

モバイルデバイスの安全性

多くのユーザーがスマートフォンを利用するようになりましたが、これらのモバイルデバイスが抱えているセキュリティの脅威について真剣に考えているユーザーはどれだけいるのでしょうか？ モバイルデバイスはさまざまな脅威を受ける恐れがあります。モバイルデバイスへの攻撃は増加しており、詐欺師は悪意のあるアプリを使用してユーザーのスマートフォンを標的にしています。悪意のあるアプリを使用すれば、ユーザーに全く気が付かれることなく、個人情報や企業の情報を盗むことが可能になります。

セキュリティアプリケーションやアンチウイルスアプリケーションをダウンロードしただけでは、スマートフォンの安全対策は十分ではありません。モバイルデバイスのセキュリティ対策を向上することは、モバイルデバイスにおけるプライバシーとセキュリティの問題に対する最善の防御策になります。

モバイルデバイスのセキュリティ対策を改善するには？

モバイルデバイスが攻撃されるリスクを最小限に抑えるために、以下のベストプラクティスを常に覚えておきましょう。

1. **スマートフォンのオペレーティングシステムが常に最新の状態であることを確認します。** オペレーティングシステムは、セキュリティの脆弱性を修正するために更新されることが多くあります。多くの脅威は、古いオペレーティングシステムを使用しているために、修正されないままになっているセキュリティの脆弱性によって引き起こされています。
2. **アプリストアに存在する悪意のあるアプリに注意してください。** 公式のアプリストアはマルウェアが含まれるアプリを定期的に削除していますが、こうした危険なアプリが検査をすり抜け、無防備なユーザーがダウンロードしてしまうこともあります。ダウンロードするアプリについては調査し、レビューを読み、ダウンロード回数にも注意してください。公式のアプリストア以外からは絶対にアプリケーションをダウンロードしないでください。
3. **アプリが、アプリ本来の機能とは関係のないスマートフォンの機能へのアクセスを要求していないことを確認します。** アプリケーションは通常、ダウンロードする前に、ファイル、フォルダ、他のアプリ、データに対するいくつかのアクセス権限を要求します。これらのアクセス権限をやみくもに承認しないでください。アクセス権限の要求が不要と思われる場合は、アプリストアで別のアプリを探してください。
4. **パスワードを設定しているか、あるいは強度の高いパスワードで保護しているかを確認してください。** スマートフォンのロックにパスワードを使用していないユーザーがまだ多く存在します。デバイスを紛失したり盗まれたりした場合、パスワードでロックしていなければ、スマートフォンに保存されているすべての情報に簡単にアクセスされるでしょう。
5. **公共のWi-Fiを使用する際には注意してください。** 詐欺師は、あなたの行動を把握することができるテクノロジーを使用しています。公共のWi-Fiでオンラインサービスにログインしたり、機密性の高い取引（振込などの銀行取引など）を行ったりするのは避けましょう。