

계정 탈취 유형 스미싱·피싱 주의 권고

□ 개요

- 최근 ‘Telegram’, ‘Apple’, ‘WhatsApp’을 사칭하여 계정 정보 탈취를 시도하는 피싱 사례가 대량 탐지됨에 따라 해당 서비스 이용자 주의 필요

□ 주요내용

- “다른 곳에서 인증되었습니다.”, “새 기기 접속 시도”, “청구서 확인” 등의 키워드를 활용하여 본인 확인 인증을 유도하는 문자가 유포됨에 따라 사용자들의 각별한 주의 필요
 - (스미싱) ‘계정 비활성화’, ‘요금 차감’, ‘미인증 시 탈퇴’ 등 이용자의 비정상 행위가 감지되었다고 속인 뒤, 문제 해결 및 본인 인증을 핑계로 문자메시지 內 악성 URL 클릭 유도
 - (주요 행위) 피싱 사이트의 로그인 단계에서 계정, 이메일, 전화번호 등 개인 정보 탈취



□ 대응방안

- 스미싱·피싱사이트 신고 및 확인 방법
 - 보호나라(카카오톡 채널) 내 ‘스미싱·피싱 확인서비스’를 이용하여 신고 및 악성여부 판별



o 스미싱 문자 신고 및 확인 방법

- 스마트폰 내 문자 수신 화면에서 확인가능한 ‘스팸으로 신고’
- 전기통신금융사기 통합신고대응센터(<https://counterscam112.go.kr>) 내 ‘간편제보하기’
- 보호나라(카카오톡 채널) 내 ‘스미싱·피싱 확인서비스’를 이용하여 신고 및 악성여부 판별



o 스미싱 문자 예방 방법

- 문자 수신 시 출처가 불분명한 사이트 주소는 클릭을 자제하고 바로 삭제
- 의심되는 사이트 주소의 경우 정상 사이트와의 일치여부를 확인하여 피해 예방
- 휴대폰번호, 아이디, 비밀번호 등 개인정보는 신뢰된 사이트에만 입력하고 본인확인 인증번호는 타인에게 전달 금지
- 정부기관 및 금융회사인 경우, 전화나 문자 등을 통해 원격제어앱 설치를 요구하지 않음
* 정상스토어에 등록된 앱인 경우도 포함

o 번호 도용 문자 발송 차단

- 악성앱 감염 및 피싱 사이트를 통한 정보 유출이 의심되는 경우, 스미싱 문자 재발송에 피해자 번호가 도용될 수 있으므로 “번호도용문자차단서비스”를 신청하여 도용 차단
* 이동통신사별 부가서비스 항목에서 무료로 신청 가능

o 모바일 결제 확인 및 취소

- 스미싱 악성앱 감염 및 피싱사이트 개인 정보 입력 시 모바일 결제 피해가 발생할 수 있으므로 모바일 결제 내역 확인
 - ① 통신사 고객센터를 통하여 모바일 결제 내역 확인
 - ② 모바일 결제 피해가 확인되면 피해가 의심되는 스미싱 문자 캡처
 - ③ 통신사 고객센터를 통해 스미싱 피해 신고 및 소액결제확인서 발급
 - ④ 소액결제확인서를 지참하여 관할 경찰서 사이버수사대 또는 민원실을 방문하여 신고
 - ⑤ 사고 내역을 확인받고 사건사고 사실 확인서 발급
 - ⑥ 사건사고 사실 확인서 등 필요서류를 지참하여 통신사 고객센터 방문 또는 팩스나 전자우편 발송
 - ⑦ 통신사나 결제대행 업체에 사실 및 피해 내역 확인 후 피해보상 요구

○ 악성어플리케이션 삭제

- 문자메시지에 포함된 인터넷주소를 클릭한 것만으로는 악성 앱에 감염되지 않으나, 인터넷주소를 통해 어플리케이션을 설치했다면 아래와 같은 방법으로 스마트폰 점검
 - 모바일 백신으로 악성 앱 설치여부 검사 및 발견시 비행기모드 전환 후 112신고
 - ※ 악성 앱이 휴대폰을 원격제어할 수 있으므로 주변 사람의 전화기를 통해 신고
 - 악성 앱 수동 삭제하기
 - 가까운 휴대폰 서비스센터 방문

○ 공인인증서 폐기 및 재발급하기

- 악성 앱에 감염되었던 스마트폰으로 금융서비스를 이용했다면 공인인증서, 보안카드 등 금융거래에 필요한 정보가 유출될 가능성이 있으므로 해당 정보를 폐기하고 재발급

○ 2차 피해 예방하기

- 스마트폰에 설치된 악성앱이 주소록을 조회하여 다른 사람에게 유사한 내용의 스미싱을 발송하는 등 2차 피해가 발생할 수 있으므로 주변 지인에게 스미싱 피해 사실을 알려야 함

□ 스미싱 제보 및 상담 문의

- 전기통신금융사기 통합신고대응센터 : 국번 없이 1394
- 한국인터넷진흥원 인터넷침해대응센터 : 국번 없이 118

□ 작성 : 국민피해대응단 스미싱대응팀