Have you ever been hack? Has your data ever been compromised? These days, we store just about everything on our mobile devices from our payment information, online passwords, health data, and many other forms of sensitive data. However, in an age where cybercrime occurs on such a regular basis, how do we combat the problem? In this post, I am going to give you some tips to stay secure, and anonymous in our mobile lives

1. Use a Passcode

This should be one of the first things we do when we get a new device. We secure all of our online accounts such as Facebook, why not our physical devices. You would be surprised how many people I know who don’t bother enabling a passcode onto their device or they just use one that almost anyone can guess. If and when you enable your password, why not step it up a bit. On iPhone you can increase the complication of the passcode by disabling simple passcode. Once you do that, you can put as long of a password as you want.



2. Encrypt Your Data

Starting in 2014, alongside their iOS 8 update, the iOS operating system became encrypted from head to toe. Google then followed suite a year later. The only way to unencrypt that data is to have your passcode. Let us say that your code is too simple, you can encrypt various parts of your device. A new addition in iOS 9.3 includes the ability to encrypt individual notes. The only way to access these notes is to use the biometric sensor through Touch ID, to unlock it.



3. Disable Unnecessary Lock Screen Add-Ons

What do I mean by this? These Add-Ons are things such as Control Center, Notification Center, and Siri. Why would I want to do that? In the past, it has been proven that these areas are where security of your device can easily be breached. A few weeks back, you could as Siri to search Twitter 🡪 Search gmail.com 🡪 Force Touch (iPhone 6s and 6s+) 🡪 Add to Contact or Create Contact, and you would have access to the person’s contacts and photos. Thankfully this has been patched or I would not have mentioned it. Control center is also a target of bypassing your device. Apple has patched numerous flaws that would grant access to the WHOLE DEVICE without your password. This is why this is on my list.



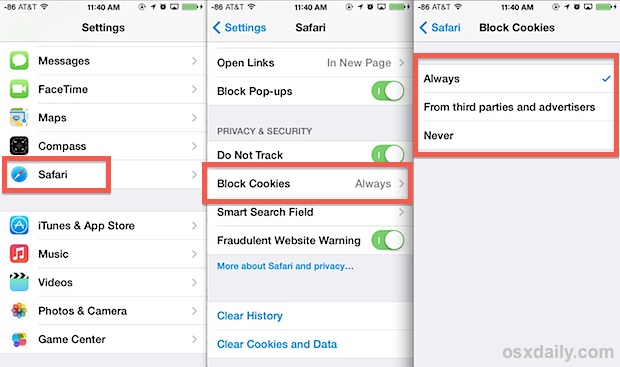
4. Use VPNs

VPN (Virtual Private Network) allows for a user to access data on the web, and at the same time, it keeps their information, such as IP Address, Location, and other forms of data out of the hands of third parties. There are many services available such as Tunnel Bear or Free Shield. Most of them, all you have to do is download an app, select a button, install, and that’s it! A nice perk to some of these services is that they also block ads!



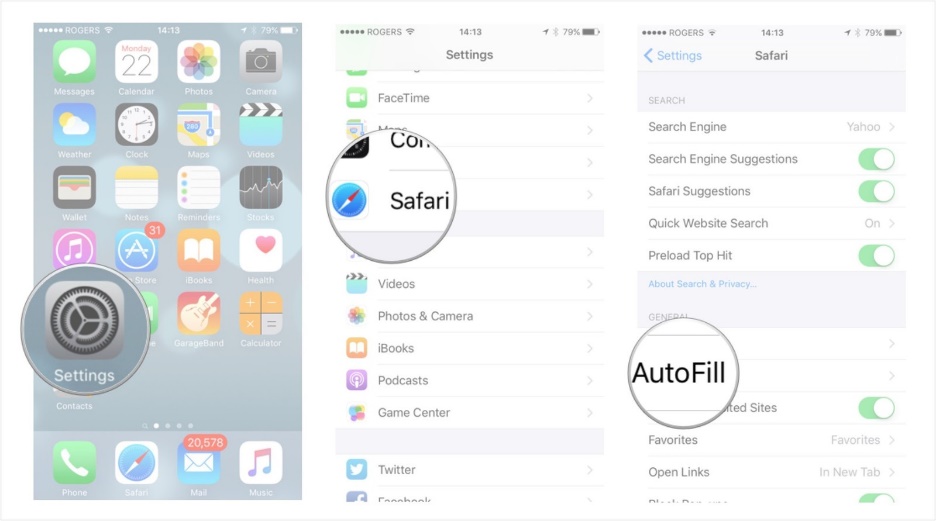
5. Disable Tracking Cookies

No these aren’t real cookies that Cookie Monster would be more than glad to devour. Cookies are actually “packets” which basically get stuck to you, and the developers of the website are then able to track your location even when you leave their site. Companies such as Verizon love to have that type of information so they can quote one quote, provide a better experience. However, typically, that data is gathered to provide you with even more ads. A nice addition with iOS is built right into the Safari browser called “Private Browsing.” Basically, with this, you become incognito to the web, and you can browse without worry of corporations gathering data on you. You may have to disable it once in a while to access certain sites, but normally, once I am done, I enable it back onto my device.



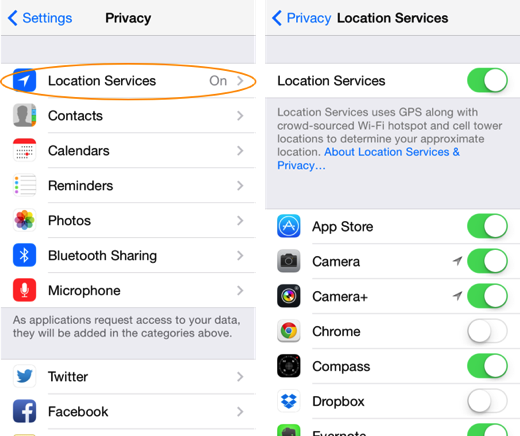
6. Do Not Use Auto-Fill

I know I am guilty about this one, but it is the smart thing to do. I know it is extremely easy to just select a button and fill in ALL of your information. My question for you is, how easy is it for someone else to do the exact same thing? The downside to this feature is that it doesn’t even require authentication to access those passcodes. Let us say you are on your banking site, and lay your phone down to grab something. How easy would it be for someone to come around and push that little button and have access to EVERYTHING! Until it becomes more secure, I try to refrain from using that tool.



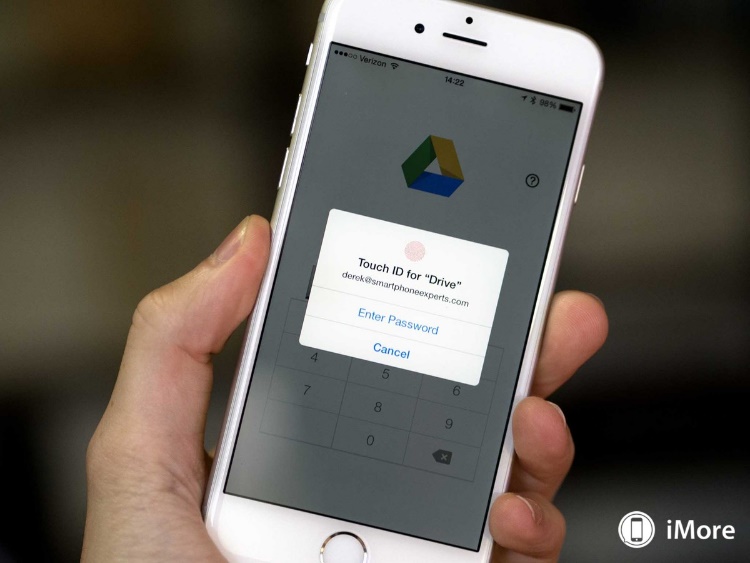
7. Disable Location Service on Nonsense

How many times have you been asked to share your location data? Apps such as Best Buy, Target, and even Apple’s own store app request that data. You may say, they are only trying to find the closest store to me. Yes that is true, but why do they need that data all the time. Some apps let you set a “home” location and that it! After the whole Target breach, I honestly don’t feel comfortable sharing so much of my information. How about those games that say “Get Extra Lives by Sharing Your Location!” That should raise a red flag right there. What are they going to do with that data? Shove more adds down your throat. While I am on the subject, if your game does not require data, disable cellular for that app or just turn of Wi-Fi; instantly, no ad! Because ads are being pulled form a server, if you cut communication, there will be nothing to show.



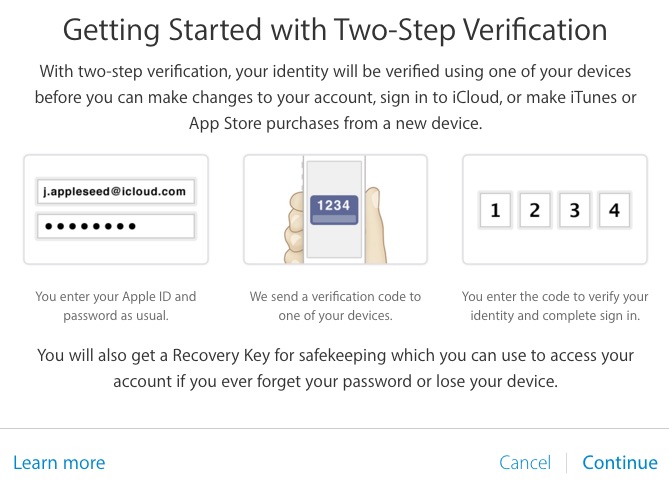
8. User 3rd Party Apps to Secure Data

I’m honestly not the biggest fan of this because it is a 3rd party storing my data, but I have begun to trust programs from Google such as Sheets, Docs, Slides, and Drive. These apps allow for a user to encrypt data within that app with their fingerprint. I would still not store very important data on these applications due to the possibility of compromise.



9. Two Step Verification

To help users secure their data, many companies are offering this service to better secure your account. You would first start off by logging into your account, and to ensure it is you, the company will then send you a verification code which you must enter to be granted access into your account. I have done this so far for my Apple, Microsoft, and Yahoo accounts. If you have not done this yet, I would strongly recommend you do.



These are my tips for staying secure and safe in the digital era. Should we refrain from storing such sensitive data on our devices? Is security becoming even more relevant? Did I forget any? If you have any recommendations to share, leave them below in the comments. I can’t wait to see what you come up with.

*If you have any recommendations for future posts, leave a comment below!!!*