

بیش از ۳/۵ میلیون کاربر آیفون و آی‌پد، بدافزارهای مخرب را از App Store اپل نصب کردند.



**Over 3.5 Million Malicious Fleeceware  
Found on Apple's App Store**

### خلاصه‌ی خبر:

بدافزارهای نوع (Fleeceware) که به اصطلاح آن‌ها را غارت‌افزار نامیده‌ایم، برنامه‌های مخربی هستند که با دسترسی به اطلاعات پرداخت کاربران به دستبرد و غارت از آنها می‌پردازد. اخیراً داندلود و نصب بیش از ۳/۵ میلیون از آن‌ها در App Store توسط کاربران اپل نیز مشاهده شده‌است. این غارت‌افزارها که از فرصت آزمایشی اپل برای حضور در App Store سوءاستفاده می‌کنند، در صورت لغو نشدن آبونمان آن‌ها مبالغ زیادی از حساب کاربران خود را بصورت دوره‌ای برداشت می‌کنند.

اخیراً بیش از ۳۰ غارت‌افزار مخرب در فروشگاه رسمی اپل یافت شد. این برنامه‌ها با هدف انجام کلاهبرداری مالی ایجاد می‌شوند. شرکت اپل یک دوره‌ی آزمایشی را به برنامه‌ها اجازه‌ی ارائه‌ی دهد و توسعه‌دهندگان آن برنامه‌ها از این فرصت سوءاستفاده کرده‌اند. اگر کاربران این برنامه‌ها را نصب کنند و آبونمان را لغو نکنند هر ماه برای شارژ مبلغ بسیار زیادی از حساب آن‌ها برداشت می‌شود.

## غارت‌افزارهای موجود در App Store اپل

Sophos تعداد ۳۰ برنامه از این دست، که پس از یک دوره‌ی آزمایشی ۳ یا ۷ روزه هزینه‌ی ۳۰ دلار در ماه یا ۹ دلار در هفته را به عنوان آبونمان از حساب کاربران برداشت می‌کنند را در Store App رسمی اپل مشاهده کرد.

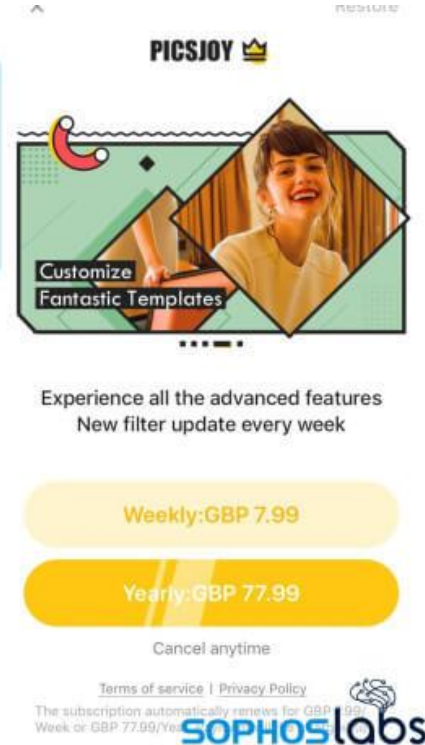
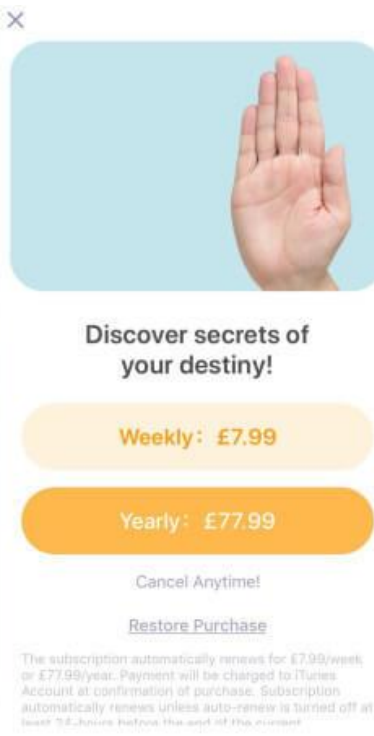
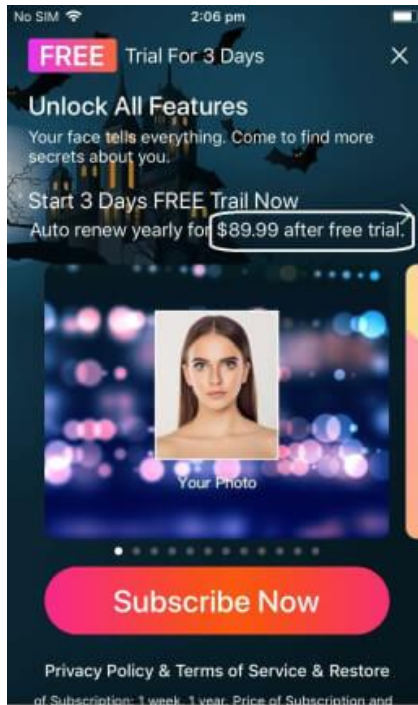


Fleeceware apps, like these ones SophosLabs discovered in the Apple App Store, overcharge users for functionality widely available in other free or low-cost applications.

**SOPHOSlabs**

### ۱- لیست برنامه‌ها

اگر برنامه‌ها بیش از یک سال نصب بمانند، از کاربران به ترتیب ۳۶۰ یا ۴۶۸ دلار دستبرد می‌زنند. این برنامه‌ها تنها ویژگی‌هایی که دارند در برنامه‌های رایگان یا سایر برنامه‌های با پرداخت عادی نیز وجود دارند و غیر از آن هیچ ویژگی خاصی را شامل نمی‌شوند.



## ۲- برنامه‌های آزمایشی رایگان

انواع برنامه‌ها شامل ویرایشگر تصویر، فال، طالع‌بینی، فالوور، کف بینی، اسکنر بارکد/ کد QR و برنامه‌های فیلتر صورت می‌شود. بسیاری از این برنامه‌ها به‌عنوان یک اپلیکیشن رایگان در AppStore تبلیغ می‌شوند اما وقتی کاربران آن‌ها را نصب می‌کنند با اعلان "آزمایشی رایگان" روبرو می‌شوند.

اطلاعی‌ها از کاربران می‌خواهند جزئیات کارت پرداخت را ارائه دهند، در بیشتر موارد برنامه‌ها فقط پس از ثبت‌نام برای اشتراک، قابل استفاده هستند. "برخی از کاربران ممکن است متون ریزی که شامل هزینه‌ی واقعی اشتراک‌ها می‌شود را خوب نخوانند و عضو شوند." App Store توجهی به تعداد کاربرانی که این برنامه‌ها را نصب می‌کنند ندارد، زیرا بسیاری از این برنامه‌ها در لیست محبوب‌ترین برنامه‌ها قرار دارند.

پیش از این Sophos چندین غارت‌افزار را در Google play store مشاهده کرده بود که منجر به خسارت مالی برای کاربران می‌شد. این غارت‌افزارها بیش از ۶۰۰ میلیون بار در کل نصب شده‌اند.

در برخی از این برنامه‌ها، انتقال متون ارسال شده توسط کاربران را سرورهای مستقر در چین، مشاهده شده است. این برنامه‌های مخرب با تبلیغات در بسترهای محبوب مانند Facebook، Instagram، TikTok و سایر منابع محبوبیت پیدا می‌کنند. همچنین، این اپلیکیشن‌ها تعداد زیادی نقد و بررسی‌های پنج ستاره دارند زیرا توسعه‌دهندگان برنامه به نوعی بررسی‌ها و نظرات را دستکاری می‌کنند.

در لینک زیر می‌توانید لیست کاملی از غارت‌افزارهای مخرب را مشاهده کنید:

<https://news.sophos.com/en-us/2020/04/08/iphone-fleeceware/>

منبع:

<https://gbhackers.com/malicious-fleeceware-apps/>