최근 개인정보 유출사고 이슈 및 대응

2023. 3. 20.

플랫폼조사팀: 이 준

최근 유출사고 관련 보도자료

LG유플러스 해킹 공격으로 18만 명 고객 정보 유출

입력 2023-01-10 17:23 | 수정 2023-01-10 17:37

자료사진

국내 이동통신사 LG유플러스에서 이달 초 해킹 공격으로 고객 18만 명의 개인정보가 유출된 것으로 확인됐습니다.

LG유플러스는 오늘 오후 홈페이지를 통해 "일부 고객의 개인 정보가 유출된 사실을 인지해 알려드린다"면서 "유출된 고객 정보는 성명과 생년월일, 전화번호 등으로 유출 정보는 개인별로 차이가 있다"고 밝혔습니다.

개인정보위, 쿠팡 관련 개인정보 46만건 유출사고 확인 중

최근 다크웹 해킹포럼에 물품 구매 기록 회원 개인정보 게시됐다는 의혹
유출된 개인정보 출처, 경위, 규모 등 검토해 관련자 확인 후 법 위반 착수 예정

[보안뉴스 김영명 기자] 개인정보보호위원회(위원장 고학수, 이하 개인정보위)는 쿠팡과 관련된 것으로 보이는 개인정보 유출 사고에 대해 사실 여부를 확인 중이라고 밝혔다.

[로고=쿠팡]

최근 쿠팡에서 물품을 구매한 기록이 있는 사람들의 개인정보 46만건이 다크웹 해킹포럼에 게시됐다는 언론보도가 나왔다. 개인정보보호위원회는 이 사건에 대해 유출된 개인정보의 출처 확인과 유출 경위, 규모 등을 검토하고, 유출 관련 개인정보처리자 등이 확인되면 개인정보 보호법 위반에 대한 조사에 착수할 계획이라고 밝혔다.

인터파크 개인정보 유출 조사 받는다… "피해 규모 파악 중"

황혜빈 기자

입력 2023.01.12 14:58 | 수정 2023.01.12 15:07

개인정보보호위원회(개보위)가 인터파크의 개인정보 유출 정황과 관련해 조사에 착수했다.

12일 관련 업계에 따르면, 인터파크는 지난 10일 '크리덴셜 스터핑'(한 곳에서 유출된 정보로 다른 곳에서 무작위 대입하는 사이버 공격)으로 추정되는 공격을 받고 개인정보 유출에 대해 공지했다. 유출 정보는 이메일, 성별, 생년월일, 전화번호, 주소, 멤버 등급 등으로 확인됐다. 규모는 확인 중이라는 입장이다.

[긴급] 중국 해커조직, 한국 정부·공공기관 타깃 대규모 해킹 작전 선포

설 연휴 기간, 중국 해커조직 "한국 인터넷 침입을 선포하다" 공지 게시
대한건설정책연구원 등 한국의 기관 및 학회, 협회 타깃으로 해킹 공격 감행
코로나에 따른 입국 규제 등 양국 간의 긴장감 고조되는 상황에서 발생

[보안뉴스 권준 기자] 중국 해커조직이 한국 정부부처 및 공공기관을 타깃으로 한 대규모 네트워크 해킹 작전을 선포한 것으로 드러나 설날 연휴에 접어든 정부 및 공공기관의 보안관리에 비상이 걸렸다.

▲중국 해커조직이 올린 한국 네트워크 해킹 작전 선포 내용[이미지=이슈메이커스랩]

개인정보 유출의 개념 및 유형

법령 또는 개인정보처리자의 **자유로운 의사에 의하지 않고**, 개인정보에 대하여 개인정보처리자가 **통제를 상실**하거나 **권한 없는 자의 접근을 허용한 것**을 의미(표준지침 제25조)

개인정보 유출 유형

서면, 이동식 저장장치, 휴대용 컴퓨터 등의 분실 또는 도난

개인정보처리시스템에 대한 권한 없는 자의 접근

개인정보처리자의 고의/과실로 인해 파일, 문서, 기타 저장매체가 권한 없는 자에게 잘못 전달

기타 권한이 없는 자에게 개인정보가 전달

유출사고 내부 대응 체계

개인정보취급자
(임직원)

- ✓ 유출사실/의심사항 발견 시 즉시 CPO 보고(전화, 이메일 등)

개인정보보호담당자
(지정된 경우)

- ✓ 담당자가 지정되어 있는 경우 담당자에게 보고 가능
- ✓ 담당자는 상황 파악 후 지체없이 CPO 구두 보고
- ✓ CPO의 지시를 받아 CPO 업무 지원

CPO
(개인정보 보호책임자)

- ✓ 개략적 상황 파악 후 지체없이 CEO 보고
  * 경미 사건의 경우 CEO 보고 생략 가능
- ✓ 신속대응팀을 소집하고 사고조사 지시 (원인, 경로, 규모 등)
- ✓ 유출 통지, 신고, 공표 등 여부 예비 판단 후 CEO 보고
- ✓ 새로운 상황 확인시 지체없이 CEO 보고 및 추가 통지·신고

CEO
(대표자)

- ✓ 유출 통지, 신고, 공표 등에 대한 최종 의사 결정
- ✓ 필요시 내부 정보보호위원회 등 개최
- ✓ 부서간 유기적 협조 지원 및 대응 방향 제시

피해 확산 최소화 및 긴급 조치

통지·신고 전 긴급조치 의무(영 제40조제1항)

유출된 개인정보의 확산 및 추가 유출 방지를 위해 접속경로 차단, 취약점 점검・보완, 유출 개인정보 삭제 등 긴급한 조치

사고 유형별 긴급조치 방법

해킹

- 시스템 분리/차단 조치, 로그 등 증거자료 확보, 유출 원인 분석, 이용자 및 개인정보취급자 비밀번호 변경 등

내부자

- 유출 경로 확인, 유출에 활용된 컴퓨터/USB/이메일/출력물 등 확보, 취급자의 접근권한 확인, 비정상 접근 경로 차단 등

이메일

- 발송 이메일 즉시 회수, 수신자에게 오발송 메일 삭제 요청, 대용량 메일 서버 운영자에게 파일 삭제 요청, 파일 전송시 암호화 등

노출

- 검색엔진 : 노출된 개인정보 삭제 요청, 로봇배제 규칙 적용 등
- 시스템 오류 : 소스 코드, 서버 설정 등 원인 파악 및 수정 등
- 홈페이지 게시 : 게시글 삭제, 첨부파일에서 개인정보 마스킹 등

주요 점검사항별 점검주기

점검사항	점검주기	점검사항	점검주기
개인정보처리방침 업데이트	연 1회 이상(권장)	개인정보 수집출처 고지 · 수집출처 고지 여부 점검	3개월 이내(의무) 정기적(권장)
내부관리계획 업데이트	연 1회 이상(권장)	고유식별정보 안전성 확보조치 조사·보고	2년 1회 이상(의무)
내부관리계획 이행실태 점검·관리 : 접근권한 관리, 접속기록 보관 및 점검, 암호화 조치 등	연1회 이상(의무)	손해배상보험 등의 유지 여부 확인·점검	정기적 (권장)
개인정보보호교육	연 1회 이상(권/의)	개인정보처리 동의서 관리 · 동의서 작성시 사전 협의	정기적(권장) 상시(권장)
수탁자 관리·감독 : 처리현황 점검, 개인정보보호교육 등	연 1회 이상(권/의)	목적외 이용·제공 대장 관리 · 목적외 이용·제공 대상 작성	정기적(권장) 상시(의무)
접속기록 확인·감독 · 접속기록 백업 또는 보관	월 1회 이상(의무) 정기적(의무)	백신, 소프트웨어 등 업데이트	1일 1회 이상(의무)
접근권한 관리 : 퇴직자, 전보자 등 모니터링	매일 (권장)	출입 통제 관리대장 점검·확인 · 출입자, 반출입 기기 및 자료 통제	정기적 (권/의) 상시(권/의)
홈페이지 취약점 점검	연 1회 이상(의무)	유관부서 협력사항 체크	상시 (권장)
파기 및 삭제 확인	정기적(권/의)	최신 정보 수집 및 공유	상시 (권장)
이용내역 통지	연 1회 이상(의무)		

* (권/의) : 점검 자체는 의무사항이지만 점검 주기는 의무사항이 아닌 경우

유출사고 신고 및 통지

유출 통지, 신고, 공표 등의 방법(영 제40조제2항)

- 유출 사실과 확인된 사항만 통지/신고 기한 내에 미리 알리고 나중에 확인된 사항은 추가 고지
- 사실관계 파악을 이유로 통지를 지연하는 경우 3천만원 이하의 과태료 부과

적용 대상		개인정보처리자	정보통신서비스 제공자 등	신용정보회사 등에서의 상거래기업 및 법안에 한정
유출신고	규모	1천 명 이상	1명 이상	1만 명 이상
	시점	5일 이내	24시간 이내	5일 이내
	기관	개인정보보호위원회 또는 한국인터넷진흥원		
유출통지	규모	1명 이상		
	시점	5일 이내	24시간 이내	5일 이내
	방법	홈페이지, 전화, 팩스, 이메일, 우편 등으로 개별 통지		
	항목	유출된 개인정보 항목, 유출될 시점과 그 경위, 정보주체 피해 최소화 조치, 개인정보처리자 대응조치 및 피해 구제절차, 피해 신고·상담 부서 및 연락처 등		

관계기관에 유출신고 방법

개인정보 유출 신고서 작성 방법

유출 신고서 양식	작성 방식
① 유출 개인정보 항목	▪ **'등'과 같이 일부 생략하거나 휴대전화번호와 집전화번호를 '전화번호'로 기재하여서는 안됨** ▪ 유출된 개인정보의 모든 항목을 적어야 하며, 유출규모도 현 시점에서 파악된 내용을 모두 기재
② 유출 시점과 그 경위	▪ 유출시점, 인지시점을 명확히 구분하여 날짜 및 시간모두 작성해야 하며, 유출경위와 인지경위를 포함
③ 정보주체가 취할 수 있는 피해 최소화 조치	▪ 유출로 발생 가능한 불법 스팸, 보이스 피싱, 금융사기와 같은 2차적인 피해 방지를 위해 이용자가 할 수 있는 조치를 기재(예: 비밀번호 변경 등)
④ 개인정보처리자 대응조치 및 피해 구제절차	▪ 유출사실을 안 후 긴급히 조치한 내용과 향후 이용자의 피해구제를 위한 계획 및 절차를 기재 ex) 경찰 신고, 일시적 홈페이지 로그인 차단 (홈페이지 해킹일 경우)
⑤ 정보주체가 피해 신고·상담 등을 접수할 수 있는 부서 및 연락처	▪ **실제 신고 접수 및 상담이 가능한 전담 처리부서와 해당 담당자**
⑥ 기타	▪ 유출된 기관명, 사업자번호, 사업자 주소, 웹사이트주소 등 기재

정보주체에 대한 유출의 통지방법

통지방법

- 서면, 전자우편, 팩스, 전화, 문자전송, 이와 유사한 방법으로 개별 통지

관련법률		개인정보 보호법		신용정보법
		개인정보처리자 (제 34조)	정보통신서비스제공자등 (제39조의4)	신용정보회사등 (제39조의4)
통지기한	원칙	서면, 전자우편, 팩스, 전화, 문자전송, 이와 유사한 방법		
	추가	**1천 명 이상 유출** ▶ 개별통지와 함께 홈페이지 또는 사업장에 7일 이상 게시	**이용자 연락처를 알 수 없는 경우** ▶ 개별통지 대신, 홈페이지에 30일 이상 게시	**1만 명 이상 유출** ▶ 개별통지 외에, 홈페이지 또는 사업장에 15일 이상 게시 또는 신문 등에 7일 이상 게시

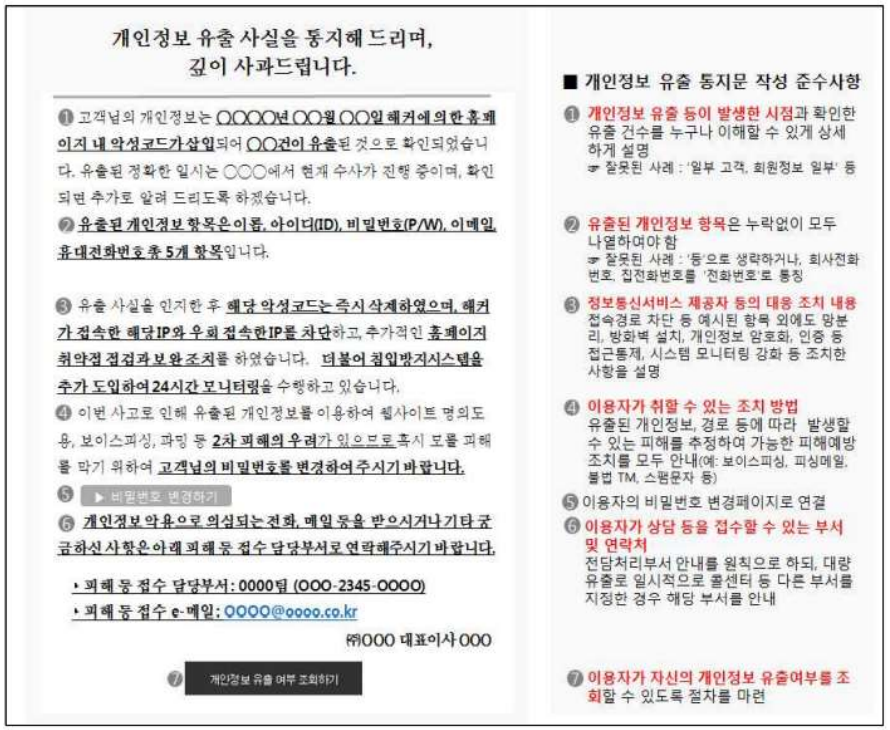
- 홈페이지에 게시할 때에는 '개인정보 유출 안내', '사과문' 등의 제목을 사용
- 대규모 유출로 24시간 이내 전체 통지가 기술적으로 불가능한 경우에는 홈페이지 팝업창 등을 통해 파악된 내용만 우선 게시 후 개별 통지
- 통지 수단은 실제 확인 가능하도록 이용 빈도가 높은 방법을 우선 활용하여 통지(휴대전화→전화→이메일→팩스→우편 등)

정보주체에 대한 유출의 통지 예시

통지내용

1. 유출 개인정보 항목
2. 유출 시점과 그 경위
3. 정보주체가 취할 수 있는 피해 최소화 조치
4. 개인정보처리자 대응조치 및 피해 구제절차
5. 피해 신고. 상담 등을 접수할 수 있는 부서 및 연락처 등

홈페이지 개인정보 유출 통지문



개인정보 유출 사실을 통지해 드리며,
깊이 사과드립니다.

❶ 고객님의 개인정보는 ○○○○년 ○○월 ○○일 해커에 의한 홈페이지 내 악성코드가 삽입되어 ○○건이 유출된 것으로 확인되었습니다. 유출된 정확한 일시는 ○○○에서 현재 수사가 진행 중이며, 확인되면 추가로 알려 드리도록 하겠습니다.

❷ 유출된 개인정보 항목은 이름, 아이디(ID), 비밀번호(P/W), 이메일, 휴대전화번호 총 5개 항목입니다.

❸ 유출 사실을 인지한 후 해당 악성코드는 즉시 삭제하였으며, 해커가 접속한 해당IP와 우회 접속한IP를 차단하고, 추가적인 홈페이지 취약점 점검과 보완조치를 하였습니다. 더불어 침입방지시스템을 추가 도입하여 24시간 모니터링을 수행하고 있습니다.

❹ 이번 사고로 인해 유출된 개인정보를 이용하여 웹사이트 명의도용, 보이스피싱, 파밍 등 2차 피해의 우려가 있으므로 혹시 모를 피해를 막기 위하여 고객님의 비밀번호를 변경하여 주시기 바랍니다.

❺ ▶ 비밀번호 변경하기

❻ 개인정보 악용으로 의심되는 전화, 메일 등을 받으시거나 기타 궁금하신 사항은 아래 피해 등 접수 담당부서로 연락해주시기 바랍니다.

- 피해 등 접수 담당부서 : 0000팀 (000-2345-0000)
- 피해 등 접수 e-메일 : 0000@0000.co.kr

㈜000 대표이사 000

❼ 개인정보 유출 여부 조회하기

■ 개인정보 유출 통지문 작성 준수사항

❶ 개인정보 유출 등이 발생한 시점과 확인한 유출 건수를 누구나 이해할 수 있게 상세하게 설명
☞ 잘못된 사례 : '일부 고객, 회원정보 일부' 등

❷ 유출된 개인정보 항목은 누락없이 모두 나열하여야 함
☞ 잘못된 사례 : '등'으로 생략하거나, 회사전화번호, 집전화번호를 '전화번호'로 통칭

❸ 정보통신서비스 제공자 등의 대응 조치 내용
접속경로 차단 등 예시된 항목 외에도 망분리, 방화벽 설치, 개인정보 암호화, 인증 등 접근통제, 시스템 모니터링 강화 등 조치한 사항을 설명

❹ 이용자가 취할 수 있는 조치 방법
유출된 개인정보, 경로 등에 따라 발생할 수 있는 피해를 추정하여 가능한 피해예방 조치를 모두 안내(예: 보이스피싱, 피싱메일, 불법 TM, 스팸문자 등)

❺ 이용자의 비밀번호 변경페이지로 연결

❻ 이용자가 상담 등을 접수할 수 있는 부서 및 연락처
전담처리부서 안내를 원칙으로 하되, 대량 유출로 일시적으로 콜센터 등 다른 부서를 지정한 경우 해당 부서를 안내

❼ 이용자가 자신의 개인정보 유출여부를 조회할 수 있도록 절차를 마련

유출 통지 위반사례

사례 #1 A쇼핑몰은 해킹으로 추정되는 이상 징후를 인지하고 5일 후, 개인정보 유출사실을 확인하고 2일 후부터 이용자에게 유출 통지

사례 #2 B사는 해커에 의해 개인정보가 유출된 사실을 확인한 후 경찰청에 신고하였으나,
수사관으로부터 해커가 검거될 때까지는 유출 통지를 유보해 달라는 구두 요청을 받고 30일 이상 통지 지연

사례 #3 C사는 개인정보 유출 사실을 알게 된 후 유출된 정보주체를 대상으로 유출 통지를 실시하였으나
'아이디' 또는 '아이디+일방향 암호화된 비밀번호'만 유출된 이용자에 대하여는 별도의 통지절차를 이행하지 않음

사례 #4 D통신사는 정보주체 10여명의 인적사항이 담긴 개인정보파일을 이메일에 첨부하여 다른 사람에게 잘못 보냈으나,
해당 파일에 담긴 이용자에게 별도의 유출 통지 절차를 이행하지 않음

유출사고 주요 사례

사례 #1 사업자가 클라우드 서비스를 이용하면서 안전한 인증수단을 적용하지 않아 해커에게 관리자 접근권한을 탈취

사례 #2 SQL 인젝션, 웹쉘 공격, 크리덴셜 스터핑 등의 해킹 공격으로 유출사고 발생

* SQL 인젝션: 데이터베이스에 대한 질의값을 조작해 해커가 원하는 자료를 DB로부터 유출하는 공격 기법

** 웹쉘(Web Shell): 시스템에 명령을 내릴 수 있는 코드로서, 웹서버 취약점을 통해 서버 스크립트가 업로드되면 해커들은 보안시스템을 피해 별도 인증 없이 시스템에 접속 가능하여 원격으로 해당 웹서버를 조종할 수 있음

사례 #3 유지보수 업체의 실수로 위탁사의 개인정보가 외부의 유출되는 사고 발생

사례 #4 웹페이지 개발 실수로 접근 통제가 이루어지지 않아 신청자명단이 인터넷에서 검색됨

사례 #4 인사담당 직원이 교육안내 메일을 보내면서 실수로 인사정보 파일을 첨부하여 사고 발생

감사합니다