

TOP 4 THINGS YOU NEED TO KNOW BEFORE BUYING ANY ENCRYPTED MOBILE!



zezel.com
Mobile: Message. Manage.

Top 4 Things You Need To Know Before Buying ANY Encrypted Mobile!

About the Author



Dwight Brown

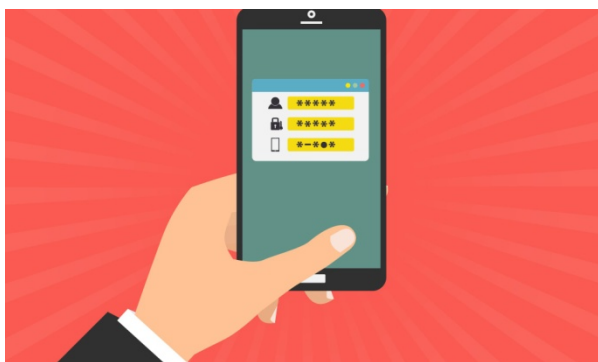


Dwight Brown is the founder of one of the world's most wide ranging encrypted mobile multi-nationals, Zezel L.L.C. With over 960 clients in 24 countries, Dwight and his team work with organizations globally in consulting and implementing security and privacy for mobile devices and endpoints. You can reach Dwight at dbrown@zezel.com or go to www.Zezel.com

We are past the days of saying that the communication through mobiles is an increasingly important part of everyday lives for the people at play or at work. We all live and breathe that now. But as the access to mobile communication has become our primary source of information, it has spawned a vast array of mobile security threats. These threats are very lucrative for the hackers and are very frustrating for the organizations I have dealt with (and those I have not) who are trying to tackle these issues.

When getting an encrypted mobile phone you need to consider several factors. Here I list the top 4 'Things' I feel you should pay attention to when you or your organization are making their choice.

Thing #1 – Do they offer Multiple Layers of Encryption?



One layer is NOT enough. To protect your privacy you should have multiple layers of encryption all working in synch to secure your communications. If you want to get into the technical aspects of this you can learn more about [Multiple Layers of Encryption by clicking here](#). When we designed and built the Zphone we knew that having these multiple layers was a must, not just for our email messaging but for our calls and secure messaging as well.

Thing #2 – Where does your encrypted data provider host their services?



Where is your service hosted in? What country? What is the laws that govern the privacy of your communication? These are all things any individual or business should consider carefully. There are countries you should avoid.

[Here is a reliable list of the top 5 countries](#), we use 2-3 of these for our services, so you can be rest assured if your Encrypted Mobile provider has these as their host countries, you should be good from that standpoint.

Thing #3 – Is secured email enough? Secured Calls and Messaging



Many people and businesses who seek encrypted mobile devices think of secured e-mail only. But with recent developments of encryption, secured calls and texts are just not for government leaders anymore. Companies like [Zezel L.L.C.](#) offers multiple communication options that don't sacrifice security regardless of the method you choose to do business with.

Thing #4 - What Mobile Encryption Protocol to rely on?



This one is a biggie... there are so many different options out there now and offerings for mobile encryption from apps, to Android and iOS. What we have found doing research into building **theZphone** is that nothing short of a native group up approach works for mobile.

We have multiple layers of additional protection. On the OS level we have encrypted bootloader and boot integrity checks. What happens is if somebody tries to push a fake secure chat, the phone can never adopt it because of the encrypted bootloader. The bootloader ensures that the application of our own (non open source) Mobile Device Management (MDM).

Summary

I hope this gives you a bit of food for thought. There are many aspects to mobile security and I encourage you to reach out to me and let's have a chat about your situation and the needs and particular challenges you face.

CONTACT ME AT:

E-mail: dbrown@zezel.com **Web:** <https://www.zezel.com>

Phone: 702-605-0390 **Toll Free:** 1-866-560-2455 ext. #3

Enjoy the day;

A handwritten signature in black ink that reads "Brown".

Dwight Brown
Zezel L.L.C.

