

(금융꿀팁) 보이스피싱 사기예방 서비스 이용!

내 계좌는 물론 배우자, 부모님, 자녀의 계좌를 안전하게 지켜 주세요.

2018.8.2(목) 보도자료

□ 금융감독원은 국민들이 일상적인 금융거래과정에서 알아두면 유익한 실용금융정보(금융꿀팁) 200가지를 선정, 알기 쉽게 정리하여 보도참고자료를 통해 안내하고, 동시에 금융소비자정보 포털사이트 “파인”(fine.fss.or.kr)에도 게시하고 있으며, 이에 따라 93번째 금융꿀팁으로, ‘보이스피싱 사기예방 서비스’ 5개를 안내해 드립니다.

(사례1) 가정주부인 A씨(55세)는 검찰청 수사관이라는 사람이 전화해 “범죄에 연루되어 조사가 필요하며, 조사가 끝나면 바로 돌려주겠으니 계좌에 있는 돈을 송금하라”고 하자, 당황한 A씨는 정기에·적금을 해지하고 3천만원을 이체했음. 2시간이 지난 후 귀가한 대학생 딸에게 사정을 얘기했더니 보이스피싱이라고 하여 즉시 은행에 연락했지만 이체한 돈은 전액 인출되었음

(사례2) 직장인 B씨는 대학생 아들(21세)이 인터넷 사이트에 개인정보, 계좌번호 및 공인인증서 비밀번호 등을 입력하고 있는 것을 발견하고 깜짝 놀라 중단시켰음. 성인이지만 금융지식이 부족한 아들의 보이스피싱 피해가 걱정됨. 특히, 이미 일부 정보를 입력했고 이런 사이트는 해외에 서버를 두고 있다고 하여 해외에서 인터넷뱅킹으로 금전을 인출할 것이 우려됨

☞ 현명한 금융소비자의 선택!

나와 내 가족의 재산을 지키기 위해 ‘보이스피싱 사기예방서비스’를 적극 활용하세요!

① 지연이체서비스 (사례1 관련)

지연이체서비스는 이체시 수취인 계좌에 일정시간(최소 3시간) 경과 후 입금되도록 하는 서비스입니다.(창구거래 비적용)

이 서비스를 이용하면 이체신청 후 일정 시간내(최종 이체처리시간 30분 전까지)에는 취소가 가능합니다. 보이스피싱에 속아서 실행한 이체를 일정시간내 취소할 수 있는 장점이 있으며 보이스피싱뿐만 아니라 착오송금으로 인한 피해도 예방하실 수 있습니다.

- 이체 지연시간은 최소 3시간 이상 일정 시간 단위로 선택 가능
- 지연이체서비스를 이용하더라도 본인이 별도로 건별한도(최대 100만원)를 설정하여 즉시이체 서비스도 이용가능
- 해당 은행 본인계좌간 송금, 사전 등록된 계좌간 이체 등 일정한 경우 즉시이체 가능

[예시] 지연이체서비스를 이용하는 경우

- 모르는 사람에게 고액 송금 : 지연이체 적용
- 사전등록한 부모님이나 자녀 용돈 송금 : 즉시이체 가능
- 사전등록한 거래처에 자금 이체 : 즉시이체 가능
- 쇼핑 등 소액 결제자금 이체 : 즉시이체 가능

* 사전 등록 필요(소액·정기·반복적 이체계좌는 사전 등록시 자유롭게 이체 가능)

※ 동 서비스는 해당 금융회사 인터넷(스마트)뱅킹, 영업점 방문 등을 통해 신청할 수 있으며, 은행마다 서비스내용에 차이가 있을 수 있음

② 입금계좌 지정 서비스(일명 ‘안심통장’) (사례1·2 관련)

입금계좌 지정 서비스는 본인이 미리 지정한 계좌로는 자유롭게 송금이 가능하지만 지정하지 않은 계좌로는 소액 송금만 가능(1일 1백만원 이내 이체한도 설정)한 서비스입니다.(창구거래 비적용)

이 서비스를 이용할 경우 계좌 비밀번호, 보안카드 일련번호 등 정보유출로 피해가 발생하더라도 피해액을 줄일 수 있습니다.

※ 동 서비스는 해당 금융회사 인터넷(스마트)뱅킹, 영업점 방문 등을 통해 신청할 수 있으며, 은행마다 서비스내용에 차이가 있을 수 있음

③ 단말기지정서비스 (사례2 관련)

단말기지정서비스는 본인이 미리 지정한 PC, 스마트폰 등에서만 이체 등 주요 거래가 가능한 서비스로, 지정하지 않은 PC 등에서는 조회만 가능하며 이체 등 거래를 위해서는 추가 인증을 거쳐야 합니다. PC는 스마트기기를 포함하여 최대 5대까지 지정할 수 있습니다.

※ 동 서비스는 해당 금융회사 영업점 방문 또는 지정을 원하는 PC나 스마트 기기(스마트폰, 태블릿PC 등)에서 인터넷(스마트)뱅킹 로그인 후 가능하며, 은행마다 서비스내용에 차이가 있을 수 있음

④ 해외IP차단서비스 (사례2 관련)

해외IP차단서비스 국내 사용 IP대역이 아닌 경우 이체거래를 할 수 없도록 차단하는 서비스입니다. 이 서비스를 이용할 경우 정보유출 또는 해킹 등으로 취득한 정보를 이용하여 해외에서 시도하는 금전인출을 방지할 수 있습니다.

※ 동 서비스는 해당 금융회사 인터넷(스마트)뱅킹, 영업점 방문을 통해 신청할 수 있으며, 은행에 따라 이용되지 않는 은행이 있거나 서비스 내용에 차이가 있을 수 있음

⑤ 개인정보노출자 사고예방시스템 (사례2 관련)

개인정보노출자 사고예방시스템은 개인정보가 노출된 금융소비자가 은행 영업점을 방문하거나 PC 또는 스마트폰을 이용하여 금감원 금융소비자정보 포털 「파인」(<http://fine.fss.or.kr>)에 개인정보 노출사실을 등록할 경우 신규계좌 개설, 신용카드 발급 등 노출자 명의의 거래시 본인확인절차를 강화하고 명의도용이 의심될 경우 거래를 제한함으로써 금융사고를 예방할 수 있는 시스템입니다.

※ 단, ‘개인정보노출자 사고예방시스템’에 등록되면 인터넷뱅킹을 통한 거래가 일부 제한될 수 있으며, 개인정보유출에 따른 위험 해소 등의 경우 즉시 PC 또는 스마트폰을 이용해 해제할 수 있습니다.

< 추가 Tip1. 보이스피싱 전화 차단 >

◆ 스마트폰에 ‘T전화’, ‘후후’, ‘후스쿨’ 등과 같은 스팸 차단 어플리케이션(이하 ‘앱’)을 설치하면 사전에 발신 번호에 대한 정보를 확인할 수 있어 보이스피싱 여부를 판단하는데 도움이 될 수 있습니다.

(이용방법) 플레이스토어, 앱스토어 등의 앱마켓에서 ‘T전화’, ‘후후’, ‘후스쿨’ 등을 검색하여 앱을 다운받아 설치하시면 됩니다.

< 추가 Tip2. 주민등록번호 변경 >

◆ 주민등록번호 유출로 인해 추가적인 피해가 걱정되는 보이스피싱 피해자는 누구나 주민등록번호를 바꿀 수 있습니다.

(변경방법) 주민등록번호 변경 신청서와 입증자료*를 가지고 주민등록지 읍·면·동 주민센터를 방문하여 신청하시면 됩니다.

* 입증자료 예시 : 금융거래내역서(송금전표 등), 사건사고사실확인원,법원 판결문 등

※ 주민등록변경제도에 대한 자세한 사항은 주민등록지 읍·면·동 주민센터로 문의하시기 바랍니다. (<http://www.rrncc.go.kr>)

끝.