

[최근 발생 보이스피싱 유형 및 진화하는 피싱사기 피해 사례]

□ 보이스피싱 유형

- 문자를 이용하는 보이스피싱
 - > 금융감독원·검찰·경찰을 사칭하여 구속영장이 발부되었다고 문자 발송 후 통화 유도
- 핸드폰으로 직접 전화를 통한 보이스피싱
 - > 사법기관(검찰·경찰 등)을 사칭하여 사기 사건에 연루되었다며 도움을 주겠다는 핑계로 특정 앱 설치를 유도하여 출금
- 몸캠피싱
 - > 특정 번호의 여자가 직접 전화하거나 랜덤채팅 어플리케이션을 통해 서로 자위행위 동영상을 같이 촬영한 후, 이를 미끼로 금전 요구
- AI와 더불어 진화한 「영상 피싱」
 - > 이미 내 핸드폰을 해킹해서 나의 사진과 동영상 등을 합성하여 지인들에게 마치 내가 영상통화로 빌리는 것처럼 돈을 요구
- 그 외, 「부고 문자」, 「카드 발급」, 「해외에서 카드 결제」를 이용하는 전화금융사기 사례가 증가

□ 예방대책

- 사법기관(금융감독원, 검찰, 경찰 등)에서는 어떠한 경우에도 전화로 개인 정보나 금융정보를 묻지 않으며, 이를 미끼로 돈을 요구하지 않는다는 인식 필요
- 낯선 번호의 전화는 되도록 받지 않으며, 나와 상관이 없는 문자는 누르지 않는 것이 좋습니다.
- 만약, 보이스피싱범이 제시하는 기관과 전화번호로 연락을 할 경우는 지인이나 동료 또는 사무실 전화를 이용하여 확인하는 방법이 좋습니다. (이미 해킹당한 내 핸드폰으로 전화하면 통화 연결이 다른 보이스피싱범에게 연결됨에 주의)
- 몸캠피싱의 경우 성적 호기심이 많은 청소년(중·고등학생)인 경우 정신적 충격 및 장래에 생각지도 못할 피해가 우려되는바, 자녀들에게도 주의 홍보 필요
- 동영상 피싱의 경우 가까운 지인의 금전적 요구를 거절할 수 없는 경우도 있는바, 통화 종료 후 다른 전화기로 확인이 필요