금융사기 관련 소비자 유의사항

+ 금융회사, 공공기관을 가장하여 대출을 권유하거나 보안강화조치를 요구하는 경우에는 우선 금융사기로 의심합니다.

+ 어떠한 명목이든 전화로 금융거래정보를 묻거나 인터넷으로 비밀번호 등의 입력을 요구하는 경우 100% **금융사기**입니다.

+ 이유를 불문하고 대출실행 전에 고객에게 먼저 수수료 등의 명목으로 입금을 요구하는 경우 100% **대출빙자사기**입니다.

+ 개인정보 불법유통 및 금융사기 피해 관련 사항은 경찰청(112) 또는 금감원(1332)으로 신고하시기 바랍니다.

---

1. **보이스피싱:** 전화로 공공기관이나 금융회사 직원을 사칭하며 피해자를 속여 자금이체 등을 유도하는 수법

   - 공공기관과 금융회사는 결코 정보유출. 보안강화절차 등을 이유로 창구. ATM 기기나 텔레뱅킹 사용을 유도하지 않습니다

2. **파밍:** PC 를 악성코드로 감염시켜 네이버 검색 등을 이용시 피싱사이트로 유도, 금융거래정보를 입력토록 하여 자금을 가로챔

   - 경찰청에서 개발하여 무료 배포하고 있는 파밍방지 프로그램(“Pharming cop”)을 설치. 활용하시기 바랍니다.

3. **메신저 피싱:** 카카오톡, 네이트온 등의 ID 도용·무작위 접속 등의 방법을 통해 피해자의 지인인 것처럼 행동하면서 ‘급전을 요구’하여 금전을 가로채는 수법

   - 메신저 등을 통해 지인으로부터 ‘급전을 요청’하는 메시지를 받았다면 반드시 유선상으로 지인의 진위 여부를 확인하셔야 합니다.

4. **스미싱:** 무료쿠폰 등의 문자메시지를 누르면 악성 앱을 설치, 소액결제용 SMS 인증번호를 탈취하여 휴대전화 소액결제 피해

   - 출처가 불명확한 문자메세지는 삭제하시고, 한국인터넷진흥원(KISA)에서 배포하는 스미싱 방지용 앱 폰키퍼(phone keeper)를 설치해서 활용하시기 바랍니다.

5. **대출사기:** 금융회사 직원을 사칭하여 대출을 주선하면서 보증보험료, 전산비용 등 명목으로 수수료 송금을 요구하고, 인출 후 잠적

   - 전화, 문자메시지 등을 통한 대출모집인의 저금리 전환 대출 약속은 거짓일 가능성이 높으므로 이 경우 대출 권유 모집인의 정식 등록여부를 확인*하셔야 합니다

   * 대출모집인 통합조회시스템(www.loanconsultant.or.kr)에서 확인