چگونه آیفون و آیپد خود را در برابر هک شدن ایمن نمائیم و از لو رفتن اطلاعات شخصی خود جلوگیری کنیم

کتابی که هر دارنده آیفون یا آیپد باید از اطلاعات آن با خبر باشد

راهنمای تصویری گام به گام

مولف : مهندس امین رضا دانشور

ویرایش اول

فهرست مطالب

مقدمه:

عصر تلفنهای هوشمند مزایای بیشماری را برای ما به ارمغان آورده است، ارتباطات بین انسانها را ساده کرده و دنیایی از امکانات را در زمینه های مختلف در اختیار ما قرار داده است تا حدی که گاهی ممکن با خود فکر کنیم چگونه پیش از این زندگی بدون تلفن های هوشمند و اینترنت امکانپذیر بوده است. در واقع خیلی از ما در انتهای شب آخرین چیزی را که میبینیم تلفن هوشمندمان می باشد و اولین چیزی که در صبح روز بعد چک میکنیم مجددا" همان صفحه تلفن هوشمندمان است.

اما آیا همه ما با خطراتی که حریم خصوصی ما را بخاطر استفاده از آیفون یا آیپد تهدید میکند آشنا هستیم؟

آیا میدانیم چگونه باید آیفون یا آیپد خود را در برابر آن تهدیدات امن نمائیم ؟

هر از مدتی خبرهایی از هک شدن و لو رفتن عکسهای خصوصی و اطلاعات شخصی ستارگان سینما و موسیقی و سایر اشخاص عادی و از بین رفتن حریم خصوصی ایشان را میشنویم که در مواردی هک آنها از طریق آیفون ایشان صورت پذیرفته است. در آن لحظه شاید خوشحال باشیم که چقدر خوب است که ما در جمع آنانی که هک شده اند قرار نداریم. اما بدانید که سپردن حفظ حریم خصوصی خود به شانس و اقبال روش درستی برای حفاظت از آن نیست. گاهی لو رفتن اطلاعات خصوصی شما ممکن است به قیمت جانتان تمام شود. پس این موضوع اصلا جای سهل انگاری ندارد. حریم خصوصی و اطلاعات شخصی ثروت بزرگی است که تا زمانیکه آنرا از دست ندهیم میزان ارزش آنرا درک نخواهیم کرد.

در جامعه ایران بالا رفتن ضریب نفوذ تلفنهای هوشمند در سالهای اخیر هر گوشی هوشمند را به یک هدف عالی برای هکرها و یک خطر امنیتی برای صاحبان آنها تبدیل کرده است. بعد از وقوع تعدادی ماجرا و حادثه هک شدن در اطرافیان خود و مشاوره هایی که در خصوص جلوگیری از این هک ها به آنها دادم متوجه شدم خطر نقص حریم خصوصی کاربران تلفنهای هوشمند در ایران بسیار بزرگتر از تصور می باشد، بعلاوه متاسفانه هیچ راهنمای جامع ، ساده و کاربردی برای کاربران آیفون و آیپد در ایران وجود ندارد. افراد با پرداخت میلیون ها تومان آیفون یا آیپدی میخرند و بدون اینکه چیزی از امنیت در فضای سایبری بدانند بلافاصله با آن تبدیل به هدفی احتمالی برای هکرها در آینده می شوند. تصور عمومی هم این است که اصولا" آیفون خیلی امن است و سیستم عامل iOS آن نسبت به سیستم عامل اندروید کاملا" ایمن است. اما با وجود اینکه سیستم عامل گوشی های شرکت اپل یکی از امن ترین سیستم عامل های تلفنهای همراه در جهان می باشد ولی کاربران آیفون و آیپد باید آگاه باشند که خطرات زیادی آنها را نیز تهدید میکند.

به سهم خویش تصمیم گرفتم از طریق انتشار این ایبوک بصورت تصویری و گام به گام شیوه بالا بردن امنیت آیفون و آیپد را طوری آموزش دهم که برای اکثر اقشار جامعه کاربران آیفون و آیپد مناسب باشد. با تحقیقاتی که انجام دادم مطالب مرتبط با موضوع کتاب بصورت کاملا پراکنده و نامنظم در اینترنت یافت میشوند پس کتاب را طوری طراحی کردم که شما بتوانید با نگاه کردن به فهرست مطالب متوجه شوید کدام قسمت از جنبه های امنیتی را برای آیفون یا آیپد خود فعال نکرده اید یا اصلا" در مورد آن اطلاع نداشته اید.

اعتقاد دارم حتی حرفه ای ترین کاربران آیفون نیز میتوانند مطالبی را در این کتاب پیدا کنند که شاید قبلا" از آنها کمترین آگاهی نداشته باشند. هرچند خود را نیز کامل نمیدانم و همواره اعتقاد به خرد جمعی دارم.

این کتاب با ارائه دستورالعملهایی تصویری و بصورت ساده و گام به گام، روش بالا بردن امنیت را در هر بخش از آیفون یا آیپد را به شما آموزش می دهد تا در آینده هکرها و سایر افراد شریر نتوانند وارد حریم خصوصی شما شده و زندگی شما را نابود کنند.

رفع مسئولیت (Disclaimer) :

اجرای اشتباه یا ناقص برخی از دستورالعمل های این کتاب ممکن است باعث پاک شدن اطلاعات آیفون یا آیپد شما بشود. نویسنده این کتاب هیچ مسئولیتی در این خصوص ندارد و شما متقبل می شوید از حداقل دانش لازم برای انجام آن دستورالعمل ها برخوردار هستید. لطفا" اگر نیاز به کمک برای انجام برخی از دستورالعملهای این کتاب دارید از دوستان مطلع و قابل اعتماد خود استفاده نمائید و گرفتن Backup از آیفون و آیپد خود را هرگز فراموش نکنید.

حق کپی :

تنظیمات امنیتی پایه در بالا بردن امنیت دستگاه شما

مواردی که در این بخش توضیح میدهیم اساسی و پایه می باشند و پرداختن به بخش های بعدی حفظ امنیت مانند این می باشد که ما برای پنجره های خانه خود دزدگیر نصب کنیم ولی در خانه را باز بگذاریم. پس آگاهی و رعایت نکات مطرح شده بسته به سطح امنیتی که نیاز دارید ضروری می باشد.

نکته ۱) حفاظت از پسورد Apple Id

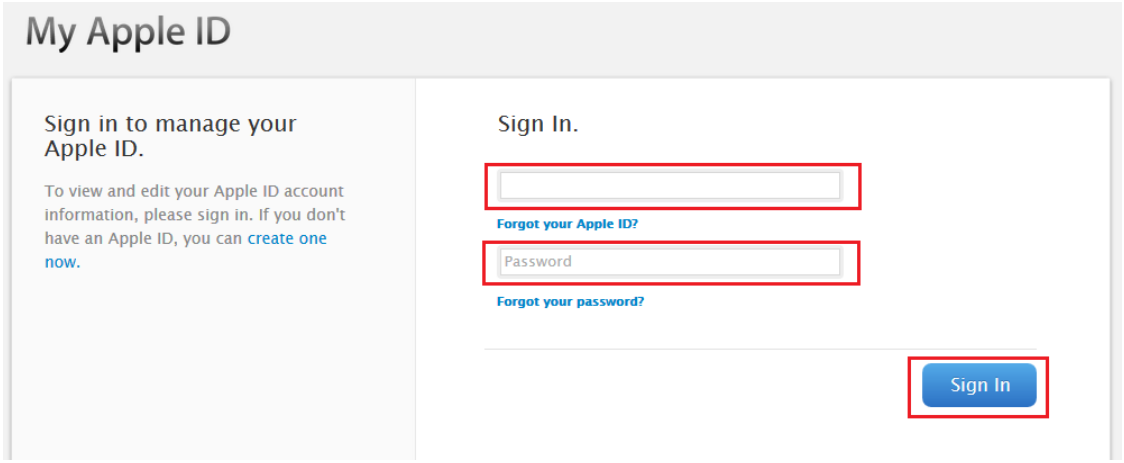
هر دستگاه اپلی مثل آیفون یا آیپد برای نصب اپ های کاربر نیاز به یک اکانت بنام Apple Id دارد که در واقع یک ایمیل و پسورد می باشد و بدون آن نمیتوان از همه امکانات دستگاه خود بهره برداری نمائید. اما نکته مهم تر در مورد Apple Id این است که رمز Apple Id شما همانند رمز حساب بانکی شما محرمانه و شخصی می باشد و هیچکس مانند فروشنده آیفون ، همکار یا دوست نباید از آن آگاه باشد!

و اگر فکر میکنید کسی جز شما از رمز اپل آی دی شما آگاه هست همین الان از طریق روش زیر رمز عبور Apple Id خود را عوض نمائید.

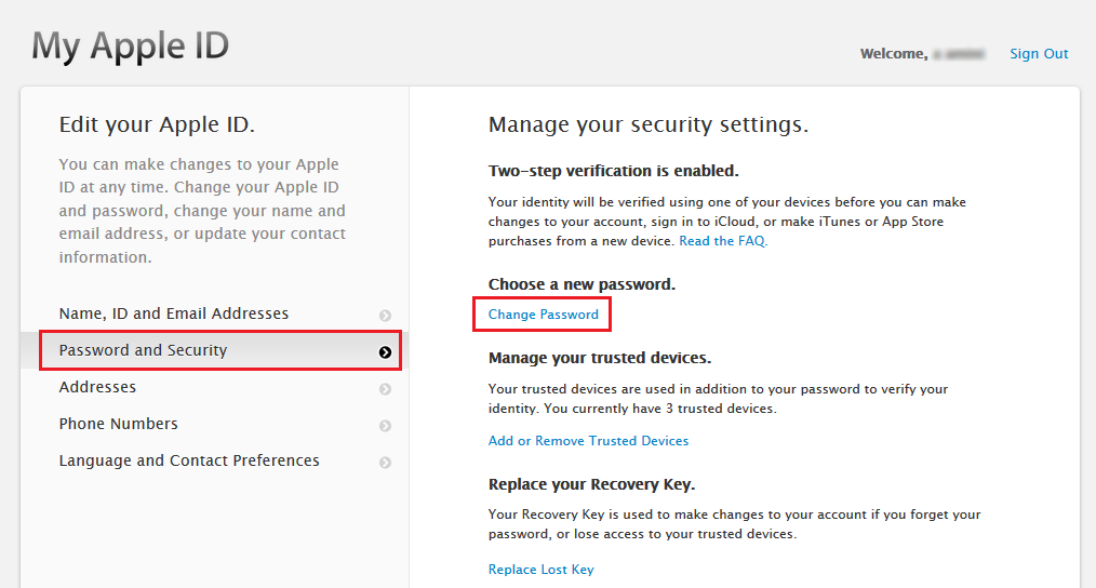
پیشنهاد میکنیم رمز شما حداقل باید ۱۵ کاراکتر شامل حروف، اعداد و سمبول ها باشد و فکر رمزهای کوتاهتر را از سر خود بیرون کنید چون باعث می شود در آینده هدف ساده ای برای هکر ها باشید.

روش گام به گام برای عوض کردن رمز Apple Id

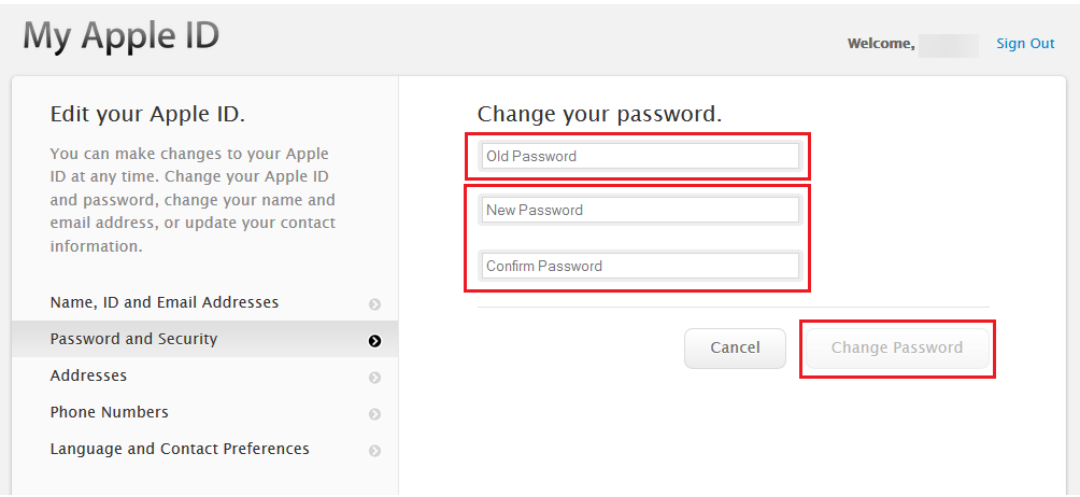
ابتدا به آدرس https://appleid.apple.com/signin در مرورگر کامپیوتر خود بروید.



سپس با ایمیل و پسورد قبلی خود وارد حساب Apple Id خود شوید



گزینه Change Password را انتخاب نمائید.



و در پایان رمز قبلی خود ، کلمه عبور جدید و تکرار آنرا وارد نمائید و با زدن دگمه Change Password با خیال راحت رمز Apple id خود را عوض نمائید.

نکته : توصیه میکنیم از تایپ پسورد جدید خود با استفاده از کیبورد کامپیوتر خودداری نمائید چون ممکن است بر روی کامپیوتر شما نرم افزار Key logger که کارش دزدیدن کلمات عبور و انتقال آن به هکر است نصب شده باشد، استفاده از کیبوردهای مجازی (Virtual Keyboard) که یک شبیه سازی از کیبورد واقعی بصورت نرم افزار می باشد گزینه بهتری است زیرا شما با کلیک کردن بر روی دگمه های آن کاراکترهای مورد نظرتان را در جایی که مکان نما در آن قرار دارد تایپ می کنید و با این روش اگر نرم افزار Key logger روی سیستم شما نصب باشد نمیتواند پسورد جدید شما را بدزدد.

هم برای کامپیوترهای مک و هم کامپیوتر های ویندوزی نرم افزاری بنام On-Screen Keyboard وجود دارد که بسادگی فعال میگردد و میتواند اینکار را برای شما انجام دهد.

تصویری از کیبورد مجازی

دلایل محرمانه بودن Apple Id چیست و چه خطراتی در صورت لو رفتن آن شما را تهدید میکند؟

۱. هکر میتواند در صورتیکه Photo Stream را در آی کلود فعال کرده باشید کلیه عکسهای خصوصی شما را مشاهده نماید.
۲. هکر میتواند بکاپهای گوشی شما را که روی iCloud تهیه کرده اید دانلود کرده و همه اطلاعات درون آنرا استخراج نماید.
۳. هکر میتواند به لیست تماسها (Contact list) شما دسترسی پیدا کند و متوجه شود شما با چه کسانی در ارتباط هستید.
۴. هکر میتواند در صورت فعال بودن گزینه Find My iPhone موقعیت جغرافیایی شما را در محل کار یا محل زندگی یا در هرمحل دیگری تشخیص دهد.

موارد بالا تنها بخشی از سناریوی ترسناکی است که میتواند برای شما اتفاق بیفتد پس لطفا در خصوص اپل آی دی خود به هیچ عنوان تنبلی نکنید و از پسورد با خصوصیات گفته شده استفاده کنید و آنرا در اختیار هیچ شخصی قرار ندهید. در آموزشهای آتی روشهای حفاظت کاملتر از Apple Id و حساب iCloud را بصورت تصویری و گام به گام به شما آموزش میدهیم.

نکته ۲) ارتقاء iOS به آخرین نسخه

شرکت اپل هر از مدتی نسخه جدیدی از نرم افزار سیستم عامل iOS شما را منتشر میکند. که هر نسخه جدیدتر شامل افزودن امکانات جدید نرم افزاری جدید به ای دیواس شما یا بستن نفوذ پذیری های امنیتی کشف شده و خطاهای نرم افزاری می باشد.

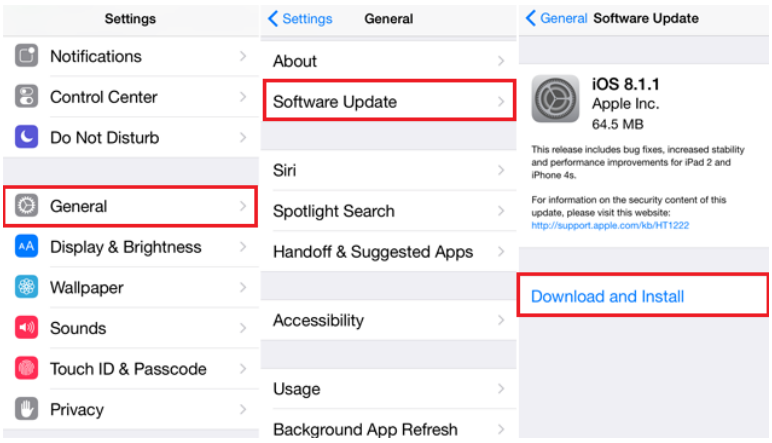
در واقع سیستم عامل iOS نرم افزار مادر و مهمی است که بین سخت افزارها و اجزای ای دیوایس شما و اپ هایی که از اپ استور نصب و اجرا میکنید قرار میگیرد و تفسیر و اجرای اپ ها و نحوه دسترسی به سخت افزارهایی مثل دوربین آیفون یا جی پی اس آیفون یا شیوه ارتباط با حافظه دستگاه و سایر سخت افزارها توسط اپ ها و غیره را به عهده دارد.

چگونه میتوانم iOS را در آیفون یا آیپد بروز رسانی کرد؟

دو روش برای بروز رسانی آیفون وجود دارد:

راه اول) درصورتیکه آیفون شما به اینترنت پرسرعت از طریق وای فای یا سیم کارت متصل باشد شما همواره میتوانید با مراجعه به بخش Setting مطابق راهنمای زیر متوجه شوید که یک بروز رسانی جدید برای ای دیوایس شما آماده دانلود و نصب می باشد.

راه دوم) دانلود نسخه جدید سیستم عامل ای او اس با پسوند ipsw از سایت *https://**ipsw**.me* و گرفتن بک آپ از گوشی و نصب نسخه جدید ای او اس با کمک ای تونز میباشد. لینک فایل ipsw در این سایت مطابق با مدل دستگاه شما نمایش می یابد و در زمان دانلود شما این فایل را مستقیما از سایت apple.com دانلود خواهید کرد. زیرا تنها فایلهایی که از سایت اپل دانلود شوند قابل اعتماد می باشند.



تنظیمات پیشنهادی برای بروز رسانی سیستم عامل آیفون

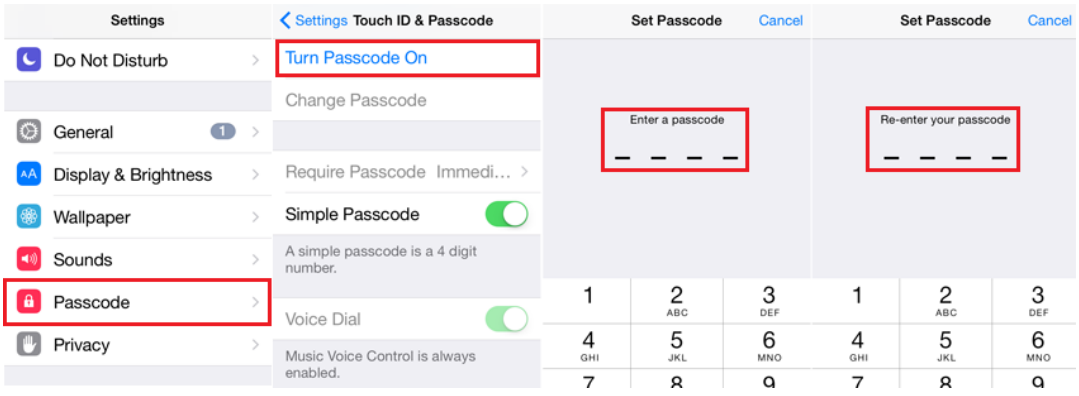
نکته ۳) رمز عبور دستگاه خود را فعال نمائید.

اولین سد دفاعی در برابر دسترسی غیر مجاز به تلفن هوشمند شما فعال کردن رمز عبور آن می باشد. بعضی اشخاص برای سادگی در دسترسی به گوشی خود آنرا فعال نمیکنند و این اشتباه بزرگی می باشد. زیرا اگر گوشی شما توسط کسی سرقت شود همین مانع می تواند تا حدود زیادی از دسترسی او به اطلاعات درون گوشی شما جلوگیری کند.

چگونه میتوان رمز عبور آیفون را فعال کرد؟

اگر گوشی شما فاقد مکانیزم Touch ID (شناسایی اثر انگشت) باشد:

۱. مطابق تصویر زیر به بخش Setting >Passcode
۲. کلمه و تکرار آنرا وارد نمائید.



تنظیمات پیشنهادی برای فعال سازی Passcode

اگر گوشی دارای مکانیزم Touch ID باشد:

۳. مطابق تصویر زیر به بخش Setting >Touch ID & Passcode
۴. کلمه و تکرار آنرا وارد نمائید.

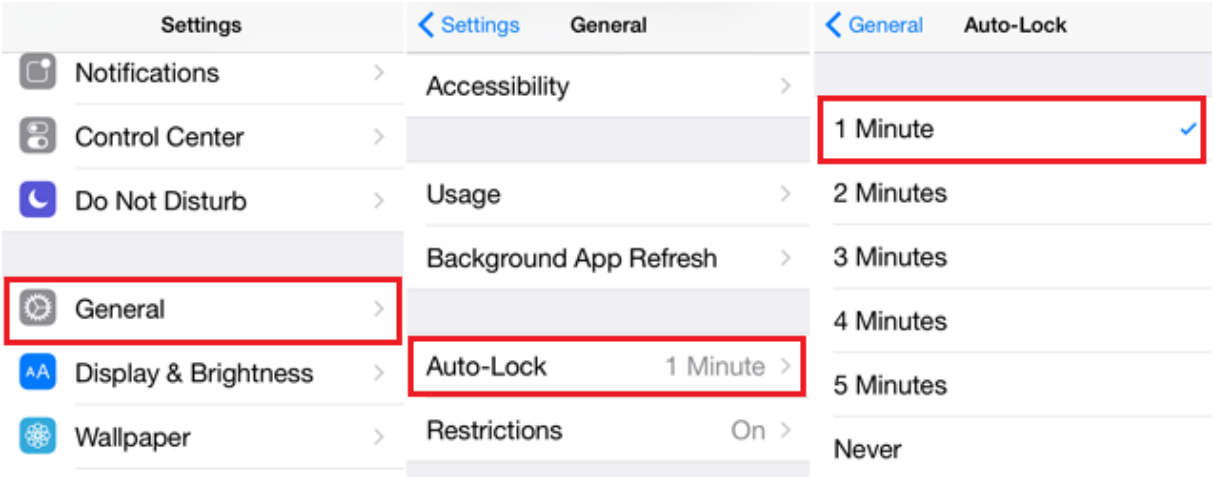
تنظیمات پیشنهادی برای فعال سازی Passcode

از انتخاب کلمات عبور ساده ای مثل ۱۲۳۴ یا ۰۰۰۰ یا چهار رقم آخر شماره تلفن همراه شما یا تاریخ تولد و موارد مشابه که با دانستن اطلاعات عمومی هویتی شما قابل دستیابی است خودداری کنید.

یک قانون عمومی در مورد هر کلمه عبوری در دنیا وجود دارد و آن این است که آنرا بعد از مدتی عوض کنید. برای آیفون پیشنهاد ما تعویض این رمز بعدا از حداکثر سه ماه می باشد.

نکته ۴) زمان فعال شدن Passcode را کاهش دهید.

آیفون این قابلیت را دارد که پس از گذشت زمان مشخصی که دستگاه بدون فعالیت بود قفل شود و پس از آن برای استفاده مجدد از دستگاه Passcode از شما پرسیده شود. البته این پیش فرض بصورت اتوماتیک در هنگام فعال سازی Passcode وجود دارد ولی هرچه این زمان بیشتر شود امنیت دستگاه شما کاهش می یابد. فرضا" افزایش این زمان به پنج دقیقه به افراد دیگر اجازه میدهد تا ۵ دقیقه از آخرین لحظه ای که شما از آیفون خود استفاده کرده اید بتوانند بدون زدن Passcode به اطلاعات گوشی شما دسترسی داشته باشند. پیشنهاد میشود این زمان را به یک دقیقه کاهش دهید.



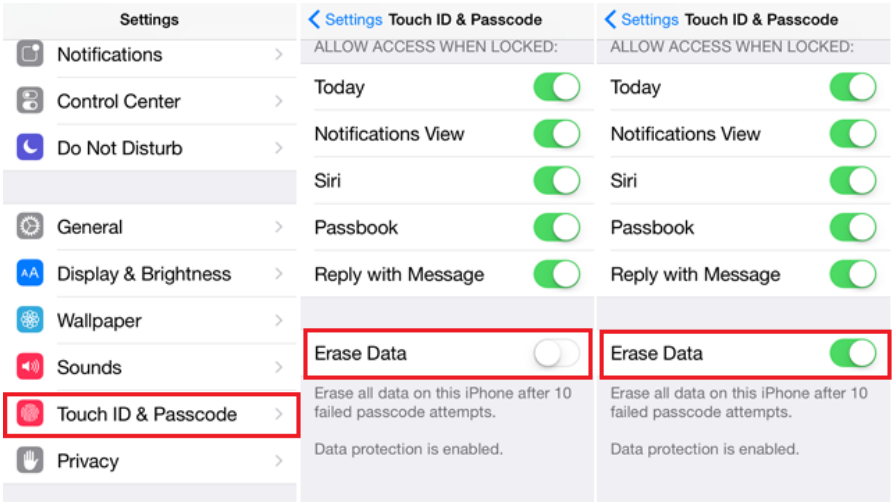
تنظیمات پیشنهادی برای Auto-lock

نکته ۵) فعال کردن پاکسازی اطلاعات(Enable Erase Data)

فرض کنید آیفون شما سرقت می شود. اولین کاری که یک دزد سعی میکند انجام دهد عبور از سد Passcode می باشد که شما آنرا قبلا فعال کرده بودید. او بارها و بارها از طریق روش Brute-force سعی می کند کلمات عبور متفاوتی را برای رمز ۴ یا ۶ رقمی شما انتخاب کند تا بلکه بتواند از این مانعی که وجود دارد عبور کند و این موضوع بنظر کمی ناراحت کننده می آید چون ۴ رقم یا ۶ رقم کلمه عبور آنقدر زیاد نیست که بتواند جلوی کسی را گوشی شما برای مدت نامحدود در اختیار دارد برای مدت طولانی بگیرد. پاکسازی اطلاعات آیفون درصورت تکرار اشتباه در ورود Passcode در آیفون وجود دارد ولی بصورت پیش فرض فعال نمی باشد.

شاید بنظر شما هم فعال سازی این امکان امنیتی در آیفون ترسناک می آید چون واقعا این امکان می تواند اطلاعات شما را کاملا پاک کرده و غیر قابل بازیابی نماید. ممکن است در ذهن خود تصور کنید کودک شما یا بچه ای از فامیل شما ممکن است از روی کنجکاوی آیفون شما را برداشته و چندین بار رمز عبور شما را وارد نمائید تا بتواند به اپ های بازی درون گوشی دسترسی پیدا کند.

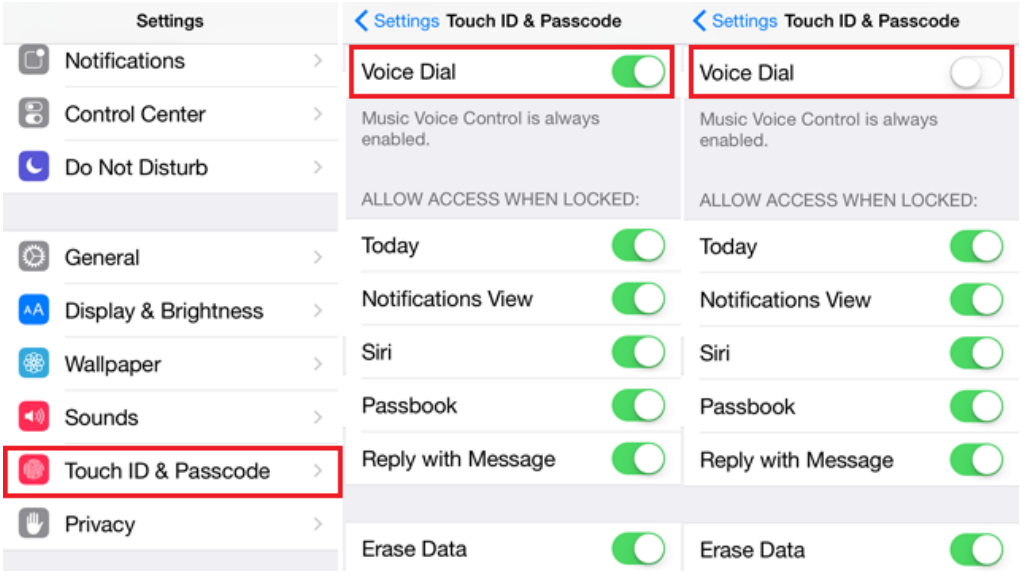
اما باید بگوییم که فعال شدن این امکان بدین گونه است که در نخستین باری که Passcode اشتباه وارد می شود آیفون برای یک دقیقه قفل میشود و اجازه ورود Passcode دیگری را نمیدهد. در تلاش بعدی آیفون برای ۵ دقیقه قفل می شود و این زمان تا ۳۰ دقیقه برای تکرارهای آخر این تلاش برای ورود به آیفون افزایش می یابد. و در بار دهم و در آخرین اقدام ناموفق است که سیستم کلیه اطلاعات شما را پاکسازی کامل میکند. و بنظر نمیرسد کسی این همه زمان در اختیار داشته باشد که بتواند تمام این مراحل را رد کند مگر اینکه به گونه تلفن شما دزدیده یا گم شده باشد.



چگونگی فعال سازی Erase data

نکته ۶) امکان تماس تلفنی بدون ورود Passcode را بگیرید.

نرم افزار دستیار صورتی "Siri" این امکان را دارد که با فشردن و نگه داشتن دگمه Home و با گفتن کلمه "Dial" به کسانی که در لیست تماس شما هستند تماس بگیرد. و اینکه یک نفر که به گوشی شما دسترسی غیر مجاز د دارد بتواند بدون زدن Passcode با گفتن این کلمه با کسی تماس بگیرد یا با گفتن عبارت "Send Message" بتواند برای شخصی در لیست تماس از طرف شما پیام کوتاه بفرستد و این نقص حریم خصوصی شما می باشد پس این امکان را غیر فعال نمائید.

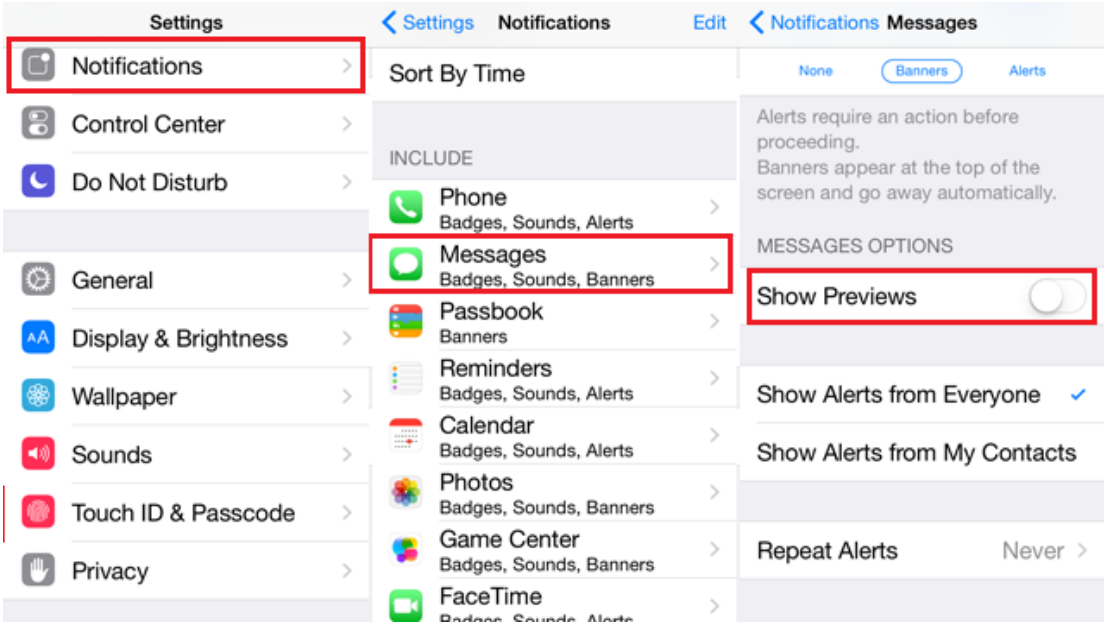


چگونگی غیرفعال کردن دسترسی Siri به امکان تماس بدون داشتن Passcode

نکته ۷) غیر فعال کردن امکان نمایش اتوماتیک SMS های رسیده بر روی صفحه آیفون

بصورت پیش فرض کلیه پیام های کوتاهی که برای شما ارسال میشوند بطور اتوماتیک بر روی صفحه نمایش می یابند. این امکان برای آسایش و راحتی شما فعال شده است ولی بعضی از سیستم های بانکی و بسیاری از اپ ها از SMS برای فرستادن اطلاعات حساس مثل کد فعال سازی نرم افزارهای ارتباطی یا حتی ریست کردن رمز عبور شما در اپ ها و نرم افزارهای مختلف استفاده میکنند.

یک هکرکه شماره شما را بداند می تواند حتی بدون دزدیدن گوشی شما در یک مهمانی یا محل کار یا در یک فرصت مناسب تنها برای دقیقه ای با گوشی شما تنها باشد و اپ مشابه را روی گوشی خود داشته باشد و تنها با رفتن به قسمت ریست کردن رمز عبور اپ ، شماره شما را بعنوان شماره ای که تقاضای ریست کردن رمز عبور را داده است ارسال کند و سپس در هنگام رسیدن کد تائید یا رمز عبور جدید براحتی و بدون دانستن Passcode شما و تنها با دید زدن پیش نمایش SMS رسیده روی صفحه آیفون شما و خواندن آن و سپس ورود کد رسیده در اپ موجود بر روی گوشی خود رمز عبور اپ شما را عوض کرده و با هویت و شماره شما وارد اپ شود و سپس با کسانیکه با شما در ارتباط می باشند و با شماره شما و بجای شما ارتباط برقرار کرده و مشکلات بعدی را برای امنیت و حریم خصوصی و نزدیکانتان بوجود آورد.



چگونگی غیرفعال کردن حالت پیش نمایش SMS

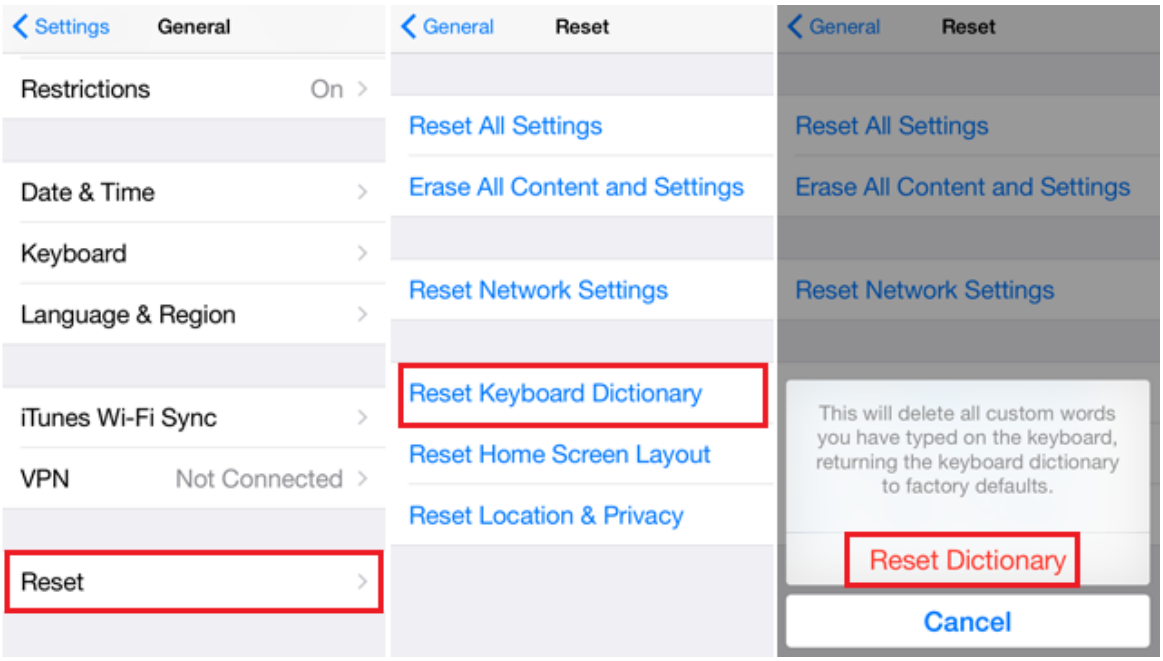
نکته ۸) پاک کردن دیکشنری صفحه کلید.

آیا میدانستید بخاطر معماری که iOS دارد و در جهت بهبود سرعت و پیش بینی کلمات تایپ شده توسط شما بوسیله آیفون و آیپد کلیه کلماتی که شما تایپ میکنید بگونه ای در حافظه دستگاه ذخیره میشود؟

این کلمات تایپ شده در یک لیست تقریبا ۶۰۰ کلمه ای قرار میگیرند.

این کلمات میتوانند شامل اطلاعات حساسی نیز گردند. اگر چه iOS ورودی های حساس مثل پین کدها و شماره کارتهای اعتباری را در این لیست ذخیره نمیکند ولی کلماتی مثل نام کاربری یا پاسخ به سوال های امنیتی پرسیده شده توسط اپ ها و سایر کلمات حیاتی می توانند در این لیست ذخیره شوند!

یک هکر میتواند با کمی تلاش به این اطلاعات دست پیدا کند. بنابراین لازم است هر از مدتی این دیکشنری کیبورد را خالی نمائید تا بعدا مورد سوء استفاده دیگران قرار نگیرد.

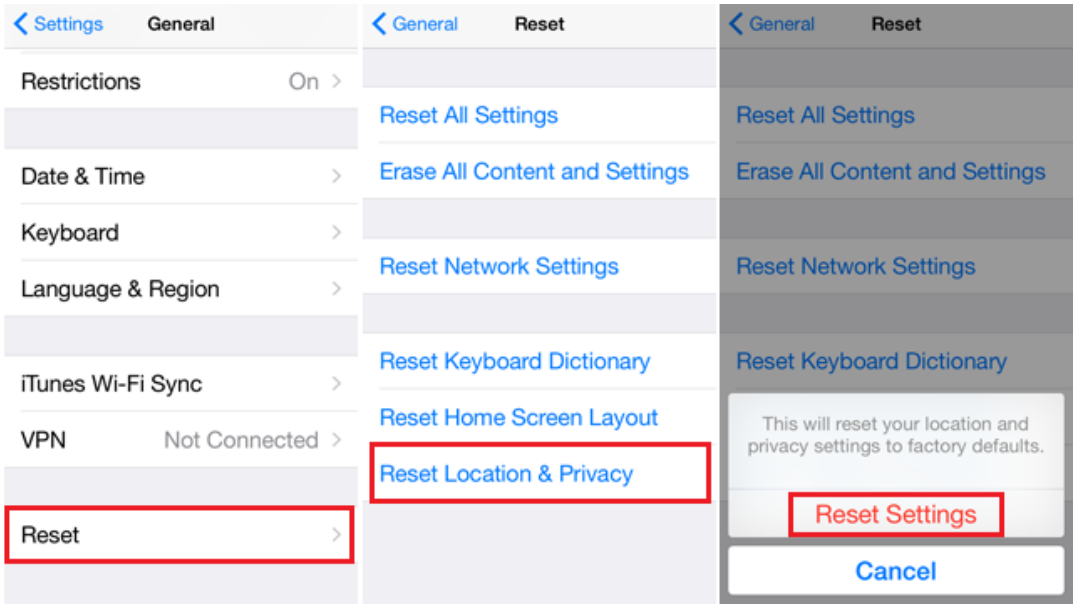


چگونگی پاک کردن حافظه دیکشنری صفحه کلید

نکته ۹) پاک کردن اطلاعات موقعیت های جغرافیایی که شما در آنها تردد داشته اید.

زمانیکه شما از امکان Find My iPhone استفاده میکنید تا بوسیله آن بتوانید به محل گوشی خود در زمان گم شدن دسترسی پیدا کنید در واقع اجازه میدهید همیشه مورد ردیابی قرار بگیرید.

زمانیکه حس میکنید تمایلی ندارید که آخرین محلهایی که شما با آیفون خود بوده اید مورد ردیابی قرار گیرد بهتر است با استفاده از Reset Location And Privacy این اطلاعات حساس را پاک نمائید.

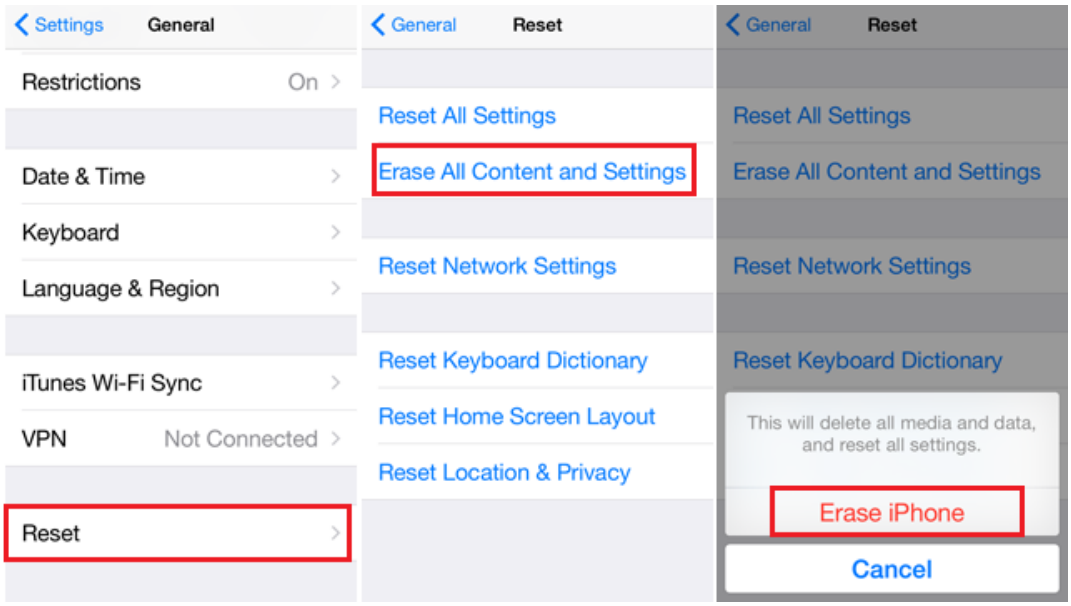


چگونگی پاک کردن اطلاعات ردیابی موقعیت گوشی شما

نکته ۱۰) حذف ایمن اطلاعات از روی آیفون یا آیپد

در زمان فروش یا بخشیدن گوشی خود اطلاعات خود را بصورت ایمن از روی دستگاه خود پاک کنید.در نظر داشته باشید که یک هکر می تواند اطلاعات شما شامل تصاویر ، فیلم ها ، پیامهای کوتاه ، لیست تماس و غیره را بازیابی نماید. بنابراین باید از یک روش ایمن و غیر قابل بازیابی برای حذف این اطلاعات استفاده نمائید. خوشبختانه iOS این امکان را برای شما تدارک دیده است.

در موقعیت هایی که حس میکنید ممکن است بزور گوشی شما توسط افرادی از شما گرفته شود و از اطلاعات درون گوشی شما برعلیه شما استفاده گردد از این گزینه برای نابودی اطلاعات خود استفاده کنید. منتها در نظر بگیرید که پاکسازی کامل گوشی شما نیازمند زمان می باشد و بصورت آنی انجام نمیشود.



چگونگی پاک کردن ایمن تمام اطلاعات آیفون

نکته ۱۱) حذف اطلاعات تصویر گرفته شده و ذخیر شده از اپ در زمانیکه دگمه Home را فشار میدهید.

فشار دادن دگمه Home در آیفون باعث پنهان شدن اپ فعلی و قرار گرفتن آن در پشت زمینه میشود. منتها آیا میدانستید که در لحظه فشردن دگمه Home یک تصویر از وضعیت فعلی اپ شما برداشته میشود؟ درست به مانند گرفتن یک عکس از صفحه آیفون.

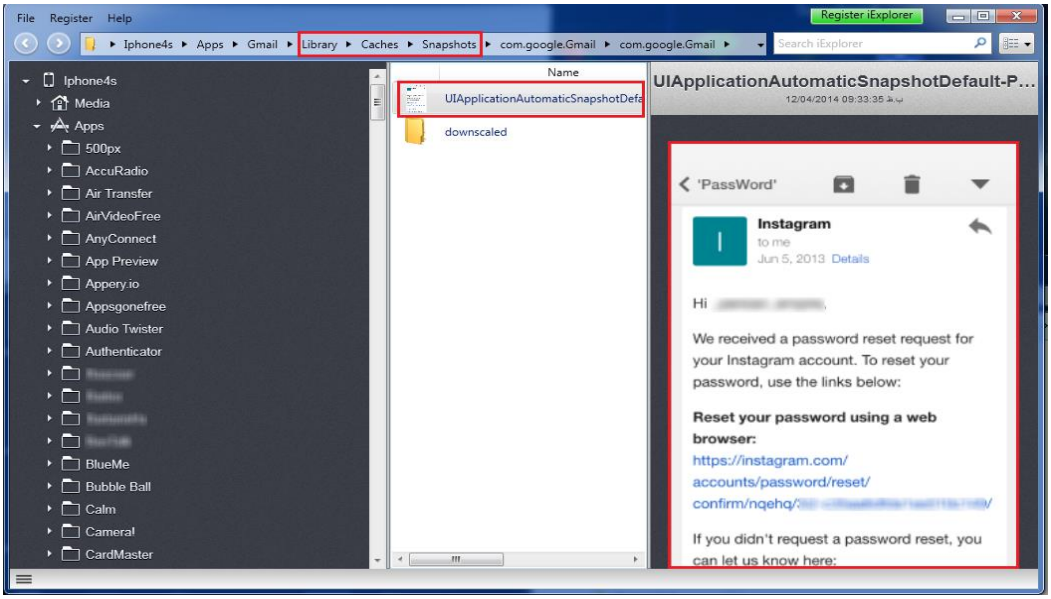
iOS از اپ ها میخواهد که در لحظه فشرده شدن دگمه Homeیک تصویر Snapshot از اپ برای استفاده در لیست اپ های پشت در اختیارش قرار دهند تا شما برای حذف هر اپ از حافظه یا فعال سازی مجدد آن اپ بتوانید آن اپ را با تصویرش تشخیص دهید.

اما iOS هرگز به سازندگان آپ ها نگفته بود که دربخشهای حساس که کاربران اپ ها درحال تماشا و بررسی اطلاعات شخصی خود می باشند اقدام به تهیه تصویر Snapshot نمایند. این تصویر توسط ابزار زیادی که کار مدیدیت فایلهای آیفون از طریق پی سی یا مک را انجام میدهد قابل دیدن می باشند. جالب اینجاست که آدرس این تصویر گرفته شده در فولدری با نام Library/Caches/Snapshots در زیر شاخه اصلی هر آپ می باشند. و نیازی به جستجو برای پیدا کردن این تصاویر به ازای هر آپ نمی باشد.

تصور کنید در لحظه فشردن دگمه Home شما تصویر شخصی خود را تماشا میکردید یا درحال خواندن ایمیلی مهم و محرمانه یا کار با یک اپ که اطلاعات حساس بانکی را ذخیره کرده است می باشید. بنابراین اگر سازندگان اپ بی توجهی کنند تصویری از این اطلاعات در گوشی شما ذخیره میشود.

متاسفانه حتی اپ هایی معروفی مثل اینستاگرام و جیمیل نیز از این مشکل مستثنا نمی باشند.

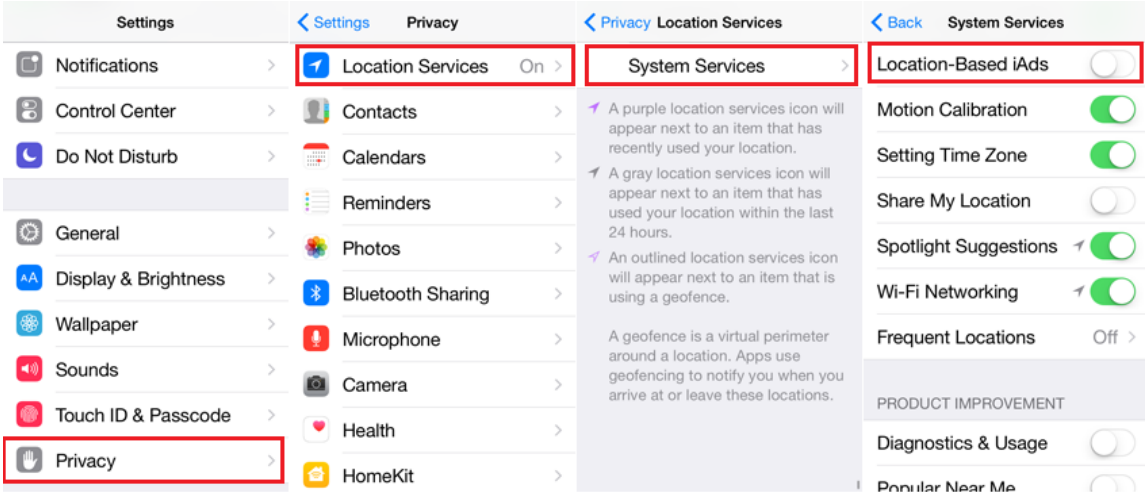
برای پاک کردن این اطلاعات شما باید گوشی خود را یک بار Soft Reset نمائید.Soft Reset کردن آیفون باعث پاک شدن اطلاعات این تصاویر ذخیره شده از حافظه داخلی آیفون می شود. برای سافت ریست کردن دگمه home و دگمه پاور آیفون را برای حدود ۱۰ ثانیه باهمدیگر فشار دهید.



کاربر در لحظه خواندن ایمیل خود کلید home را فشرده است و الان تصویری از آن ایمیل بوجود آمده است.

نکته ۱۲) غیر فعال کردن Location-Based iAds

این گزینه به تبلیغ کنندگان امکان میدهد که موقعیت جغرافیایی آیفون شما را در هر لحظه بدست آورده و بر اساس آن تبلیغات مرتبط را روی اپ های خود نمایش دهند. هرچند اپل مدعی است که جز این موضوع اطلاعات دیگری در اختیار شرکتهای تبلیغ کننده قرار نمیگیرد ولی بهتر است برای تقویت حریم خصوصی خود این گزینه را غیر فعال نمائید.

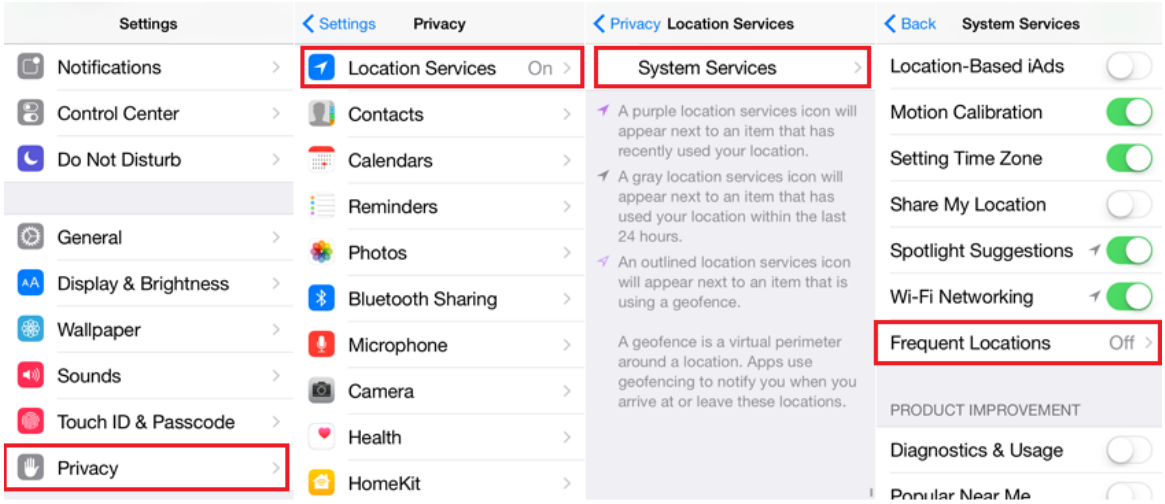


چگونگی غیر فعال کردن امکان Location-Based iAds

نکته ۱۳) غیر فعال کردن Frequent Locations

این گزینه به گوشی شما اجازه میدهد که در مورد مکانهایی که شما بیشتر در آنها به همراه آیفون خود تردد دارید اطلاعاتی جمع آوری کند. البته هرچند هدف اپل از اینکار ارائه خدمات مفید بر اساس موقعیت جغرافیایی به شما می باشد. ولی آیا علاقه دارید اگر گوشی شما گم یا دزدیده شد یک هکر بتواند به اطلاعاتی مثل محل زندگی ، محل کار ، مسیرهای ورزشی شما و محل خانواده شما دسترسی داشته باشد؟

پس بهتر است این گزینه نیز کاملا غیرفعال گردد.



چگونگی غیر فعال کردن امکان Frequent Locations

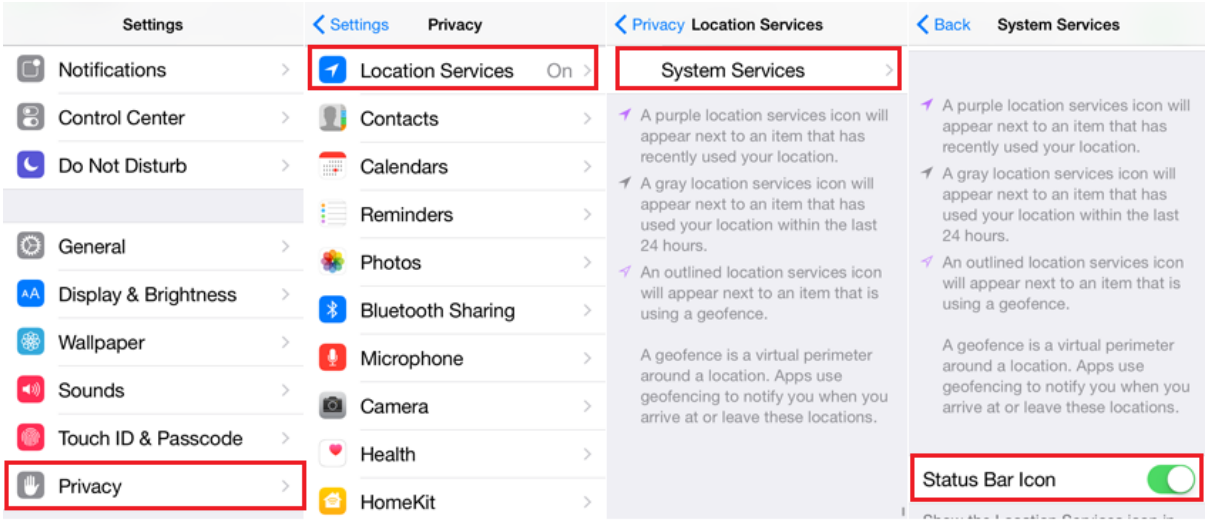
نکته ۱۴) فعال کردن Location Status Bar Icon

این آیکن که در کنار فهرست اپ هایی که در بخش System Services لیست شده اند و اجازه دارند از موقعیت جغرافیایی شما استفاده کنند قرار میگیرد و نشانگر وضعیت استفاده اپ ها از موقعیت جغرافیایی شما می باشد. این نشانگر در چند رنگ نمایش می یابد که هر رنگ معنی بخصوصی دارد. در حالت پیش فرض این آیکن غیر فعال می باشد.

رنگ بنفش : نشان میدهد اپ از موقعیت جغرافیایی شما استفاده کرده است

رنگ خاکستری : نشان میدهد اپ در ۲۴ ساعت گذشته از موقعیت جغرافیایی شما استفاده کرده است.

حالت نمایشی توخالی (outlined) : بیانگر این است که اپ تشخیص داده است شما وارد یک محدوده خاص شده اید.



چگونگی فعال کردن آیکن وضعیت استفاده از موقعیت جغرافیایی

نکته ۱۵) جلوگیری از ردیابی شما توسط سایتها:

هر گوشی آیفون دارای یک کد منحصر بفرد ۴۰ حرفی بنام UDID (Universal Device Identifier) می باشد که معمولا توسط تبلیغ کنندگان برای ردیابی کاربران موبایل در سطح وب مورد استفاده قرار میگرفت. اپل در سپتامبر ۲۰۱۲ جلوی دسترسی تبلیغ کنندگان را به این شماره سریال گرفت و در عوض یک به ازاء هر آیفون یک شماره سریال دیگر بنام Advertising Identifier در اختیار تبلیغ کنندگان و صاحبان اپ ها قرار داد. هرچند با اینکار حریم خصوصی کاربران بالاتر رفت ولی این موضوع کافی نیست.

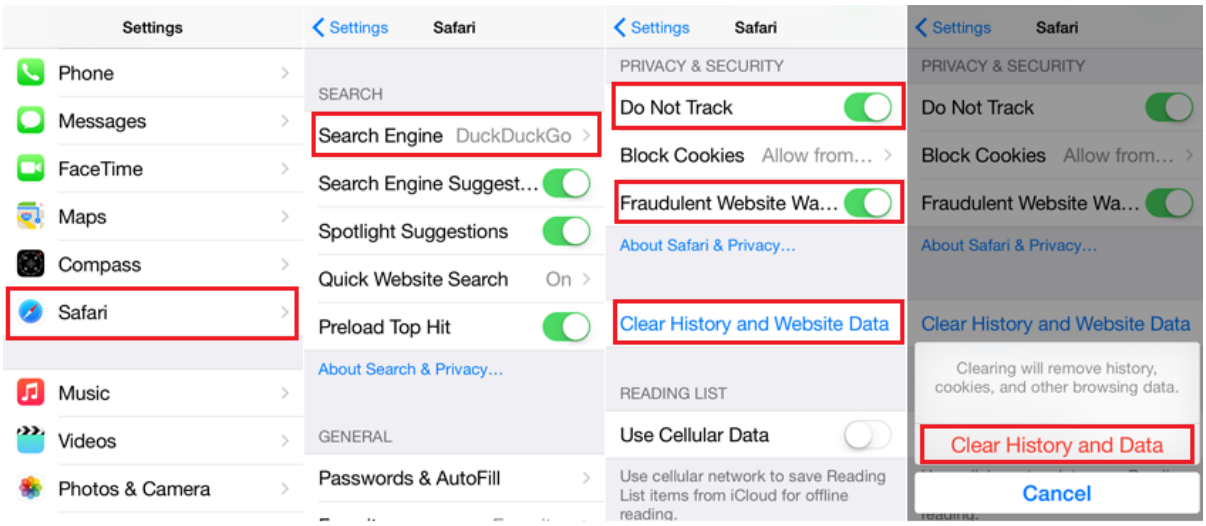
زیرا همچنان سایتها و تبلیغ کنندگان به Advertising Identifier دسترسی دارند و عدم آگاهی کاربران از جلوگیری به این شماره سریال یا حتی عوض کردن گاه به گاه آن باعث ردیابی بسیاری از کاربران آیفون شده است. پس در گام نخست بهتر است که جلوی دسترسی به این شماره سریال نیز گرفته شود یا هر از مدتی این شماره سریال را عوض نمود.

چگونگی جلوگیری از ردیابی تبلیغ کنندگان و سایتها

نکته ۱۶) بالا بردن امنیت مرورگر Safari

یک سری تنظیمات در iOS وجود دارد که باعث میشود با امنیت بالاتری از مرورگر سافاری استفاده کنید.

بعنوان مثال استفاده از موتور جستجوی امن DuckDuckGo که هیچگونه اطلاعاتی را از جستجوی شما جمع آوری نمیکند بجای Google یا پاک کردن اطلاعات ذخیره شده از سایتهایی که استفاده کرده اید.



بالابردن حریم خصوصی در مرورگر سافاری

نکته ۱۷) فعال کردن Find My iPhone

ویژگی Find My iPhone این توانائیهای زیر را در اختیار شما قرار میدهد:

- پیدا کردن موقعیت جغرافیایی آیفون/ آیپد خود :

در واقع اگر گوشی خود را جا بگذارید یا اگر گوشی شما دزیده شود میتوانید به موقعیت تقریبی آن دسترسی پیدا کنید البته به شرطی که گوشی شما به اینترنت متصل باشد.

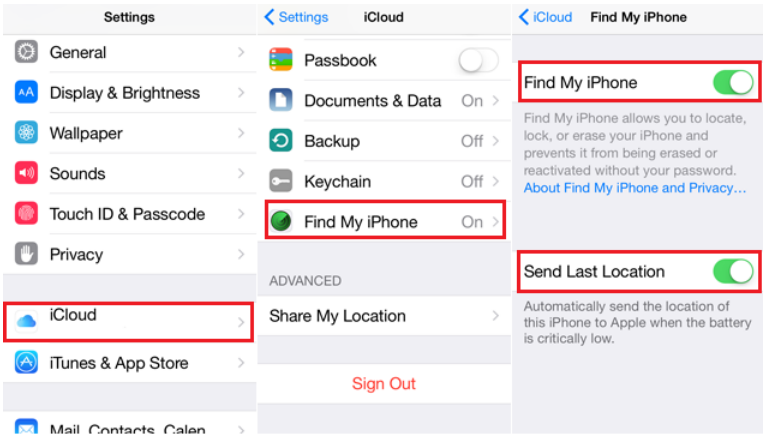
- امکان فعال سازی آلارم برای پیدا کردن دستگاه خود در محل خود از روی صدا
- امکان پاک کردن اطلاعات شما از راه دور :

اگر آیفون گم شده یا دزدیده شما حاوی اطلاعات ارزشمند خصوصی شما بود و شما مایل نیستید تحت هیچ شرایطی این اطلاعات در اختیار کسی قرار بگیرد از راه دور میتوانید این اطلاعات را پاک کنید.

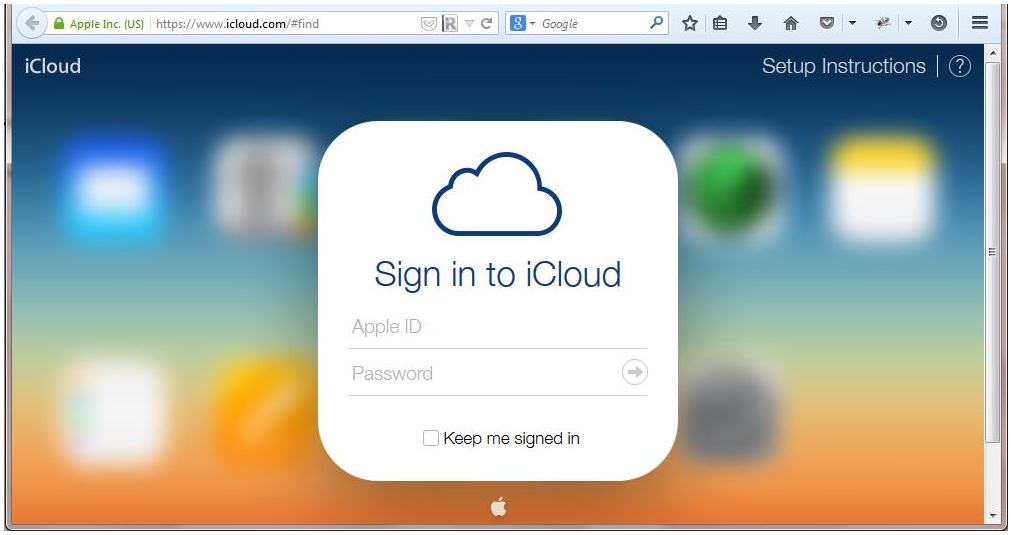
- دریافت آخرین موقعیت جغرافیایی دستگاه شما از طریق ایمیل
- فرستادن پیام یا شماره تلفن بر روی صفحه آیفون یا آیپد برای ارتباط با شخصی که دستگاه شما را پیدا کرده است.

روش فعال سازی :

۱. از مسیر زیر گزینه Find My iPhone را در آیفون یا آیپد خود فعال کنید.



۲.به سایت https://www.icloud.com/#find مراجعه کنید.



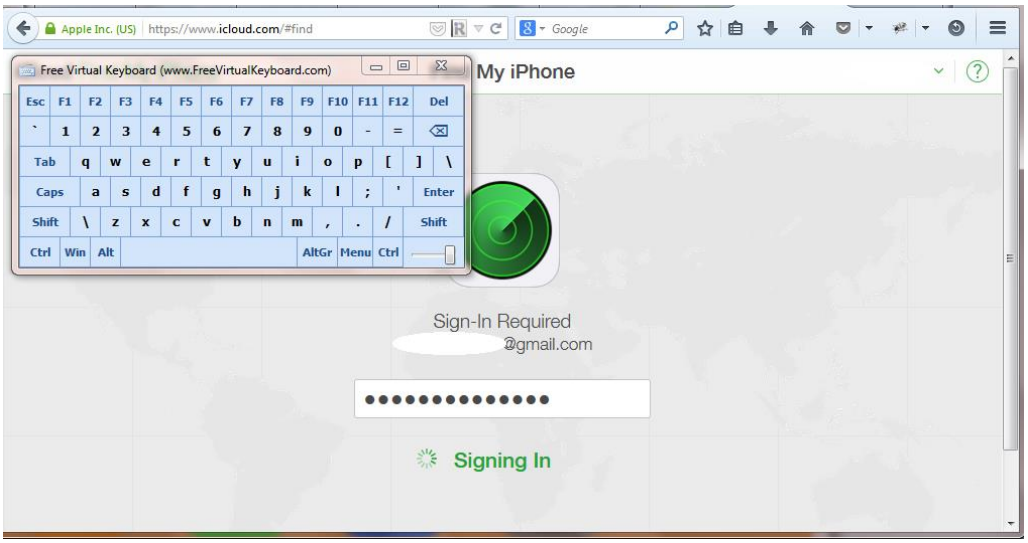
۳.اپل ایدی خود به همراه رمز عبور را با رعایت موارد امنیتی وارد نمائید.

توجه۱ : لو رفتن رمز شما عواقب بسیار بدی میتواند داشته باشد پس برای اطمینان بیشتر و جلوگیری از دزدیده شدن رمز عبور خود توسط نرم افزارهای Key logger شما میتوانید از یک صفحه کلید مجازی مثل On-Screen Keyboard در مک یا ویندوز استفاده کنید. در این مثال ما یک صفحه کلید مجازی را از سایت www.freevirtualkeyboard.com دانلود کرده ایم و بجای تایپ رمز عبور خود با صفحه کلید کامپیوتر از کلیک کردن نشانگر موس بر روی حروف و اعداد مورد نظر خود استفاده کرده ایم.

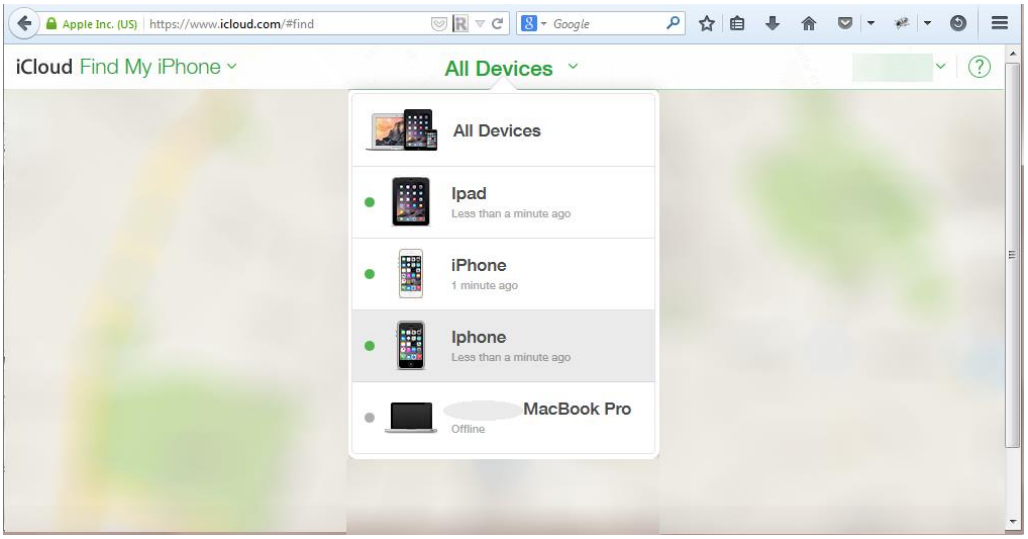
توجه ۲: رمز عبور اپل ایدی خود را به هیچکس ندهید و آنرا ساده و قابل حدس زدن انتخاب ننمائید.از قرار دادن رمز عبور مثل نام همسر ، شماره تلفن ، تاریخ تولد و غیره خود داری کنید و رمز عبور خود را ترکیبی از اعداد و حروف و سمبولها قرار دهید که طول ترکیب آن کمتر از ۱۵ کاراکتر نباشد.

۴.گزینه Find My iPhone را انتخاب کنید.

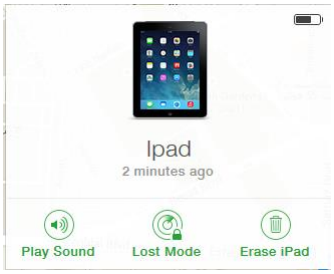
۵.رمز عبور اپل ای دی خود را مجددا با رعایت موارد امنیتی لازم وارد نمائید.



۶.کلیه دستگاههای شما که دارای Apple Id مشترک میباشند در لیست نمایش خواهند یافت و شما میتوانید هرکدام را که خواستید انتخاب نمائید.

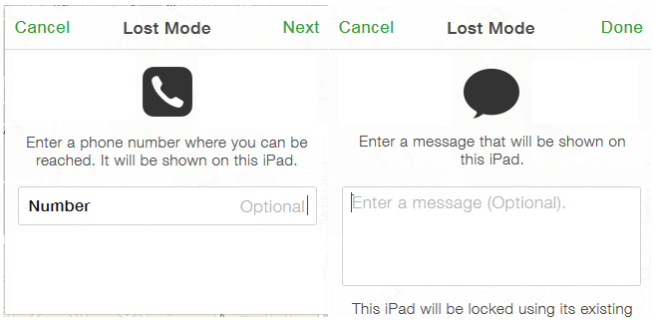


۷.از لیست دستگاهها برای مثال فرض کنید آیپد را انتخاب میکنیم.

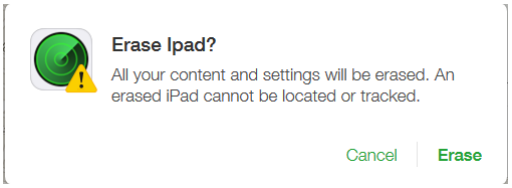


برای پخش شدن آلارم هشدار در جهت پیدا کردن محل آیپد در اطراف خود از گزینه Play Sound استفاده کنید.

برای اعلام اینکه دستگاه شما گم شده است از گزینه Lost Mode استفاده کنید. در این حالت اطلاعات جغرافیایی دستگاه شما برای شما ایمیل خواهد شد و همچنین میتوانید شماره تلفن و پیامی را به یابنده دستگاه خود ارسال کنید.



برای پاک کردن همه اطلاعات خود از راه دور از گزینه Erase استفاده کنید.



نکته ۱۸) چگونه Jail Break کردن آیفون، باعث به مخاطره افتادن امنیت شما خواهد شد.

اصطلاح jail break به زبان ساده روشی است برای دسترسی کامل به ساختار نرم افزار سیستم عامل iOS می باشد و به شما اجازه میدهد به برخی از منابع ریشه ای گوشی خود دسترسی داشته یا از منابع دیگری جز اپ استور نرم افزارهایی را روی گوشی خود نصب نمائید. یا برخی از نرم افزارهای پولی را بصورت رایگان استفاده نمائید. اما هر چیزی بهایی دارد و بهای اینکار میتواند برای شما به اندازه از دست رفتن حریم خصوصی شما سنگین باشد.

درحالت عادی iOS در مورد اپ ها بسیار سختگیر بوده و مثلا طراحی اپی که بتواند تمام کلماتی که شما تایپ کرده اید را ذخیره کرده و برای کسی ارسال کند (Key logger) امکانپذیر نمیباشد. زیرا تمام اپ ها قبل از قرارگیری در اپ استور مورد بازرسی امنیتی نیز قرار میگیرند و بعلاوه دستگاهی که اصطلاحا jail break نشده باشد اساسا" چنین امکانی را نمیتواند در اختیار هیچ اپی قرار دهد.

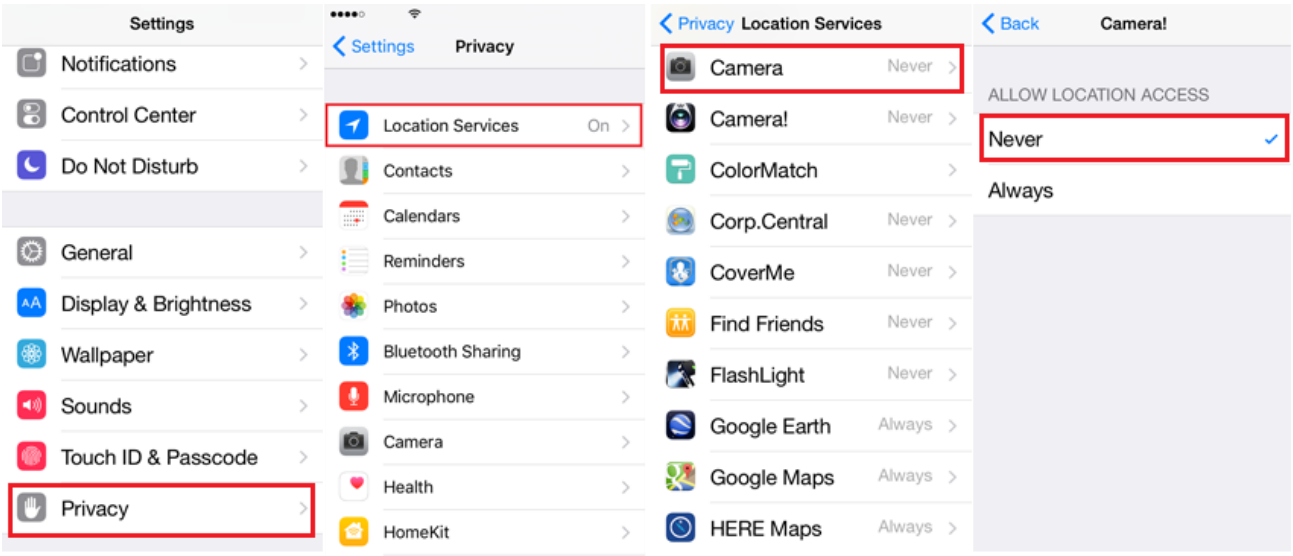
اگر دستگاه خود را jail break نمائید و گوشی شما برای مدت کوتاهی در دست یک هکر قرار گیرد. او میتواند یک اپ مثل ikeymonitor را که برای دستگاههای jail break شده طراحی شده است را روی آیفون یا آیپد شما نصب کند و بدون اطلاع شما کلیه حروف تایپ شده ، پسورد ها ، اس ام اس ها ، وب سایتهای دیده شده و اسکرین شات ها را از صفحه آیفون یا آیپد قربانی شده شما برای هکر ارسال نماید!

پس بهای نپرداختن چند دلار برای هزینه اپ ها را ممکن است با به خطر انداختن تمام حریم خصوصی خود پرداخت نمائید.

نکته ۱۹) هیچ عکسی را بدون انجام این تنظیمات در اینترنت به اشتراک نگذارید.

این امکان در آیفون فراهم شده است که مختصات جغرافیایی و محل دقیق گرفتن یک عکس را در درون عکس ذخیره نماید. حال اگر شما بدون غیر فعال کردن این ویژگی عکسی را با دوربین آیفون خود تهیه کنید و مایل باشید آنرا درجایی بصورت ناشناس ارسال کرده یا به اشتراک بگذارید باید بگوییم اشتباه بزرگی را مرتکب می شوید.

چون موقعیت دقیق شما در اطلاعات درون عکس ضمیمه گردیده است و ممکن است طعمه خوبی برای هکرها و دزدهایی که وسایل ارزشمند شما را درعکس دیده اند بشوید بعلاوه سایر افراد و سازمانها نیز میتوانند از موقعیت جغرافیایی محل گرفته شدن تصاویر توسط شما آگاه گردند.



جلوگیری از ثبت موقعیت مکانی شما در عکسهای آیفون

نکته ۲۰) چگونه آیفون با یک کلیک و حتی بدون اینترنت و تنها از طریق Wi-Fi هک میشود.

شناخت مدلهای توزیع و نصب App بر روی آیفون:

اپل چندین مدل توزیع نرم افزار را ارائه داده است.

Single device distribution:

این معماری اجازه میدهد یک برنامه تنها بر روی یک آیفون قابل نصب باشد و اگر طراح برنامه بخواهد اپ را روی آیفون دیگری انتقال دهد. این اپ قابل استفاده در دستگاه جدید نخواهد بود.

Ad Hoc distribution:

این معماری توزیع اپ به نویسنده اپ اجازه میدهد تا اپ خود را بر روی ۱۰۰ دستگاه آیفون و آیپد و غیره نصب نماید. معمولا این روش برای تست اپ ها قبل از انتشار نهایی آنها روی اپ استور صورت میگیرد.

In-house distribution:

این معماری در توزیع اپ به کمپانی ها و شرکتها اجازه میدهد تا اپ های خود را بدون اینکه توسط اپل تائید گردند بر روی شبکه های خصوصی خود و برای استفاده کارمندان خود توزیع نمایند و هیچگونه محدودیتی از لحاظ تعداد نصب بروی آیفون ها یا آیپد ها وجود ندارد.

Over the air (OTA) distribution:

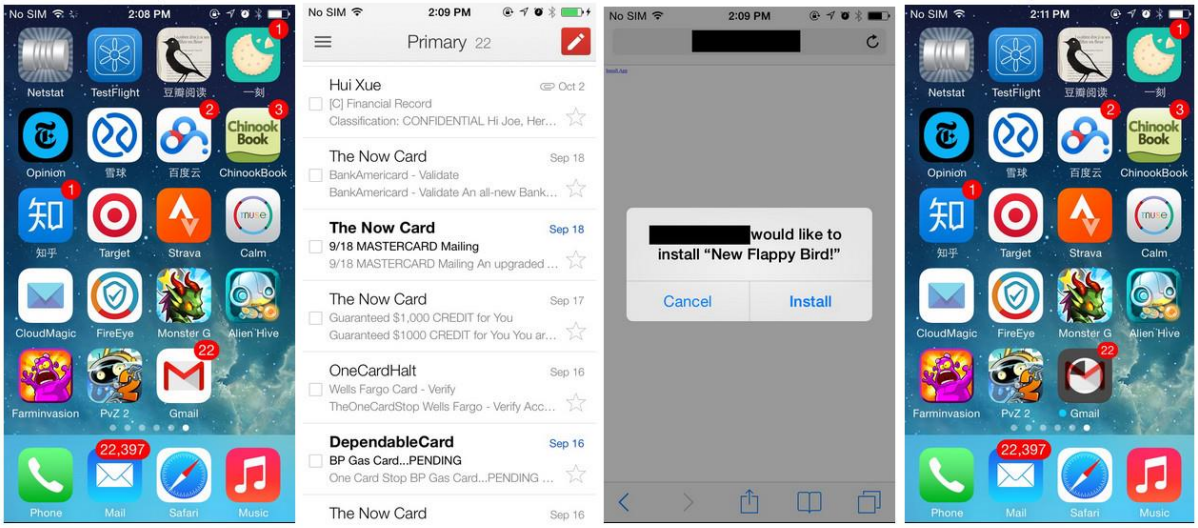
این مدل توزیع اپ به سازمانها و شرکتها اجازه میدهد اپ های خود را براحتی از طریق یک لینک بر روی سایت خود در اختیار هرکسی که تمایل دارد آنرا روی آیفون خود نصب کند قرار دهد.

App Store distribution:

مدل توزیع آپ در فروشگاه اپل می باشد که دارای یک سری قوانین سفت و سخت برای نوشتن و توزیع اپ ها و همچنین بررسی امنیتی و کارایی اپ ها قبل از انتشار انها در فروشگاه اپل (App Store) می باشد. این روش امن ترین روش توزیع اپ برای استفاده کنندگان اپ ها می باشد.

در مدلهایی دیگر به غیر از روش توزیع اپ در اپ استور این امکان فراهم میباشد که نویسنده اپ بدون بازرسی امنیتی اپل اپی را نوشته و آماده نصب نماید.

بررسی سناریوی واقعی از هک کردن یک آیفون که به آخرین نسخه iOS مجهز می باشد و jail break هم نشده است.



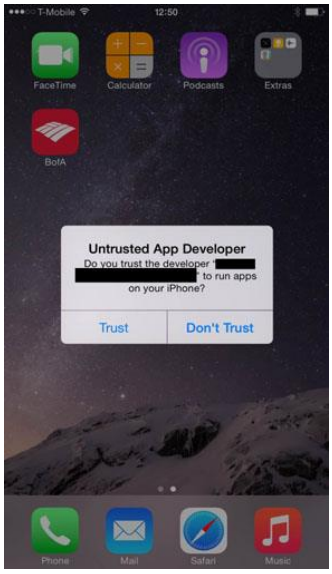
۱. کاربر اپ جیمیل خود را باز میکند.
۲. ایمیلی را میخواند که پیشنهاد میکند آخرین نسخه بازی Falppy Bird را نصب کند.
۳. کاربر متوجه این حقه نمیشود و بر روی گزینه Install کلیک میکند.
۴. اپ هک طوری طراحی شده است که در واقع خود اپ جیمیل را هدف قرار میدهد و با خواندن اطلاعات آن ظاهری کاملا مشابه با آنرا پس از نصب نمایش میدهد. (در این مثال متخصصین امنیتی در بالای اپ جیمیل عبارت "You Are pwned" نمایش داده اند تا نشان دهند اپ تغییر یافته است در حالیکه هکر واقعی هیچوقت این ترحم را در مورد شما نخواهد داشت.

توضیح ۱ : این روش هک بنام روش ماسک (Masque) نیز مشهور است

توضیح ۲: لینک اپ آلوده از طریق شبکه وای فای و بدون اتصال به اینترنت قابل نصب می باشد.

چگونه از هک شدن گوشی خود از این طریق جلوگیری میتوان کرد.

۱. تحت هیچ شرایطی از هیچ منبعی به جز اپ استور نرم افزاری را نصب نکنید. این شامل سازمانهایی که در آن کارمیکنید و منابع third-party دیگر نیز می باشد.
۲. در جاهایی مثل گیتهای بازرسی فرودگاهها و محل هایی که مجبور به جدایی موقتی از آیفون خود میشوید حتما از قبل امکان Passcode یا Touch id را بر روی گوشی خود فعال نمائید. و آیفون خود را بصورت خاموش تحویل دهید.
۳. در مهمانی ها و اماکن عمومی و حتی دوستان و آشنایان گوشی خود را در اختیار کسی قرار ندهید چون یک هکر تنها در چند دقیقه میتوان گوشی شما را هک نماید بدون اینکه شما متوجه تغییری در اپ های آیفون خود بشوید.
۴. زمانیکه در وبگردی خود پنجره ای باز میشود و به شما پیشنهاد میکند که اپ مربوط به این سایت را نصب کنید. به هیچ عنوان گزینه Install را انتخاب نکنید بلکه نام اپ مورد نظر را در اپ استور جستجو کرده و از آنجا اپ را نصب نمائید.
۵. مطابق تصویر زیر اگر یک اپ را باز کردید و iOS پیام هشدار " Untrusted App Developer" را نمایش داد این هشدار را کاملا جدی بگیرید و بر روی گزینه "Don't Trust" کلیک کرده و بلافاصله آن اپ را حذف کنید.



جلوگیری از نصب Untrusted App

چگونه میتوانید متوجه شوید که آیا تا الان هدف این هک قرار گرفته اید؟

کاربران iOS نسخه ۷ میتوانند کلیه پروفایلهایی که روی دستگاه آنها نصب شده است را در آدرس

Settings - > General -> Profiles مشاهده نمایند و لیست پروفایل های نصب اپ را روی دستگاه خود ملاحظه کنند.

کاربران iOS ۸ به بالا باید دقت بیشتری نمایند زیرا تا نسخه iOS ۹,۰ (زمان نوشتن این کتاب) شرکت اپل امکان دیدن پروفایلهای نصب را برای کاربران برداشته بود. پس اگر به آیفون خود مشکوک هستید

مجددا از دیتاهای خود بک آپ تهیه کنید و پس از Erase کردن گوشی خود مجددا از اپ استور اپ های خود را نصب نمائید.

نکته ۲۱) iCloud Photo Steam خطری که میان ابرها در کمین عکسها خصوصی شماست.

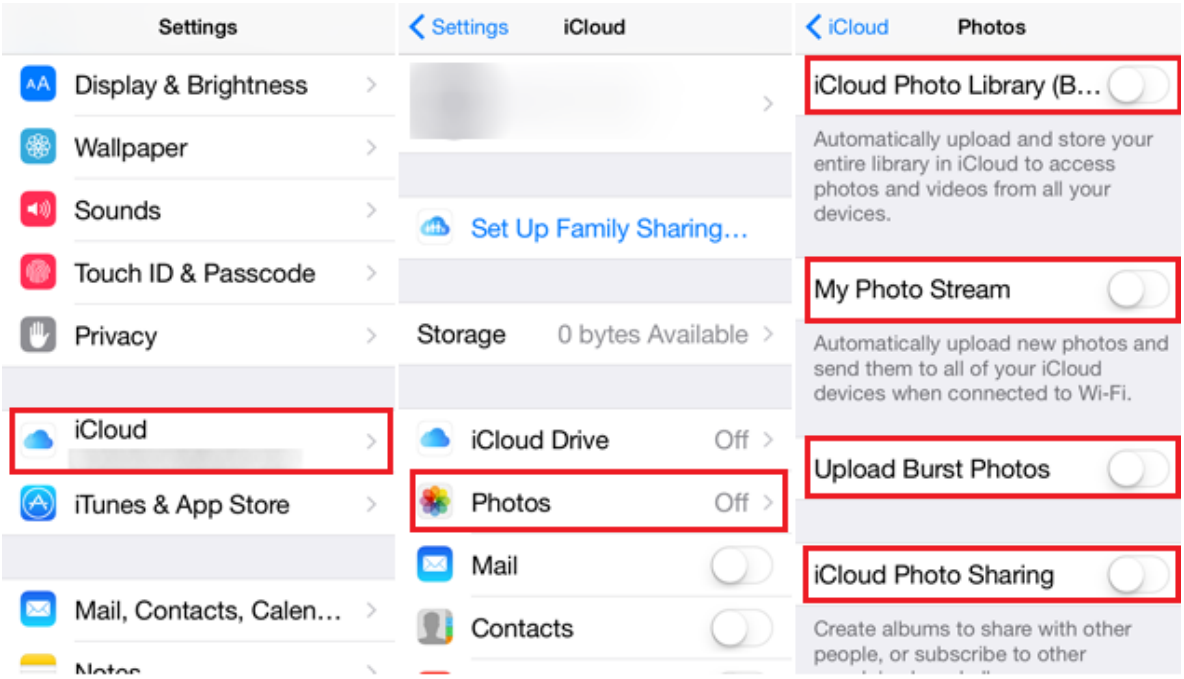
زمانیکه شما امکان iCloud را درگوشی خود فعال میکنید این قابلیت را پیدا میکنید که از فضایی که در سرورهای اپل برای شما اختصاص یافته است برای ذخیره کردن اطلاعات خود مثل (بک اپ ها ، تصاویر ، لیست تماس ها و غیره) استفاده کنید.

اگرچه این امکان بدی نمی باشد و به شما اجازه میدهد که همواره اطلاعات خود را با سایر ابزار خود سینک کنید. از مزایای آن استفاده کنید اما این ویژگی در عین حال در iOS ۸ به بالا بطور پیش فرض این اجازه را به اپل میدهد تا از هر تصویری که شما با دوربین آیفون خود میگیرید یا در آن ذخیر میکنید یک کپی هم بصورت اتوماتیک در فضای iCloud ذخیره نماید و به این امکان Photo Stream میگویند.

آگاه باشید که اپل تطبق توافق نامه ای که در زمان استفاده از iOS آنرا میپذیرید این اختیار را دارد که اطلاعات شما را در اختیار نهادهای قانونی قرار دهد.

تصور کنید شما تعداد تصاویر شخصی در گوشی خود داشته باشید که علاقمند نباشید که هیچ کس تحت هیچ شرایطی آنها را ببیند. آیا بازهم مایل هستید از این امکان iCloud استفاده کنید؟

این ویژگی از iOS ۸ در آیفون ها بوجود آمد و متاسفانه باید بگویم که Photo Steam بصورت پیش فرض فعال می باشد.



غیر فعال کردن Photo Stream در iOS ۸+

نکته ۲۲) شیوه صحیح پاک کردن تصاویر منتقل شده بهiCloud Photo Steam

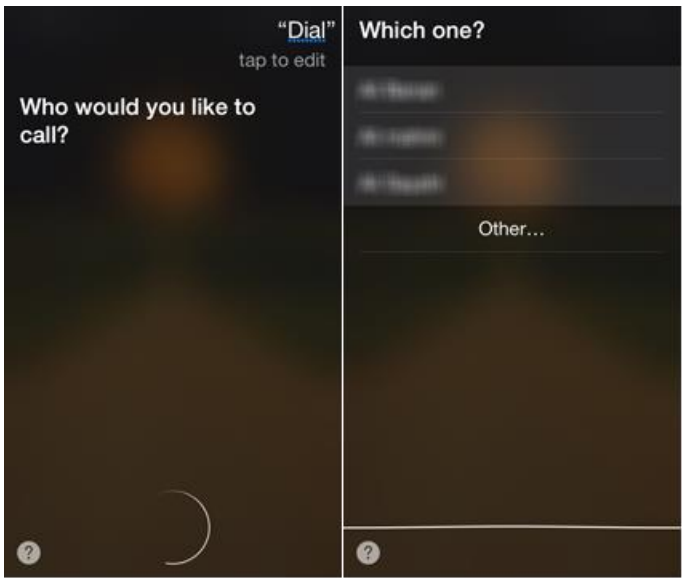
اگر پیش از خواندن این کتاب Photo Stream شما در تنظمیات iCloud فعال بوده باشد و شما تعدادی عکس شخصی با آیفون خود گرفته باشید به موارد زیر عمل کنید:

۱. پاک کردن تصاویر در Camera Roll باعث حذف آن تصاویر در حافظه آیفون شما می شود ولی همچنان آن تصاویر در Photo Stream و بر روی فضای اختصاصی شما در iCloud وجود دارند. همچنین در Album tab در بخش آلبومی بنام Recently Deleted وجود دارد که تا ۳۰ روز تصویر شما قبل از پاک شدن دائمی در آن قرار میگیرد.
۲. شما میتوانید تصاویر خود را در بخش Photo Stream پاک کنید ولی آن تصاویر هنوز در بخش Camera Roll شما موجود میباشند.
۳. اگر میخواهید تصاویر خصوصی شما هم در Camera Roll و هم از Photo Stream حذف شوند شما کافیست ابتدا تصاویر خود را در Photo tab پاک کنید ، سپس به Album tab بروید و آن تصاویر را در آلبوم Recently Deleted نیز پاک نمائید.

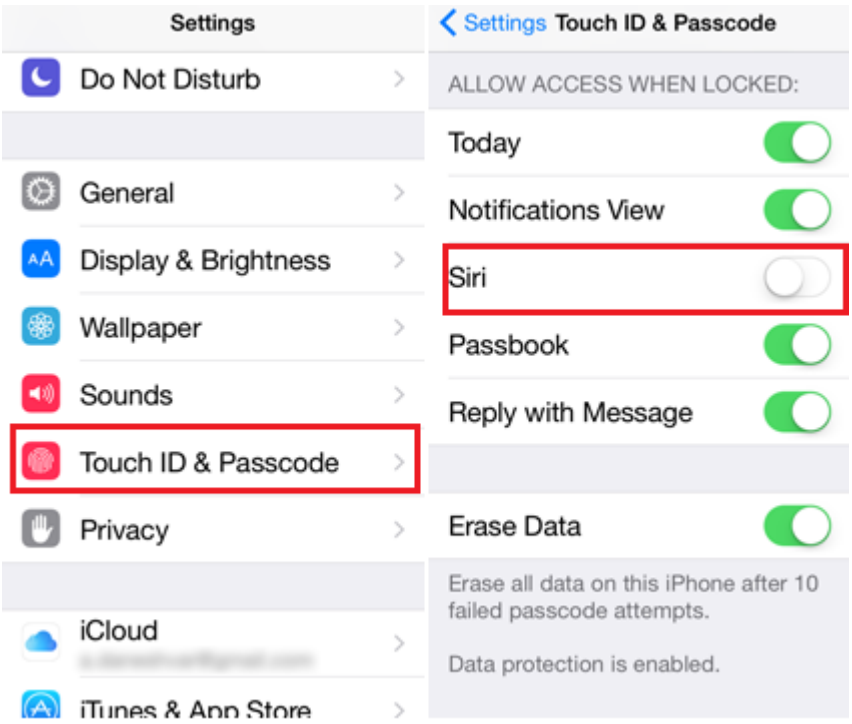
تصاویر حذف شده در iOS ۸ به بالا

نکته ۲۳) جلوگیری از دسترسی به لیست تماسها از طریق سیری در زمان قفل بودن آیفون

در زمانیکه آیفون شما قفل می باشد اگر شما به دستیار صوتی سیری اجازه دسترسی داشته باشید. هرکس با گفتن کلمه "Call" یا "Message" و با گفتن اسمی که دنبال شماره تلفن آن است تماس برقرار کند یا شماره او را بردارد. برای جلوگیری از این اقدام شما باید دسترسی سیری را به لیست تماسهای خود در زمانیکه آیفون شما قفل می باشد بگیرید.



دسترسی به لیست تماس در زمان قفل بودن آیفون و توسط سیری



غیر فعال کردن سیری در زمان قفل بودن آیفون

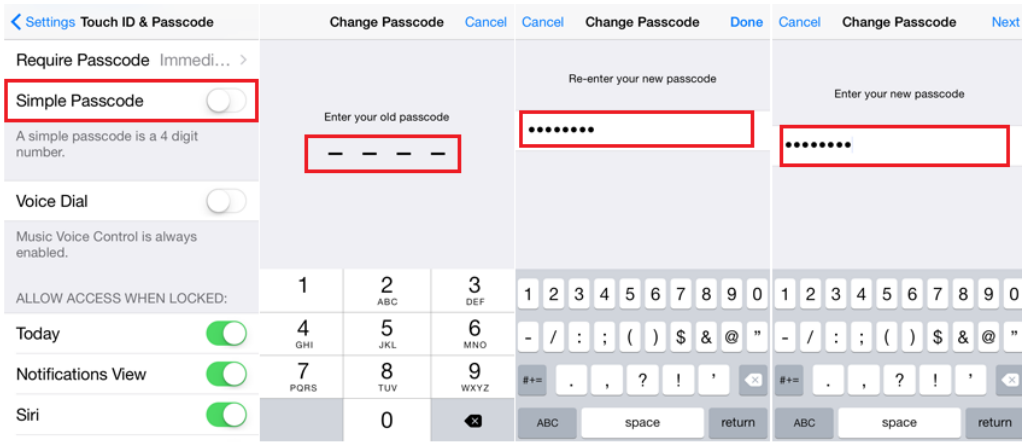
نکته ۲۴) Passcode چهار یا شش رقمی کافی نیست !

Passcode شما یک مانع بین هکر و اطلاعات درون گوشی شما می باشد.

و با برداشته شدن آن حجم زیادی از اطلاعات شخصی شما لو میرود. اگرچه زدن مداوم این کد در طول روز ممکن است ده ها بار رخ دهد و کوتاه بودن آن انجام این کار را ساده تر میکند. ولی از طرف دیگر ساده بودن Passcode کار هکر ها را نیز ساده تر خواهد کرد.

توصیه میکنیم از Passcode با طول بین ۱۵ تا ۲۰ کاراکتر یا بیشتر (شامل اعداد ، سمبل ها ، حروف) استفاده نمائید. در iOS ۹ شرکت اپل کاربران را مجبور کرد که از حداقل ۶ رقم برای رمز عبور خود استفاده کنند که اگر چه بهبود خوبی نسبت به چهار رقم قبلی بود ولی کافی نیست.

با آمدن آیفون ۵ اس و مکانیزم Touch id کار ورود به آیفون به اندازه لمس یک انگشت ساده گردید. پس بهتر است لااقل Passcode را پیچیده تر انتخاب کنید.



فعال کردن Passcode باطول بیشتر از ۴ عدد

نکته ۲۵) فعال کردن Touch id همیشه فکر خوبی نیست !

در خصوص مکانیزم Touch id یک توصیه دارم و آن این است که اگر چه امکان خوب و راحتی برای دسترسی به آیفون توسط شما با یک لمس می باشد اما آیا زمانیکه در خواب هستید و خواب شما هم از قضا سنگین است امکان خوبی برای دیگران نیست؟ آیا اگر توسط چند سارق در یک کشور خارجی گرفتار بشوید و بزور انگشت های شما را روی سنسور آن بکشند آیا باز هم هنوز امکان خوبی است؟ چنین امکانی بسته به شرایط می تواند خوب یا بد باشد پس مطابق با شرایط محیطی خود این امکان را فعال نمائید.

نکته ۲۶) بالا بردن امنیت iCloud با Two-Step Verification for Your Apple Id

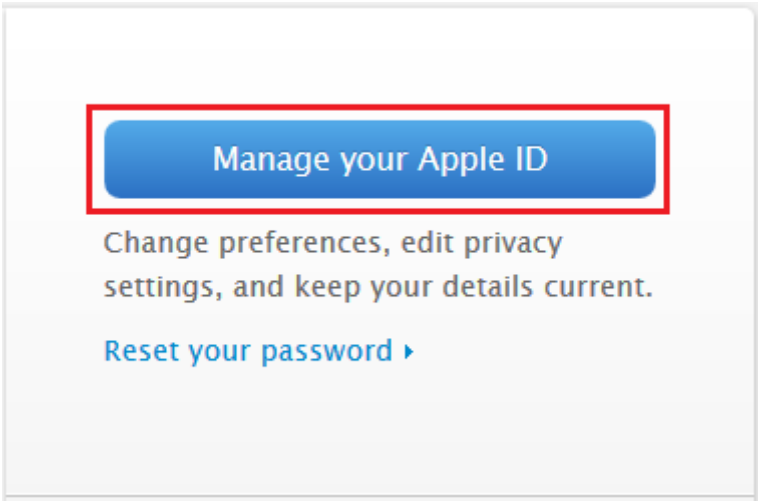
هک شدن اکانت iCloud ستارگان سینما و لو رفتن عکسهای موجود در Photo Stream اکانت آنها درس بزرگی به همه ما داد و آن این است که امنیت iCloud را جدی بگیریم. اپل با معرفی Two-Step Verification for Your Apple ID این امکان را به همه ما میدهد که هکرها صرفا با داشتن Apple Id و کلمه عبور ما نتوانند به حساب کاربری ما در iCloud دسترسی داشته باشند و اپل برای ورود به اکانت ما در iCloud یک کد تصدیق به یکی از iDevice های ما ارسال نماید تا مطمئن شود که این ما هستیم که داریم وارد اکانت خود می شویم و نه شخصی دیگر.

خوشبختانه فعال سازی این مکانیزم امنیتی بسیار ساده می باشد و شما با انجام مراحل زیر می توانید آنرا برای اکانت خود فعال نمائید.

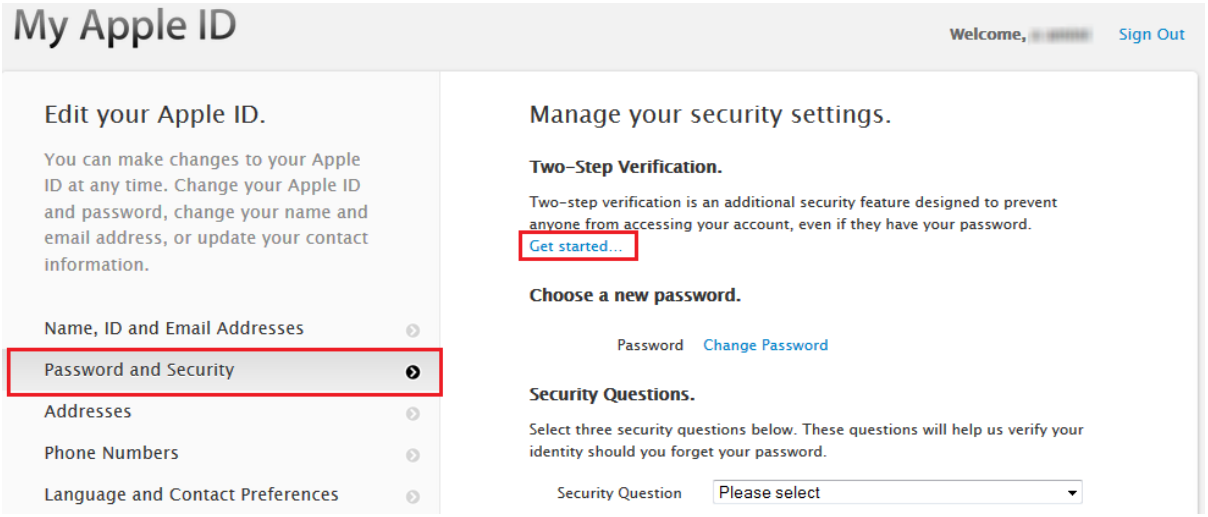
به یاد داشته باشید فعال سازی این سیستم به معنی حفاظت کامل از دستگاه شما نمی باشد اما راهی برای تقویت بهتر حریم خصوصی شما در زمان دسترسی به اکانت خود در iCloud است.

۱. به قسمت مدیریت اکانت در سایت اپل به آدرس زیر بروید:
https://appleid.apple.com/account/home
تذکر : شما برای اینکه از طریق اینترنت و بدون دریافت SMS نیز بتوانید در آینده از کد تائیدیه ایی که اپل برای شما می فرستند آگاه شوید باید نخست امکان Find My iPhone را که قبلا توضیح دادیم فعال نمائید.

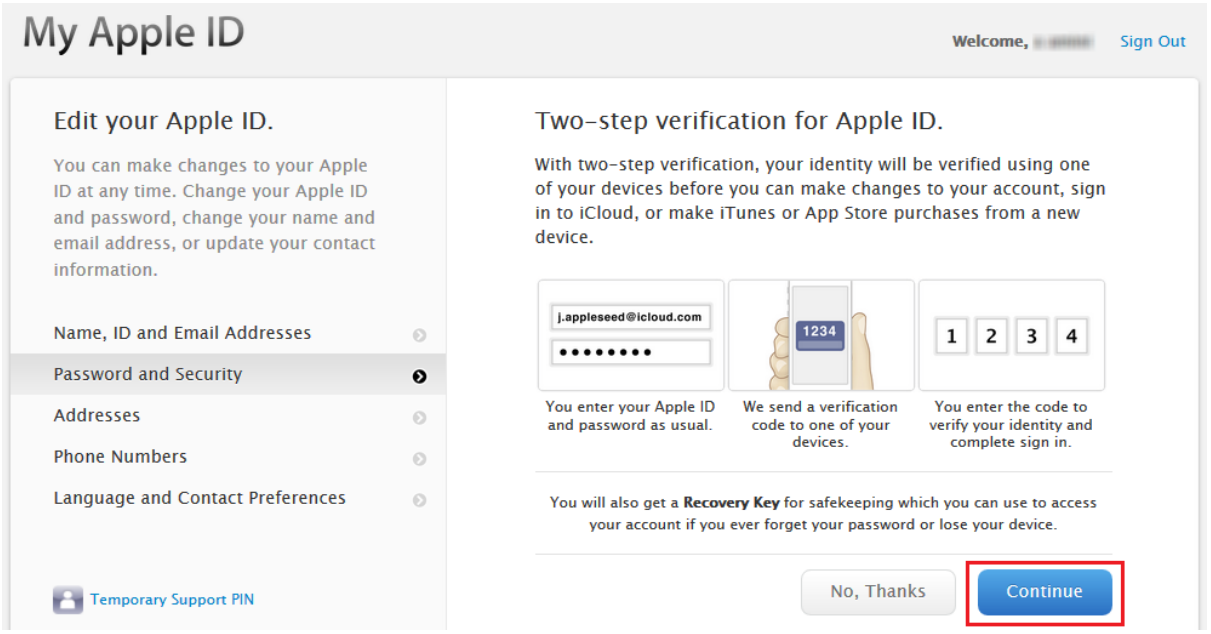
۲. Manage your Apple ID را انتخاب نمائید.



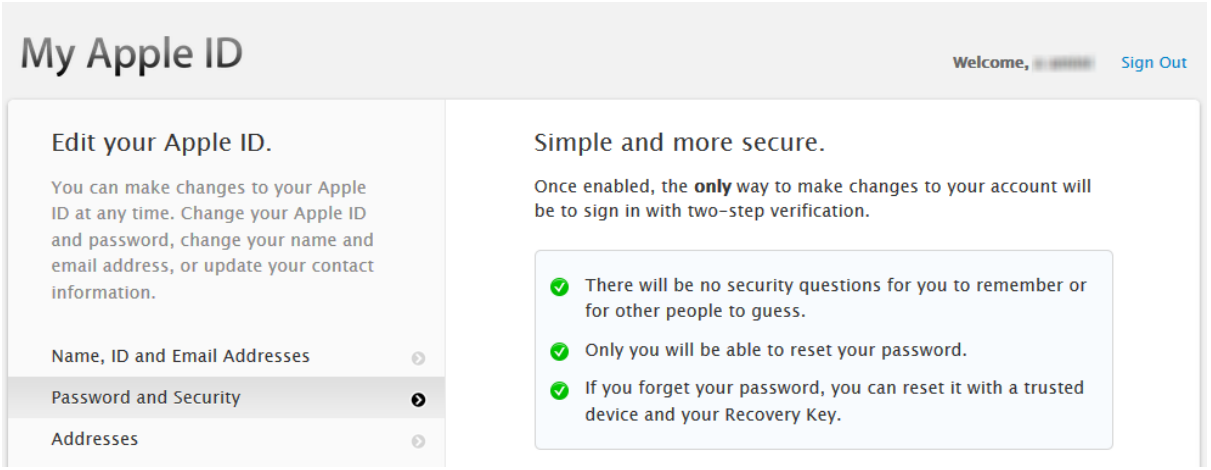
۳. به بخش Password and Security بروید و گزینه Get started را انتخاب کنید.



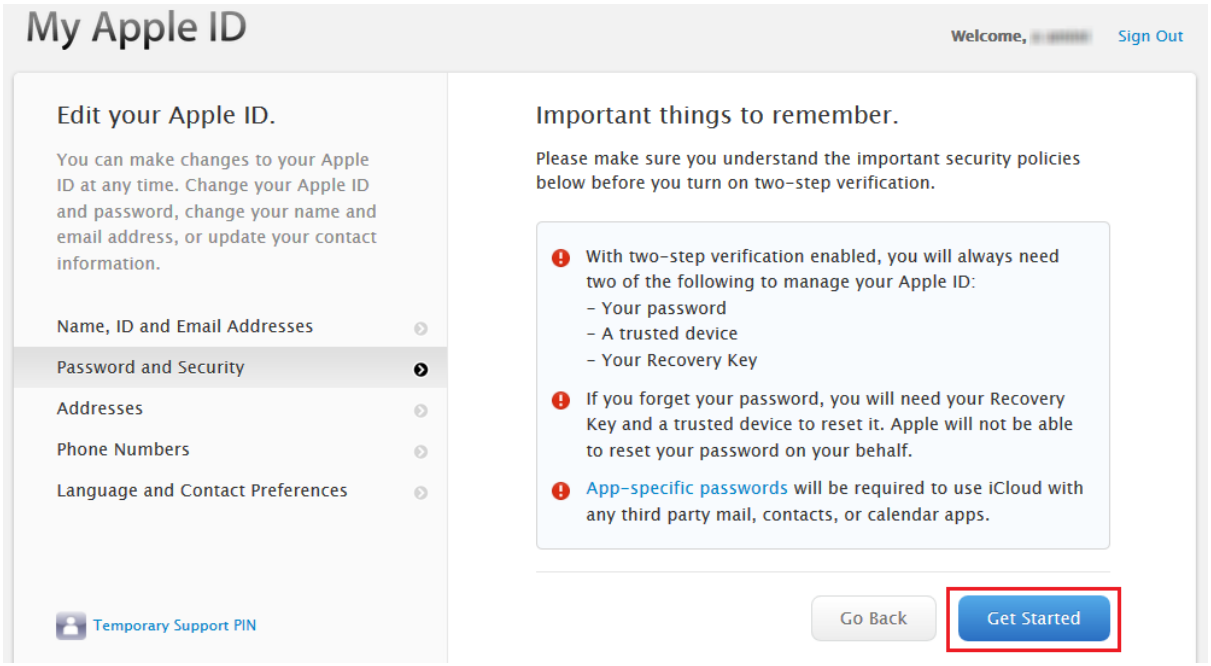
۴. اپل در این قسمت توضیح می دهد که در زمان ورود به اکانت خود برای شما یک کد تائیدیه به آیفون شما می فرستد که باید آنرا برای احراز هویت خود وارد نمائید.



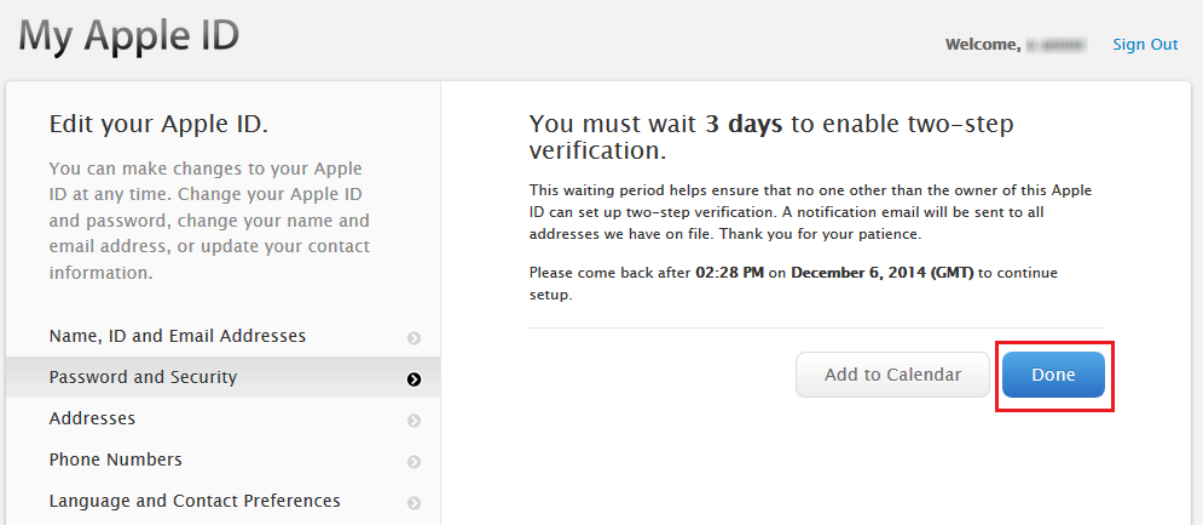
۵. اپل به شما توضیح میدهد که پس از فعال سازی تائید دو مرحله ای تنها شما خواهید توانست اکانت خود را ریست نمائید و حتی اپل نیز توانایی اینکار را نخواهد داشت و همچنین یک Recovery key در اختیار شما قرار خواهد گرفت که در موقع فراموشی پسورد اکانت خود با آن خواهی توانست اکانت خود را ریست نمائید.



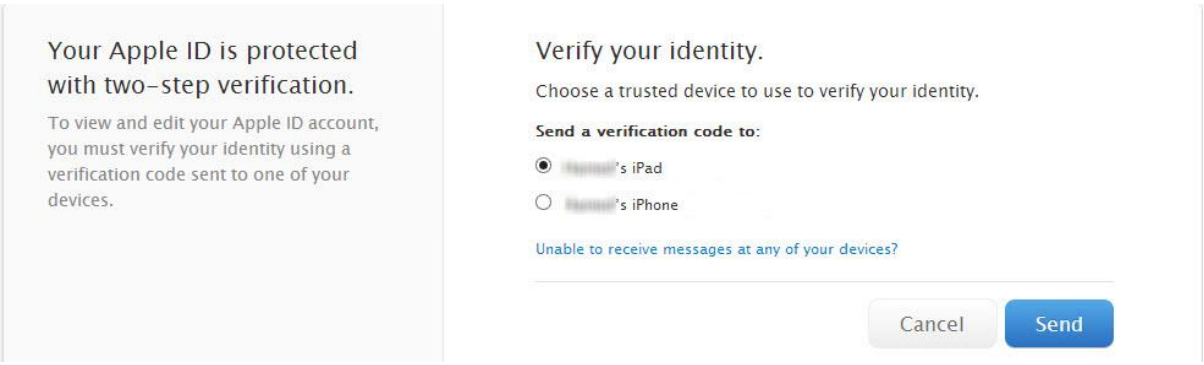
۶. اپل آخرین موارد مهمی که باید در نظر داشته باشید را به شما یادآوری میکند.



۷. اپل برای اطمینان از اینکه شما فرمان فعال سازی دو مرحله ای را صادر کرده اید به تمام ایمیل هایی که شما در زمان ساخت اکانت خود معرفی کرده بودید یک پیام می فرستد و سه روز فعال سازی دو مرحله را به تعویق می اندازد تا اطمینان حاصل کند شما از این موضوع خبر دارید و کسی بجای شما در حال فعال سازی تائید دومرحله ای نمی باشد.

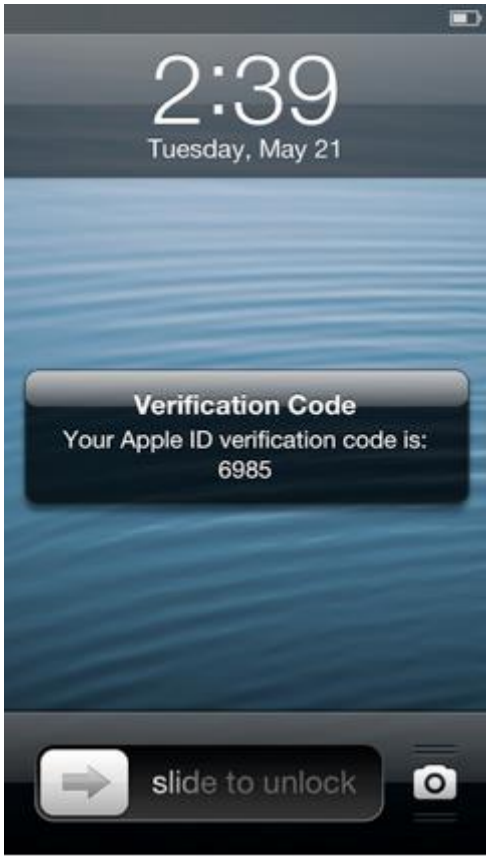


۸. پس از سه روز تائید دو مرحله ای برای اکانت شما فعال می شود و وقتی به حساب iCloud خود مراجعه کنید با صحنه زیر مواجه میشوید.



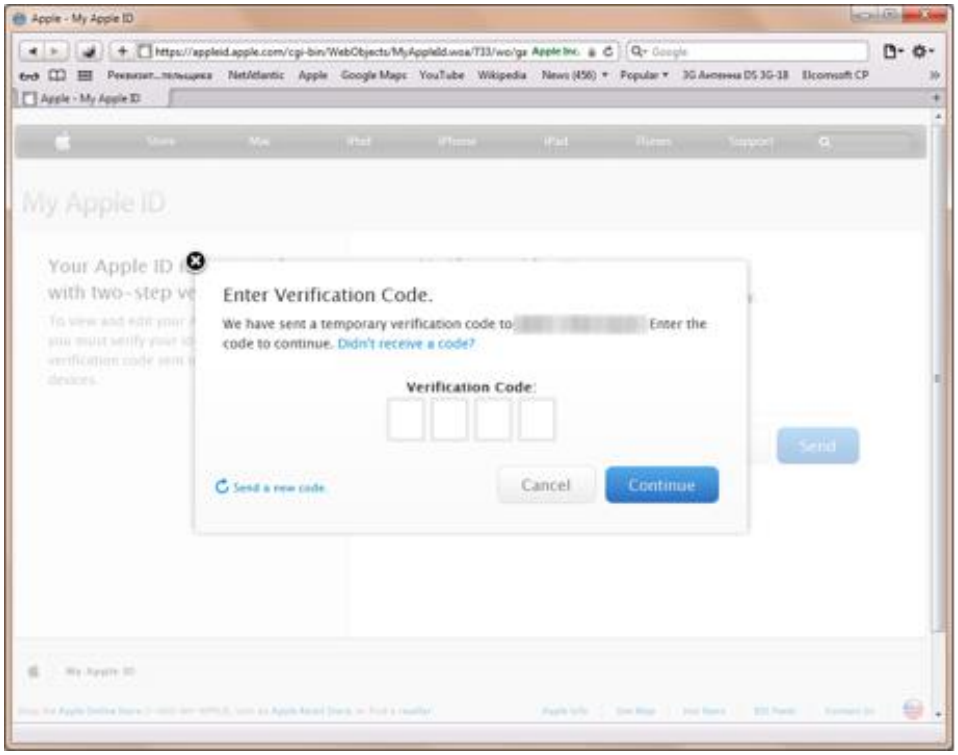
توضیح ۱: ارسال کد تائیدیه از طریق SMS برای همه کشورها امکانپذیر نمی باشد.

توضیح ۲: برای دریافت کد تائیدیه بدون دریافت SMS باید امکان Find My iPhone را فعال کرده باشید در غیر اینصورت کد می بایست از طریق SMS فرستاده میشود.



توضیح : نمونه ای از کد تائیده ارسالی از اپل

۹. اکنون باید کد تائیدیه دریافتی خود را در محل مربوطه وارد کنید تا وارد اکانت iCloud خود شوید.



نکته ۲۷) بالا بردن امنیت دسترسی به Backup هایی که در کامپیوتر خود از آیفون خود میگیرید.

هر زمان که آیفون شما به یک کامپیوتر که مجهز به نرم افزار iTunes می باشد وصل شود این امکان فراهم می باشد تا یک پشتیان کامل از همه دیتاهای خود تهیه کنید تا اگر مشکلی برای آیفون شما پیش آید بتوانید از این Backups ها استفاده نمائید.

در واقع Backup هایی که از آیفون خود تهیه میکنید یک کپی کامل از اطلاعات دستگاه شما می باشند. بنابراین اصلا منطقی نمیباشد که شما امنیت گوشی خود را بالا ببرید ولی توجهی به Backup های روی لپ تاپ یا دسک تاپ خود نداشته باشید

چون ابزارهایی وجود دارند میتوانند Backup های شما را از روی کامپیوتر بخوانند و تمام اطلاعات درون Backup های شما مانند شماره تماس ها ، پیامک ها ، تصاویر و یک سری از اطلاعات اپلیکشن ها را آشکار سازند.

برای بالا بردن امنیت Backup های خود از روش زیر استفاده کنید:

۱. آیفون یا آیپد خود را به کامپیوتر خود متصل نمائید و آنرا انتخاب کنید.
۲. گزینه encrypted iPhone Backup را انتخاب نمائید
۳. آیتونز از شما میخواهد که یک کلمه عبور و تکرار آنرا برای رمز کردن بک آپ وارد نمائید. پیشنهاد ما استفاده از کلمه عبوری بطول بیش از ۱۶ کاراکتر شامل حروف کوچک و بزرگ ، اعداد ، سیمبل ها می باشد. زیرا در غیر اینصورت و با انتخاب یک کلمه عبور مثلا ۴ حرفی ابزارهای هک کردن می توانند تنها در ۲۰ دقیقه پسورد بک آپ شما را پیدا کرده و در اختیار هکر قرار دهند.
۴. بک آپ گیری به شیوه امن و کاملا رمز شده انجام میشود.
۵. در زمان restore کردن بک آپ روی دستگاه خود حتما باید این پسورد را بدانید وگرنه بک آپ غیر قابل استفاده خواهد بود.

توضیح ۱ : هرگز بر روی کامپیوترهایی نامطمئن مثل کامپیوترهای شرکت ، مدارس و غیره بک آپ نگیرید.

توضیح ۲: بک آپ هایی که روی iCloud تهیه می شوند خارج از این موضوع بوده و با Apple id محافظت میگردند.

توضیح ۳ : برای امنیت بیشتر هرگز بر روی iCloud بک آپ های خود را ذخیره نکنید حتی اگر Two Step verification را فعال کرده باشید. چون اپل می تواند با حکم مراجع قانونی آن اطلاعات را در اختیار ایشان قرار دهد. بعلاوه ابزارهای هکی وجود دارد که میتواند اطلاعات بک آپهای iCloud شما را دانلود کرده و در کامپیوتر هکر قرار دهد.

نکته ۲۸) چگونه Backup گیری روی iCloud میتواند برای شما تبدیل به کابوسی بزرگ شود.

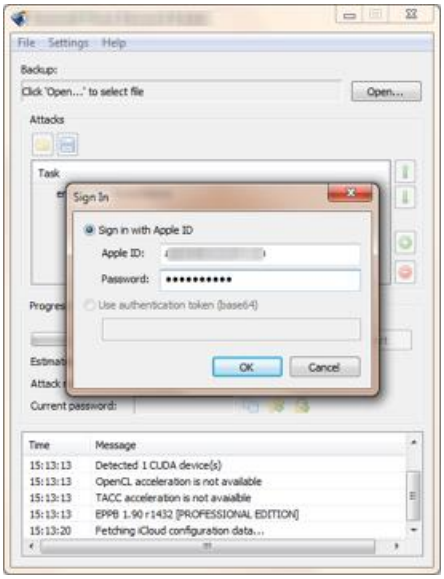
همانطور که توضیح دادیم Backup گیری بر روی iCloud گزینه خوبی نمی باشد اما شاید شما مایل باشید بیشتر در این خصوص بدانید.

متاسفانه حتی اگر Two step verification را برای iCloud خود فعال کرده باشید این گزینه تاثیری در بازیابی بکاپ های گرفته شد بر روی اکانت iCloud شما ندارند. زیرا ابزارهای هک و نفوذی وجود دارد که میتوانند فقط با داشتن اپل ایدی و کلمه عبور آن به این بک اپ ها دسترسی داشته باشند.

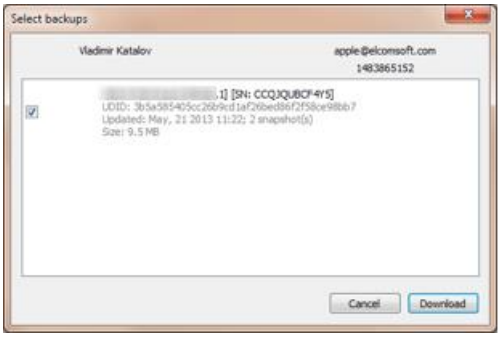
بررسی روش هک شدن Backup های شما را در iCloud:

گام اول : هکر از طریقی Apple Id و پسورد شما را سرقت میکند. (مهندسی اجتماعی ، Key logger و غیره)

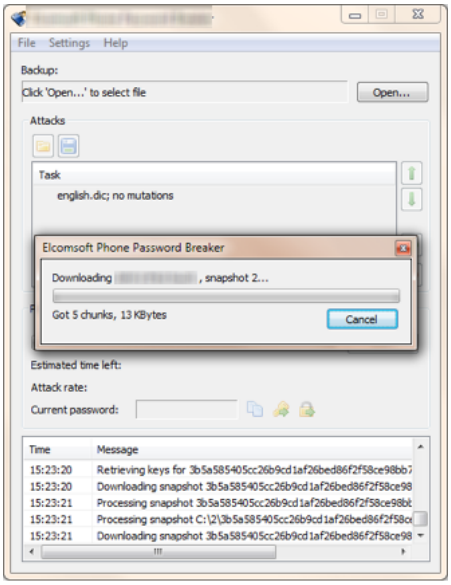
گام دوم: هکر از یکی از ابزارهای هک برای ورود اپل ای دی و پسورد شما استفاده میکند.



گام سوم : ابزار هک لیست کلیه بک آپ های موجود در iCloud شما را به هکر نمایش میدهد.



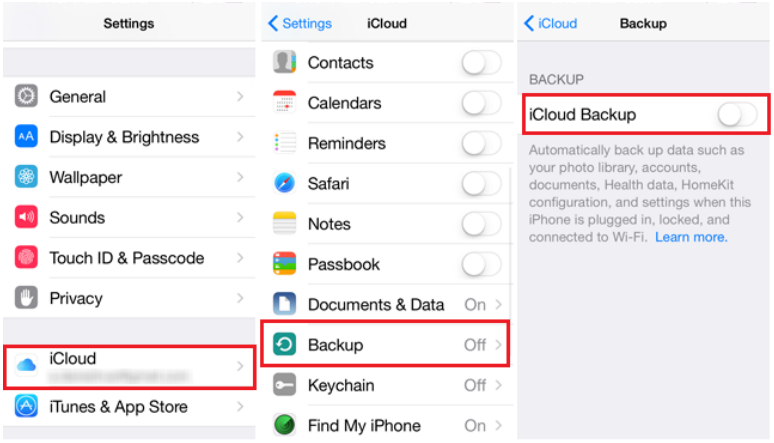
گام چهارم : هکر یکی از بک آپ ها را انتخاب کرده و آنرا بر روی کامپیوتر خود دانلود میکند.



گام پنجم : هکر از یکی از ابزارهای رایگان آنالیز و بررسی بک آپ های آیتونز مثل iBackupBot استفاده کرده و تمام اطلاعات شما شامل عکسها ، فیلم ها ، لیست تماس ها ، یادداشت ها ، SMS ها و غیره را مورد دستبرد قرار میدهد.

سناریوی هک بالا بنظر برای هرکسی میتواند ترسناک شود اگر اطلاعات خصوصی در بک آپ خود داشته باشد و هرکسی میداند که در هر صورت اطلاعاتی در بک آپ خود دارد که نخواهد برای دیگران برملا شود.

نتیجه : اگر اطلاعات محرمانه ای روی آیفون یا آیپد خود دارید بک آپ گیری روی iCloud را انجام ندهید.



غیر فعال کردن بکاپ گیری روی iCloud

نکته ۲۹) آیا دسترسی به Backup های iCloud بدون پسورد امکانپذیراست ؟ پاسخ: آری!

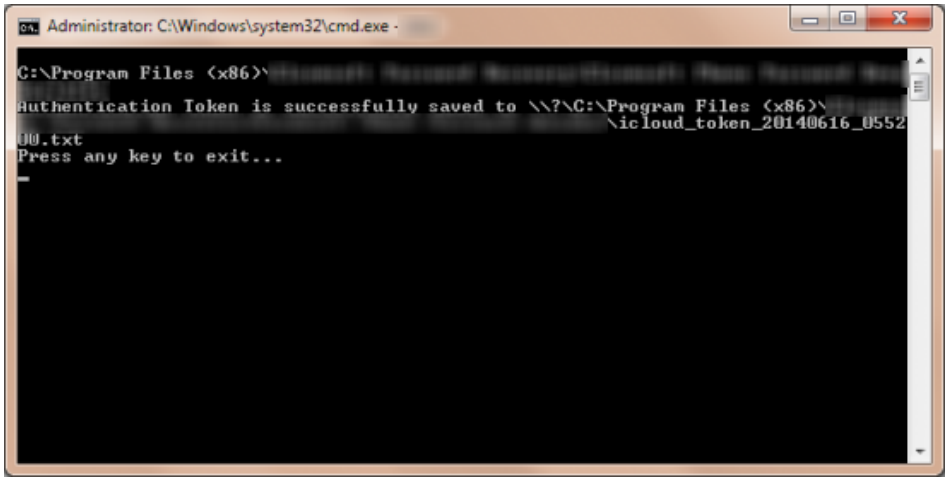
هرچند انجام اینکار کمی پیچیده می باشد ولی با داشتن شرایط زیر یک هکر میتواند بدون داشتن پسورد آیکلود شما بکاپ های موجود بر روی آنرا دانلود کرده و اطلاعات درون آنرا استخراج نماید.

۱. دسترسی فیزیکی به کامپیوتر شخص قربانی (از طریق سرقت ، یا داشتن وقت کافی برای انجام عملیات بدون سرقت و یا مصادره کامپیوتر شما توسط مراجع قانونی)
۲. نرم افزار آیکلود کنترل پنل بر روی کامپیوتر شما نصب باشد و شما قبل دسترسی اشخاص دیگر به کامپیوترتان در آیکلود کنترل پنل لاگین کرده باشید.
۳. ابزار هک بک آپ (بدلیل اینکه نمیخواهیم این کتاب به راهنمایی برای هکر ها تبدیل شود و هدف ما محافظت از کاربران می باشد از افشای نام ابزارهای هک خودداری میکنیم)

iCloud Control Panel (mac/windows)

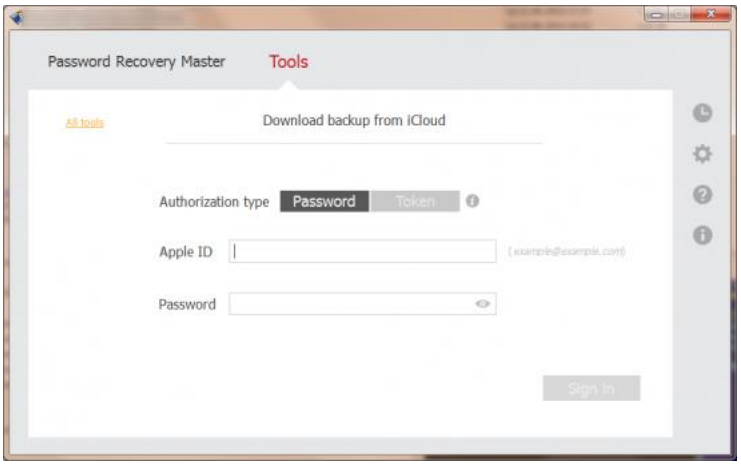
چگونه این هک صورت می پذیرد؟

این ابزار که بصورت خط فرمان کار میکند بر روی کامپیوتر بدست آمده اجرا می شود و کلیه Token های تائیدیه لاگین بر روی سیستم را به پیدا میکند و میتواند در یک USB ذخیره کند.

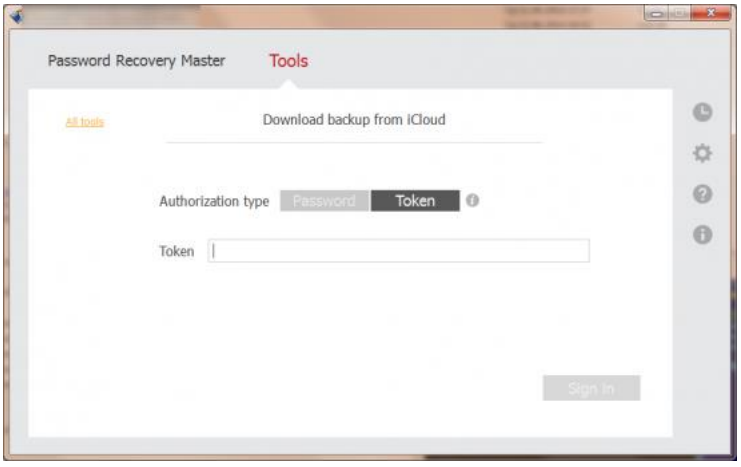


Authentication Token چیست؟ زمانیکه شما یکبار با موفقیت در iCloud Control Panel لاگین میکنید. یک کد منحصر بفرد بر روی کامپیوتر شما بوجود می آید تا سری بعد مجبور نباشید دوباره نام و کلمه عبورiCloud خود را وارد نمائید.

هکر با پیدا کردن Authentication Token و با نرم افزار دیگری از ابزار هک خود به شیوه زیر و فقط با داشتن Token میتواند iCloud را مجاب کند که یک کاربر مجاز برای دسترسی به بکاپ ها روی حساب iCloud می باشد. و از آن پس می تواند به کلیه اطلاعات درون بکاپ های شما پس از دانلود دسترسی پیدا کند.



هکر کلمه عبور شما را ندارد پس از این قسمت استفاده نمیکند



هکر بخش ورود به iCloud شما را توسط Token انتخاب میکند و کار تمام میشود.

نکاتی که باید در خصوص هک شدن از طریق Authentication Token آیکلود بدانید:

- هکر نمی تواند Apple Id و پسورد شما را از روی این Token بدست آورد.
- اگر از iCloud Control Panel خارج شوید. Sign-out کردن باعث پاک شدن Token می شود اما یادتان باشد که هنوز هم خطر اسکن کردن و بازیابی Tokenحذف شده از روی هارد دیسک توسط هکر وجود دارد.
- هر بار که شما در iCloud Control Panel لاگین کنید Token جدیدی بر روی کامپیوتر شما بوجود می آید. اما متاسفانه همچنان اگر کسی Token قدیمی شما را داشته باشد بازهم میتواند به حساب iCloud شما با ابزار هک خود وارد شود!
- زمان استفاده از این Token ها توسط هکر نامحدود نیست، اما اطلاعاتی از مدت زمان قابل استفاده بودن آنها تا الان افشا نشده است.
- هکر میتواند فقط با داشتن یک USB Drive و اتصال آن به کامپیوتر شما Token را بر روی آن ذخیره کند . ابزار هک نیاز به نصب ندارد و او میتواند بعد سرفرصت روی کامپیوتر دیگر بک آپ های شما را دانلود کند و به اطلاعات شما دسترسی پیدا کند.

چگونه میتوان جلوی این هک را گرفت اگر iCloud Control Panel را بر روی کامپیوتر نصب کرده باشید؟

۱. iCloud Control Panel را از روی کامپیوتر خود حذف کنید.
۲. به قسمت مدیریت اکانت در سایت اپل به آدرس زیر بروید:
https://appleid.apple.com/account/home
۳. در قسمت Change Password کلمه عبور خود را عوض کنید. تا کلیه Token هایی که تا این مدت بوجود آورده بودید بی مصرف گردند.

نکته ۳۰) روش حفاظت از اطلاعات آیفون حتی اگر بزور مجبور به ارائه Passcode خود شوید (روشی که هکرها و FBI دعا میکنند کاربران آنرا یاد نگیرند)

در زمان ارائه iOS ۸ سازمان FBI جنجالی را در مورد شرکت اپل بخاطر قرار دادن قابلیت های امنیتی جدید در نسخه جدید iOS به پا کرد و رئیس وقت FBI یعنی آقای James Comey اپل را در خصوص سخت تر شدن پیگیری پرونده های خلافکارانی که از iOS ۸ به بالا استفاده خواهند کرد مورد سرزنش قرار داد. این جنجال پس از مدتی فرو نشست اما حقیقت ماجرا چه بود؟ رئیس وقت FBI از چه قابلیتی در iOS ۸ نگران بود؟

حقیقت این است که تکنولوژی نیز مانند سایر ابزارها میتواند در خدمت تبهکاران نیز درآید. مانند یک چاقوی آشپزخانه که در خانه ابزار بسیار مفیدی است اما در دست یک انسان تبه کار میتواند ابزار جرم باشد.

بنابراین این ما هستیم که روش صحیح استفاده از ابزار را مشخص میکنیم و یقینا اکثر شهروندان به قانون متعهد هستند.

این ویژگی فوق العاده جذاب و تا حدودی پنهان iOS ۸ باعث میشود که هرکسی که در گوشی آیفون خود دارای اطلاعات مهمی است مانند وکلا ، مدیران شرکتها ، دیپلمات ها ، مدیران بانکها و تجار و حتی شما بتوانید از اطلاعات زیادی که بصورت پنهان درون گوشی خود دارید حتی اگر به زور مجبور به ارائه passcode یا کشیدن اثر انگشت خود روی finger print آیفون بشوید محافظت کنید.

شاید الان بپرسید که اگر من مجبور به ارائه Passcode خود بشوم دیگر همه چیز مانند عکسها ، لیست تماسها و اپ هایی که با انها کار میکردم در دسترس اشخاص دیگر قرار میگیرد، پس چه چیز دیگری قرار است افشا شود؟

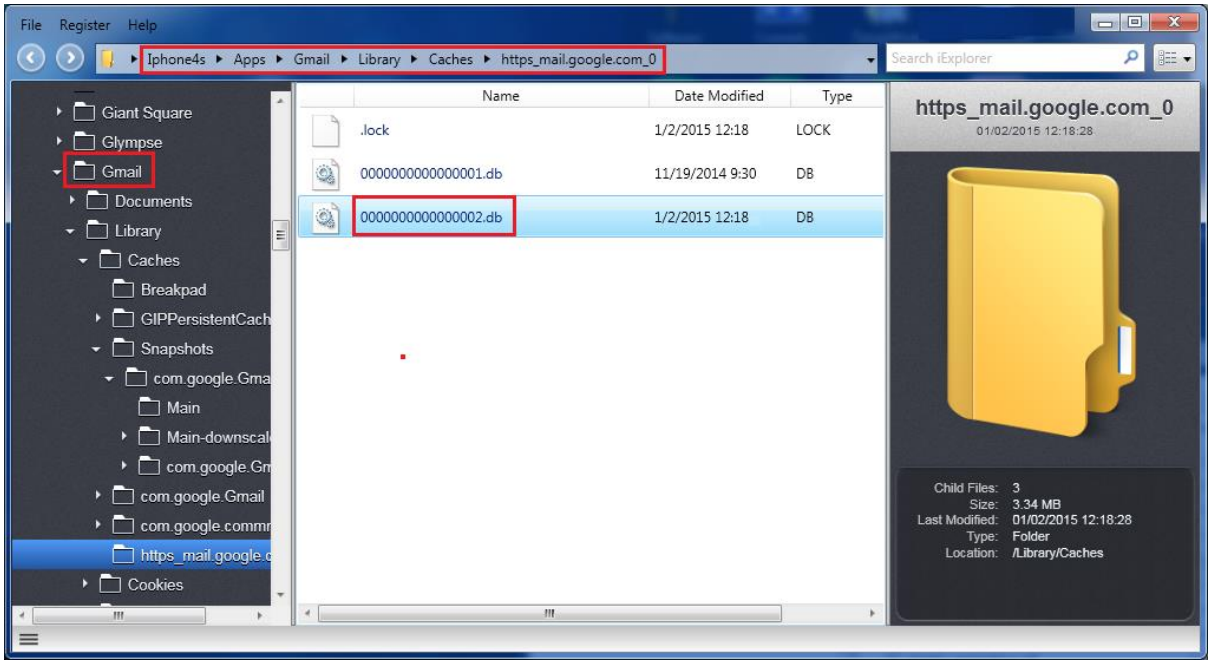
اشتباه نکنید ! شما اطلاعات بسیار بیشتر از آنچه تصور میکنید در گوشی خود دارید. اطلاعاتی که تصور میکنید پاک شده اند اما هنوز در گوشی شما موجود هستند. اطلاعاتی که اپ ها یا iOS بصورت موقتی ذخیره کرده اند ولی همچنان بصورت رها در درون گوشی شما وجود دارند و اگر در دستان اشتباهی قرار گیرند عواقب زیادی ممکن است برای شما داشته باشند.

چه نوع اطلاعاتی در گوشی شما یافت میشوند که در حالت عادی حتی توسط شما قابل دیدن نیستند اما یک هکر یا سازمان میتواند به آنها دسترسی داشته باشد؟

- متن چت هایی که در اپهای پیغام رسانی انجام داده اید و بعد آنها را حذف کرده اید.
- ایمیل هایی که خوانده اید یا فرستاده اید که میتوانند شامل اطلاعات مهم شخصی ، کاری و بانکی باشند.
- تصویر اسکرین شات آخر هر اپی که آنرا مینیمایز کرده بودید.
- تصاویری که توسط اپ های عکاسی یا فیلم برداری آنها را ویرایش کرده بودید یا گرفته بودید و بعدا آنها را حذف کرده بودید اما اپ برای انجام کارهای خود از آنها نمونه موقتی ساخته بوده است.
- تصاویری که توسط اپ های مختلف پیغام رسانی دریافت کرده یا ارسال بودید و بعدا آنها را پاک کرده اید.
- اطلاعات موقتی که بعضی اپ ها در مورد موقعیتهای جغرافیایی شما برای انجام سرویس بهتر به شما ذخیره کرده بودند. که نشان میدهد شما در چه زمانهایی در کجا به سر میبردید.

بررسی یک مثال واقعی در خصوص میزان اطلاعات مهمی که در درون گوشی شما یافت میشود اما توسط شما دیده نمی شوند:

در این مثال ما بعنوان کسی که توانسته است به گوشی شما دسترسی فیزیکی پیدا کرده و بزورpasscode شما را نیز گرفته است (گاهی زور هم نیازی نیست) سعی میکنیم به آخرین ایمیلهایی که در اکانت جیمیل خود با آنها کار کرده اید دسترسی پیدا کنیم حتی اگر الان دیگر از جیمیل logout کرده باشید.

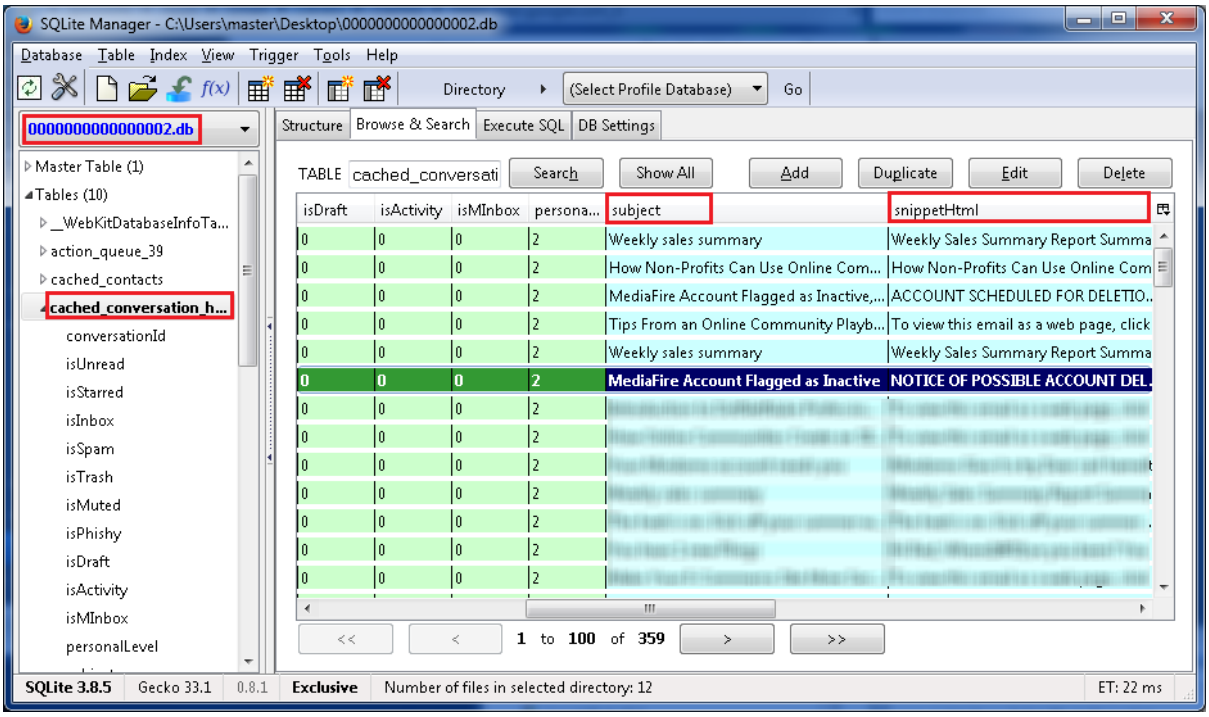


تصویر: هکر آیفون شما را به کامپیوتر وصل کرده و با استفاده از یک نرم افزار محتویات گوشی شما را میخواند.

همانطور که میبینید فولدرها و فایلهای زیادی برای بررسی و کنجکاوری وجود دارند ولی در این مثال ما فقط اپ جیمیل را هدف بازرسی قرار میدهیم. و در مسیری که در تصویر مشخص است دو فایل با پسوند db را پیدا میکنیم. اصولا iOS بطور پیش فرض و برای سرعت اجازه میدهد که برنامه ها بانک اطلاعاتی بنام SQLite را برای ذخیره سازی داده ها مورد استفاده قرار دهند که پسوند این بانکهای اطلاعاتی db می باشند.

اکنون با کمک یک نرم افزار دیگر (SQL lite manager) نگاهی به داخل فایل دیتابیس درون اپ جیمیل می اندازیم. چندین جدول اطلاعاتی درون این دیتابیس دیده میشود.

روی جدول cached_converstion_header کلیک میکنیم و با کمال تعجب میبینیم که تمام ایمیل های اخیر این آیفون در این جدول اطلاعاتی براحتی دیده میشوند!



تصویر: هکر با خواندن بانک اطلاعاتی اپ جیمیل درون آیفون شما براحتی به تمام ایمیل های اخیر شما دسترسی کامل پیدا میکند.

نیازی به گفتن نیست که این ایمیل ها میتوانستند حاوی چه اطلاعات مهمی باشند (از رمز عبور سایتها و اپ های مختلف تا رمز اینترنت بانک و مکاتبه های محرمانه)

درواقع این وضعیت کم و بیش در اکثر اپهای نصب شده روی آیفون شما وجود دارد و مقدار زیادی اطلاعات بصورت محافظت نشده در درون آیفون شما یافت میشود که درحالت طبیعی برای کار اپ ها بکار می روند و حتی خود شما هم از آنها اطلاعی ندارید.

گاهی حتی حذف کردن اطلاعات با استفاده از اپ عملا چیزی را از آیفون شما پاک نمیکند بلکه تنها با یک نشانه (Flag) در دیتابیس SQLite و در برابر آن رکورد اطلاعاتی علامتی بعنوان حذف شده قرار میدهد درحالیکه عملا" اطلاعاتی که مایل به حذف آن بودید به شیوه بالا قابل دسترسی است.

Apple’s Configurator Utility

اگر دقت کرده باشید سرچشمه نفوذ به هر آیفون و محتویات آن از آنجا شروع میشود که آن آیفون بتواند با یک کامپیوتر اطلاعات رد و بدل نماید یا اصطلاحا" Pair شود.

اگر میشد کاری کرد که آیفون شما نتواند با هیچ کامپیوتری Pair شود تمام ابزار نفوذ و خواندن اطلاعات حیاتی از درون آیفون شما از کار می افتند حتی اگر شما مجبور به ارائه passcode خود به هکر یا کسانی بشوید که به زور از شما بخواهد که آیفون خود را آنلاک نمائید.

با از کار انداختن ارتباط و pair شدن آیفون خود با سایر دستگاهها عملا همه راه را برای هرگونه ابزار نفوذی که میخواهد از اطلاعات درون آیفون شما جاسوسی نمائید خواهید بست.

Apple’s Configurator Utility یک ابزار تکنیکی بسیار موثر در برابر هر نیرویی است که سعی دارد به آیفون شما نفوذ نماید.

با تغییر روش رمز گذاری در iOS ۸ انقلابی در زمینه امنیت آیفون بوجود آمد به گونه ای که حتی اپل خود نیز نمی تواند در صورت فشار آوردن مراجع قانونی برای استخراج اطلاعات درون یک آیفون کمکی بکند. لازم به ذکر است که این روش کاملا قانونی است و نیاز به jail break کردن دستگاه شما وجود ندارد زیرا شما از امکانات iOS ۸ برای اینکار استفاده خواهید کرد.

عدم pair lock شدن آیفون به این معناست که دیگر کسی نمیتواند اطلاعات درون فولدرهای داخلی آپ ها و iOS شما را بخواند، کسی نمیتواند اپ جاسوسی روی گوشی شما نصب کند ، هیچ کاری جز دیدن اطلاعات استاندارد گوشی شما نمیتواند انجام دهد. حتی خود شما نیز نمی توانید اینکار را انجام دهید.

پس بعد از pair lock کردن آیفون خود دیگر نگران افشا شدن اسرار پنهان درون آیفون خود حتی اگر بصورت فیزیکی و به زور به آیفون شما دسترسی پیدا کرده باشند نباشید.

روش pair lock کردن آیفون بصورت گام به گام :

درصورتیکه iDeivce به کامپیوترمتصل باشد آنرا از کامپیوتر جدا میکنید.

سپس به مسیر Setting-> General -> Reset رفته و Reset Location & Privacy را انتخاب نمائید. با اینکار کلیه کامپیوترهایی که مجوز دسترسی و pair شدن را با آیفون شما داشته اند دسترسی خود را از دست میدهند. (حتی آنهایی که شما در مورد آنها چیزی نمیدانسته اید)

بعد از اینکه Reset Location & Privacy را انجام دادید مجددا آیفون خود را به کامپیوتر خود با کابل متصل نمائید.

اگر find my iPhone را قبلا برای آیفون خود فعال کرده بودید فعلا آنرا از کار بیندازید بعدا در پایان کار میتوانید آنرا مجددا فعال نمائید.

آخرین نسخه Apple configurator را از Mac App Store دانلود نمائید.

توجه: در حال حاضر فقط برای کامپیوترهای مجهز به سیستم عاملهای اپل (OS x) این ابزار موجود می باشد و اپل هنوز این ابزار را برای کامپیوترهای ویندوز ارائه نداده است !

Apple Configurator را باز نمائید

البته این راهنما بر اساس نسخه ۱,۶ برای iOS ۸ نوشته شده است که قابل استفاده در نسخه های آینده نیز خواهد بود.

Apple Configurator بر اساس ثبت نام iDevice ها در پروفایلهایی ساخته شده است که شما میتوانید روی هر پروفایل محدودیت های خاصی را قرار دهید و آن را تحت نظارت (Supervise) یک تیم امنیتی قرار دهید.

قبل از انجام هرکاری در قسمت Configuration رفته و تیک زیر را بردارید:

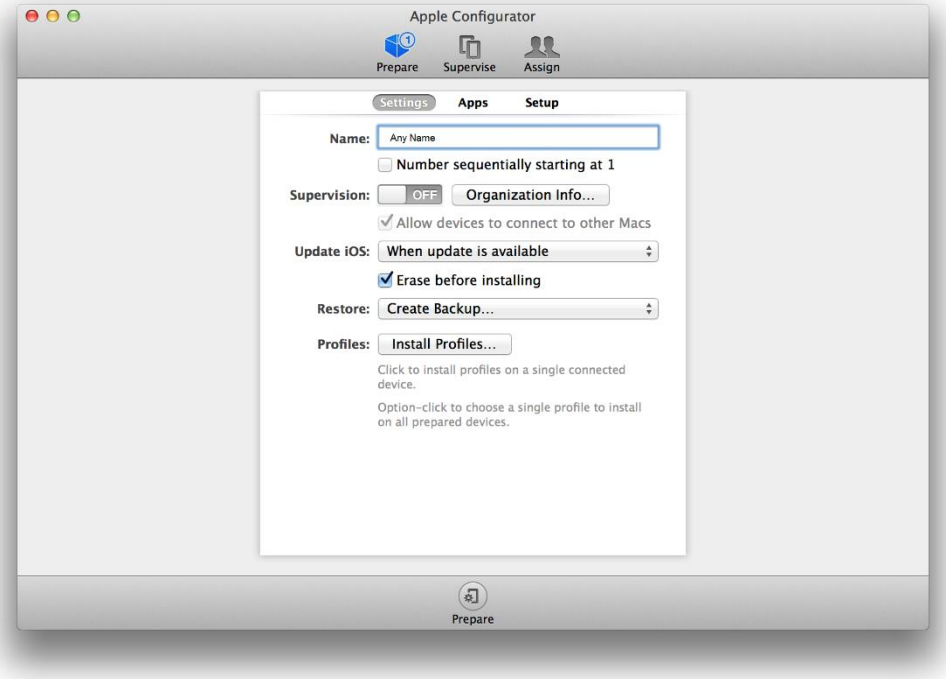
When a supervised device is refreshed:

☐ Remove apps and profiles Configurator did not install

زیرا اگر اینکار را نکنید زمانیکه دفعه بعد دستگاه خود را متصل نمائید کلیه اپ هایی قبل از provisioning نصب کرده اید پاک میشوند!

تهیه پشتیبان از دستگاه شما Create a Backup in Configurator

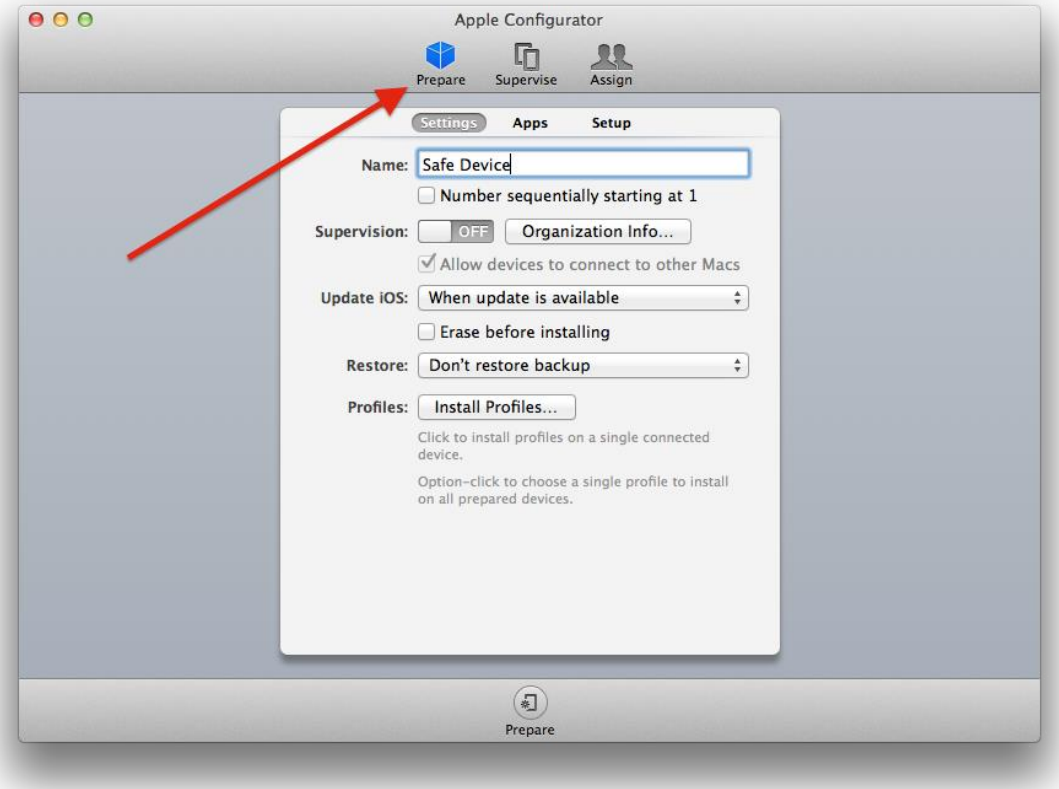
زمانیکه یک iDevice با Apple configurator مدیریت شد شما به شکل قدیم نمی توانید Backup ها را با استفاده از iTunes به آن برگردانید. اگر اینکار را بکنید کلیه اطلاعات شما روی iDevice پاک خواهند شد که این شامل پاک شدن اطلاعات pair lock نیز می باشد.



از منوی Restore گزینه Create Backup را انتخاب نمائید که به شما میگوید که یک آرشیو بک آپ روی کامپیوتر شما بوجود خواهد آورد.

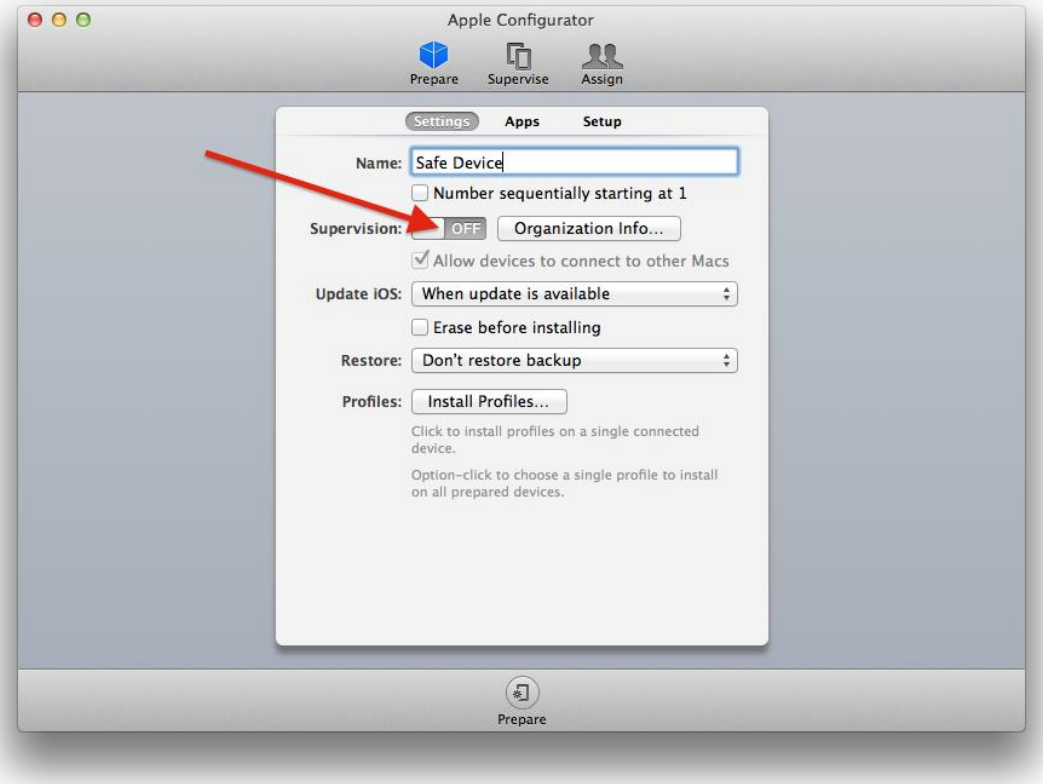
ایجاد نسخه BackUp توسط Apple configurator

آغاز Pair lock کردن آیفون بصورت گام به گام:



بر روی دگمه Prepare کلیک نمائید.

برای دستگاه خود یک اسم انتخاب نمائید (هر اسمی)

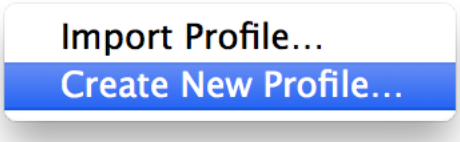


دگمه Supervisioning را به حالت on ببرید

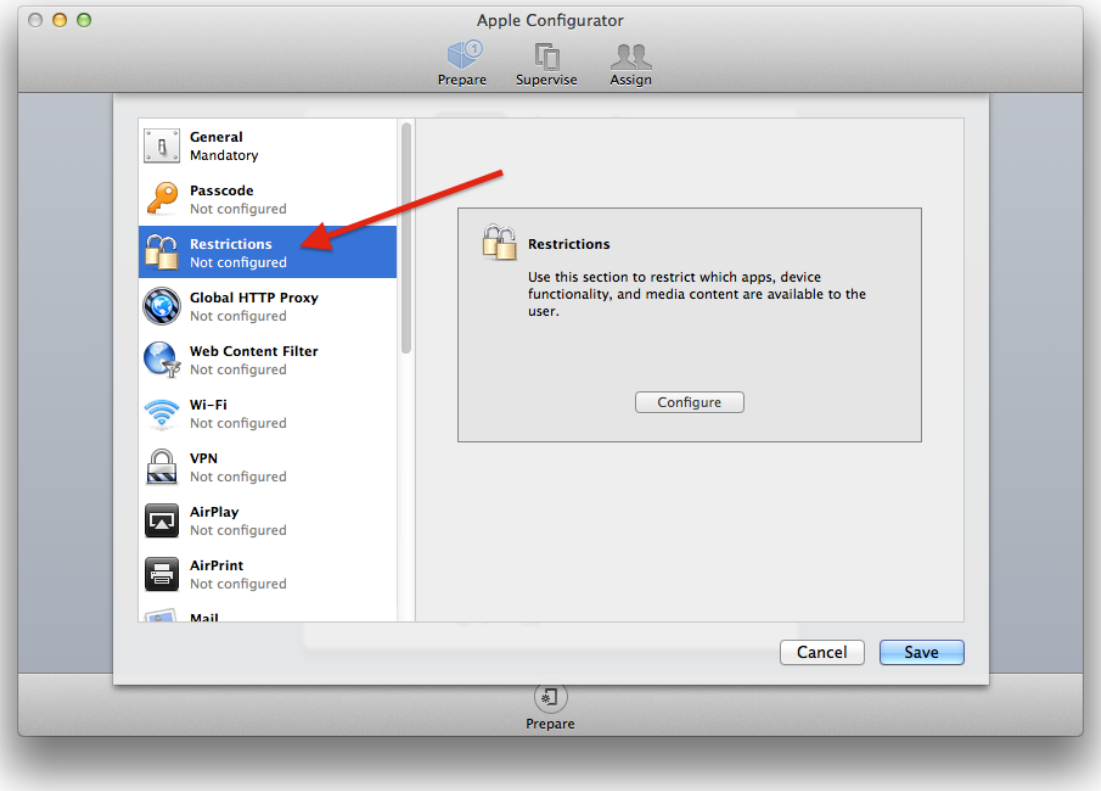
تیک "Allow devices to connect to other Macs" را بردارید.

اگر این کامپیوتر تنها کامپیوتری در دنیا است که میخواهید به آن اجازه دهید که با آیفون شما ارتباط برقرار کند تیک Allow devices to connect to other Macs را بردارید.

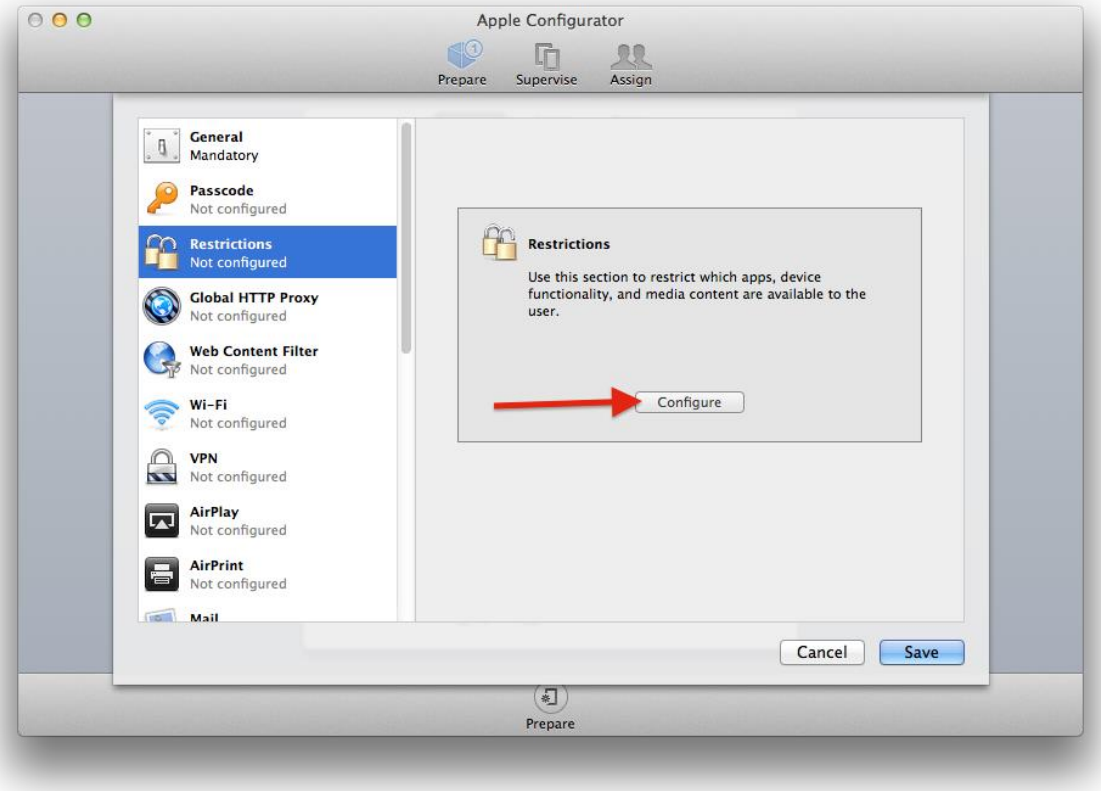
بر روی علامت + در پائین پنجره کلیک نمائید



گزینه "Create New Profile" را انتخاب نمائید



آیتم Restrictions را انتخاب نمائید



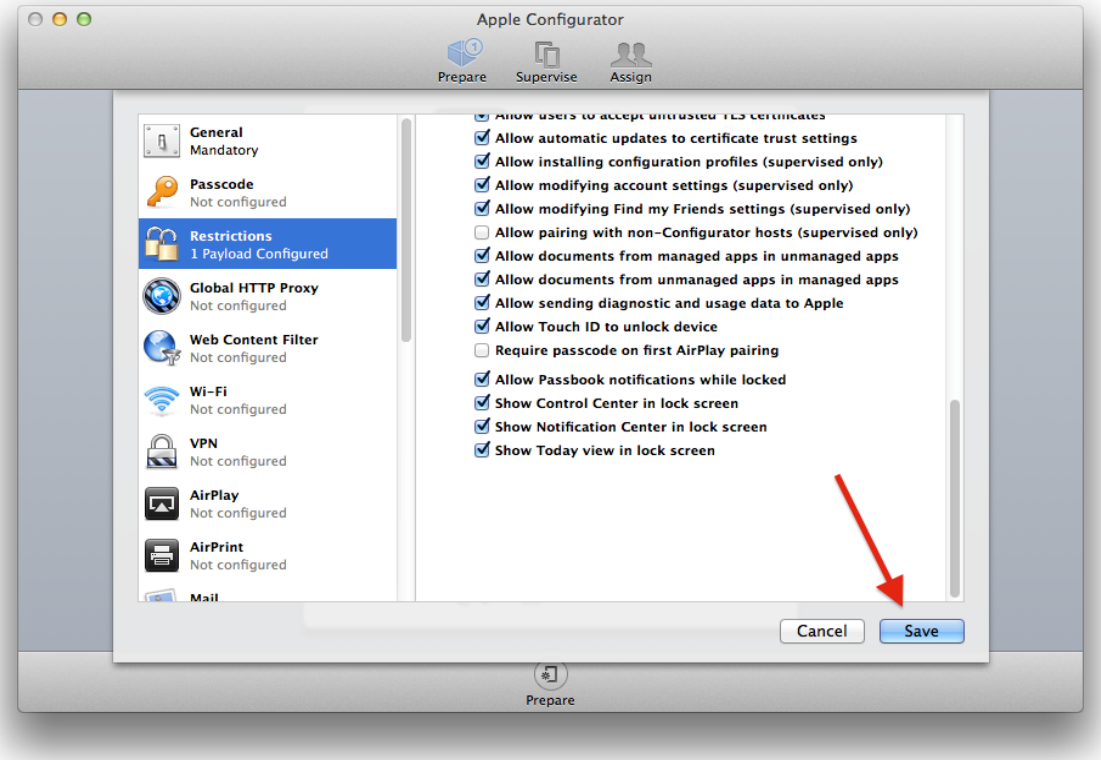
بر روی دگمه Configure کلیک کنید.

روی لیست انتخاب هایی که نمایش می یابد اسکرول نمائید و

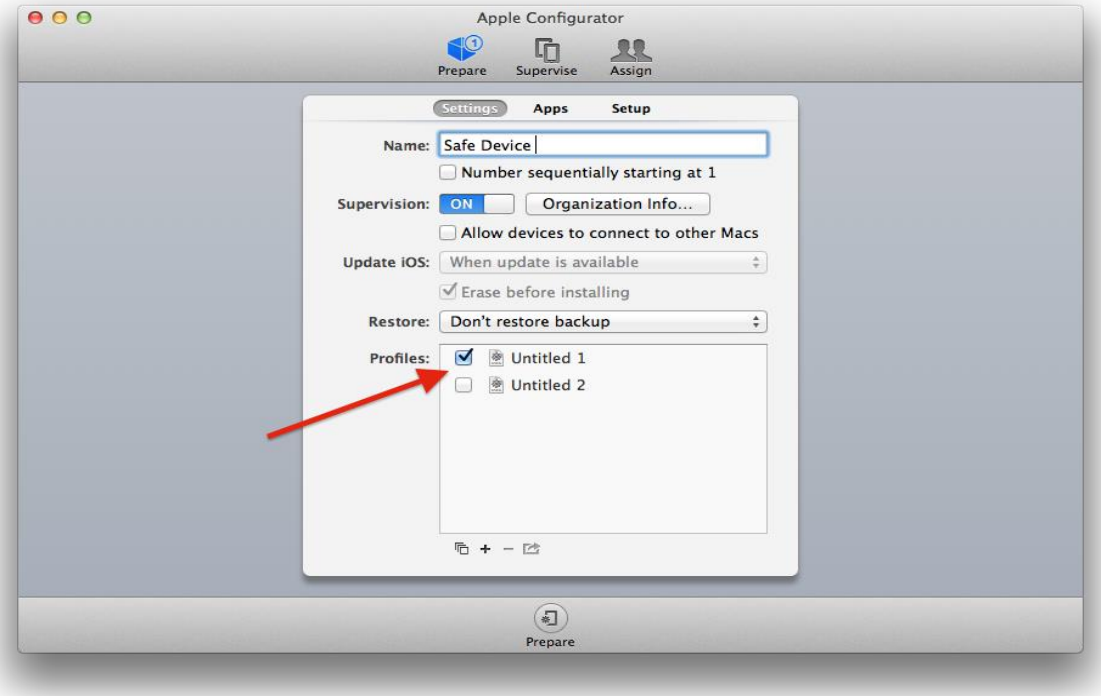
تیک کنار گزینه "Allow pairing with non-Configurator hosts (supervised only)" را بردارید.

بقیه محدودیت ها مثل iCloud restrictions باعث میگردند که هرگز امکان بک آپ گیری روی iCloud یا استفاده از photo Steam برای آیفون شما وجود نداشته باشد.

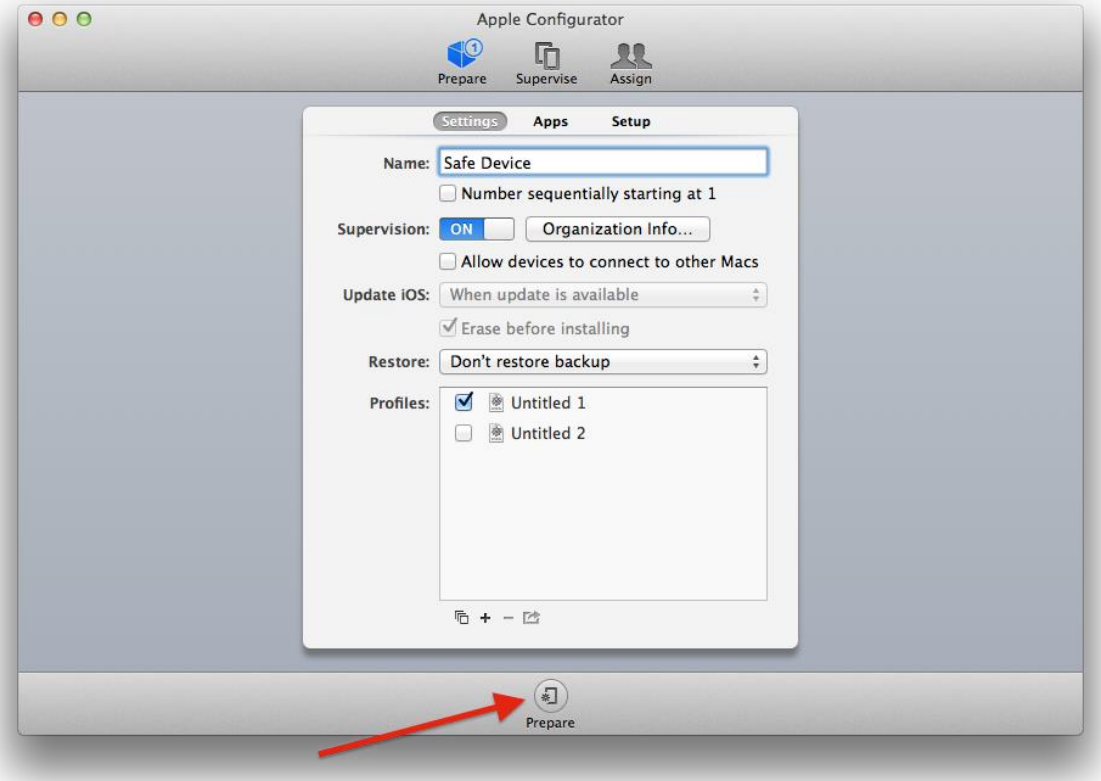
شما میتوانید این محدودیت ها را بسته به امنیتی که نیاز دارید فعال یا غیر فعال نمائید



روی دگمه Save کلیک نمائید تا تغییرات ذخیره شوند.



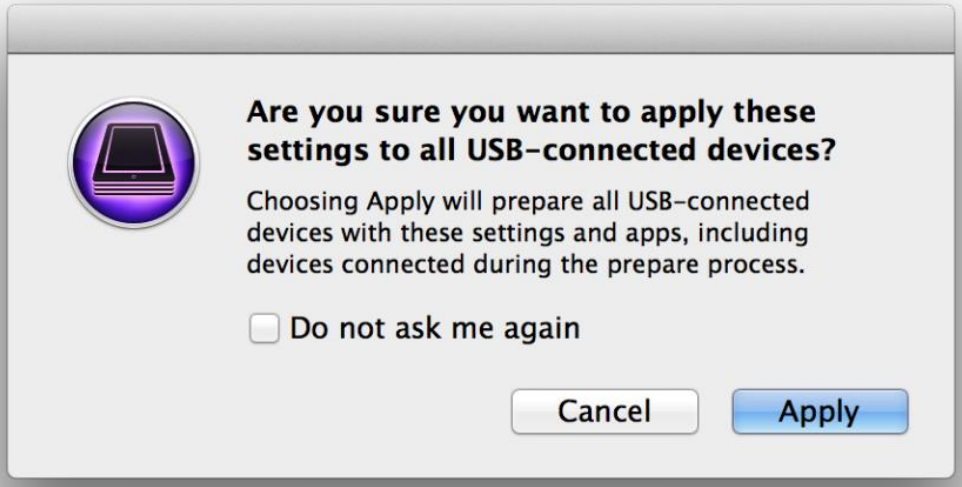
روی تیک پروفایلی که تغییرات را روی آن انجام داده بودید کلیک نمائید و انرا فعال کنید.



بر روی دگمه Prepare کلیک نمائید.

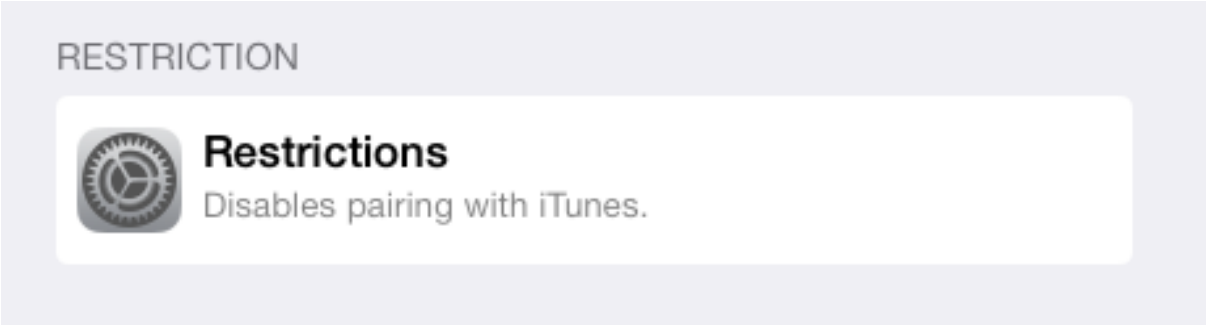
اطلاعات organization information را با هرآنچه مایلید پر نمائید. فقط پر کردن گزینه نام با هر اسمی کافی است.

سپس بر روی دگمه done کلیک کنید.



مطمئن شوید که iDevice شما با کابل به کامپیوتر متصل است و بر روی دگمه Applyکلیک کنید.

بعد از پایان عملیات نصب iOS دستگاه شما از وصل شدن به هردستگاهی خود داری خواهد کرد و بسادگی تمام تقاضاهای Pair شدن را رد خواهد کرد. و کلیه ابزارهای نفوذ و جاسوسی که سعی در ارتباط با آن را دارند بی اثر خواهد کرد حتی اگر passcode شما را نیز داشته باشند.



اگر به قسمت Setting->General->Restrictions مراجعه کنید با شکل بالا روبرو میشوید که اعلام میکند این آیفون pair نمیشود.

Removing a Pairing Profile

اگر پس از چند ماه تصمیم گرفتید که آیفون pair lock شده خود را با یک کامپیوتر یا تعدادی کامپیوتر دیگر pair نمائید بشرط اینکه Set Removal Password را در پروفایل خود Set کرده بوده باشید می توانید lock را بردارید و پروفایل را ذخیره نمائید و سپس روی دگمه رفرش کلیک نمائید تا مشاهده کنید که تغییرات پروفایل روی آیفون شما ثبت گردیده است تا بتوانید از این به بعد آنرا با کامپیوترهای دیگر pair نمائید.

Pair Lock کردن iDevice شما شاید کمی کار داشته باشد ولی در حال حاضر مطمئن ترین روش جهان برای جلوگیری از نفوذ به اطلاعات زیادی میباشد که در درون دستگاه شما موجود می باشد.

چگونه از اینترنت وای فای هتل ها ،فرودگاهها ، کافی شاپ ها و رستوران ها به شکل ایمن استفاده کنیم؟

این روزها ارائه یک اینترنت رایگان به مشتریان توسط صاحبان کسب و کارهایی مانند کافی شاپها و هتل ها و رستوران ها و غیره یک مزیت رقابتی محسوب می شود و مشتریان تمایل دارند از این سرویس رایگان استفاده نمایند. اما باید این موضوع را در نظر گرفت که استفاده از این نوع اینترنت میتواند حریم خصوصی شما را به شدت در خطر قرار دهد.

اگر ارتباط با این نوع اینترنت ها به شکل صحیح رمز نگاری و برقرار نشود یک هکر در همان مکان میتواند اطلاعات رد و بدل شده بین شما و اینترنت را با ابزار نرم افزاری خاصی مورد جاسوسی قرار دهد.

چه نوع اطلاعاتی در یک ارتباط نا امن Wi-Fi توسط هکرها قابل دستیابی است؟

نامهای کاربری و پسورد های محافظت نشده متعلق به ایمیل هایی که توسط پروتکل pop۳ محافظت نشده باشد و همچنین ترافیک و اطلاعاتی که به وب سایتهای اینترنتی میفرستید مانند متن چت ها، آدرس سایتها و متن آنها نیز در معرض خطر می باشند.

استفاده از یک اتصال VPN برای ایمن سازی ارتباطات اینترنتی شما:

Virtual Private Networkingیا به اختصار VPN به زبان ساده روشی است برای اتصال امن به اینترنت از طریق یک کامپیوتر سرور متصل به می باشد. در واقع بصورت مجازی یک تونل رمز شده دیجیتالی در درون اینترنت بین آیفون شما و آن سرور ایجاد میگردد که کلیه اطلاعات در درون این تونل مجازی رمز گذاری شده است و تنها چیزی که هکر ها یا کسانی درصدد فهمیدن کارهای شما با اینترنت هستند این است که شما به آن سرور وصل هستید و دیگر هیچ چیزی قابل ردیابی نیست.

با کمک VPN دیگر اهمیتی ندارد از طریق وای فای رایگان یک کافی شاپ به کارهای بانکی خود برسید یا در زمانیکه یک ساعت مانده به پرواز خود در فرودگاه به ایمیل های شخصی خود رسیدگی کنید در هر صورت VPN اتصال شما را با اینترنت ایمن میکند.

البته توجه داشته باشید که یک فروشنده اتصال VPN باید معتبر باشد و در زمینه ایجاد VPN امن تخصص داشته باشد و همچنین توصیه میکنم از خرید اکانتهای VPN متفرقه و ارزان ایرانی خود داری نمائید.

نحوه اتصال و تنظیم آیفون شما برای کار با اینترنت در سایت این فروشندگان حرفه ای VPN وجود دارد و شما بعد از دریافت اطلاعات VPN خود میتوانید به کمک آن سایتها تنظیمات لازم را انجام دهید.

سایر مزایای استفاده از اتصال VPN عبارتند از:

- جلوگیری از شنود اطلاعاتی که بین شما و سرور VPN مبادله میشود شامل اطلاعات بانکی ، ایمیل ها ، متن چت ها ، سایت هایی که مشاهده میکنید و سایر اطلاعات خصوصی.
- تغییر IP آدرس شما و پنهان کردن آدرس اینترنتی واقعی شما که باعث میشود تمامی سایتها و سرویسهای اینترنتی تصور کنند شما از جای دیگری به غیر از محل خود به اینترنت وصل میشوید. چون عملا IP کامپیوتر سروری که شما از طریق آن به اینترنت هستید برای آنها بعنوان آدرس اصلی شناسایی میشود و خوداین موضوع به افزایش حریم شخصی شما کمک میکند.
- بالا رفتن امنیت در زمان کار با اینترنت زیرا اطلاعات شخصی شما مانند نام ، شماره کارت اعتباری ، کلمات عبور بصورت امن با کمک VPN منتقل میشوند و نه تنها جاسوسی برای هکر ها بلکه برای سایر سازمانهایی مثل NSA نیز که ماهیتا نقش جاسوسی دارند بسیار مشکل و گاها" غیر ممکن میشود.
- باز کردن سایتهایی که در یک کشور محدود شده اند یا سایتهایی که فقط برای یک سری کشورهای خاص قابل استفاده هستند نیز با کمک VPN میسر میباشد چون از لحاظ تئوری شما میتوانید از فروشنده سرویس VPN خود بخواهید اتصال به سرورهایی را که در کشورهایی که مورد نظر شما هستند را فراهم آورد تا بدینگونه از مزایای داشتن آدرس اینترنتی در خاک آن کشورها نیز برخوردار گردید.
- اگر مایل هستید بصورت ناشناس در اینترنت وبگردی نمائید و کمترین اطلاعاتی از خود را در اختیار در اختیار آن سایتها قرار ندهید باز هم استفاده از VPN گزینه بسیار خوبی می باشد.
- شرکتی که اینترنت را برای شما فراهم کرده است نمیتواند بررسی کند که شما از کدام سایتها دیدن کرده اید و اصولا نمی تواند ردی از کارهای اینترنتی شما داشته باشد.جز اینکه شما به یک سرور VPN وصل بوده اید.

انواع پروتکل های VPN و انتخاب ایمن ترین VPN برای آیفون شما.
تعدادی از پروتکلهای استاندارد VPN عبارتند از :

نام استاندارد VPN	میزان رمز گزاری	ساپورت توسط آیفون	آیا توصیه میشود؟
PPTP VPN	ندارد	بله	خیر
L۲TP VPN	متوسط	بله	برای امنیت ساده
SSTP VPN	بالا	خیر	ساپورت نمی شود
OPEN VPN	بالا	بله	برای امنیت بالا

همانطور که در جدول مشاهده میکنید تنها پروتکل های l۲tp و open VPN برای آیفون مناسب می باشند و در بین این دو OPEN VPN انتخاب بهتری بوده و بسیار امن می باشد.

کدام اپلیکیشن های پیام رسان ایمن هستند؟

بسیاری از ما شاید کار خاصی انجام ندهیم یا حرفی نمی زنیم که نگران افشا شدن آن باشیم اما با این وجود همه ما دوست داریم حریم خصوصی ما حفظ شود و شخص دیگری در جریان مکالمات و پیامهای ارسالی و دریافتی ما قرار نگیرد.

آیا شما علاقمند هستید حتی وقتی دارید در مورد مسائل ساده روزانه خود با همسر یا دوست خود صحبت میکنید شخص سومی درحال گوش کردن باشد؟

مسلما جواب خیلی از شما منفی است. در هر صورت مکالمات شما متعلق به شماست و حریم شخصی شما می باشد پس نباید اجازه دهید تا جایی که ممکن است هیچ شخص سومی آنها را شنود نماید.

امنیت اپلیکشن های موبایل پیام رسان بسیار مهم می باشد چون عملا بجز تماس تلفنی اصلی ترین راه ارتباطی بین افراد شده است. به همین دلیل تلاش برای جاسوسی از آنها از روشهای مختلف وجود دارد.

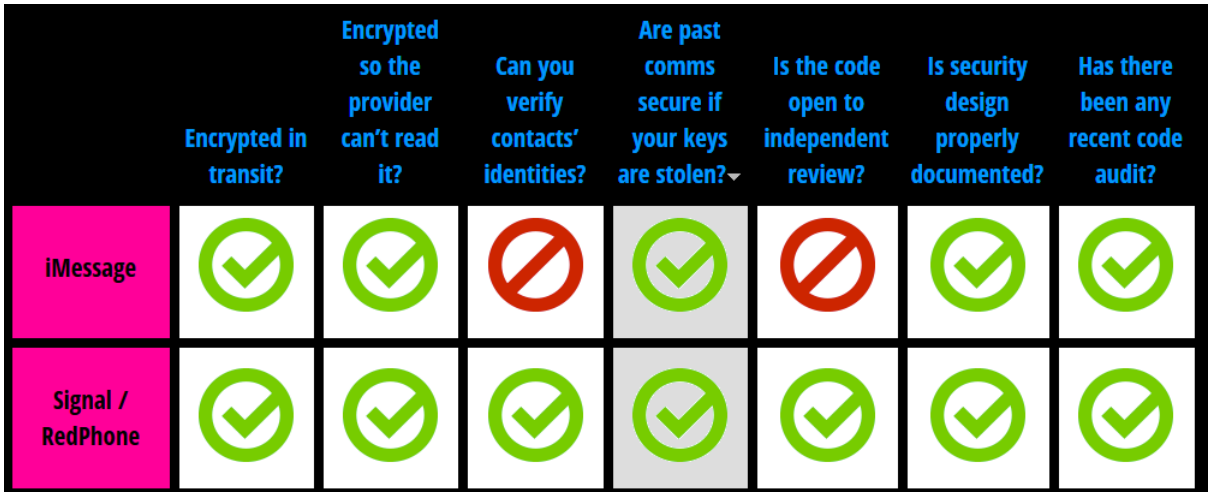
اما نگران نباشید هنوز راههایی برای ایمن ماندن ارتباطات شما وجود دارد.

بنیاد Electronic Frontier که در زمینه حفاظت از امنیت سایبری کاربران اینترنت فعال است تحقیقات جدی را در این خصوص انجام داده است و ده ها نرم افزار پیام رسانی معروف را از چند جهت مورد مطالعه امنیتی قرار داده است.

این پارامترها عبارتند از:

- رمزگذاری پیام در مسیر بین فرستنده و گیرنده
- غیر قابل خوانده شدن پیام رمزگذاری شده برای ارائه دهنده اپلیکیشن/سرویس
- امکان تائید هویت لیست دوستان برای کاربر
- حفظ ایمنی پیام‌های رد و بدل شده پیشین کاربر، حتی در صورت دزدیده شدن یا افشای کلید برنامه رمزگذاری
- در دسترس بودن برنامه رمزگذاری برای بررسی ایمنی آن توسط کارشناسان مستقل
- ثبت و اسنادی کردن دقیق و درست طراحی امنیتی برنامه
- انجام ارزیابی عملکرد برنامه رمزگذاری

مسلما هرچه تعداد بیشتری از این پارامترها در اپ مورد تائید قرارگرفته باشد آن آپ قابلیت اطمینان بیشتری دارد. این نتایج در https://www.eff.org/secure-messaging-scorecard برای بررسی شما و انتخاب اپ امن متناسب با نیاز شما قابل دسترسی است.



تصویر بررسی نتایج ارزیابی در مورد نرم افزار iMessage Apple و Signal و RedPhone

در حال حاضر و طبق تحقیقات این بنیاد اپ های ارتباطی زیر دارای بالاترین امنیت نسبت به سایر اپهای پیام رسانی برخوردار هستند:

Signal (By Open Whisper Systems)

Silent Phone

Telegram (In secret chat mode only)

بد نیست نگاهی هم به چند اپ معروف غیر ایمن بیندازیم

تصویر- وضعیت امنیتی چند اپ پیام رسانی معروف جهان که بسیار نامناسب می باشند.

بحث اصلی این است که همه باید اهمیت رمزگذاری را درک کنند و زمانیکه اپ هایی ایمن و رایگان برای اینکار وجود دارد واقعا چه دلیلی دارد از اپهای غیر ایمن استفاده نمائید و امنیت و حریم خصوصی خود را به خطر بیندازید.

پس همین امروز با قاطعیت به دوستان و آشنایان خود اطلاع دهید که از این به بعد شما فقط در اپ های امنی مثل Signal ، ChatSecure + Orbot، CryptoCat، Signal / RedPhone، Silent Phone، Silent Text، TextSecure و Telegram حضور دارید. تا این فرهنگ رفته رفته جای خود را در میان باز نماید که امنیت ارتباطات یک ضرورت است و این حق شماست که حریم خصوصی شما توسط هیچ هکر یا سازمانی نقض نشود.

برای انتقال و اشتراک ایمن فایلهای شخصی خود با دیگران از چه اپ ها و سرویسهایی استفاده کنیم؟

شاید اولین چیزی که در ذهن شما بعنوان خواننده این مطلب خطور نماید سرویسهای google drive , drop box باشد. اما باید بگویم این سرویسها اگرچه امکانات فوق العاده ای در اختیار شما قرار میدهند اما صاحبان آنها کاملا به اطلاعاتی که در درون این سرویسها آپلود میکنید دسترسی داشته و اصولا به یاد داشته باشید هرآنچه که به سرویسهای به اصطلاح ابری اپلود میکنید و بعدا سعی در حذف آن داشته باشید عملا بصورت واقعی حذف نخواهند شد بلکه تنها بصورت منطقی حذف میگردند و توسط صاحبان این سرویس ها قابل دسترسی در آینده نیز میباشند.

آیا شما حاضر هستید که اطلاعات و اسرار و تصاویر مهم خود را در دست کس دیگری غیر از کسانی که به آنها اعتماد دارید قرار دهید؟ بعلاوه این سرویسها در صورت نیاز همه اطلاعات شما را با حکم قضایی در اختیار مراجع قانونی نیز قرار میدهند.

حالا باز هم در این مورد فکر کنید که طرح های تجاری ، اطلاعات مالی ، شرکتی ، اطلاعات شخصی ، تصاویر شخصی و خانوادگی و دهها مطلب مهم و غیر مهم میتوانند در این سرویسها قرار بگیرید و اگر روزی در دست هکر یا سازمانی قرار بگیرند می توانند عواقب غیر قابل جبرانی برای شما داشته باشند.

گزینه اول: Spider Oak

Spider Oak یک سامانه اشتراک فایل ابری مانند دراپ باکس یا گوگل درایو است با این تفاوت مهم که 'Zero-knowledge' میباشد یعنی اینکه هرگز اطلاعات شما بدون رمز گزاری روی سرورهای ابری قرار نمیگیرد و هرگز اطلاعات شما توسط کارمندان این شرکت بدلیل رمز نگاری شدن قابل خواندن نیست همچنین از بیرون نیز هکرها نمیتوانند فایلهای شما را تحت هیچ شرایطی بخوانند و حریم خصوصی شما را به خطر بیندازند.

این سیستم از سه قاعده برای رمز نگاری شما استفاده میکند.

یک Encrypted Storage :

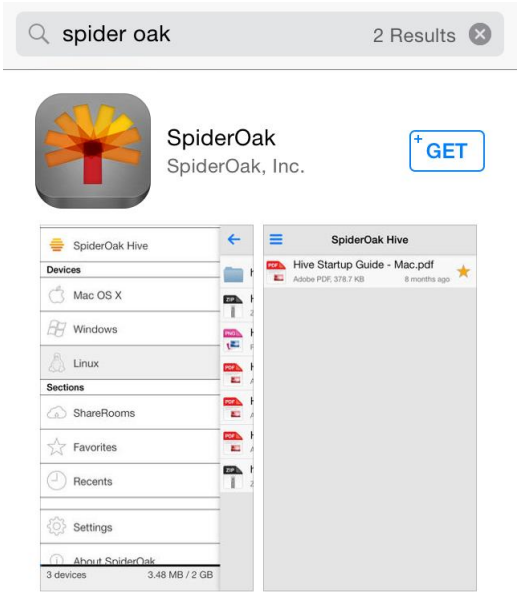
کلیه اطلاعات شما در سرورهای این سرویس بصورت end-to-end رمز نگاری میشوند و تنها شما میتوانید با دادن پسورد خود به آنها دسترسی داشته باشید.

دو Password Protection :

رمزنگاری کردن داده های شما روی سرورهای ابری تنها نیمی از موضوع امنیت شما را تامین میکند، اما اگر کسی به غیر از شما به این کلمه عبور دسترسی داشته باشد یعنی اینکه اطلاعات شما در دسترس او نیز خواهد بود. در Spider Oak هیچ کلمه عبوری از شما ذخیره نمیگردد و معنی آن این است که شما مالک داده ها و فایلهای خود خواهید بود.

سوم No Knowledge

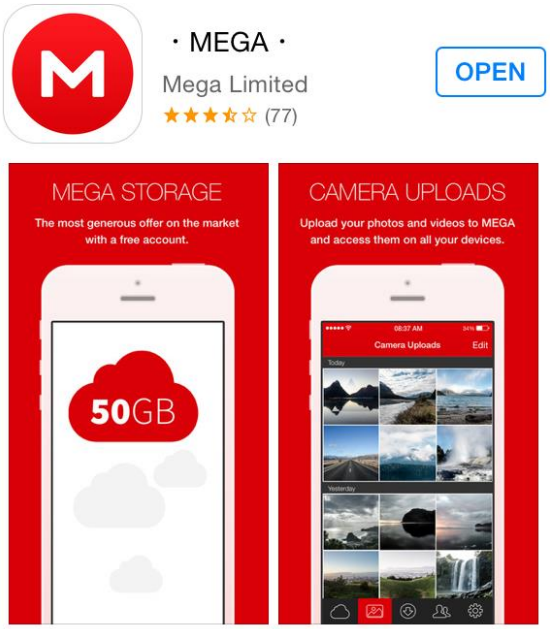
اگر کارمندان خود شرکت Spider Oak به سرورهای شرکتشان دسترسی فیزیکی پیدا کنند آنها حتی قادر به دیدن نام فایلها و فولدرهای شما نخواهند بود و تنها تعدادی اعداد اتفاقی را میبینند که شامل اطلاعات رمز نگاری شده شما می باشد و قادر به آشکارسازی فایلهای رمز نگاری شده شما نخواهند بود.



نمایی از اپ SpiderOak در AppStore

گزینه دوم Mega

Mega نیز یک گزینه دیگر برای آپلود ایمن اطلاعات شما روی اینترنت می باشد که در حالت رایگان تا ۵۰ گیگابایت فضا در اختیار شما قرار میدهد. و از End-to-End Encryption در زمان انتقال داده های شما استفاده کرده و کلیه اطلاعات شما بصورت رمز نگاری شده و توسط یک کلید نگهداری میشوند که تنها با این کلید میتوان این اطلاعات را از حالت رمز درآورد.



گزینه سوم : Bleep

Bit torrent که در زمینه انتقال داده ها بدون سرور مرکزی مشهور می باشد آپ جالبی به اسم Bleep ساخته است که دارای امکانات امنیتی بالایی می باشد.

اگر میخواهید تعدادی از تصاویر و فایلهای خود را برای کسی بفرستید اما اصلا تمایلی به نگهداری آنها در فضای ابری حتی ایمن هم ندارید این گزینه برای شما وجود دارد . با کمک اپ bleep شما میتوانید عکسهایی و فایلهایی را که مایل به ارسال آنها به گوشی هوشمند شخص دیگر هستید را ارسال نمائید.

همچنین امکان چت صوتی و متنی کاملا ایمن نیز وجود دارد.

نکته جالب این است که برخلاف نرم افزاری مثل WhatsApp که شما را مجبور به ارائه دسترسی به کل لیست تماس خود میکند شما میتوانید دسترسی به لیست تماس خود را از نرم افزار bleep بگیرید و تنها با اسکن کردن تصویر(QR barcode) رمز بلیپ دوستان خود (bleep code) می توانید به شکل کاملا ایمن با آنها ارتباط برقرار نمائید و دوستان شما میتواند مستقیما با شما از طریق صدا و متن در ارتباط باشند و در این میان هیچ چیزی در سرورهای ابری ذخیره نخواهد شد و همه چیز رمز خواهد گردید.

این اپ برای وقتی که مایل به ارسال فایلهایی برای مخاطب خاصی باشید روش خوب و ایمنی می باشد و کلیه اطلاعات شما در زمان انتقال به تلفن همراه مخاطب شما بصورت End-To-End رمزگذاری میشود.

همچنین در حالت "Go to Whisper" بعد از زمان مشخصی کلیه چت های شما از موبایل طرف مقابل نیز پاک میشود.

	Bleep	Whatsapp	iMessage	Viber	Snapchat	Facebook
Free Service	✓	Freemium	✓	✓	✓	✓
Voice Calls	✓	✓	✓	✓	✗	✓
P2P: No Cloud, No Leak, No Metadata	✓	✗	✗	✗	✗	✗
End-to-end Encryption	✓	✗	✓	✗	✗	✗
Native App for All Platforms	✓	✗	✗	✓	✗	✗

جدول مقایسه امنیت Bleep با تعدادی از App های مشهور پیام رسانی دیگر

توصیه های امنیتی در خصوص دو نرم افزار معروف پیام رسانی :

چرا واتساپ انتخاب امنی برای انتقال پیامها ، عکس ها و ویدئوهای خصوصی شما نمی باشد؟

انتقال پیام ها ، عکس ها و فیلم های کوتاه در این نرم افزار رواج فراوان دارد و من میدونم که اکثر شما و دوستانتان یا از این اپ معروف استفاده میکنید یا حداقل آن را میشناسید و همانطور که میدانید کمپانی فیس بوک مالک آن می باشد.

اما بنا به دلایل زیر از ارسال پیامهای خصوصی مثل اطلاعات مالی شرکت و فایلهای خصوصی خود با استفاده از این نرم افزار خود داری کنید و از اپ های امن تری که قبلا معرفی کردم استفاده کنید.

واتساپ در مرحله ثبت نام شماره تلفن شما را درخواست میکند و درصورتیکه هک شوید برای هکر کاملا مشخص است که این اطلاعات متعلق به چه کسی بوده است و راه سوء استفاده های بعدی فراهم می باشد.

واتساپ از ذخیره سازی ابری در سرورهای خودشان استفاده میکنند یعنی همواره یک کپی کامل از چت ها ، عکس ها و فیلم های شما بر روی سرورهای آنها موجود است. این موضوع برای پیامهای عادی ظاهرا" اهمیتی ندارد اما بنظر شما این مساله برای پیامها و عکسهای خصوصی شما هم بی اهمیت می باشد؟

اطلاعات شما تنها در زمان انتقال رمز نگاری میشود اما بر روی سرورهای فیسبوک و توسط کمپانی فیسبوک کاملا" قابل دسترسی است.

چگونه از Telegram به شیوه امن برای انتقال پیامهای خصوصی خود استفاده کنیم و از هک شدن اکانت تلگرام خود جلوگیری نمائیم.

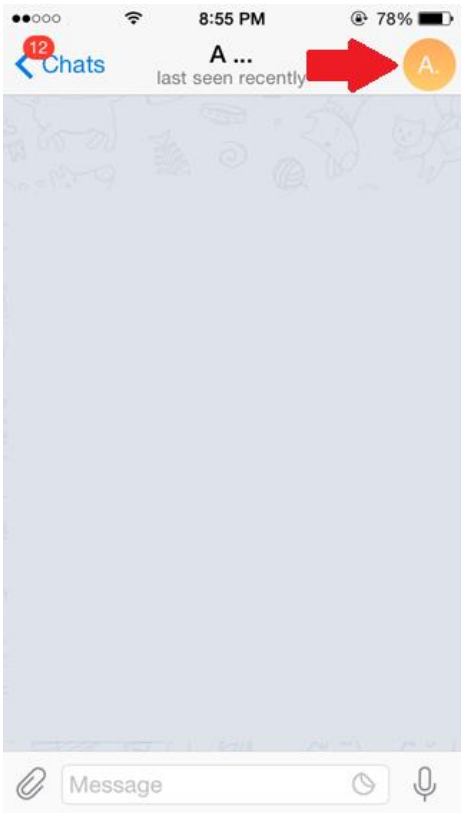
نرم افزار پیام رسانی Telegram نرم افزار محبوب دیگری می باشد که بعد از WhatsApp علاقمندان زیادی پیدا کرده است. نکته مهم در خصوص این نرم افزار آن است که این نرم افزار اگر به شیوه درست استفاده شود میتواند برای ارتباط امن مورد استفاده قرار گیرد ولی در صورت استفاده غیر صحیح میتواند امنیت شما را به خطر اندازد.

برای استفاده امن از تلگرام موارد را رعایت نمائید.

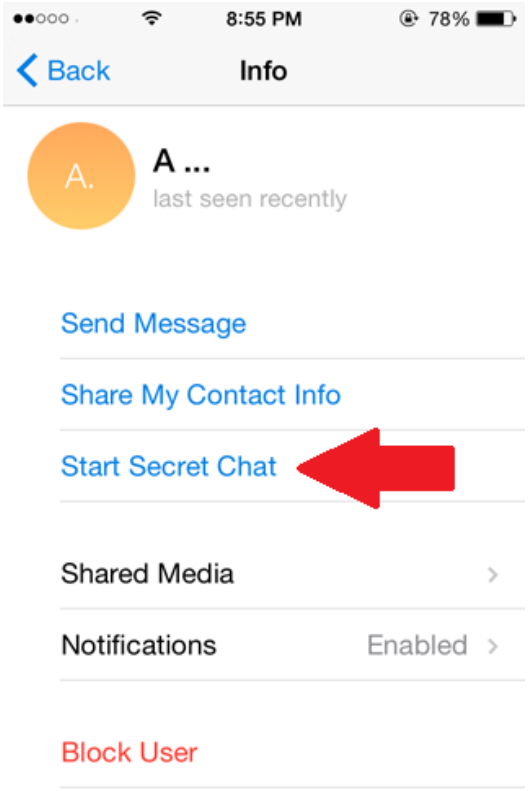
اگر میخواهید هیچ سابقه ای از چت ها و پیامهایی که برای یک شخص خاص می فرستید بر روی سرورهای تلگرام باقی نماند:

ابتدا شخص مقابل را از روی لیست دوستان انتخاب نمائید

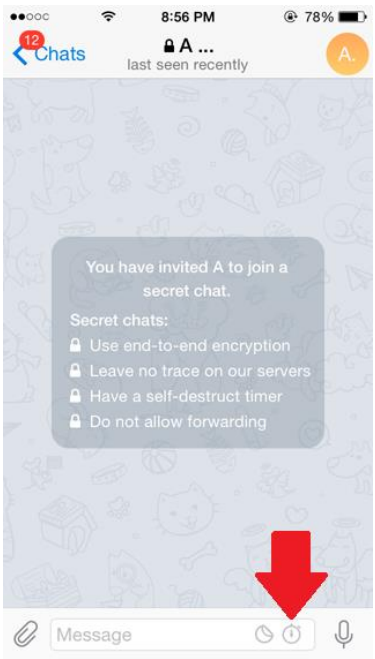
سپس آیکون پروفایل تصویر دوست خود در قسمت گوشه سمت راست صفحه انتخاب نمائید.



گزینه Start Secret Chat برای شروع ارتباط امن انتخاب نمائید



تلگرام در این حالت تمام ارتباطات و فایلهای ارسالی و دریافتی را رمز میکند و برای مدت زمان محدودی اجازه می دهد طرف مقابل اطلاعات دریافتی را بخواند و پس از آن اطلاعات رد و بدل شده را کاملا پاک میکند و هیچ اثری از آنها بر روی سرورهای تلگرام وجود نخواهد داشت . با انتخاب آیکون ساعت میتوانید مدت زمانیکه شخص مقابل مجاز است اطلاعات را از لحظه دیدن آنها داشته باشد تنظیم نمائید. که این زمان بین یک ثانیه تا یک هفته قابل تنظیم است .



توجه داشته باشید که کلیه چت ها و عکس های ارسالی فقط برای همین مدت زمان توسط شخص مقابل قابل دیدن می باشد و در صورتیکه او سعی کند از صفحه اپلیکیشن تلگرام عکس بگیرد، تلگرام این موضوع را به اطلاع شما خواهد رساند.

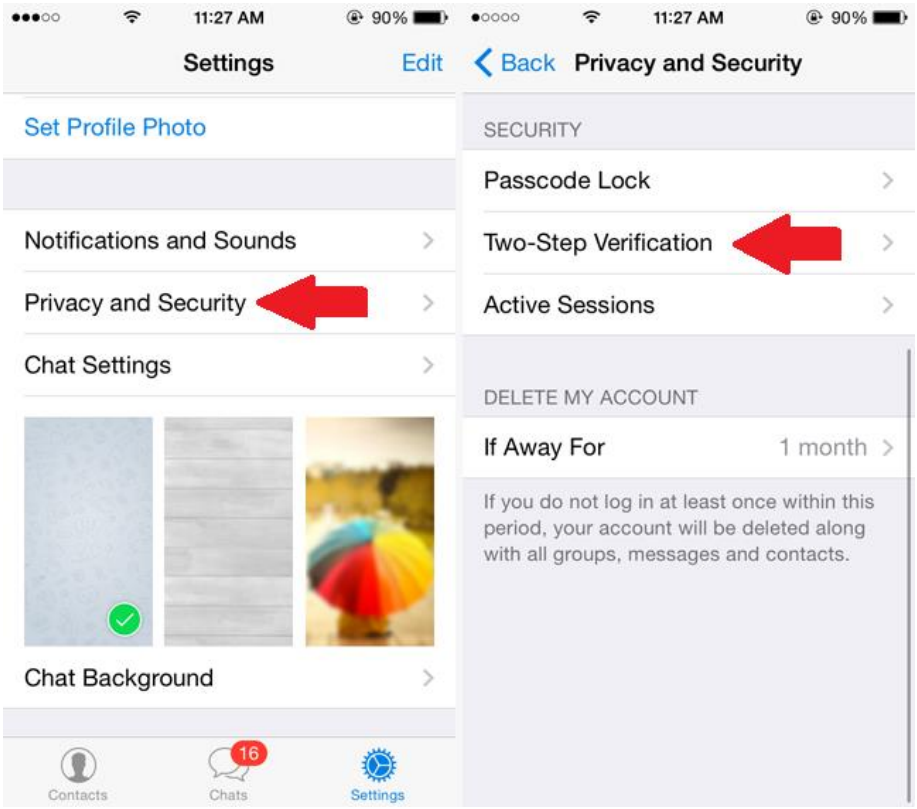
چگونه از هک شدن اکانت Telegram جلوگیری کنیم

اپلیکشن تلگرام برای ثبت نام شما کدی منحصر به فرد را به شماره تلفنی که وارد کرده اید ارسال میکند تا شما با ورود آن کد نشان دهید که صاحب آن شماره موبایل می باشید و هویت خود را تائید نمائید.

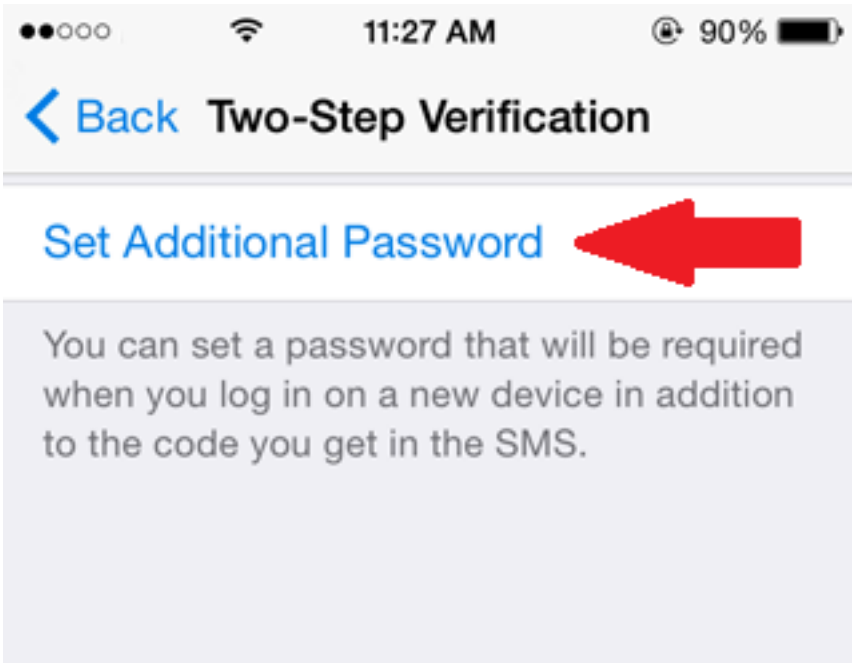
اما این راه حل کافی نمی باشد و ممکن است هکر با سرقت سیم کارت شما یا دسترسی غیر مجاز به آیفون شما سعی کند به اکانت تلگرام شما نفوذ نماید.

برای سخت کردن کار هکرها در هک کردن اکانت تلگرام اکیدا" توصیه میکنم سیستم تائید دو مرحله ای را به شیوه زیر فعال نمائید. سیستم تائید دو مرحله ای باعث می شود هر زمان شخصی سعی نماید از طریق موبایل یا نسخه تحت وب تلگرام وارد اکانت شما گردد یک کلمه عبور که شما قبلا تعیین کرده اید از او پرسیده شود و به این ترتیب جلوی هک شدن اکانت شما گرفته شود.

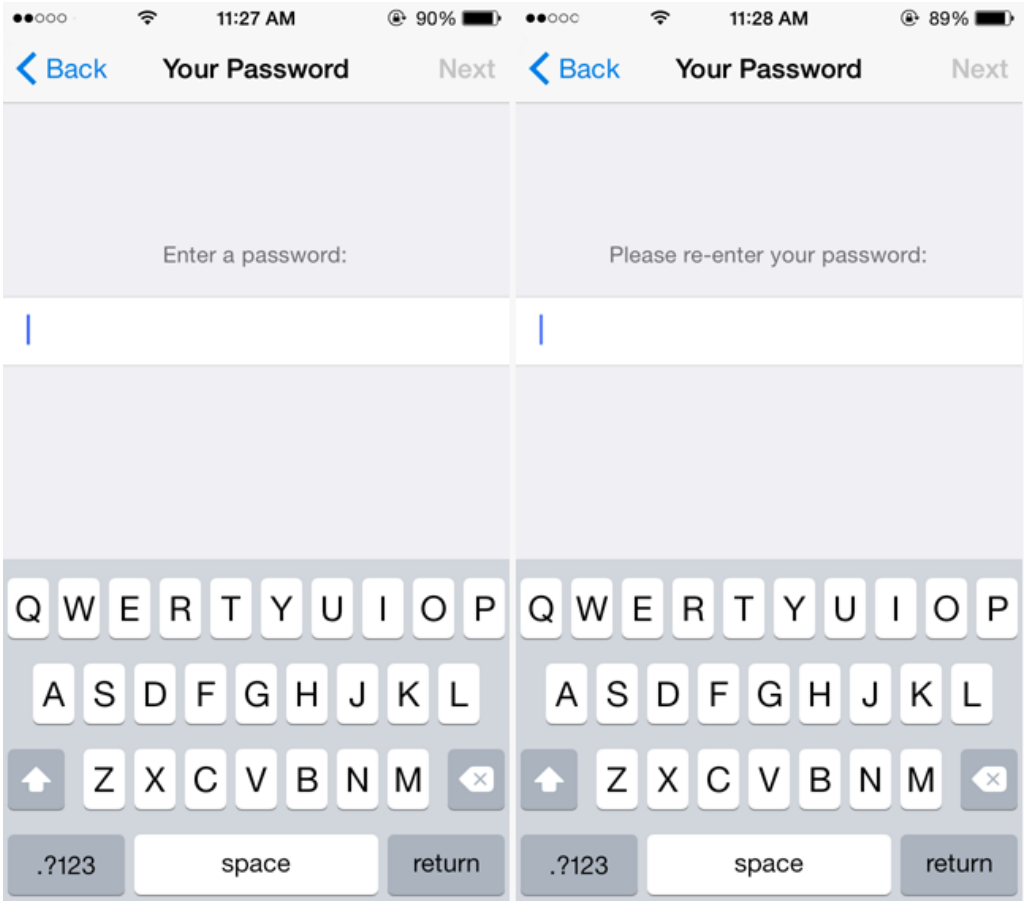
۱. وارد اپلیکیشن Telegram شوید و این گزینه را
انتخاب نمائید: Setting->Privacy and Security -> Two-Step verification



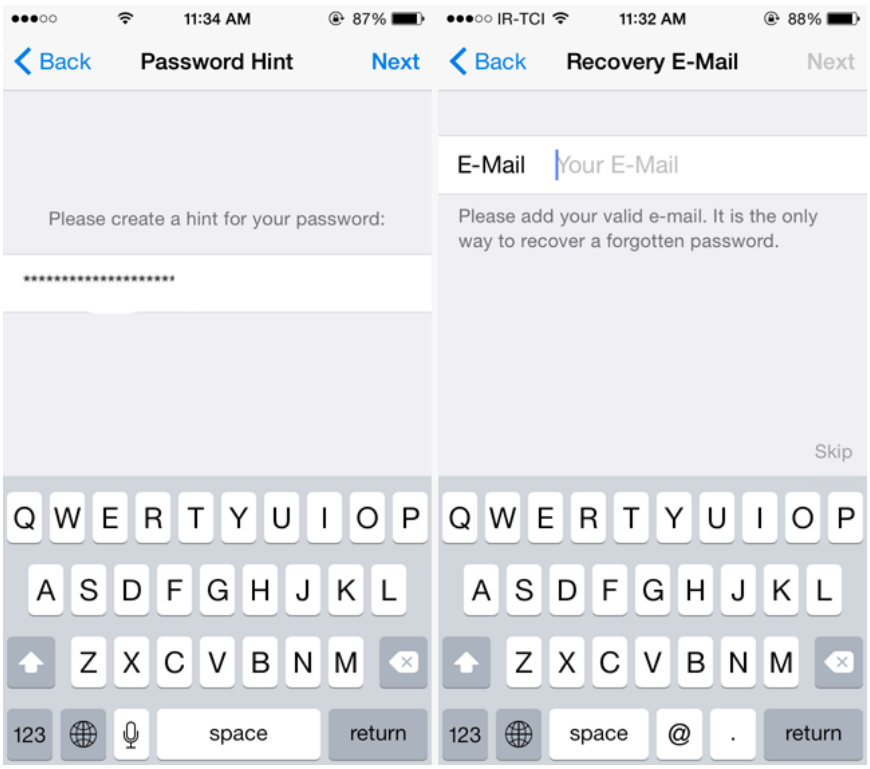
۲. گزینه Set Additional Password را انتخاب نمائید. با وارد کردن این پسورد و پس از تائید آن در آینده برای ورود به اپلیکیشن تلگرام چه نسخه موبایل و چه نسخه وب این پسورد از شما پرسیده خواهد شد پس آنرا بخاطر بسپارید. همچنین دقت کنید که طول این پسورد کمتر از ۱۵ کاراکتر نباشد تا هکرها براحتی نتوانند پسورد شما را حدس بزنند.



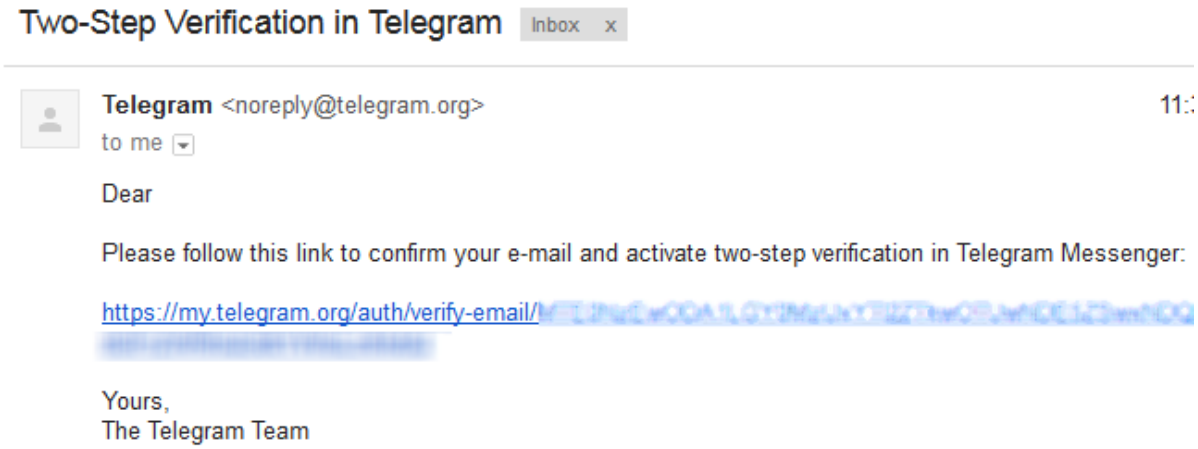
۳. پسورد انتخابی خود و تکرار آنرا وارد نمائید.



۴. در مرحله بعدی از شما درخواست میگردد اگر تمایل دارید حروفی برای یادآوری پسورد توسط خودتان وارد نمائید .همچنین یک ایمیل معتبر برای ارسال لینک تائیدیه نیز به تلگرام معرفی کنید.



۵. ایمیل خود را باز نمائید و بر روی لینک ارسالی توسط نرم افزار Telegram کلیک نمائید تا ثابت کنید این ایمیل متعلق به شما می باشد.



۶. پس از کلیک بر روی لینک ارسالی ، تلگرام به شما اطلاع میدهد که از این پس سیستم تائید دو مرحله ای برای شما فعال گردیده است.

عکاسی ایمن و مخفی کردن عکسها و فیلم های خصوصی

پیشنهاد ما این است که هیچ وقت عکس یا فیلم های خیلی خصوصی خود را برای بر روی آیفون خود ذخیره ننمائید.

اما بدلیل اینکه دوربین عکاسی قدرتمند آیفون جز مهمی از توانایی آن می باشد و آیفون در هرصورت یک وسیله شخصی می باشد احتمال گرفتن تصاویر خانوادگی و شخصی که شما علاقه ندارید دیگران آنها را ببینند قطعا" وجود دارد.

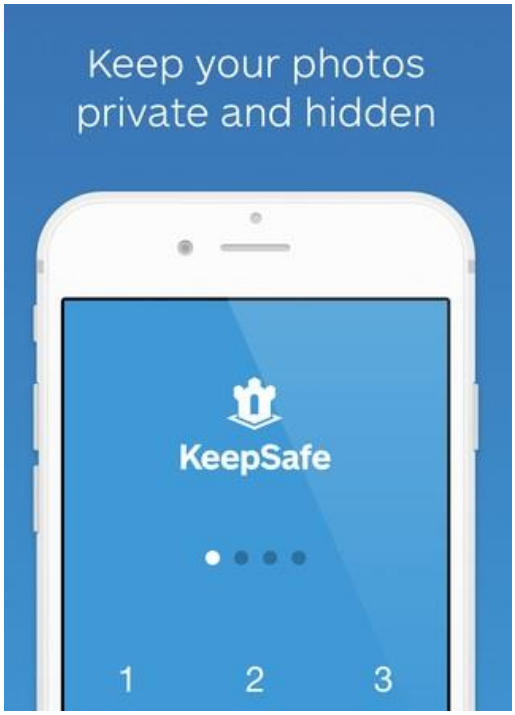
پس بیاییم تا جائیکه ممکن است این تصاویر را بصورت ایمن در درون آیفون خود ذخیره نمائیم.

به یاد داشته باشید هر اپلیکیشنی که مدعی حفظ اسرار شما می باشد ممکن است دارای نقاط ضعفی نیز باشد اما در اینجا اپی را معرفی میکنیم که روند رمز گذاری عکس های شما را به شیوه مطمئن انجام میدهد و پیش از معرفی توسط کارشناسان امنیتی مورد بازبینی قرار گرفته است.

معرفی : Keep Safe Private Photo Vault

این اپلیکیشن قابلیت رمز کردن و مخفی کردن عکسها و فیلم های شما را دارا می باشد و دسترسی به عکسهای خصوصی شما از طریق یک PIN کد صورت میگیرد.

نکته جالب درباره این اپ آن است که شما میتوانید با کمک نرم افرار دوربین متصل به این اپ عکس و فیلم بگیرید و کلیه تصاویر و فیلم های گرفته شده مستقیما وارد این اپ میشوند و هیچ اثری از آنها در قسمت photos آیفون دیده نخواهد شد. سپس میتوانید به کمک Pin کد وارد اپ بشوید و تصاویر و فیلم های خود را مشاهده نمائید.



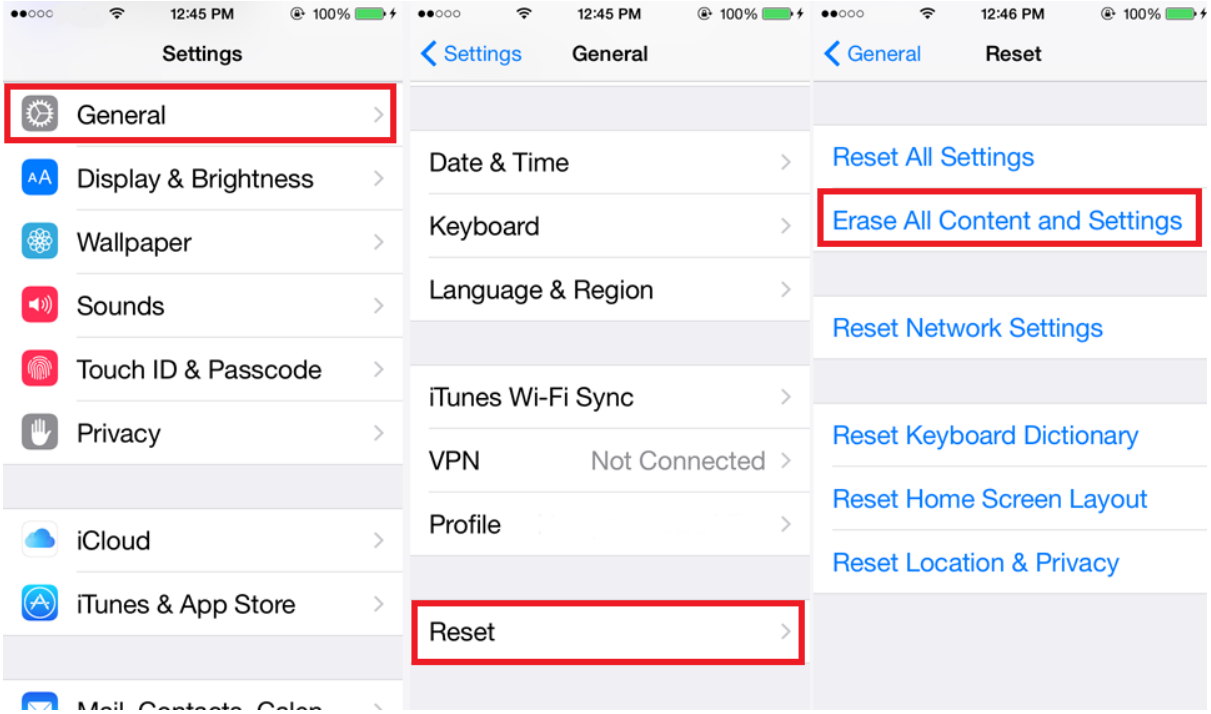
روش استفاده از برنامه KeepSafe

۱. برنامه KeepSafe را باز نمائید و عکسهای مهمی را که مایل به پنهان کردن آنها در درون برنامه هستید انتخاب نمائید و منتقل کنید.
۲. پس از اتمام انتقال و رمز گزاری آن تصاویر، به photo album آیفون بروید و آن تصاویر را پاک نمائید.
۳. تصاویر پاک شده شما در درون Deleted album منتقل میشوند. به آنجا بروید و آنها را از آنجا نیز پاک کنید.
۴. همانطور که قبلا آموزش دادم مطمئن شوید که PhotoStream شما فعال نمی باشد و یا اگر فعال است تصاویر را از PhotoStream نیز پاک کنید.

پیش از هدیه دادن یا فروش آیفون یا آیپد قدیمی خود چه نکاتی امنیتی را باید رعایت کنیم؟

شاید بعد از مدتی علاقمند شوید آیفون یا آیپد جدیدی خریداری نمائید و دستگاه قبلی خود را به کسی هدیه دهید و یا بفروشید. باید توجه کنید که پاک کردن پیامهای کوتاه ، عکس ها ، تماسها و اپلیکیشن ها به تنهایی نمیتواند همه اطلاعات شما را بصور کامل از بین ببرد.

خوشبختانه شرکت اپل راه حل مفیدی را برای شما در iOS قرار داده است و آن پاک کردن کامل اطلاعات و محتوا بدون قابلیت بازیابی می باشد.



از طریق مسیر General->Setting->Reset گزینه Erase All Content and Setting را انتخاب نمائید. سیستم از شما Passcod را سوال میکند تا مطمئن شود شما واقعا میخواهید همه اطلاعات را پاک نمائید. پس از گرفتن تائید از شما iOS شروع به کار کرده و کلیه اطلاعات شما را بصورت کاملا مطمئن پاک میکند و آیفون یا آیپد شما پس از پایان کار به حالت آغازین باز میگردد و آماده تحویل به هر شخصی که مایل هستید می گردد.

نکته : لطفا پیش از پاک کردن کامل اطلاعات خود مطمئن شوید از کانکت لیست ، عکسها و اطلاعات مهم خود قبلا پشتیان تهیه کرده اید زیرا پس از انجام عمل پاکسازی دیگر راهی برای دسترسی به آن اطلاعات وجود نخواهد داشت!

چگونه میتوانید از این کتاب حمایت کنید؟

هدف اولیه و محرک من برای نوشتن این ایبوک کمک به همه کسانی است که احتمال دارد هر لحظه فقط بدلیل ناآشنایی با حفظ حریم خصوصی خود در آیفون یا آیپد خویش دچار خسارات مادی و معنوی فراوانی از افشای اطلاعات خصوصی خود بشوند. بعلاوه همیشه علاقه داشتم چیزهایی را که میدانم با دیگران از طریق کتابهای الکترونیکی به اشتراک بگذارم.

امیدوارم نکات مهمی را که در این کتاب به شما آموزش دادم را در عمل نیز استفاده نمائید چون هیچکس نمیداند چه موقع ممکن است به هر دلیلی قربانی بعدی افشا شدن اطلاعات خصوصی خود باشد و همانطور که میدانید همیشه پیشگیری بهتر از درمان است. همچنین به یاد داشته باشید که امنیت در حوزه فناوری اطلاعات نسبی می باشد و هیچگاه مطلق نیست. پس یادگیری مداوم و احتیاط شرط لازم برای حفظ امنیت شما در فضای سایبری است.

اگر عزیزان ، دوستان و آشنایانی دارید که برای شما اهمیت دارند و از آیفون یا آیپد استفاده میکنند خواندن این کتاب را به آنها نیز توصیه نمائید تا آنها نیز بتوانند از حریم خصوصی خود بدرستی حفاظت نمایند و قربانی احتمالی فضای سایبری نباشند.

من برای تحقیق ، آماده سازی تصاویر و ایجاد این کتاب تصویری صدها ساعت زمان صرف کردم. هرچند میتوانستم این کتاب را بصورت قفل شده به فروش برسانم اما دیدم مجبورم از فرمتی به غیر از PDF که در تمام وسایل الکترونیکی قابل خواندن است استفاده کنم که اینگونه تعداد زیادی از خوانندگان هیچوقت با مطالب این کتاب آشنا نمی شدند و آنهایی هم که کتاب را میخرند نمیتوانستند براحتی آنرا با وسایل الکترونیکی مختلف خود مطالعه کنند پس تصمیم گرفتم این کتاب را بصورت کامل و بدون هیچ محدودیتی و با فرمت جهانی PDF و بر اساس اعتماد به شما خواننده گرامی منتشر کنم.

هر چیزی در این دنیا دارای قانونی است. زمانیکه محبت میکنیم در قبالش محبت میگیریم. زمانیکه چیزی را می بخشیم ، در واقع داریم چیزی را بدست می آوریم. کائنات همواره همان چیزی را به ما خواهند داد که ما به دنیا می دهیم.

من از این ایبوک حمایت میکنم
زیرا میخواهم به مولف آن انگیزه انتشار
کتابهای بعدی را در اینترنت بدهم

پرداخت بهای این کتاب را بر اساس اعتماد به شما خواننده عزیز در نظر گرفته ام . یعنی هیچ سیستمی برای کنترل اینکه چه کسی بهای این کتاب را بعد از دانلود کردن آن پرداخته است قرار نداده ام.

شما اگر کتاب را مطالعه کردید و مایلید هستید از من بعنوان نویسنده این کتاب حمایت کنید تا کارها و کتابهای بعدی خود را ادامه دهم ، می توانید **هر مبلغی بین ۱۰۰۰ تا ۱۰،۰۰۰ تومان** به شماره حساب زیر واریز نمائید. درآمدی که از این طریق جمع آوری می شود مشوق من برای تولید و انتشار کتابهای بعدی یا ایجاد نسخه بعدی از همین کتاب برای شما خواهد بود و یقینا" بدون این حمایت ها، انگیزه لازم برای ایجاد تولیدات فرهنگی مثل ایبوک در آینده خیلی کمتر خواهد شد.

شماره کارت بانک ملت	۶۱۰۴ ۳۳۷۹ ۱۲۷۴ ۵۴۳۵
به نام	امین رضا دانشور

امیدوارم با این موضوع موافق باشید که ضرری که در قبال ندانستن مطالب این کتاب ممکن است بکنید بسیار بیشتر از بهایی است که برای خرید آن میپردازید. اگر هم به هر دلیلی تمایلی برای پرداخت هزینه این ایبوک ندارید آنرا بعنوان هدیه ای از طرف من بپذیرید.

عضویت در لیست حامیان مالی کتاب:

ضمن تقدیر و تشکر از عزیزانی که از این کتاب حمایت مالی میکنند، خواهشمند است یک پیامک با متن عدد "۱" را به شماره سامانه پیامکی ۵۰۰۰۱۳۳۳۱۱۶۶۰۰ ارسال نمائید تا در لیست حامیان مالی این کتاب قرار بگیرید تا در آینده اگر نسخه جدیدی از این کتاب یا کتاب دیگری از من منتشر شد اخبار آنرا از طریق همین سامانه پیامکی به اطلاع شما برسانم.

ایرانیان و فارسی زبانان عزیز خارج از کشور نیز برای قرار گیری در این لیست ، ایمیلی با موضوع "حمایت" به ایمیل آدرس من که در انتهای کتاب ذکر کرده ام ارسال نمایند تا در جریان آخرین بروز رسانی ها و کتابهای بعدی من قرار بگیرید.

همچنین شما میتوانید بهای این کتاب را پرداخته و آنرا بصورت یک هدیه ارزنده برای عزیزانتان ایمیل نمائید.

تماس با نویسنده:

تمام شما خوانندگان فهیم و دانا برای من مهم و محترم هستید، اگرچه من هرگز همه شما را نخواهم دید اما اگر توانسته باشم مانع از خطر هک شدن و از بین رفتن حریم خصوصی حتی یک نفر از شما شده باشم از این موضوع خیلی خرسند خواهم بود و حس میکنم وظیفه خود را تا حدی به انجام رسانیده ام. همچنین خوشحال میشوم من را از نظرات خود آگاه نمائید.

راههای تماس با من برای گرفتن بازخورد ، نظرات ، مشاوره و ارتباط با شما دوستان عزیزم به شرح زیر می باشد.

۱. آدرس ایمیل : a.daneshvar@gmail.com
۲. ارسال پیام کوتاه توسط شما به سامانه پیامکی ۵۰۰۰۱۳۳۳۱۱۶۶۰۰
۳. ارسال عدد "۱" به سامانه پیامکی: برای عضویت در لیست حامیان مالی کتاب و دریافت خبر از کتابها و نسخه های بعدی این کتاب
۴. ارسال عدد "۲" به سامانه پیامکی: برای دریافت آخرین شماره کارت بانکی معتبر من (برای سال ۱۳۹۷ به بعد)

پائیز ۱۳۹۴

با احترام

امین رضا دانشور

لطفا" این ایبوک را به هرکسی که
برای شما مهم است و از آیفون یا آیپد
استفاده میکند معرفی یا ایمیل کنید
شاید بتوانید جلوی خطر احتمالی را برای او بگیرید