

If not properly protected – just about anybody can! Android applications are run client-side, which means that the actual code for the application is downloaded onto the user’s mobile device.

Through a process called “decompilation”, hackers can use simple tools to reverse engineer your app, reproducing the original source code.

If not properly protected, decompiled code can potentially reveal usernames and passwords to back-end databases. This means that anyone could have access to your sensitive data.

Your data can remain safe and secure if your Android app has been protected with techniques such as obfuscation and the encryption of login information.

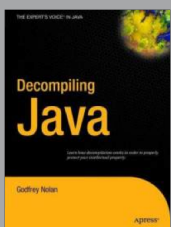
## HOW DO I KNOW:

If you have an Android app (especially one that connects to your backend databases) ask your developers:

- Has our app been properly obfuscated? Has all the login information been removed from our Java code? The answer should be “Yes”.
- If another developer were to download our app and decompile it – what would they find? The answer should be, “Gibberish”.

## GET A SECOND OPINION

RIIS offers code-auditing services. We’ll download your Android app, decompile it and determine your security exposure. We’ll report back to you with the risks we uncovered and suggestions for mitigating them.



LEADING EXPERTISE IN EXPOSING THE RISKS OF DECOMPILED

Godfrey Nolan, Founder and President of RIIS  
- Wrote the book on Decompilation.

# CALL NOW

248.351.1200 | [www.riis.com](http://www.riis.com)