼 수 있으니 통장을 한 달만 관리하겠다."라고 제안했습니다. B씨는 일을 구했다는 기쁜 마음에 과장이 요구한 통장과 카드, 카드 비밀번호 등을 모두 넘겼습니다. 하지만 과장은 그 다음날부터 전화를 받지 않았고, 2주 뒤 경찰서에서 '통장 양도 행위'와 관련하여 조사를 받으라는 통보가 왔습니다.

전자금융거래법을 위반한 혐의자 신분으로 조사를 받은 B씨는 이후 신규 예금계좌 개설 제한, 전자금융 거래 제한 등으로 금융생활을 하는 데 아주 큰 불편을 겪어야만 했습니다.

3 내 통장이 대포통장으로 범죄에 연루되는 것을 예방할 수 있는 방법

■ 통장과 체크(현금)카드, 계좌 비밀번호를 절대 대여하거나 양도하면 안 됩니다.

통장과 체크(현금)카드, 계좌 비밀번호를 다른 사람에게 대여하거나 양도하는 행위는 스스로 본인을 범죄에 연루되도록 만드는 매우 위험한 행동으로 절대 해서는 안됩니다. 또한, 통장이나 체크(현금)카드 등 실물을 넘기지 않더라도 신분증이나 통장 사본, 계좌 비밀번호 등의 금융거래정보를 넘겨주는 것만으로도 대포통장 명의인이 될 수 있으니 주의해야 합니다. 만약, 통장 등을 다른 사람에게 건넨 경우 즉시 통장을 발급한 금융회사에 지급정지 또는 해지 신청을 하고, 경찰에 신고하시기 바랍니다.

■ 안 쓰는 통장은 정리하고 평소에 안전하게 보관합니다.

사기범들은 '통장 양도 시 대가 지급', '집에서 안 쓰는 통장을 빌려주면 거래기록을 만들어 신용등급을 올려주거나 대출 한도를 늘려준다.'는 식으로 유혹하여 사용하지 않는 오래된 통장을 대여·양도하도록 유도합

니다. 따라서 불필요한 통장(계좌)을 정리하여 분실 및 범죄에 노출될 가능성을 줄이고, 사용하는 통장은 다른 사람이 접근할 수 없는 안전한 장소에 잘 보관해 두어야 합니다.

■ **다른 사람에게 통장을 양도하거나 금융거래정보를 알려준 경우에는 즉시 지급정지나 계좌 해지를 요청합니다.**

통장이나 체크(현금)카드를 분실하거나 다른 사람에게 대여 또는 양도한 경우, 금융거래정보(계좌번호, 계좌 비밀번호, 보안카드번호 등)를 알려준 경우에는 즉시 발급 금융회사에 지급정지나 계좌 해지를 요청하고, 경찰에 신고해야 합니다. 신분증, 인감증명서 등의 전달로 추가피해가 우려되는 경우에는 신분증 등을 재발급 받고 '개인정보 노출자 사고예방 시스템'에 등록합니다.

■ **불법행위를 발견했을 때에는 반드시 신고합니다.**

인터넷 등에서 통장 매매 광고나 모집책을 발견하는 경우에 경찰청(☎ 112)이나 금융감독원(☎ 1332)으로 신고하여 금융범죄를 예방하도록 합니다.

궁금해요

낯선 사람에게 내 통장과 체크(현금)카드, 계좌 비밀번호를 건넨 경우 어떻게 해야 하죠?

그런 경우, 즉시 해당 계좌의 금융회사 콜센터나 경찰청(☎ 112)으로 연락해서 계좌 지급정지를 신청하고, 경찰에 해당 사실을 신고를 합니다. 사후적인 안전조치는 금융회사 직원에게 안내 받으세요.

내 통장이 금융사기에 이용되어서 전자금융 거래 제한 대상자로 지정되었습니다. 어떻게 하면 전자금융 거래 제한이 종료될 수 있나요?

피해자에 대한 금융감독원의 환급절차가 진행되는 경우에는 특별법*에서 정한 바에 따라 환급절차가 모두 종료되어야 합니다. 그러나 환급절차가 진행되지 않는 경우에는 경찰 · 검찰 · 법원에서 발급한 최종 처분결과에 관한 문서 등을 이용하여 금융회사의 확인 과정을 거쳐야 합니다.

* 전기통신금융사기 피해 방지 및 피해금 환급에 관한 특별법

Ⅲ 금융소비자, 이렇게 행동하세요.

1 금융사기 예방을 위한 금융생활 습관

2 금융사기 피해 시 대처 요령

금융사기 예방을 위한 금융생활 습관

공공기관 및 금융회사는 어떠한 경우에도 금전의 이체를 요구하거나, 금융거래정보를 수집하지 않음을 명심하세요.

사기범이 공공기관이나 금융회사 직원을 사칭하는 경우든, 또는 범죄 사건 연루, 개인정보 유출 등의 이유로 접근하는 경우든 결국에는 금전을 요구하거나 계좌 비밀번호, 보안카드번호 등 금융거래정보를 요구합니다. 따라서 낯선 사람으로부터 이러한 요구를 받을 경우 금융사기일 가능성이 매우 높습니다. 해당 기관의 공신력 있는 전화번호 등을 이용하여 반드시 사실 여부부터 확인하시기 바랍니다.

전화 또는 문자 메시지를 이용한 대출광고를 보고 절대 연락하지 마세요.

전화나 문자 메시지를 통한 대출 광고는 사기업체의 대출 광고일 확률이 높습니다. 대출 알선 문자나 전화, 광고물에 현혹되지 말고 대출이 필요하면 반드시 정식 금융회사를 통해 상담받아야 합니다. 정식 등록된 대출업체인지 여부는 금융감독원이나 한국대부금융협회를 통해서 확인할 수 있습니다.

신 입금계좌지정제를 이용하세요.

고객이 사전에 지정하지 않은 계좌에 대해서는 소액만 이체를 허용하는 서비스로서, 미지정계좌로 이체 시 최대 100만 원(1일 누적 기준) 한도 내에서만 송금이 가능합니다.

보안카드보다 안전성이 높은 보안매체(OTP)를 적극 이용하세요.

금융 거래 시 OTP[1] 사용을 권장합니다. 사기범에게 속아 보안카드번호 전부를 알려주는 경우 사기범이 무제한으로 동 정보를 이용해 피해를 입힐 수 있는 반면, OTP는 이러한 무제한적인 피해를 예방할 수 있습니다.

⊙ OTP의 종류

•토큰 1형

OTP 기기에 버튼이 없고, OTP값이 자동으로 출력되며, 1분에 한 번씩 자동으로 값이 변경됩니다.

•토큰 2형

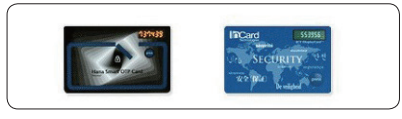
OTP 기기에 있는 키패드에 4자리의 PIN 번호를 입력하면 OTP값이 화면에 출력됩니다.

•토큰 3형

OTP 기기에 있는 전원 버튼을 누르면 OTP값이 화면에 출력됩니다.

•카드형

카드 형태로서 생성 버튼을 누르면 OTP값이 화면에 출력됩니다.



〈출처: 금융보안연구원〉

1) **일회용 비밀번호 생성기(OTP, One-Time Password)** 전자금융 거래 시마다 고정된 비밀번호 대신 새롭게 생성된 비밀번호로 인증하는 보다 안전한 전자금융 거래 방식

출처가 불분명한 파일이나 인터넷 주소가 포함된 이메일 · 문자 메시지는 절대 클릭하지 말고 바로 삭제하세요.

출처가 불분명한 파일이나 의심스러운 인터넷 주소가 포함된 이메일이나 문자 메시지를 받았을 때, 해당 파일이나 인터넷 주소를 클릭하면 악성코드나 악성 앱에 감염될 확률이 높습니다. 이들 악성코드(악성앱)는 금융 거래 시 파밍과 피싱사이트 피해, 메모리 해킹 등을 일으키는 주요 원인이 됩니다. 따라서 클릭하지 말고 바로 삭제해야 합니다. 만약 클릭한 경우 컴퓨터 및 휴대전화 A/S센터를 통해 반드시 치료하기 바랍니다.

타인에게 절대 개인정보와 금융거래정보를 알려 주지 마세요.

주민등록번호, 주소, 통장이나 신분증 사본, 계좌번호 및 보안카드번호, 문자 메시지 인증번호 등 개인정보 및 금융거래정보를 다른 사람에게 알려 주는 경우 전기통신금융사기 피해를 입을 확률이 높습니다. 또한, 통장 사본, 휴대전화 등을 대출권유업체에게 건네주는 경우 대포통장이나 대포폰으로 이용되어 본인도 모르게 범죄에 연루될 수 있으니 주의해야 합니다.

한국인터넷진흥원(KISA)의 '주민등록번호 클린센터'를 이용하면 인터넷상에서 자신의 주민등록번호가 이용된 내역을 간편하게 확인할 수 있습니다.

금융회사의 보안강화 서비스를 적극 활용하세요.

은행 등 금융회사에서는 전기통신금융사기로 인한 피해를 예방하기 위해 다양한 서비스를 제공하고 있습니다. 거래하는 금융회사 영업점이나 홈페이지를 방문하여 나에게 알맞은, 안전거래를 위한 서비스에 대해 알아보고 적극 이용하기 바랍니다.

「전자금융사기 예방 서비스」에 가입하세요.

공인인증서를 (재)발급받거나 인터넷뱅킹으로 300만 원 이상(1일 누적) 이체 시 ① 미리 지정된 단말기(컴퓨터, 스마트폰 등)를 이용하게 하거나, ② 추가 본인 확인(SMS인증, 전화확인 등)을 하여 본인인증을 강화하는 서비스로 거래은행 홈페이지에서 가입할 수 있습니다. 사기범이 타인 명의의 공인인증서를 (재)발급받거나 인터넷뱅킹을 통해서 부정이체하는 것을 예방할 수 있습니다.

평소 악성코드 탐지 및 제거를 생활화하세요.

본인의 컴퓨터나 스마트폰이 악성코드에 감염됐거나 의심되는 증상을 발견한 즉시 한국인터넷진흥원(☎ 118)에 문의하거나, 컴퓨터 백신 프로그램을 이용하여 악성코드를 제거해야 합니다. 특히 평소 인터넷뱅킹 등을 자주 이용하는 경우 악성코드 탐지 및 제거를 주기적으로 수행하여 보안 점검을 생활화해야 합니다.

컴퓨터나 스마트폰에 계좌 비밀번호나 보안카드 사진 등 금융거래정보를 저장해 두지 마세요.

전자기기의 분실이나 메모리 해킹 등이 발생했을 때 금융거래정보가 유출되어 큰 피해로 이어질 수 있습니다.

통장의 이체 및 인출 한도는 내게 필요한 만큼만 유지하세요.

나의 금융생활을 잘 고려해서 꼭 필요한 수준으로 이체 및 인출 한도를 설정해 놓으면, 금융사기 발생 시 사기범들이 자유롭게 피해금을 이체하거나 인출하는 것을 막아 피해를 최소화할 수 있습니다.

2 금융사기 피해 시 대처 요령

상황 1

***계좌와 공인인증서의 비밀번호, 보안카드번호 등 금융거래정보가 노출된 경우**

***사기범에게 속아서 돈을 송금·이체한 경우**

이렇게 대처하세요

"금융회사 콜센터 또는 경찰청(☎112)으로 즉시 전화하여 계좌의 지급정지를 요청하세요."

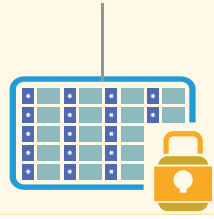
사기범이 내 예금을 인출해가지 못하도록 신속히 계좌의 지급정지 조치를 하는 것이 피해 예방을 위해 가장 중요합니다.

☞ 금융회사 콜센터 또는 경찰청(☎112)에서 요청

"경찰에 피해 신고를 한 후, 금융회사에서 피해금 환급제도를 신청하세요."

신속한 계좌 지급정지 조치를 함으로써 나의 피해금이 인출되지 않고 남아 있는 경우 소송절차 없이 되찾을 수 있습니다.

☞ 금융회사 영업점을 방문하여 신청



상황 2

* 통장과 체크(현금)카드, 계좌 비밀번호를 분실·대여·양도한 경우

이렇게 대처하세요

"금융회사 콜센터로 즉시 전화하여 통장과 카드의 이용정지를 요청하세요."

사기범이 내 통장과 체크(현금)카드를 범죄에 이용하지 못하도록 신속히 이용정지 조치를 해야 합니다. 이용정지 조치를 하지 않으면 대포통장의 명의인이 되어 민 · 형사 책임 및 다양한 금융 거래 불이익이 따를 수 있습니다.

☞ 금융회사 콜센터에서 신청

"통장의 거래를 유도하는 불법 광고나 모집책을 신고하세요."

통장거래를 유도하는 불법행위를 보았을 때는 즉시 경찰청(☎ 112)이나 금융감독원(☎ 1332)으로 신고해야 합니다. 적극적인 불법행위 신고를 통해서 금융범죄의 핵심 수단인 대포통장을 근절해 나갈 수 있습니다.

☞ 경찰청(☎112) 또는 금융감독원(☎1332)에 신고

상황 3

*주민등록번호, 각종 신분증의 분실 등 개인정보가 노출된 경우

이렇게 대처하세요

"명의도용방지서비스에 가입하세요."

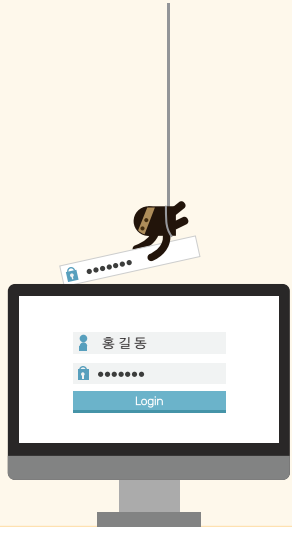
내 명의가 도용되어 이동전화 등 통신서비스가 불법 개통되는 피해를 예방할 수 있습니다.

☞ 한국정보통신진흥협회(www.msafer.or.kr)에서 가입

"개인정보노출자 사고 예방시스템을 신청하세요."

개인정보 노출로 인해 금융사기 피해가 우려되는 경우 금융회사로부터 보호조치를 제공받을 수 있습니다.

☞ 금융회사 영업점 또는 금융감독원을 방문하여 신청



전기통신금융사기 사례로 배우는
안전한 금융생활 안내서

알아두면 든든한
금융사기 예방법

발 행 일 2014년 12월

저 작 권 자 금융감독원

발 행 인 진웅섭

발 행 처 **금융감독원** www.fss.or.kr
서울특별시 영등포구 여의대로 38

편집 · 디자인 **(주)씨마스커뮤니케이션** www.cmass21.com