과학기술정보통신부 보도자료 국민이 만든 회복과 도약, 모두의 1년 대전환의 길

보도 시점 배포 시점 배포 2026. 6. 3.(수)

과기정통부, 티빙(TVING) 침해 사고 조사 착수

- 침해 사고 조사 심의위원회 심의를 거쳐, 민관합동조사단 구성·운영 결정 -

과학기술정보통신부(부총리 겸 과기정통부 장관 배경훈, 이하 '과기정통부')는 **티빙(TVING)*** **회원 정보 유출로 인한 피해 현황 및 사고원인 등**을 **조사**하기 위해 **민관합동조사단**을 **6월 3일(수)**에 구성하고 **본격적인 조사**에 **착수**했다고 밝혔다.

* 온라인 동영상 서비스(OTT) 제공 사업자

티빙은 **6월 1일 침해 사고**를 **신고**하였다. **신고 즉시**, 과기정통부와 한국 인터넷진흥원(원장 이상중)은 **티빙 측에 관련 자료 보전을 요구**(6.1)하였으며, **사고원인 및 피해 규모 등에 대해 조사**를 진행하였다.

이에, **침해 사고 조사 심의위원회***를 **긴급 개최**(6.3)한 결과, 이번 사고가 **중대한 사고**에 해당하여 **민관합동조사단 구성이 필요**하다고 **의견을 모았다.**

* 침해 사고에 대한 선제 대응을 위해 신설될 법정 위원회로, '26.5.19부터 사전 가동 중

과기정통부는 위원회 심의 결과를 토대로, 대규모 정보 유출 및 추가 피해 발생 가능성 등을 종합 고려하여 **민관합동조사단**(단장 : 과기정통부 정보보호네트워크정책관)을 구성하기로 **최종 결정**하였다.

민관합동조사단은 과기정통부 및 한국 인터넷진흥원(KISA) 외에도 **디지털 증거 분석(포렌식) 및 인터넷 기반 자원 공유(클라우드) 서비스 분야 등 민간 전문가**를 포함하여 구성하였으며, **철저하게 조사**하여 **그 결과**를 **국민에게 투명하게 공개할 계획**이다.

아울러, 유출 정보 등을 악용해 문자 결제 사기(스미싱) 등 **2차 피해 발생 가능성**을 방지하기 위해 보호나라 누리집(www.boho.or.kr)을 통해 **대국민 보안 공**지도 진행하였다.

담당 부서	과학기술정보통신부 사이버 침해조사팀	책임자	팀장	김우철 (044-202-6490)
		담당자	사무관	김재남 (044-202-6493)
		담당자	사무관	김성환 (044-202-6491)
관련 기관	한국인터넷진흥원 위협분 석단	책임자	단장	김광연 (02-405-4800)
		담당자	팀장	김홍석 (02-405-4830)

붙임 **티빙 침해사고 2차 피해 방지를 위한 대국민 보안공지**

< "OTT 플랫폼" 개인정보 유출 사고 악용 스미싱·피싱 등 주의 권고 >

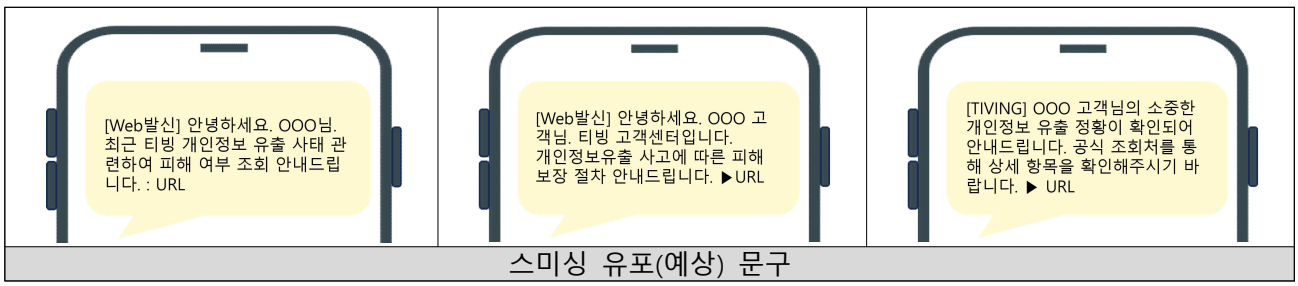
□ 개요

o 최근 **'OTT 플랫폼(티빙) 개인정보 유출 사고'**를 악용하여, 스미싱, 보이스피싱 등을 통한 개인정보 및 금전 탈취 시도가 우려되므로 2차 피해로 이어지지 않도록 사용자 주의 필요

□ 주요내용

o **"피해보상", "피해사실 조회", "환불"** 등의 키워드를 활용한 피해 기업 사칭 스미싱 유포 및 피해보상 안내를 빙자한 보이스피싱 등의 사이버사기 범죄 시도 예상

- **(스미싱) "긴급 앱 업데이트", "피해보상 신청", "환불"** 등 문자메시지內 악성 인터넷 주소(URL) 클릭을 유도해 피싱사이트 및 악성앱 설치 유도
- **(피싱사이트) "피해사실 조회"** 등 정보유출 피해 관련 키워드를 악용해 포털사이트 검색 시 **피싱사이트를 검색결과 상단 또는 광고로 노출**시켜 사용자 접속 유도
- **(보이스피싱) 정보유출 대상자 통보 및 보상·환불 절차 안내** 등을 빙자하여 유선 연락을 통한 **원격제어 앱 설치 유도, 피싱사이트 접속 유도**



스미싱 유포(예상) 문구

□ 대응방안

o **스미싱·피싱사이트 신고 및 확인 방법**

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

o 스미싱 문자 신고 및 확인 방법

- 스마트폰 내 문자 수신 화면에서 확인가능한 **‘스팸으로 신고’**
- 전기통신금융사기통합신고대응센터(https://counterscam112.go.kr) 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 자제**하고 바로 삭제
- 의심되는 사이트 주소의 경우 **정상 사이트와의 일치여부를 확인**하여 피해 예방
- 휴대폰번호, 아이디, 비밀번호 등 **개인정보는 신뢰된 사이트에만 입력**하고 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 신청**하여 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 피해**가 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

o **악성어플리케이션 삭제**

- 문자메시지에 포함된 인터넷주소를 클릭한 것만으로는 악성 앱에 감염되지 않으나, **인터넷주소를 통해 어플리케이션을 설치**했다면 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 삭제**하기

  • 가까운 **휴대폰 서비스센터** 방문

o **공인인증서 폐기 및 재발급하기**

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

o **2차 피해 예방하기**

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

□ 스미싱 제보 및 상담 문의

o **전기통신금융사기 통합신고대응센터 : 1566-1188**

o **한국인터넷진흥원 인터넷침해대응센터 : 국번없이 118**

□ 작성

o **국민피해대응단 스미싱대응팀**