

지역사랑상품권 담당공무원을 가장한 피싱 조치 방법 안내

□ 비피해 사건

- (상담·안내) 유출된 정보 등 상황에 따른 조치 방법(붙임 1 참조)을 안내하거나 전기통신금융사기 통합대응단 신고대응센터(1566-1188)로 연락
※ 센터에서는 계좌 지급정지 요청, 휴대폰 소액결제 차단 요청 등도 가능
- (전화번호 제보) 전기통신금융사기로 의심할 만한 사유가 있는 경우 통합대응단 홈페이지(www.counterscam112.go.kr)에서 번호 제보* 가능
* 대응단에서는 제보 내용 분석 후 통신사에 번호 긴급차단·이용중지 요청 중
- (계좌번호 신고) 전기통신금융사기 의심 계좌가 확인된 경우 금감원 사이트(www.fss.or.kr)에서 사기 이용 계좌로 신고 가능
- 신고 방법: ① 금감원 사이트 접속 > ② 민원·신고 > ③ 불법금융 신고센터 > ④ 전기통신금융사기 이용계좌 신고 > ⑤ 신고하기 메뉴

□ 금전 피해 사건

- (계좌 지급정지) △ 피해자금 송금 △ 금융정보 유출 △ 악성 파일 실행 시, 경찰청(☎112) 또는 금융감독원(☎1332)으로 전화하여 즉시 지급정지*
* 지급정지 요청 후 ① 피해사실확인서(사건사고사실확인원) ② 신분증 사본 ③ 피해구제신청서를 은행에 제출(3영업일 이내)해야 지급정지 효력 유지
- 휴대폰 원격제어, 악성 파일 실행 시, 악성앱·파일 점검 조치까지 필요
- (경찰관 출동) 현장성이 있는 대면편취형 범죄가 발생한 경우, 즉시 112에 신고하여, 현장으로 경찰관이 출동할 수 있도록 조치
- (사건접수) 현장성이 없는 상황에서 민원인이 수사진행을 희망하는 경우 관할 경찰서에 방문하여 사건 접수(신분증, 증거자료 지참) 필요

붙임 1**상황별 조치 방법 상세 내용****▶ 악성 파일을 설치하거나 원격제어앱을 실행한 경우**

- ① 악성 파일(apk.) 삭제
 - 안드로이드(갤럭시): 설정 > 내 파일 > APK 설치파일 카테고리 확인
 - iOS(아이폰): 파일앱 > 다운로드 폴더 확인
- ② 모바일백신(알약, V3 등) 악성코드 치료

▶ 명의도용 유무 확인이 필요한 경우

- ① 계좌/카드/대출 조회
 - 금융결제원 '어카운트인포' 앱 또는 계좌정보통합관리 사이트(www.payinfo.or.kr)에서 확인
- ② 본인확인 내역 및 가입 사이트 조회
 - 개인정보포털 사이트(www.privacy.go.kr)에서 확인

▶ 개인정보가 유출된 경우(아래 항목 중 필요한 조치 진행)

- ① 명의도용방지 서비스 조회 및 신청
 - 엠세이퍼(www.msafes.or.kr, PC/모바일 가능, 인증서 필요), 모바일(PASS, 카카오뱅크) 앱 또는 통신사 직영점 방문하여 신청 가능
- ② 개인정보 노출자 사고예방 시스템 등록
 - 명의도용 금융거래 사고 예방
 - 은행 방문 또는 금감원(<http://pd.fss.or.kr>)에서 신청
- ③ 여신거래 안심차단 서비스 신청(신용대출, 카드론, 신용카드발급 등 제한)
 - 은행방문 / 모바일 / 인터넷뱅킹 가능(단, 해제는 은행 방문 필요)
 - 인터넷전문은행(카카오뱅크, 케이뱅크, 토스뱅크 등)은 은행 앱 통해 신청(단, 해제는 타은행 영업점 방문 통해 가능, 거래 유무 무관)
- ④ 소액결제/콘텐츠 이용료 내역 확인 및 차단, 번호도용차단서비스 신청
 - 고객센터 전화 또는 통신사 앱 통해 신청(원천차단 신청은 각 통신사별로 상이하므로 고객센터로 문의)
- ⑤ 주민등록증 재발급 신청(발급일자 포함 노출된 경우)
 - 주민센터 방문 또는 정부24(www.gov.kr)에서 신청
- ⑥ 운전면허증 재발급 신청(노출된 경우)
 - 경찰서 민원실, 운전면허시험장 방문 또는 안전운전통합민원(www.safedriving.or.kr)에서 신청
- ⑦ 여권재발급 신청(노출된 경우)
 - 영사콜센터(☎02-3210-0404) 또는 각 구청 민원여권과
- ⑧ 공동(금융)인증서(노출된 경우)
 - 발급받은 기관(은행)을 통해 폐기 후 재발급