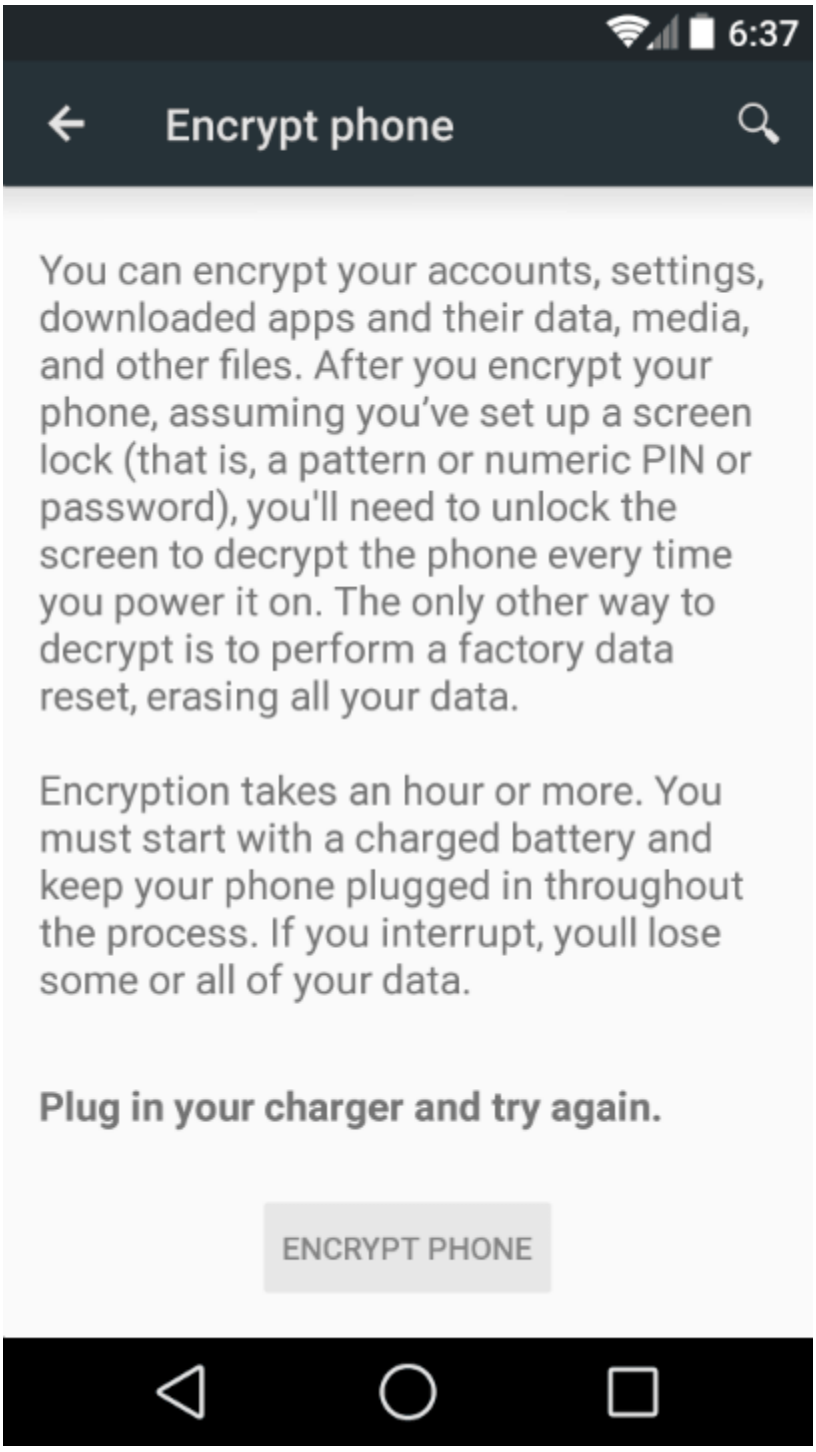
Protect Yourself: New Encryption Software Coming for iOS and Android

October 7, 2014 | Jeff Taylor

After the major data leaks at Target and Home Depot and the recent celebrity hacking scandal on iCloud, people are worried about their private data being hacked. Rightfully so, every year, 15 million U.S. residents have their identities used fraudulently, resulting in $50 billion in losses, according to the Federal Trade Commission. And ever since Edward Snowden leaked information about NSA spying, people have become more worried about government access to our personal data and a Big Brother-type government.



As a result, both Apple and Google have announced higher levels of encryption that will automatically be set up on all new devices. With iOS 8 and Android L, even law enforcement will not be able to access the encrypted data, because the agencies will not have the users' personal passwords. Here's what this mean for smartphone users and the government.

For Users

This latest encryption data will give users peace of mind that their information is secure from hackers and the government. Their pictures, videos and communication such as texts and emails can only be accessed by somebody who has the device's password, reports The Washington Post. This is part of an attempt by companies to make their products safer and more resistant to government snooping.

Apple makes some bold statements on a new privacy page on their website. They state, "At Apple, your trust means everything to us. That's why we respect your privacy and protect it with strong encryption, plus strict policies that govern how all data is handled." They continue to explain that they are making improvements, and they urge all customers to use two-step verification and protect their Apple ID account information.

Google has been offering data encryption services for three years. However, it was not an automatic setting. If you had an older smartphone you had to manually turn encryption on, and only a handful of people knew about it and did so. Now, with Android L, encryption will be a default setting, so users will not have to worry about activating it.

For Johnny Law

Encrypted data will make investigations more tedious for law enforcement and lawyers. The Washington Post reports that law enforcement officials have warned that restrictions on their access make it harder to prevent and solve crimes. Although the Supreme Court ruled that police need search warrants in order to access data on smartphones, it will no longer be relevant with the new data encryption, because Google and Apple will not be able to access their customers' data.

Discord Brews

Many officials are against the new data encryption. U.S. Attorney General Eric Holder has been one of the highest officials to speak out, saying that it is possible for law enforcement to do its job and protect people's personal privacy.

The main angle is that with the new encryption, it will be more difficult to find kidnappers and pedophiles. According to a Sept. 30 report by Reuters, Holder told the Global Alliance Against Child Sexual Abuse Online, "When a child is in danger, law enforcement needs to be able to take every legally

available step," adding that, "It is worrisome to see companies thwarting our ability to do so." According to Justice Department officials, he is asking for cooperation from these companies, Week reports

Apple and Google do not seem to be backing down. Apple's website has an entire page devoted to government requests. They explain that under iOS 8, users' personal data is under their passcode and they cannot bypass it to access the data. Therefore, they claim, "It's not technically feasible for us to respond to government warrants for the extraction of this data.

Even though many law officials are making it seem as though it will be nearly impossible to solve crimes without this data, many believe that is not the case. Writing for CNN, security technologist Bruce Schneier explains that you can't build a back door that only good guys can walk through, because this also leaves data open to cybercriminals, competitors and other countries' governments. He claims that the FBI is just "pumping up the fear" with threats of kidnappers and sexual predators. As an example he cites John J. Escalante, the chief of detectives in Chicago, who said that "Apple will become the phone of choice for the pedophile." Schneier also noted that most people back up their data to the cloud, which can still be accessed with a search warrant.

Enhanced data encryption is coming to your Android. Be sure to check your settings or update your software to Android L, when (or if) it's released for your device. This way, you are sure to be protected.