

# The Honey Stick Project: An Experiment in Smartphone Snooping



Recently, the research team here at Norton conducted an experiment to find what people would do if they found a lost smartphone. Would they try to contact the owner? Would they make a few calls first? The answers may surprise you.

## The Lure of Honey

Labeled the “Honey Stick Project,” Norton teamed up with Scott Wright of [Security Perspectives, Inc.](#) to design a study that would provide reliable data as to what happens to smartphones and all the information they contain, after we lose them. 50 devices were each loaded with a set of simple applications that had icons and names that would be easily recognizable to someone picking up the phone. These apps weren’t functional, but anytime someone tried to access them, data was sent to a central logging facility. In order to obtain accurate behavioral information, no security software or passwords were enabled on the devices.

Once configured, Norton dropped these devices in elevators, malls, office food courts and other publicly accessible places in Los Angeles, San Francisco, New York, Washington DC and Ottawa, Canada. Activity was monitored on the smartphones for up to seven days.

The result? Half of the studied population isn’t as honest as we’d hope. Only 50% of finders tried to contact the owner of the smartphone (as measured by the number of people who accessed the “Me” entry under the “Contacts” applications, and tried to initiate communication). Another surprising statistic was that even if they showed intention to return the phone, many still tried accessing personal and business-related applications such email, online banking, corporate documents, and more.

## The Outcome

The team audited activity on the following applications, as well as using GPS tracking to monitor

the device location and to make sure it was working normally:

- Social Network Applications
- Online Banking
- Webmail
- Private Pictures
- Passwords
- Calendar
- Contacts
- Cloud-based Documents
- HR Cases
- HR Salaries
- Corporate Email
- Remote Admin

Several of the applications also had a mock login page with the user id and password already populated, just to see if people would try to click through the app authentication.

The data highlights:

- 96% of smartphones were accessed by finders
- 89% were accessed for personal apps and information
- 83% were accessed for company apps and information
- 70% of devices were accessed for both personal and company-related apps and information
- 53% of finders tried to access a file titled “HR Salaries”
- 40% tried to access a file titled “HR Cases”

When a company-owned mobile device was lost, there was more than an 80% chance the finder will try to breach corporate data and/or networks:

- Online banking apps were accessed 43% of the time
- 66% of finders tried to click through the already populated app login page.

Our smartphones contain personal and business information that is both vital and sensitive. Lost company devices can result in unauthorized access to confidential corporate information, intellectual property, financial plans, etc. and could cost an employer in terms of lost revenue or legal action. On a personal level, owners can experience embarrassment, psychological distress, extortion and discrimination.

There are logical reasons that someone would try to access your phone upon finding it—they could be trying to return it to you, or maybe they’re looking for information of value to them that has nothing to do with you or your company. Regardless, the odds are they will find something not meant for their eyes.

To read tips on protecting the mobile devices in your possession and employ, see our article on [Securing Your Smartphone](#).

Download the complete study [here](#). For media inquiries, get the press kit [here](#).

Mobilesecurity