



KT 경제경영연구소에 따르면, 2016년 우리나라 국민의 스마트폰 보급률은 91%에 이른다. 이처럼 스마트폰 보급이 급증하면서 우리의 생활과 업무에 큰 도움을 주기도 하지만, 스마트폰을 통한 개인정보 유출 피해가 계속해서 발생하고 있다. 이러한 개인정보 유출은 제2차, 3차 피해를 초래한다. 그러나 기본적인 보안설정만 잘 해도 n차적인 피해를 최대한 줄일 수 있다.

여기 스마트폰으로부터 당신의 개인정보를 보호할 스마트폰(아이폰/안드로이드) 보안설정 꿀팁을 소개한다.

🍏 아이폰 보안설정 (iOS)

• iOS 10.2.1 기준으로 버전 차이가 있을 수 있습니다.

1. 위치정보 수집 제한 설정

[새로운 애플리케이션 설치 → 위치정보 수집 허용팝업 → 허용하지 않음]

애플리케이션을 사용하지 않아도 위치정보는 계속 수집되기 때문에 애플리케이션 사용 외에는 항상 꺼두는 것이 좋다.

2. 나의 위치 공유 비활성화

[설정 → 개인정보보호 → 위치서비스 → 나의 위치공유 → 비활성화]

아이폰으로 메시지 전송 시 다른 아이폰 유저들에게 위치 정보까지 공개될 때는 나의 위치 공유를 활성화 시켰기 때문이다. 이로 인한 정보 유출 가능성이 있기에 꼭 비활성화하는 것을 권장한다.

3. 위치기반 추적 기능 해제

[설정 → 개인정보보호 → 위치서비스 → 시스템 서비스 → 위치 기반 Apple Ads → 비활성화]

이 기능을 활성화 시 사용자의 위치를 기반으로 한 주변의 음식점, 병원 등의 광고나 알림이 수시로 제공된다.

4. 광고추적 제한설정

[설정 → 개인정보보호 → 광고 → 광고추적제한 → 활성화]

광고들이 자체적으로 사용자의 위치와 데이터를 수집하는 것을 막는 기능을 활성화시키는 것이다.

5. 애플리케이션 접근 요청 기능

[설정 → 개인정보보호 → 연락처/각각의 애플리케이션 → 허용여부설정 → 비허용]

애플리케이션 접근에 대한 설정이 자동으로 되어있으면 애플리케이션들은 마음대로 사용자의 데이터를 조회하기 때문에 데이터 조회가 불필요한 애플리케이션은 꼭 비허용 해야 한다.

6. 백업 후 메시지 음성, 동영상에 대한 만료 기한 설정

[설정 → 메시지 → 메시지 유지 → 기한설정]

악성코드가 담긴 애플리케이션 다운로드로 인해 사용자의 사진이나 동영상이 다른 핸드폰으로 전송되는 경우가 많이 일어나고 있어, 주기적으로 백업을 해야 한다. 또한 만료 기한 설정을 통해 보관기간을 설정하고 자동으로 데이터들이 삭제되도록 하는 것이 바람직하다.

7. 나의 IPHONE 찾기 기능 활성화

[설정 → 개인정보보호 → 위치서비스 → 시스템 서비스 → 나의 iPhone 찾기/ 마지막 위치 보내기 → 활성화]

휴대폰 분실 시 사용자가 원격으로 잠금 시키거나 저장된 데이터를 삭제할 수 있다.

8. 데이터 지우기 활성화

[설정 → Touch ID 및 암호 → 데이터 지우기 → 활성화]

암호 입력 시도를 10번 실패하면 모든 데이터가 지워지는 기능으로 만에 하나 분실했을 때를 대비해서 사용한다.

🤖 안드로이드 보안설정 (Android)

• Android 7.0 기준으로 버전 차이가 있을 수 있습니다.

1. USIM 카드 잠금 설정

[설정 → 잠금화면 및 보안 → 기타 보안 설정 → USIM 설정 → USIM 카드 잠금 설정 → 활성화]

애플리케이션을 사용하지 않아도 위치정보는 계속 수집되기 때문에 애플리케이션 사용 외에는 항상 꺼두는 것이 좋다.

2. 화면 잠금 설정

[설정 → 잠금화면 및 보안 → 화면 잠금 방식]

휴대폰이 잠김 후 스크린을 해제하기 위해서 코드, 패턴 혹은 비밀번호 입력이 필요하다. 보안상 화면 잠금 방식은 PIN이나 비밀번호를 권장한다.

3. 기기 암호화

[설정 → 잠금화면 및 보안 → 보안 설정 → 디바이스 전환을 켤 때마다 그리기 체크]

안드로이드 4.0 이상 사용 가능한 기능으로 암호화를 이용하기 전 화면 잠금 비밀번호를 설정해야 한다.

4. 네트워크 보안 설정

[설정 → 연결 → 모바일 핫스팟 및 테더링 → 비활성화]

기본적으로 와이파이와 블루투스는 켜둔다. '모바일 핫스팟 및 테더링'은 사용하지 않을 경우 꺼야 한다.

5. 위치 보안 설정

[설정 → 연결 → 위치 → 비활성화]

무선 및 GPS는 사용하지 않을 때 항상 끈다.

6. 발신자 신원 보안 설정

[전화다이얼 → 설정 → 추가 설정 → 내 발신번호 표시 → 발신번호 표시 제한]

전화번호가 수신자 휴대전화에 표시되기를 원치 않을 때 사용한다.

7. 소프트웨어 업데이트

1) 휴대전화 운영체제 업데이트

[설정 → 기기 → 업데이트 → 업데이트 체크]

2) 설치한 앱 업데이트

[플레이스토어 앱 → 측면 메뉴 중 내 앱 → 업데이트]

스마트폰이 안전하기 위해서는 소프트웨어 업데이트를 유지하는 것이 가장 중요하다.

스마트폰 이용자 개인정보 10대 안전수칙

01. 의심스러운 애플리케이션 다운로드 하지 않기
02. 신뢰할 수 없는 사이트 방문하지 않기
03. 발신인이 불명확하거나 의심스러운 메시지 및 메일 삭제하기
04. 비밀번호 설정 기능을 이용하고 정기적으로 비밀번호 변경하기
05. 블루투스 기능 등 무선 인터페이스는 사용시에만 켜 놓기
06. 이상증상이 지속될 경우 악성코드 감염여부 확인하기
07. 다운로드 한 파일은 바이러스 유무를 검사한 후 사용하기
08. PC에도 백신 프로그램을 설치하고 정기적으로 바이러스 검사하기
09. 스마트폰 플랫폼의 구조를 임의로 변경하지 않기
10. 운영체제 및 백신 프로그램을 항상 최신 버전으로 업데이트 하기