

# iPhone Users Lose Cloak of Invincibility to Malware Authors

The screenshot shows the Google Play Store page for the app 'Find and Call'. The page is divided into several sections:

- OVERVIEW**: Contains the app's description and developer information.
- USER REVIEWS**: Shows a bar chart of user ratings and an average rating of 1.0.
- WHAT'S NEW**: A tab for updates.
- PERMISSIONS**: A tab for app permissions.
- Description**: The app's description, which includes the text: "Have you forgotten the number? Do you remember the email? CALL!!! Find and call is a new technology for your mobile phone. For the first time in the world, you may not only make calls from your mobile phone, but also search for subscribers you need. Free calls from your mobile phone to domains, email, Skype, social networks. Forget about numbers!!!".
- App Screenshots**: Three screenshots showing the app's interface, including a search bar, a list of contacts, and a call log.
- ABOUT THIS APP**: Provides details about the app, including its rating (1.0), update date (May 21, 2012), current version (0.9.167), and category (Communication).
- INSTALLS**: A box indicating the number of installs, which is 100 - 500.
- PRICE**: The app is free.
- CONTENT RATING**: The app has a low maturity rating.

[mobilesecurity.com](http://mobilesecurity.com) [London, UK] Security researchers made the headlines this week after discovering an app on Apple's [App Store](http://App Store) and [Google Play](http://Google Play) that secretly copied address books and spammed their contacts with an SMS link to download the app themselves. Heralded as the first truly malicious app for iOS, *Find and Call* - a tool that claimed to make it simpler to sync up your phone numbers and email addresses – has since been removed from these two app markets.

The description in Google Play should have caused alarm bells to ring before any English speaker even considered installing the app. It begins: "*Have you forgotten the number? Do you remember the email? CALL!!!*"

It then continues with a vague description of features and benefits of the app - although I

take my hat off to anyone with sufficient skills to conclusively decipher the following prose: "*For the first time in the world, you may not only make calls from your mobile phone, but also search for subscribers you need. Free calls from your mobile phone to domains, email, Skype, social networks. Forget about numbers!*"

So what exactly is this app offering? I guess those 100-500 customers who downloaded the app were expecting it to merge their contact lists from all these sources, and then provide a way to contact them without needing to make paid-for calls. When I select a contact on my *Samsung Galaxy SII*, it offers all the above methods for getting in touch – I can choose to send an email to any of the various addresses I have for that particular person. I can call them or send an SMS to any of the numbers I have for them, and I can make those calls using Skype or my standard paid-for phone service. I can also chat via Google Talk, Windows Live, AIM or Yahoo, or if I choose to enable additional features, there's the option to use Facebook chat or send a direct message via Twitter.

It's not clear exactly what users were expecting when they downloaded this app, but I'm confident they weren't expecting their full address books to be uploaded in plain text format to a server which then spammed all their contacts. The spam message was sent in Russian via SMS to all contacts saying "*Now I'm here and it's easier to reach me with the help of this free application...*" It also included a link to the download page for Find and Call. It's not clear what other plans the app developer had in mind for the contact details they were harvesting, but you might assume they didn't have the best intentions.

According to [Wired.com](http://Wired.com), the app developer sent an emailed statement to [AppleInsider.ru](http://AppleInsider.ru) which attempted to explain the spam issues. They claimed "*[the] system is in process of beta-testing. In result of failure of one of the components there is a spontaneous sending of inviting SMS messages. This bug is in process of fixing.*" While this response seems disingenuous, it will be interesting to see whether the developer does fix the 'bug' and re-submit the app to Google Play and Apple App Store. Rarely do actual malware authors and cybercriminals attempt to justify their actions – and the mere fact that the developer responded to publicity suggests there's more to this story than meets the eye. It will certainly lead to more headlines if either Apple or Google accept a new, revised version of *Find and Call* after further reviews.

In their favor is the fact that there's discussion among the experts regarding whether *Find and Call* should really be classed as malware, or whether it would be more appropriate to classify it as a tool for spammers.

Whether this is malware, spyware, clumsily-developed software or a sign of the next area of focus for cybercriminals, it provides another lesson that everyone should remain vigilant when installing apps on their mobile devices. It's also a warning sign to iPhone and iPad users that perhaps their days of security obscurity may be numbered. Here are three simple rules to follow when you're having doubts about installing an app on your smartphone:

- Check the app comes from a recognised developer, and that its user and security ratings are positive on mobilesecurity.com's [APP VIEW tool](#)
- Be wary of app descriptions that are vague, inaccurate or poorly-written, it's a sign that the app may not have been QA'd as thoroughly as you might hope
-

Pay attention to the permissions required for the app you're installing if you're using an Android device. You can check app permissions on mobilesecurity.com's [App Permissions Comparison](#) widget.

Mobilesecurity