

داکیومنت فنی واحد IT

راهنمای افزایش امنیت شبکه‌های اجتماعی

نسخه ۱.۰.۰

۱۴۰۰/۰۹/۰۸

تهیه شده توسط واحد IT



مقدمه

باتوجه به اهمیت شبکه‌های اجتماعی و استفاده مکرر اعضای رهاپ از آن، جهت تبادل و ذخیره‌سازی اطلاعات، برآن شدیم نکاتی را به منظور حفظ امنیت اطلاعات اعضاء آماده کنیم.

فهرست

- ۱ افزایش امنیت تلگرام
- ۲ Two-Step Verification -۱
- ۲ نصب نسخه‌های اصلی تلگرام -۲
- ۳ Privacy and Security -۳
- ۳ عدم نصب بد افزارها -۴
- ۴ Secret Chat -۵
- ۴ تنظیمات رمز دسترسی به برنامه «Passcode Lock» در تلگرام -۶
- ۵ افزایش امنیت واتساپ
- ۶ تاییدیه گرفتن از کد گذاری برای مکالمات حساس -۱
- ۷ اعلامیه‌های امنیتی را روشن کنید -۲
- ۷ تاییدیه دو مرحله‌ای را فعال کنید -۳
- ۸ روش رمزگذاری روی واتساپ -۴
- ۸ اپلیکیشن دسکتاپ رسمی واتساپ را دریافت کنید -۵
- ۸ از حریم خصوصی خود در واتساپ محافظت کنید -۶
- ۹ افزایش امنیت اینستاگرام
- ۱۰ احراز هویت دو عامله را فعال کنید -۱
- ۱۰ بررسی دسترسی اپلیکیشن‌ها به حساب اینستاگرام -۲
- ۱۱ درخواست تایید حساب کاربری اینستاگرام -۳

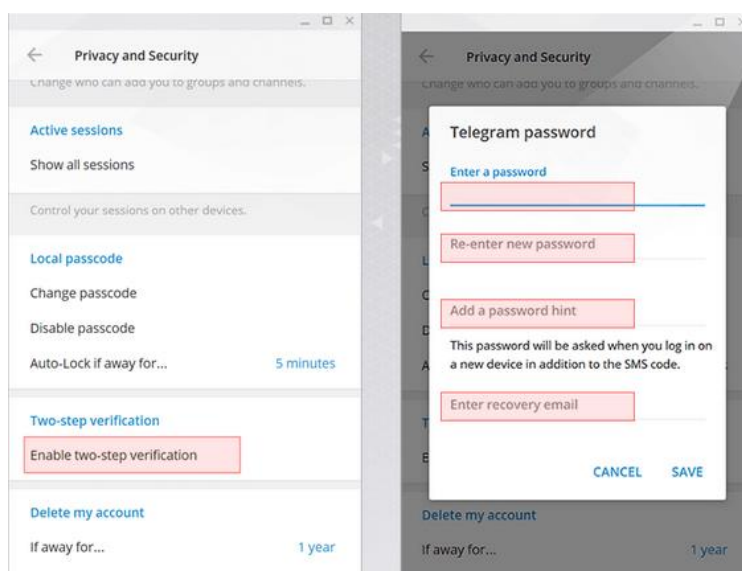
افزایش امنیت تلگرام

چگونه امنیت تلگرام را بالا ببریم ؟

۱- Two-Step Verification

با این روش حتی اگر کد ۵ رقمی شما در اختیار شخص نفوذگر قرار بگیرد باز هم نمی‌تواند به وارد تلگرامتون شود:

۱. به **Setting** برید و روی **Privacy and Security** کلیک کنید.
۲. بر روی **Two-Step Verification** کلیک کنید.
۳. یک رمز امن وارد کنید و ایمیل خودتون رو وارد کنید.



نکته: حتما ایمیلتون رو صحیح وارد کنید تا در صورتی که پسورد دومتون یادتون رفت بتوانید از طریق ایمیل بازیابی کنید.

۲- نصب نسخه‌های اصلی تلگرام

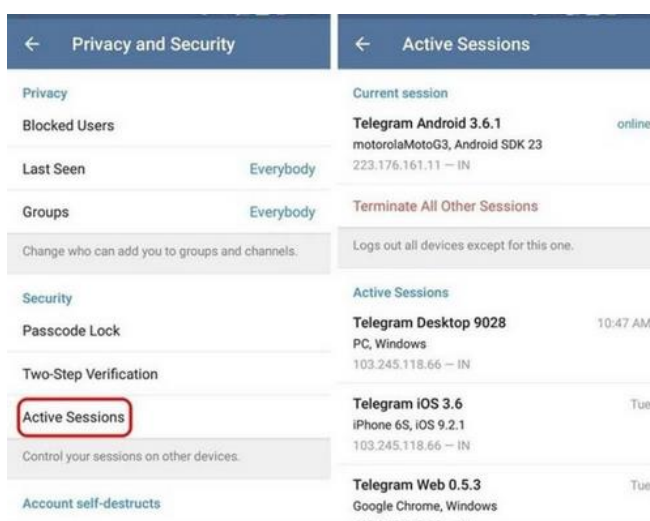
همیشه نسخه رسمی تلگرام را نصب کنید زیرا در سایر نسخه‌های تلگرام امکان دارد ابزارهای جاسوسی که موجب هک شدن شما می‌شوند را قرار بدهند. همچنین رعایت این نکته که تلگرام را فقط از سایت رسمی‌اش دانلود کنید.

Privacy and Security –۳

با استفاده از این روش می‌توانید دستگاه‌هایی که به اکانت شما وصل هستند را ببینید:

۱. به **Setting** بروید و روی **Privacy And Security** کلیک کنید و روی گزینه **Active Sessions** کلیک کنید.

۲. اکنون دستگاه‌های متصل شده به اکانت شما را نشان می‌دهد. اگر دستگاهی متعلق به شما نیست، می‌توانید آن را حذف کنید.



نکته: با این روش می‌توانید ببینید که آیا هک شدید یا نه!

۴- عدم نصب بد افزارها

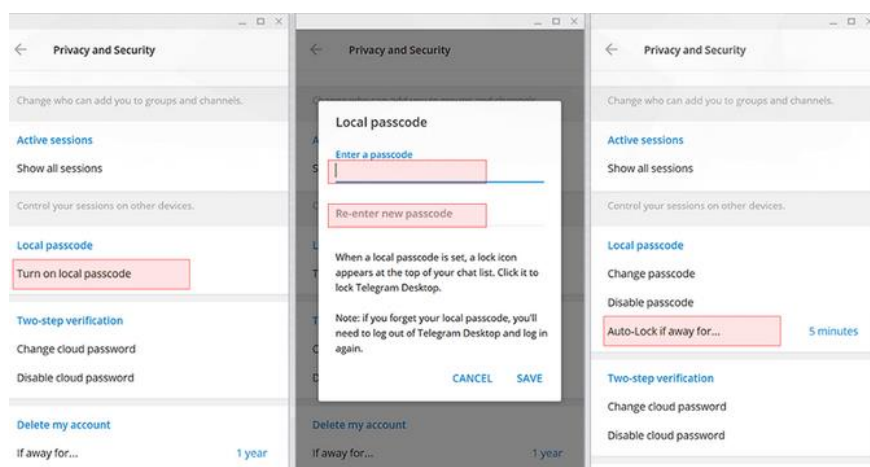
برنامه‌هایی که به اسم هک تلگرام و شبکه‌های اجتماعی در کانال‌ها می‌فروشند را به هیچ عنوان روی دستگاه خودتون نصب نکنید. (تمامی این برنامه‌ها فیک هستند.)

Secret Chat – ۵

برای امنیت بیشتر هنگام مکالمات در تلگرام می‌توانید از امکان secret chat استفاده کنید. در این بخش امکاناتی برای شما فراهم می‌شود که از گفتگوهایتان محافظت خواهد کرد. حتی شخصی که دارد با شما چت میکند امکان اسکرین شات گرفتن از پیام‌ها را هم ندارد.

۶- تنظیمات رمز دسترسی به برنامه «Passcode Lock» در تلگرام

یکی از موارد قابل توجه در موضوع امنیت حساب‌های کاربری در پیام‌رسان‌ها، نحوه تامین امنیت است. اهمیت این مساله زمانی بیشتر از همیشه مورد توجه قرار می‌گیرد که برای مثال زمانی که شخصی به موبایل یا لپ‌تاپ شما دسترسی پیدا می‌کند، نتواند به راحتی به اطلاعات خصوصی و حساس شما، مانند پیام‌های رد و بدل شده در تلگرام‌تان دسترسی پیدا کند. از همین رو تلگرام برای تامین فیزیکی کاربران پیام‌رسان خود، قابلیت تنظیم رمز دسترسی به برنامه به صورت محلی را با عنوان «Local Passcode/Passcode Lock» فراهم کرده است.



نکته: برای غیرفعال کردن این قابلیت از بخش تنظیمات رمز دسترسی، گزینه Disable passcode را انتخاب کرده و برای تایید غیرفعال‌سازی، رمز دسترسی به کار رفته در زمان فعال‌سازی را بنویسید.

افزایش امنیت واتساپ

چگونه امنیت اینستاگرام را بالا ببریم؟

۱- تاییدیه گرفتن از کد گذاری برای مکالمات حساس

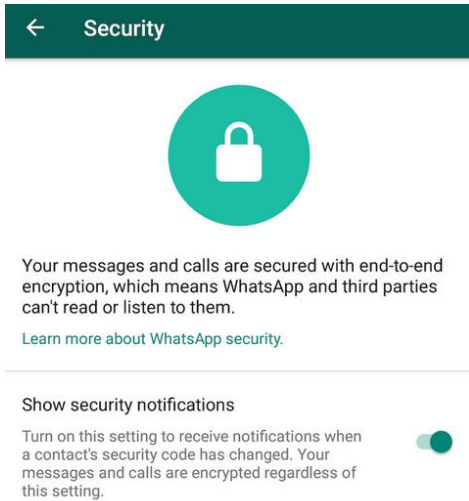
با وجودی که واتس اپ به طور پیش فرض تمام گفتگوها را کد گذاری می‌کند، گاهی اوقات ضرورت ایجاب می‌کند تا شما سطح امنیت را از این هم بالاتر ببرید. مثلا در زمان‌هایی که قصد ارسال اطلاعات حساب بانکی خود را دارید بهتر است به سراغ این روش بروید.

برای تایید رمزگذاری یک مکالمه را با مخاطب مورد نظر خود آغاز کنید. در پنجره گفتگو روی نام مخاطب ضربه بزنید، سپس Encryption را انتخاب کنید. بعد از آن چیزی شبیه به این را مشاهده خواهید کرد:



این الگوی ۴۰ رقمی کد امنیتی شما است. شما می‌توانید از مخاطب خود درخواست کنید تا این کد QR را اسکن کند تا شما بتوانید با مقایسه این ارقام این کد را به صورت دستی تایید کنید. همچنین می‌توانید با استفاده از دکمه Scan Code مخاطبین خود را اسکن کنید.

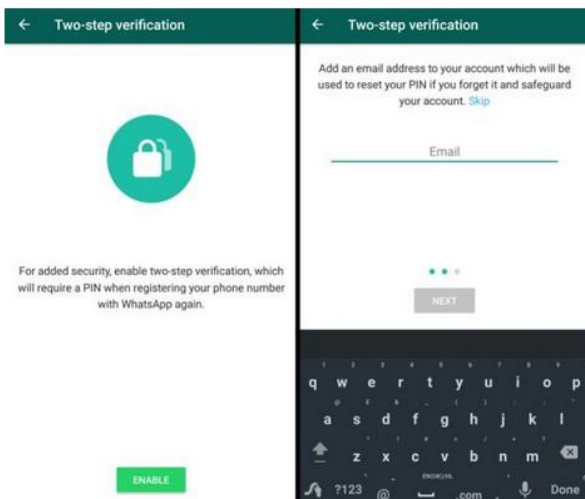
۲- اعلامیه‌های امنیتی را روشن کنید



وقتی یک شماره جدید یا لپ‌تاپ به یک گفتگوی موجود دسترسی پیدا می‌کند، یک کد امنیتی جدید برای هر دو گوشی تولید می‌شود. واتس‌آپ می‌تواند در زمان تغییر پیدا کردن این کد امنیتی یک اعلامیه ارسال کند.

برای فعال کردن اعلامیه‌های امنیتی به بخش WhatsApp <- Settings <- Account <- Security <- Show security notifications بروید و دکمه مربوط به آن را روی وضعیت روشن (سبز) قرار دهید.

۳- تاییدیه دو مرحله‌ای را فعال کنید



در حالت کلی باید گفت که هر سرویسی که از سیستم تایید هویت دو عامله پشتیبانی می‌کند، شما حتما باید از آن استفاده کنید. این یک گذرواژه دوره‌ای را به واتس‌آپ اضافه می‌کند و این اطمینان را به وجود می‌آورد که داده‌های شما توسط دیگران قابل دسترس نخواهد بود.

برای فعال کردن تاییدیه دو مرحله‌ای به Menu <- Settings <- Account <- Two-step verification <- Enable بروید. طبق دستورالعمل پیش بروید و یک پین کد شش رقمی که بتوانید در آینده به یاد بیاورید ایجاد کنید. بسیار مهم است که آدرس ایمیل خود را نیز اضافه کنید تا زمانی که این پین کد را فراموش کردید بتوانید از این طریق آن را بازیابی کنید.

بررسی‌های دوره‌ای این گذرواژه به صورت تصادفی است، بنابراین اصلاً شبیه به قفل کردن گفتگو با استفاده از کلمه عبور نیست. هدف از فعال کردن تاییدیه دو مرحله‌ای این است که از دسترسی دیگران به حساب **واتس اپ** شما بدون اطلاع شما جلوگیری شود.

۴- روش رمزگذاری روی واتس‌اپ

کاربران هنگام ورود می‌توانند بر روی واتس‌اپ خود رمز بگذارند. برای این کار باید مراحل زیر را طی کنید.

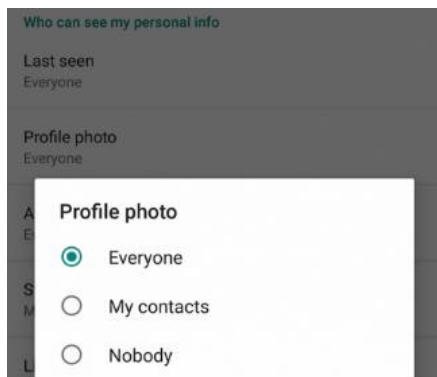
Setting->Account->Privacy->Screen Lock

۵- اپلیکیشن دسکتاپ رسمی واتس‌اپ را دریافت کنید

برای استفاده از **واتس‌اپ** روی کامپیوتر شما باید گوشی خود را با رابط تحت وب **واتس‌اپ** یا اپلیکیشن دسکتاپ **واتس‌اپ** همگام سازی کنید. به همین منظور حتماً از نسخه رسمی دسکتاپ این اپلیکیشن استفاده کنید.

دلیل اصلی برای انجام این کار این است که **واتس‌اپ** تحت وب را می‌توان به راحتی دستکاری کرد. بنابراین برای جلوگیری از این نوع تهدیدات حتماً از نسخه دسکتاپ رسمی اپلیکیشن **واتس‌اپ** استفاده کنید.

۶- از حریم خصوصی خود در واتس‌اپ محافظت کنید



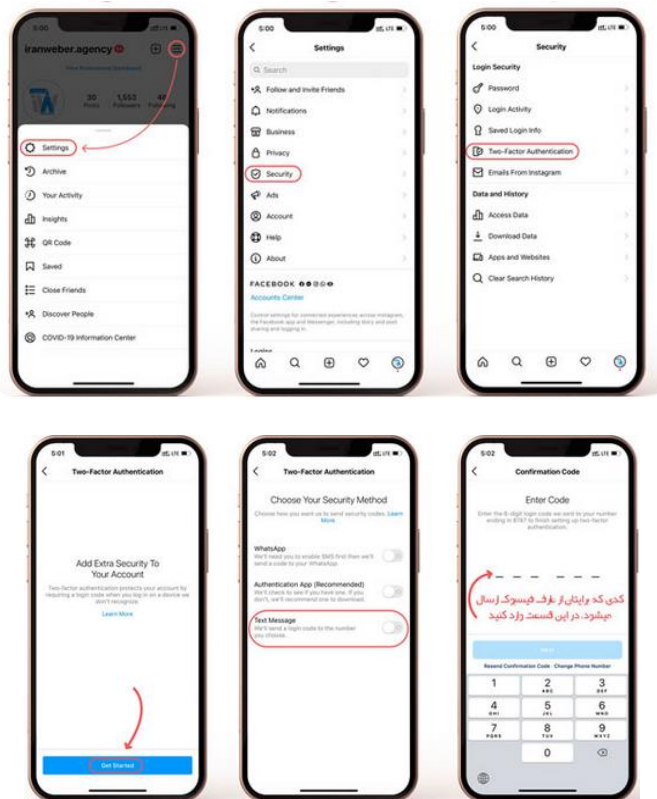
واتس‌اپ خصوصی‌ترین پیام رسان موجود نیست، اما امکانات کنترل کننده خوبی را در اختیار کاربران قرار می‌دهد. به بخش Privacy <- Account <- Settings بروید تا امکاناتی را که در این مورد در اختیار شما گذاشته شده است را مشاهده کنید.

افزایش امنیت اینستاگرام

چگونه امنیت اینستاگرام را بالا ببریم؟

۱- احراز هویت دو عامله را فعال کنید.

یکی از نکته‌های مهم **حفظ امنیت حساب اینستاگرام** فعال کردن احراز هویت دو عامله است. احراز هویت دو عامله در واقع یک لایه امنیتی دیگری برای حفاظت از حساب آنلاین شما اضافه می‌کند. در مواقعی که مجرمان سایبری از هر طریقی به رمز عبور شما دسترسی داشته باشند، با فعال بودن احراز هویت دو عامله نمی‌توانند وارد حساب آنلاین شما شوند زیرا به کد دوم دسترسی ندارند.



۲- بررسی دسترسی اپلیکیشن‌ها به حساب اینستاگرام

۱. روی لپ‌تاپ یا کامپیوترتان وارد حساب کاربری اینستاگرام شوید
۲. روی عکس پروفایلتان کلیک کنید و Edit Profile را انتخاب کنید

۳. از منوی باز شده Manage Applications را انتخاب کنید. در این صفحه می‌توانید دسترسی اپلیکیشن‌های غیر ضروری یا غیر قابل اعتماد را قطع کنید.

۳- درخواست تایید حساب کاربری اینستاگرام

این ویژگی برای شفافیت و صحت اعتبار حساب‌های برخی کاربران اینستاگرام است.

ارسال درخواست تایید حساب کاربری به این معنی نیست که حساب شما حتما تایید خواهد شد. برای ارسال درخواست تایید مسیر زیر را دنبال کنید:

از منوی Settings، و بخش Account روی گزینه Request Verification کلیک کنید. سپس نام خود را بنویسید و کپی کارت رسمی هویت که عکس، نام و تاریخ تولد شما مشخص باشد را ارسال کنید.