텔레그램을 악용한 신종 사기수법 전파

□ 피해 사례

【 텔레그램 사칭 해킹 사례 】

※ "텔레그램 계정 재인증 필요...이 링크 클릭하면, 해킹당한다."(7. 18. 중앙일보)

▸ '23. 7. 17. 정부세종청사 공무원 A씨는 텔레그램에서 "계정 재인증이 필요하니 전화번호를 입력하라"는 메시지 수신

▸ 전화번호를 입력하고 몇 분 후, A씨의 휴대전화 주소록에 있는 지인들에게 A씨 명의로 "텔레그램 업데이트가 필요하니, 첨부한 링크로 접속하라"는 해킹 메시지 재전파

□ 수법 분석

문자·카톡과 달리 **피싱 탐지 앱**(피싱아이즈 등)에 **검출되지 않는 텔레그램**을 **활용**하여 **계정을 해킹**

○ **(1차-계정 사칭) 텔레그램(사)의 명의로 악성 앱이 포함된 메시지 전송**

○ **(2차-지인 사칭) 위의 해킹으로 수집된 개인정보를 이용, 피해자 명의**로 주소록 내 **지인들에게 악성앱이 포함된 메시지 추가 발송**

○ **(해킹 절차) 휴대전화 번호 입력 요청 → 전송받은 인증코드 입력 요청 → 텔레그램 계정 해킹 및 개인정보 탈취 → 피해자로부터 해킹한 지인 연락처에 악성앱 메시지 추가 발송 順**

⇨ 획득한 개인정보를 이용, 보이스피싱 범죄를 저지를 가능성이 높음

□ 예방 수칙

⚠ 텔레그램 계정 및 지인사칭 해킹 주의 안내

최근 텔레그램 정상 계정 및 지인을 사칭하여 '계정 재인증 및 업데이트'를 빙자, 피해자의 휴대전화 해킹을 통해 개인정보를 탈취하고, 악성 앱을 유포하는 수법이 확산되고 있어 다음과 같이 유의사항을 안내드립니다.

1. 출처 불명의 링크(URL) 클릭 절대 금지(지인 명의 메시지라도 전화 등을 통해 확인 후 접속)
2. 텔레그램 개인정보 및 보안인증 강화(비밀번호 입력 후 생체인증 등 추가)
3. 악성 앱 차단·삭제를 위해 V3·피싱아이즈·시티즌코난 등 보안 앱 설치