

iCloud و رفتن به بخش Devices گوشی خود را انتخاب کنید و گزینه Erase iPhone را فشار دهید تا بار بعدی که گوشی به اینترنت متصل شد به صورت خودکار تمام اطلاعات ذخیره شده را پاک کند.

### طولانی کردن رمز عبور

هر چقدر رمز عبورتان طولانی تر و پیچیده تر باشد، امکان شکستن رمز آن و دستیابی به اطلاعات شما هم سخت تر می شود. شاید اسم رمز شکن GrayKey به گوشتان خورده باشد؛ دستگاهی که برای استفاده سازمان های دولتی توسعه داده شد و با اتصال به گوشی تنها در چند ساعت می تواند رمز عبور چهار عددی شما را بشکند.

هرچند اپل در iOS 12 راه نفوذ این ابزار را بست، دلیلی وجود ندارد تصور کنیم هیچ دستگاه یا فناوری مشابه جدیدی برای شکستن رمز آیفون تولید نشده باشد. راه مقابله با این روش نفوذ، اما بسیار ساده است. کافی است کمی محتاط باشید و رمز عبوری انتخاب کنید که بیشتر از شش عدد باشد. شکستن یک رمز هشت عددی حدود دو ماه و شکستن یک رمز ده عددی بیشتر از یک دهه زمان لازم دارد. برای امنیت هرچه بیشتر می توانید از گذرواژه هایی استفاده کنید که ترکیبی از حروف و اعداد هستند و شکستن آنها به مراتب دشوارتر است. فقط به خاطر داشته باشید گذرواژه عبورتان قابل حدس زدن نباشد و تا حد امکان اعداد و حروف ترتیب منطقی نداشته باشند.



## چند نکته برای افزایش امنیت گوشی های آیفون

# سیب امن

خشیار مریدپور

شکی نیست که شرکت اپل با سختگیری خاص خود در زمینه مشخصات سخت افزاری و نرم افزاری محصولات اکوسیستم خود، امن ترین سیستم عامل گوشی های هوشمند را توسعه داده است.

با این حال همیشه افرادی تلاش می کنند امنیت کاربران را به خطر بیندازند و به اطلاعات شخصی و میلیون ها کاربر اپل دسترسی یابند. نتیجه هم نبردی دائمی بین متخصصان امنیت سایبری اپل از یک سو و هکرها و سارقان اینترنتی از سوی دیگر است. اگر شما هم به هر دلیل نگران اطلاعات حساس شخصی، مشخصات حساب های کاربری در سایت های مختلف، آدرس های ایمیل، پیام های متنی و حتی عکس ها و فیلم های ذخیره شده روی گوشی خود هستید، پیشنهاد می کنیم این راهنما را با دقت بخوانید. نکات ساده ای که در ادامه می آید جزو قابلیت های خود سیستم عامل iOS 13 هستند و در صورت به کار بستن آنها، نفوذ به گوشی هوشمند شما و سرقت اطلاعات آن اگر نه ناممکن، ولی بسیار دشوار خواهد شد.

### به روز نگه داشتن سیستم عامل

همیشه سعی کنید از آخرین نسخه ارائه شده از سیستم عامل iOS استفاده کنید و حتی به روزرسانی های جزئی و امنیتی را هم از قلم نیندازید. این حرکتی پیشگیرانه ولی مفید است، چراکه هکرها گاه حفره هایی در نرم افزارهای اپل پیدا می کنند که به صورت بالقوه به آنها اجازه می دهد به صورت مستقیم به اطلاعات شخصی شما دسترسی پیدا کنند. برای این که مطمئن شوید از آخرین نسخه سیستم عامل اپل استفاده می کنید یا نیازمند به روزرسانی هستید نباید کار زیادی انجام دهید. کافی است وارد Settings شوید و با لمس گزینه General به قسمت Software Update بروید. در صورتی که از آخرین نسخه سیستم عامل برای گوشی تان استفاده نمی کنید، با ورود به این قسمت فرآیند دریافت آخرین به روزرسانی به صورت خودکار شروع خواهد شد. آخرین نسخه سیستم عاملی

که اپل عرضه کرده 13.1.2 است.

### فعال کردن Find My iPhone

یکی دیگر از قدم هایی که می توانید برای افزایش امنیت گوشی و اطلاعات شخصی خود بردارید، فعال کردن گزینه Find My iPhone است.

این یکی از کاربردی ترین قابلیت های گوشی های هوشمند است که به شما امکان می دهد در صورت مفقود شدن یا به سرقت رفتن گوشی با ورود به حساب کاربری اپل خود از موقعیت فیزیکی آن مطلع شوید. آنچه شاید مهم تر باشد، قابلیت پاک کردن کامل اطلاعات روی گوشی از راه دور است که به شما این اطمینان را می دهد هیچ کس نمی تواند به اطلاعات حساس شخصی شما دست پیدا کند. قابلیت جالب جدیدی که در iOS 13 به این قسمت اضافه شده امکان مکان یابی بدون دسترسی به اینترنت است که با استفاده از

بلوتوث انجام می شود و در صورت اتصال گوشی به فرستنده های بلوتوث حتی بدون سیم کارت و اتصال به وای فای هم می تواند موقعیت گوشی را برای شما ارسال کند. در صورت تمایل به استفاده از این قابلیت (هرچند شاید در ایران هنوز خیلی کاربردی نباشد) می توانید گزینه Offline Finding را فعال کنید. برای فعال سازی این قابلیت باید ابتدا وارد بخش Settings شوید و تصویر/ نام کاربری خود در بالای صفحه را لمس کنید. سپس به iCloud بروید و وارد Find My iPhone شوید و آن را فعال کنید.

برای پاک کردن اطلاعات گوشی از راه دور هم می توانید با ورود به حساب کاربری در

گزینه  
Find My iPhone  
از کاربردی ترین قابلیت های  
گوشی های هوشمند است که به شما  
امکان می دهد در صورت مفقود شدن  
یا به سرقت رفتن گوشی با ورود  
به حساب کاربری اپل خود  
از موقعیت فیزیکی آن  
مطلع شوید

### محدود کردن دسترسی ها

در iOS 13 جمع آوری اطلاعات از کاربران بدون آگاهی آنها حتی سخت تر از قبل شده و اپل با چند راهکار، دسترسی غیرمجاز به اطلاعات شخصی شما را دشوارتر کرده است. برای مثال می توانید به

نرم افزارهای مختلف سطوح متفاوتی از دسترسی به موقعیت مکانی خود را بدهید. همچنین در iOS 13، برای استفاده از بلوتوث نیازمند دریافت اجازه از شما هستند که برای پیشگیری از دزدی اطلاعات مکانی کاربر بدون رضایت او افزوده شده است. به علاوه در سیستم عامل جدید به صورت پیش فرض امکان دسترسی نرم افزارها به اطلاعات ذخیره شده در قسمت Notes مسدود شده است.

البته اپل همواره مساله حفظ حریم خصوصی کاربران را جدی گرفته و هر نرم افزاری که اقدام به دزدی اطلاعات شخصی کاربران کند به صورت خودکار از اکوسیستم اپل حذف می شود.

با این حال اگر به بعضی از نرم افزارهای نصب شده روی گوشی خود اطمینان کامل ندارید، می توانید با مراجعه به قسمت Settings و رفتن به بخش Privacy دسترسی های هر نرم افزار را بنابر صلاحدید خود تغییر دهید. پیشنهاد ما این است که این محدودسازی دسترسی را برای تمام نرم افزارهایی که اطلاعات بسیاری از شما طلب می کنند، انجام دهید

## استراحت دادن به سیری

دستیار صوتی هوشمند اپل یکی از جذاب ترین قابلیت های گوشی هوشمند این شرکت است. البته همین ویژگی فوق العاده می تواند راه نفوذ هکرها به گوشی شما هم باشد.

سیری معمولاً قبل از اجازه دسترسی به مخاطبان، عکس ها، فیلم ها و دیگر اطلاعات حساس سعی می کند هویت مالک گوشی را تأیید کند، اما هکرها تاکنون چند روش برای دور زدن سیستم امنیتی و دستیابی به اطلاعات گوشی معرفی کرده اند که می تواند خطرناک باشد. بهترین توصیه برای پیشگیری از چنین معضلی، غیرفعال سازی سیری در حالت قفل بودن صفحه است که تمام روش های ابداعی هکرها را بی اثر می کند. روند کار هم بسیار ساده است: به Settings بروید و وارد بخش Touch ID & Passcode (یا Face ID & Passcode) شوید و گزینه Allow access when locked را به حالت غیرفعال درآورید.



کارگاه



اگر مطالب این صفحه را می پسندید، عدد ۷۲۶ را به شماره ۳۰۰۱۱۲۲۶ پیامک کنید