

‘메신저∙문자 속 확실하지 않은 URL은 클릭하지 마세요’

SKT, 추석 앞두고 스팸/스미싱 주의 당부

**- 지인사칭 ∙ 허위결제 등 메신저피싱 증가 추세… 정보 등 제공 전 꼭 확인해야**

**- 기관 사칭 전화금융사기 급증… ‘수사기관, 문자나 메신저로 공문서 보내지 않아’**

**- T전화 이용, 백신 앱 설치 등 스팸/스미싱 방지 위한 선제적 조치 필요**

|  |
| --- |
| **엠바고 : 배포 즉시 보도 가능합니다.** |

**[2022. 9. 4] -보도참고자료-**

SK텔레콤(대표이사 사장 유영상, [www.sktelecom.com)](http://www.sktelecom.com))은 추석 연휴기간 수사기관, 금융사, 택배회사 등을 사칭한 스팸 ∙ 스미싱 문자가 크게 늘어날 것으로 우려된다며 이동통신 이용자들의 각별한 주의를 당부했다.

SKT는 보이스피싱의 경우 지난해 피해액이 2020년 대비 28.5%가 줄어든 반면 메신저피싱 피해액은 165.7%가 증가\*하는 등 코로나19 이후 메신저를 활용한 사기가 크게 늘었다고 밝혔다. (※ 금융감독원 조사 결과)

특히, 이동과 선물 구매 등이 빈번해지는 추석 연휴를 맞아 가족을 사칭하거나, 허위 결제를 가장하거나, 한시적 특별대출 등 정책자금을 빙자하는 등의 경우가 늘어날 것으로 예상돼 이용자들의 각별한 주의가 필요하다고 설명했다.

또한, 최근 들어 검찰이나 경찰, 금융감독원 등을 사칭하는 기관사칭형 범죄가 예년보다 크게 늘고 있어\* 이들 기관 사칭 메시지에 포함된 악성앱을 잘못 설치하면 정보 탈취는 물론, 전화 가로채기 수법 등에 의해 피해가 발생할 수 있다고 덧붙였다. (※ ‘22년 1~7월 기관사칭형 범죄 발생 건수 예년 대비 16%P 증가 / 경찰청 국가수사본부 조사 결과)

SKT는 기관사칭형 범죄의 경우 일반인들이 수사기관의 조사 등을 거의 경험하지 못한다는 점을 악용하는 만큼 사회 경험이 풍부한 사람들도 피해를 겪는 경우가 적지 않아 주의해야 한다고 밝혔다.

**■ 주요 사례별 대응 방법**

SKT는 이 같은 피해를 사전에 차단하기 위해선 주요 사례별로 꼼꼼하게 문자나 메신저의 내용을 확인하는 노력이 중요하다고 강조했다.

1. **전화로 검찰 등 사법기관을 사칭해 범죄에 연루되었다고 접근**

검찰, 경찰, 금융감독원 등의 기관들은 어떠한 경우에도 문자나 메신저로 공문서를 보내지 않는다. 또한, 현금 이체를 요구하거나, 개인의 금융거래 정보를 수집하지 않는다고 공식적으로 밝히고 있다. 만약, 사법기관이라며 개인의 금전 이체나 금융거래 정보를 요구하는 문자나 전화 등을 받을 경우 보내는 URL을 클릭하거나, 출처를 알 수 없는 앱을 설치하기 전 해당 기관의 공신력 있는 전화번호 등을 이용해 사실 여부를 확인한 후 대응해야만 한다.

1. **문자메시지로 가족이나 지인을 사칭해 정보 또는 송금을 요구하는 경우**

가족이나 지인이 사고를 당하거나 휴대폰이 고장 나 친구나 주변 지인 휴대폰으로 긴급한 상황에 처했다는 문자를 받을 경우, 해당 가족이나 지인에게 직접 연락을 취해 메시지 내용이 맞는지 확인해야만 한다. 급한 마음에 상대방이 요구하는 신분증이나 은행 계좌정보, 송금 요청 등에 응할 경우, 피해를 당할 수 있다.

1. **금융회사를 사칭해 저리대출, 소상공인 특별대출 등을 안내하는 경우**

금융회사라며 문자나 메신저를 통해 대출 안내를 할 경우, 메시지에 포함된 전화번호로 연락하거나 URL을 클릭하지 않는 것이 바람직하다. 통화를 했을 경우 상대방이 메신저나 문자메시지로 보낸 인터넷주소(URL)의 클릭이나 앱(App.) 설치를 피해야 한다. 금융 전문가들은 은행과 카드사 등의 금융서비스가 필요할 경우, 본인이 직접 금융사를 찾아가는 것이 바람직하다고 권고한다.

**④ 범칙금, 택배 주소지 정정 등을 이유로 앱 설치 또는 URL 클릭을 유도할 경우**

어떤 경우라도 문자메시지를 통해 인터넷주소(URL)와 출처를 알 수 없는 앱(App.) 설치를 유도하는 문자메시지는 절대로 클릭하면 안되며, 앱(App.) 설치 시 모바일 백신을 활용해 즉시 삭제해야 한다.

1, 3, 4번 사례에서 상대방이 보내온 인터넷주소(URL)을 클릭하거나, 앱을 설치할 경우 스마트폰에 보이지 않는 악성 앱을 설치하여 피해자가 걸고 받는 모든 전화와 문자를 금융사기조직으로 연결하는 일명 ‘강수발신(강제수신∙발신)’ 상태가 되게 하거나, 스마트폰 내부의 모든 정보를 탈취하는 경우가 생길 수 있다.

**■ 피해 발생 시 대처 방법**

금융 피해 등이 의심되는 일이 발생하면 즉시 해당 금융사 고객센터, 경찰청(112), 금융감독원(1332)에 문의해 본인 계좌를 통한 지급 정지 등을 신청하는 것이 바람직하다.

한국인터넷진흥원(KISA)에도 스팸 등에 대해 신고할 수 있으며, SKT는 이와 별도로 고객의 스팸 등에 의한 사기 피해에 즉시 대응하기 위해 자체 신고 접수와 대응 채널도 운영하고 있다. 스팸 등 의심문자를 #8239로 전달하면, SKT에서 해당 문자를 분석해 시스템에서 차단하는 등의 조치를 취하게 된다.

또한, 직접적인 금융 피해가 발생하지 않았더라도 의심 문자나 전화를 받을 경우 경찰(112)에 신고하면 사기조직의 범죄 행위를 조기에 차단하는데 큰 도움이 될 수 있다.

**■ T전화 이용, 문자 스팸 필터링 서비스 가입, 백신 앱 등으로 사전 대응 나서야**

SKT의 통화어플 T전화를 이용하는 것은 피해를 사전에 예방하는데 도움이 된다. T전화는 전화 수발신 및 전화번호 검색 시 해당 번호의 스팸 유형을 이용자에게 보여주고, ‘OO은행 고객센터’ 정보도 표시해 준다.

T전화에서 상호 확인이 불가능하거나 정보가 없는 전화번호는 수발신에 주의하는 것이 좋다.

통신사, 금융사, 정부기관 등이 보내는 스팸 및 스미싱, 보이스피싱 등의 주의 당부 안내문자를 미리 읽어보고 숙지하는 습관도 중요하다. 아울러 스마트폰에 스미싱 문자 탐지 백신을 설치하는 것도 피해를 예방하는 방법이 될 수 있다.

SKT는 이 같은 개인 차원의 예방 노력에 더해 T전화를 통해 고위험 및 보이스피싱 피해 신고가 많은 번호로 걸려오는 전화를 자동으로 차단해주는 ‘안심차단’ 기능을 제공하는 동시에 안심벨소리 기능을 통해 스팸전화나 보이스피싱 전화를 고객에게 안내하고 있다.

이와 함께 확인된 스팸과 스미싱 번호 차단은 물론, 이용자 스스로 수발신을 원하지 않는 전화번호를 직접 차단할 수 있도록 가입자 대상 AI 기반의 문자 스팸 필터링 서비스를 무료로 제공 중이다.

또한, 서울경찰청과 함께 경찰에 피해신고 접수된 보이스피싱 번호로 SKT 고객에게 전화를 걸거나 받을 수 없도록 차단하는 ‘보이스피싱 번호차단 서비스’를 제공하고 있다.

이 밖에도, AI 기반의 차단시스템을 도입해 스팸 및 스미싱 문자에 대응하고 있으며, 다중 스팸필터링 시스템도 적용하고 있다.

손영규 SKT 정보보호담당은 “한층 교묘해진 스팸이나 스미싱, 보이스피싱 등이 이번 추석 연휴에 이동통신 이용자들의 피해를 나을 수 있는 만큼 사회적인 관심과 대응 노력에 힘을 모으길 바란다”고 밝혔다.

**▶ 관련문의 : SK텔레콤 PR담당 혁신PR팀 문진호 매니저 (02-6100-3837)**

