보 도 참 고 자 료

보도	배포 후 즉시	배포	2020. 3. 11.(수)

담당부서	불법금융대응단	이선진 팀장(3145-8521), 신상주 선임조사역(3145-8125)

제 목 : 코로나19관련 마스크·손 소독제 물품구매를 사칭한 보이스피싱 피해사례 발생!, 소비자경보 "주의" 발령!

▣ 소비자경보 2020-2호			
등급	주의	경고	위험
대상	금융소비자 일반		

소비자 경보 내용

◈ 코로나19 확산에 따른 국민들의 불안감을 악용하여 마스크·손소독제 긴급구매 등을 사유로 한 보이스피싱 피해사례 발생

1 출처가 불분명한 문자메시지 수령시

⇒ 바로 삭제!(앱 설치 요구시 바로 전화 끊기)

2 가족 및 지인을 사칭하여 메신저로 금전 요구시

⇒ 전화로 본인 여부를 반드시 확인!

1 소비자경보 발령 배경

□ 최근 코로나19가 확산됨에 따라 마스크, 소독제를 필요로 하는 국민들의 심리를 이용한 보이스피싱 피해사례가 발생하였으므로 이에 대한 각별한 주의가 요망

2 보이스피싱 실제 피해사례

1 결제 문자메시지로 보이스피싱 유도

○ 사기범은 **결제가 승인**되었다는 **가짜 문자메시지**를 발송한 후 피해자가 문의 전화를 하면 **명의가 도용** 또는 **범죄**에 **연루**되었다고 속이고,

- 다른 사기범이 **경찰 등을 가장**하여 피해자에게 전화한 후 **안전계좌**로 자금을 이체해야 한다는 명목으로 **송금을 요구**하거나, **악성앱** 등을 설치한 후 **개인정보를 알아내는 방법** 등으로 **자금 편취**

(1) 마스크 결제 문자를 이용하여 개인정보를 알아낸 후 자금을 편취

◆ 보이스피싱 사기범은 "OOO님, 00만원 승인되었습니다. △△KF94마스크 출고예정"이라는 문자메시지를 피해자에게 발송

◆ 이를 본 피해자는 사기범에게 전화를 걸어 문의하니 '▽▽mall' 이라고 하면서 결제를 하지 않았으면 서울지방경찰청 직원을 소개해주겠다라고 설명

◆ 이후 서울지방경찰청 경위 ▲▲▲을 사칭한 자가 전화하여 귀하 명의계좌가 대포통장으로 보여 자산보유검사보호신청을 해야하니 스마트폰에 TeamViewer QuickSupport(원격조정 앱) 어플을 설치하고, 계좌번호, 주민번호, 주소, 핸드폰 번호, OTP번호 등 금융정보를 입력하도록 요구

◆ 이러한 과정을 통해 피해자는 보이스피싱 사기범에게 개인정보를 제공하고, 이를 사기범이 활용하여 피해자 명의의 예금 OO만원을 편취

2 가족, 친구 등 지인을 사칭한 메신저피싱

○ 사기범은 메신저 ID를 도용하여 **지인을 사칭**하며 **카카오톡, 네이트온** 등 대화창을 통해 **돈을 요구**하여 편취

(2) 마스크 구매자금 부족을 사유로 지인에게 자금 이체를 요구

◆ 보이스피싱 사기범은 카카오톡을 통해 피해자에게 친언니를 사칭하여 접근, "동생, 마스크하고 손소독제를 싸게 대량으로 살 수 있는데, 내가 지금 돈이 없어서... 지금 알려주는 계좌로 90만원 정도 보내줄 수 있니?" 라고 피해자를 기망하여 90만원을 편취

※ 이체 요청금액을 100만원 이하 금액을 요청하여 피해자의 자금부담을 줄이고, 실제 물품구매 목적인 것으로 오인시키고자 개인명의가 아닌 법인계좌로 이체토록 유도

3 소비자 행동 요령

□ **(대금결제 등 출처 불분명 문자메시지 수신시)** 출처가 불분명한 문자메시지는 보는 즉시 바로 삭제할 것

☞ **추가 행동 요령**

① (부득이 유선통화 연결이 된 경우) 악성앱 설치 요구시 **통화중단**

② 결제된 업체명은 인터넷 포털사이트에를 통해 검색하여 정식업체 인지 확인하고, **대표번호로 전화**하여 **사실여부를 확인**

□ **(메신저를 통한 금전요구시)** 가족, 친구 등을 사칭하여 **메신저**로 **금전**을 **요구**하는 경우 반드시 **전화로 본인 및 사실여부를 확인**할 것

☞ **추가 행동 요령**

① (핸드폰을 분실하여 잠시 빌린 폰이라는 이유 등으로) **통화를 거절**하는 경우 **대화중단**

② 주기적으로 메신저나 SNS 비밀번호를 변경하고 바이러스 검사 실시

□ 아울러, 다양한 유형의 보이스피싱 위험으로부터 스스로를 보호하기 위해 **보이스피싱 단계별 예방 원칙**(첨부1)을 **숙지하시길 당부드리며,**

○ **금융회사의 '사기 예방 서비스'**(첨부 2)도 적극 활용하시기 바랍니다.

☞ 본 자료를 인용하여 보도할 경우에는 출처를 표기하여 주시기 바랍니다.(http://www.fss.or.kr)

첨부 1 보이스피싱 단계별 예방 원칙

1 보이스피싱 예방을 위한 서비스에 사전에 적극 가입하세요!

➡ 지연이체서비스, 입금계좌지정서비스 등에 가입시 보이스피싱 피해를 예방할 수 있습니다. [첨부 2]

2 질병관리본부(☎1339), 건강보험심사평가원(☎1644-2000), 기타 보건의료기관에서 전화나 문자가 왔다면?

➡ 정부부처, 공공기관, 보건의료기관 등은 어떤 일이 있어도 금전을 요구하거나, 금융정보를 요구하거나, 앱 설치 등을 요구하지 않습니다!
해당 내용으로 전화가 온다면 즉시 끊어주세요!

3 신종 코로나 안내 의심 문자를 받았다면?

➡ 메시지에 있는 의심스러운 전화번호, 인터넷 주소(URL)등은 클릭하시면 안 돼요!

4 휴대폰에 앱(App)을 설치하거나, 인터넷 주소로 들어가라고 한다면?

➡ 악성 앱을 설치하거나 불법 사이트로 접속하는 경우 계좌번호, 개인정보가 유출될 수 있으므로 의심되는 앱 설치 또는 사이트 접속은 절대 안 돼요!

5 만약 실수로 이미 앱을 설치했다면?

➡ 즉시 앱을 삭제하고, 비밀번호 등 금융관련 개인정보 입력은 절대 안 돼요!

6 이미 송금 · 이체까지 해 버렸다면?

➡ 즉시 전화로 은행(고객센터) 또는 경찰(☎112, 182), 금융감독원(☎1332)에 송금·이체한 계좌에 대해 지급정지를 요청하세요!

첨부 2 보이스피싱 피해예방 주요 서비스

1 지연인출 제도

□ **(개요) 1회에 100만원 이상 금액**이 **송금·이체**되어 **입금**된 경우 입금된 때로부터 해당금액 상당액 범위 내에서 **30분간 자동화기기**(CD/ATM기 등)를 통한 **인출·이체가 지연**

* 다만, 금융회사 창구에서는 즉시 인출·이체가 가능

2 지연이체 서비스

□ **(개요) 이체시** 수취인 계좌에 **일정시간**(최소 3시간) **경과 후 입금되도록 하는 서비스**

* 다만, 금융회사 창구 거래는 적용되지 않음

○ 이체신청 후 **일정 시간내**(최종 이체처리시간 30분 전까지)에는 **취소가 가능**하며, **이체 지연시간**은 **일정 시간 단위**(최소 3시간 이상)로 **선택 가능**

○ 별도로 **건별한도**(최대100만원)를 **설정**하거나 해당은행 **본인계좌간 송금, 사전 등록된 계좌간 이체** 등 일정한 경우 **즉시 이체 가능**

※ 동 서비스는 해당 금융회사 인터넷(스마트) 뱅킹, 영업점 방문을 통해 신청할 수 있으며, 은행마다 서비스 내용에 차이가 있을 수 있음

〈 지연이체 서비스 구조 〉

3 입금계좌 지정서비스

□ **(개요)** 본인이 미리 지정한 계좌로는 본인의 전자금융 이체 한도 내에서 자유롭게 송금이 가능하지만, **지정하지 않은 계좌**로는 **소액 송금만 가능**(1일 1백만원 이내 이체한도 설정)한 서비스

* 다만, 금융회사 창구 거래는 적용되지 않음

※ 동 서비스는 해당 금융회사 인터넷(스마트) 뱅킹, 영업점 방문을 통해 신청할 수 있으며, 은행마다 서비스 내용에 차이가 있을 수 있음

〈 입금계좌 지정서비스 구조 〉

4 해외IP 차단 서비스

□ **(개요) 국내 사용 IP대역이 아닌 경우** 이체거래를 할 수 없도록 **차단하는 서비스**로 정보유출 또는 해킹 등으로 취득한 정보를 이용하여 해외에서 시도하는 금전 인출을 방지

※ 동 서비스는 해당 금융회사 인터넷(스마트) 뱅킹, 영업점 방문을 통해 신청할 수 있으며, 은행마다 서비스 내용에 차이가 있을 수 있음

〈 해외IP 차단 서비스 구조 〉