

# 여러분의 모바일 기기는 얼마나 안전하나요?

대부분의 사람이 스마트폰을 가지고 있지만, 이러한 모바일 기기가 직면한 보안 위협에 대해 진지하게 생각하는 사람이 얼마나 될까요? 모바일 기기는 다양한 유형의 위협에 취약합니다. 사기꾼은 모바일 기기를 점점 더 빈번하게 공격하고, 악성 애플리케이션을 사용하여 여러분의 휴대폰을 노리고 있습니다. 이러한 방법을 통해 배드 가이는 사용자가 전혀 눈치채지 못하는 사이에 개인 정보와 업무 정보를 훔칠 수 있습니다.

보안 또는 바이러스 백신 애플리케이션만으로는 스마트폰을 보호하는 데 충분하지 않습니다. 모바일 보안 습관을 개선하는 것이 모바일 기기와 관련된 개인정보 보호 및 보안 문제에 대한 최선의 방어책입니다.

## 모바일 보안 습관을 개선하려면 어떻게 해야 하나요?

모바일 기기에 대한 익스플로잇 위험을 최소화하려면 다음 모범 사례를 항상 기억하세요.

- 1. 휴대폰의 운영 체제를 항상 최신 상태로 유지합니다.** 운영 체제는 보안 결함 수정을 위해 자주 업데이트됩니다. 많은 악성 위협은 오래된 운영 체제로 인해 수정되지 않은 보안 결함으로 인해 발생합니다.
- 2. 앱 스토어 내 악성 앱을 주의합니다.** 공식 앱 스토어에서는 맬웨어가 포함된 애플리케이션을 정기적으로 삭제하지만, 때로는 이러한 위험한 앱이 그대로 남아 있어 사용자가 의심 없이 다운로드할 수 있습니다. 조사하고, 리뷰를 읽고, 다운로드 횟수에 주의하세요. 공식 앱 스토어 이외의 출처에서 애플리케이션을 다운로드하지 않습니다.
- 3. 애플리케이션이 기능과 무관한 휴대폰 항목에 액세스 권한을 요청하지 않는지 확인합니다.** 애플리케이션은 일반적으로 다운로드 전에 파일, 폴더, 다른 애플리케이션 및 데이터에 대한 액세스 권한을 요청합니다. 이러한 권한을 맹목적으로 승인해서는 안 됩니다. 권한 요청이 불필요해 보인다면 앱 스토어에서 대체 애플리케이션을 찾아봅니다.
- 4. 암호가 없거나 암호 보호 기능이 약합니다.** 많은 사람이 여전히 암호를 사용해 휴대폰을 잠그지 않습니다. 기기를 분실하거나 도난당하면 도둑이 휴대폰에 저장된 모든 정보에 쉽게 액세스할 수 있습니다.
- 5. 공용 WiFi에 주의합니다.** 사기꾼은 사용자가 무엇을 하는지 볼 수 있는 기술을 사용합니다. 공용 WiFi를 통해 온라인 서비스에 로그인하거나 민감한 거래(뱅킹 등)를 실행하지 않도록 합니다.