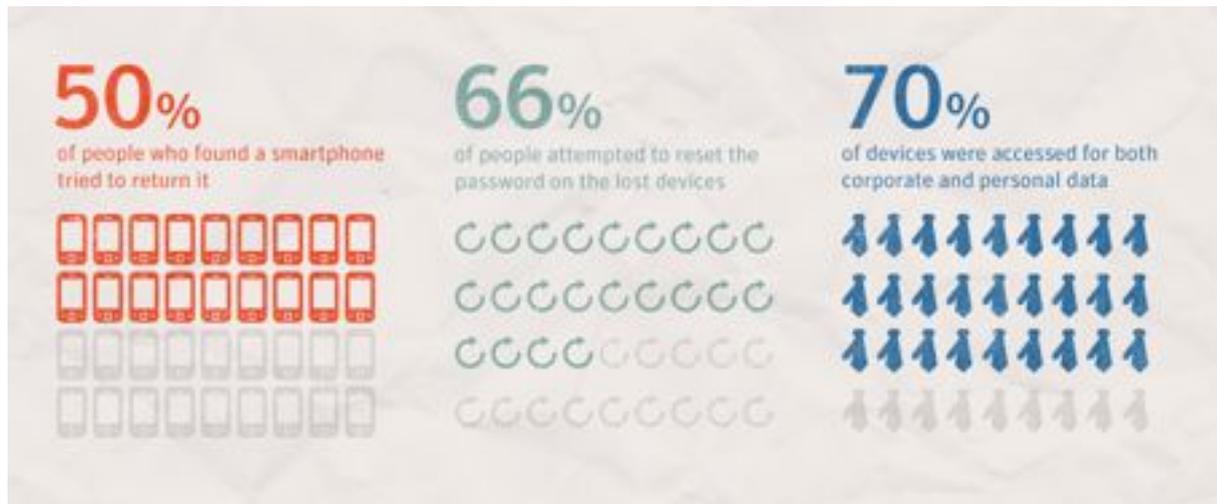


Safe From Prying Eyes



No one likes losing his or her smartphone. There are contacts to replace, apps to re-download and the inconvenience of being without mobile communication. But there's more to it than that. Losing your smartphone could put your personal and professional reputation at risk.

The research team here at Norton recently conducted a study that tested theories behind what happened to lost mobile devices after they left owners' hands and their findings may surprise you. If you had to guess the percentage of finders who tried to return the device to its owner, what would you say? 80%? Maybe 60%? Try 50%. That doesn't sound like good odds, does it?

Users can replace smartphones easily and for a relatively low cost. What they can't replace is the access to personal and business information they just granted whoever happened to pick it up.

Companies have a lot to lose if one of their employees misplaces their work-connected smartphone, including control over who has access to confidential information. Here are some tips that can ensure your internal data stays that way:

- Develop and enforce strong security policies for employees who carry mobile devices for work. At the very least, require they enable their screen lock with a strong password and install mobile security software to protect information in the case of loss or theft.
- Educate your employees about the digital and physical risks associated with mobile devices. Make sure they understand just how easy it is for someone to gain access to their phone via online spyware or information by accessing their home screen.
- You can't protect what you don't know about so take inventory of the mobile devices connected to your company's networks.
- Use mobile device management software to put a formal "lost and retrieval" process in place so that everyone knows what to do if a device is lost or stolen.
- Manage mobile device security within your overall security framework and administer it in the same way you would protect a company computer.

Consumers who use smartphones for personal use also have much to lose. People use mobile devices for everything from online banking to photo storage and allowing a stranger access to

this information could result in embarrassment, extortion, or worse. Here are some tips for maintaining your digital privacy:

- Enable the screen lock feature and secure it with a strong password or “draw to unlock” pattern. This may sound basic, but it can be the critical barrier to someone accessing your information.
- Use security software specially designed for smartphones. It can stop hackers and cybercriminals from stealing information or tracking your keystrokes and gaining access to your passwords. Many programs also help locate lost or stolen phones.
- Differentiate your phone from others by using a colored case or sticker(s), and then when out and about, make sure you keep an eye on it. Don't ever set it down and walk away.

Get the rest of the stats in [Lost and Found: an Experiment in Smartphone Snooping](#).

Mobilesecurity