
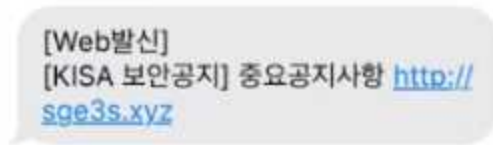
	<h1 style="text-align: center;">보도 자료</h1> <p style="text-align: center;">4차산업혁명의 큰 길로 대한민국이 달려갑니다.</p>	 <p style="text-align: center;">사람 중심의 4차산업혁명 실현</p>
<p style="text-align: center;">2020. 1. 31.(금) 배포시점부터 보도 가능합니다.</p>		
<p>담당부서</p>	<p>탐지팀 이재형 팀장(전화: 02-405-5421, 전자우편: jhlee@kisa.or.kr) 탐지팀 이동은 책임(전화: 02-405-6717, 전자우편: eastgrace@kisa.or.kr)</p>	
<p>참고자료</p>	<p>사진 있음 <input checked="" type="checkbox"/> 사진 없음 <input type="checkbox"/></p>	<p>총 3매</p>

KISA 보안공지를 사칭한 스미싱 문자 주의

- 출처가 불분명한 문자 내 인터넷주소(URL) 클릭 주의 -

한국인터넷진흥원(KISA, 원장 김석환)은 KISA를 사칭하여 스마트폰 악성앱을 유포하는 스미싱 문자에 대한 이용자의 주의를 당부했다.

해당 스미싱 문자는 「 [KISA 보안공지] 중요공지사항 URL」 형태로 유포되고 있으며, 스미싱 문자 내 인터넷 주소(URL)를 클릭하면 크롬 브라우저 업데이트를 권고하는 내용으로 악성앱 설치를 유도한다.

	
<p style="text-align: center;">< 스미싱 문자 ></p>	<p style="text-align: center;">< 크롬 브라우저 업데이트 권고 문구 ></p>

현재 KISA는 이용자 피해확산 방지를 위해 국외 소재의 악성앱 유포지 및 정보 유출지를 긴급 차단 조치 완료했다.

그러나 악성앱 유포지는 지속적으로 변경될 수 있고, 악성앱을 설치할 경우 공인인증서·수신문자 등 개인정보가 유출될 수 있으므로 출처가 불분명한 문자 및 앱에 대한 이용자의 주의가 계속해서 요구되는 상황이다.

이에 KISA는 이용자 주의사항으로 ▲앱 설치 전 기기 접근권한 요구 시 무심코 동의 버튼을 누르지 말 것, ▲악성앱을 이미 설치한 경우, KISA가

제시하는 대응 지침*에 따라 번호도용문자 차단 및 모바일 결제 내역 확인 등의 조치를 통해 2차 피해를 예방할 것을 당부했다.

* (불임) 스미싱 문자를 통해 악성앱을 설치한 경우 대응 지침

KISA 이상헌 침해대응단장은 “최근 보안공지를 사칭한 스미싱 문자가 지속적으로 유포되고 있으며, 향후 주요 공공기관을 사칭한 문자로 변형되어 유포될 수 있으므로 주의가 요구된다”며, “출처가 불분명한 문자 수신 시 발신자 번호를 확인하고 악성앱 설치를 유도하는지 반드시 확인해야 한다”고 말했다.

【붙임】 스미싱 문자를 통해 악성앱을 설치한 경우 대응 지침

○ 번호 도용 문자 발송 차단

- 악성앱 감염 및 피싱 사이트를 통한 정보 유출이 의심되는 경우, 스미싱 문자 재발송을 위해 피해자 번호가 도용될 수 있으므로 "번호도용문자차단 서비스*"를 신청하여 번호 도용 차단

* 이동통신사별 부가서비스 항목에서 무료로 신청 가능

○ 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 사고 내역 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
 - ① 모바일 백신으로 악성 앱 삭제하기
 - ② 악성앱 수동 삭제하기
 - ③ 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