과학기술정보통신부 보도자료 APEC 2025 KOREA

보도시점 배포시점 배포 2025.10.1.(수)

정부시스템 화재 이슈를 악용한 정부기관 사칭 스미싱·피싱 주의

- 보호나라(www.boho.or.kr) 알림마당에 스미싱·피싱 주의 보안공지 -

과학기술정보통신부(부총리 겸 과기정통부 장관 배경훈, 이하 '과기정통부')와 한국인터넷진흥원(원장 이상중, 이하 'KISA')은 최근 발생한 **정부시스템 화재로 인한 대민서비스 중단 이슈를 악용**하여 **정부·공공기관 사칭 및 민원서비스 안내를 미끼**로한 **스미싱*** 위협이 증가함에 따라 **개인정보 탈취 및 금전적 피해로 연계되지 않도록 특별한 사용자 주의를 당부했다.**

* 스미싱(smishing) : 문자메시지(SMS)와 피싱(Phishing)의 합성어로 악성 앱 주소가 포함된 휴대폰 문자(SMS)를 대량 전송 후 이용자가 악성 앱을 설치하거나 전화를 하도록 유도하여 금융정보·개인정보 등을 탈취하는 수법

정부시스템 장애 **관련 공식 안내 문자·SNS 안내 문자에는 인터넷주소(URL)가 포함되어 발송되지 않으며,** 특히, 안내 메시지 첫 머리에 **[국제발신]/[국외발신] 문구**가 포함된 경우, 개인정보 탈취 및 금전피해로 이어지는 스미싱 문자이므로 **절대로 URL 클릭을 하지 말아야** 한다.

만약 스미싱 의심 문자를 받았거**나 문자 내 인터넷 주소 바로가기(URL)를 클릭한 이후 악성 앱 감염 등이 의심**되는 경우, **24시간 무료로 운영**하는 **한국인터넷진흥원 118상담센터**(☎118)로 **신고하고 상담**받을 수 있다.

과기정통부와 KISA는 **보호나라**(www.boho.or.kr) → 알림마당 → 보안공지를 통해 **정부시스템 화재 이슈를 악용한 정부기관 사칭 '스미싱', '피싱' 주의에 관한 보안공지문을 게시하였다.** 또한, KISA는 **스미싱 공격에 대한 모니터링을 강화**할 계획이다.

담당 부서	과학기술정보통신부 사이버침해대응과	책임자	과 장	최광기 (044-202-6460)
		담당자	사무관	김성환 (044-202-6461)
	한국인터넷진흥원(KISA) 국민피해대응단	책임자	단 장	이동연 (02-405-4900)
		담당자	팀 장	김은성 (02-405-4940)

참고 **보호나라(www.boho.or.kr) 보안공지**

〈 정부시스템 화재 이슈를 악용한 정부기관 사칭 스미싱·피싱 주의 〉

□ 개요

o 최근 발생한 정부시스템 화재로 인한 대민서비스 중단 이슈를 악용하여 정부·공공기관 사칭 및 민원서비스 안내를 미끼로한 스미싱·피싱 위협이 증가함에 따라 개인정보 탈취 및 금전적 피해로 연계되지 않도록 사용자 주의 필요

□ 주요내용

o “정부24”, “대체 사이트”, “피해보상” 등의 키워드를 활용한 정부·공공기관 사칭 스미싱 유포 및 대체서비스 안내를 빙자한 보이스피싱 등 피싱 시도 예상

- (스미싱) “정부24”, “모바일신분증” 등 특정 서비스 대체시스템 아낸 문자메시지內 악성 인터넷주소(URL) 클릭을 유도해 피싱사이트 및 악성앱 설치 유도
- (피싱사이트) “대체 사이트” 등 정부서비스 장애 관련 키워드를 악용해 포털사이트 검색 시 피싱사이트가 검색 결과 상단 또는 광고로 노출시켜 사용자 접속 유도 가능
- (보이스피싱) 정부서비스 장애로 인한 행정지연 보상절차 안내 등을 빙자하여 유선 연락을 통한 원격제어 앱 설치 유도 및 피싱사이트 접속 유도 가능

스미싱 유포(예상) 문구

o 정부시스템 장애 관련 **공식 안내 문자·SNS 안내 문자에는 인터넷주소(URL)가 포함되어 발송되지 않음**

- 특히, 안내 메시지 두문에 [국제발신]/[국외발신] 문구가 포함된 경우, 개인정보 탈취 및 금전피해로 이어지는 스미싱 문자이므로 URL 클릭 금지

o 악성 앱 실행 시 아래와 같은 행위를 수행하여 2차 피해로 연계될 수 있으므로, 사용자 주의 필요

① 기기명, IMEI 등 단말 정보 유출

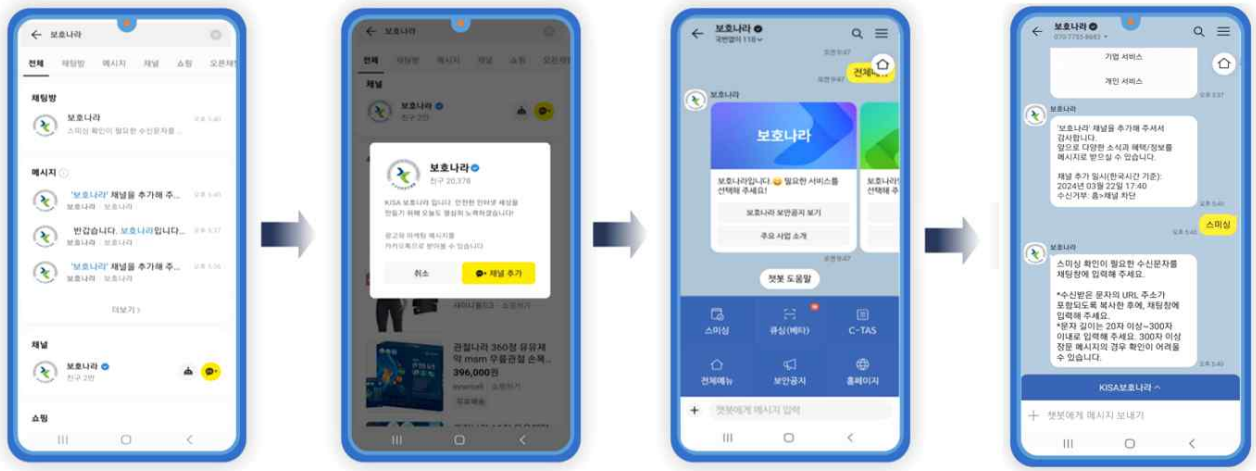
② 저장된 연락처 및 문자 메시지 정보 유출

③ 피해자 기기를 이용한 스팸, 스미싱 등 문자 발송

□ 대응방안

o 스미싱·피싱사이트 신고 및 확인 방법

- 보호나라(카카오톡 채널) 내 '스미싱·피싱 확인서비스'를 이용하여 신고 및 악성여부 판별



보호나라 채널 검색 | 보호나라 채널 추가 | 스미싱·피싱 서비스 클릭 | 피싱사이트 주소(URL) 입력하기

o 스미싱 문자 신고 및 확인 방법

- 스마트폰 내 문자 수신 화면에서 확인가능한 '스팸으로 신고'

- 전기통신금융사기통합신고대응센터 내 '스미싱 문자 신고'

- 보호나라(카카오톡 채널) 내 '스미싱·피싱 확인서비스'를 이용하여 신고 및 악성여부 판별

<스팸으로 신고하기>

<전기통신금융사기통합신고대응센터>

<보호나라 카카오톡 챗봇>

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 인증번호의 경우 모바일 결제로 연계될 수 있으므로 한 번 더 확인
- 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 재발송을 위해 피해자 번호가 도용될 수 있으므로 “번호도용문자차단서비스*”를 신청하여 번호 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 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

o 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

o 공인인증서 폐기 및 재발급하기

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

o 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 : 1566-1188

한국인터넷진흥원 인터넷침해대응센터 : 국번없이 118

□ 작성 : 국민피해대응단 스미싱대응팀