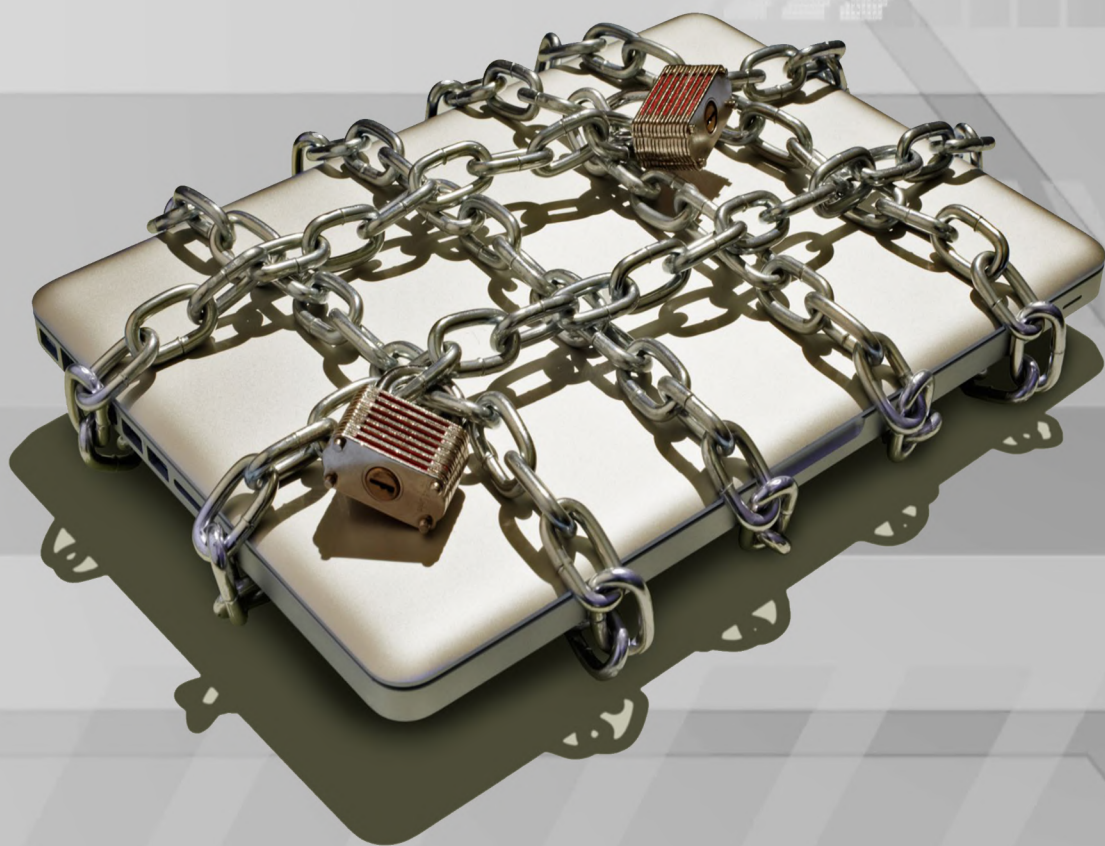


حریم خصوصی در شبکه‌های اجتماعی

نویسنده: سعید منافی، زینب رضایت پور





سازمان فناوری اطلاعات ایران
معاونت امنیت فضای تولید و تبادل اطلاعات

این کتاب در پروژه "صیانت از کودکان و خانواده در اینترنت" به سفارش معاونت امنیت فضای تولید و تبادل اطلاعات با همکاری پلیس فتا ناجا تهیه شده است.

حریم خصوص در شبکه هاے اجتماعے

سعد منانی، زینب رضایت پور

بہ سفارش:

سامرمان فناوری اطلاعات ایران

معاونت امنیت فضای تولید و تبادل اطلاعات



ناشر: عترت نو

تألیف: سعید منافی، زینب رضایت پور

تصویرساز: مژگان کمیجانی

ویراستاری: محمد یوسفی

مشاور طرح: علی محمد رجبی

ناظر و مجری طرح: شرکت فناوران توسعه امن ناجی

آدرس سایت: ceop.ir

شمارگان: ۱۰۰۰ جلد

قیمت: ۱۹۰۰۰ تومان

شابک: ۹۷۸-۶۰۰-۶۰۹۴-۵۷-۱

چاپ: سیمین پرداز کامه ۹-۶۶۴۸۱۶۳۸

نشانی: خیابان انقلاب، خیابان فخر رازی، خیابان

نظری، کوچه فرزانه، پلاک ۱، واحد ۱۳

تلفن: ۹-۶۶۴۸۱۶۳۸



انتشارات عترت نو

سروشنامه : منافی، سعید، ۱۳۶۳

عنوان و نام پدیدآور: حریم خصوصی در شبکه‌های

اجتماعی / سعید منافی، زینب رضایت پور؛ ویراستار محمد یوسفی؛

به سفارش سازمان فناوری اطلاعات ایران، معاونت امنیت فضای

تولید و تبادل اطلاعات

مشخصات نشر: تهران، عترت نو، ۱۳۹۷.

مشخصات ظاهری: ۹۵ص؛ مصور(رنگی).

شابک: ۹۷۸-۶۰۰-۶۰۹۴-۵۷-۱

وضعیت فهرست‌نویسی: فیا

موضوع: شبکه‌های اجتماعی پیوسته - - جنبه‌های

اجتماعی

موضوع: Online social networks -- social aspects

موضوع: اعتماد اجتماعی

موضوع: Trust -- social aspects

موضوع: حق صیانت از حریم شخصی

موضوع: Privacy, Right of

موضوع: حریم شخصی

موضوع: Privacy

موضوع: شبکه‌های اجتماعی پیوسته - - تدابیر

ایمنی

موضوع: Online social networks -- social aspects

شناسه افزوده: رضایت پور، زینب، ۱۳۶۶-

شناسه افزوده: سازمان فناوری اطلاعات،

معاونت

امنیت فضای تولید و تبادل اطلاعات

رده بندی کنگره: HMV۴۲/۱۵/م۸ح۴ ۱۳۹۷

رده بندی دیویی: ۰۰۶/۷۵۴

شماره کتابشناسی ملی: ۵۲۶۰۰۲

فهرست مطالب

۷.....	مفاهیم پایه
۷.....	مقدمه
۸.....	شبکه‌های اجتماعی
۱۰.....	حریم خصوصی
۱۲.....	اینترنت و حریم خصوصی
۱۵.....	تهدیدات حریم خصوصی کاربران شبکه‌های اجتماعی
۱۵.....	مقدمه
۱۶.....	جاسوسی از کاربران
۲۰.....	ردیابی کاربران براساس سیستم موقعیت‌یابی
۲۱.....	نفوذ در شبکه‌های اجتماعی
۲۳.....	جعل هویت
۲۳.....	انتشار بدافزارها و باج‌افزارها در میان کاربران شبکه‌های اجتماعی
۲۵.....	ایجاد مزاحمت و هرزنگاری
۲۶.....	قلدری اینترنتی
۲۷.....	اغفال کودکان در این نوع از ارتباطات
۲۸.....	استفاده از VPN و پروکسی

۳۱	راهبردهای حفظ حریم خصوصی در شبکه‌های اجتماعی
۳۱	مقدمه
۳۲	اصول استفاده از شبکه‌های اجتماعی
۳۸	سازوکارهای تأیید هویت شبکه‌های اجتماعی
۴۳	روش‌های حفظ حریم خصوصی در شبکه‌های اجتماعی و پیام‌رسان‌ها
۴۳	شبکه اجتماعی فیس‌بوک
۵۰	شبکه اجتماعی اینستاگرام
۵۴	پیام‌رسان تلگرام
۶۵	شبکه اجتماعی توییتر
۷۳	سایت اشتراک‌گذاری ویدئوی یوتیوب
۷۷	شبکه اجتماعی واتس‌آپ
۸۸	پست الکترونیکی جی‌میل
۹۱	سخن پایانی
۹۴	منابع و مآخذ

فصل اول: مفاهیم پایه



حریم خصوصی

- شبکه‌های اجتماعی
- حریم خصوصی
- اینترنت و حریم خصوصی

مفاهیم پایه

مقدمه

امروزه استفاده از اینترنت در سرتاسر دنیا بسیار فراگیر شده است. تعداد کل کاربران اینترنت بر اساس گزارش لحظه‌ای سایت internet live state نزدیک به ۴ میلیارد نفر است که روزانه ۶۰ میلیون عکس در اینستاگرام به اشتراک می‌گذارند و حدود یک میلیارد توییت انجام می‌دهند. این آمارها نشان از میزان نفوذ اینترنت در دنیا دارد.

براساس مطالعات آماری شرکت سیسکو، تا سال ۲۰۲۰ حدود ۵/۵ میلیارد نفر از جمعیت دنیا، دستگاه‌های هوشمند متصل به اینترنت خواهند داشت؛ یعنی تا آن موقع ۷۰ درصد از ساکنان زمین، با گوشی، تبلت، اسمارت‌واچ و یا لپ‌تاپ خود، به اینترنت وصل هستند (سالمی و همکاران، ۱۳۹۳).

کشور ما ایران هم از این موج عظیم عقب نمانده و نفوذ اینترنت به‌شکلی چشمگیر در همه‌جای آن افزایش یافته است. مطابق با آخرین آماری که در اوایل سال ۲۰۱۶ منتشر شده، از بین ۸۰ میلیون نفر جمعیت کشور، نزدیک به ۵۷ میلیون نفر کاربر اینترنت‌اند (شبانیان، ۱۳۹۴).

همان‌طور که گفته شد، فضای مجازی روزبه‌روز در حال فراگیرتر شدن است و عدم آشنایی با مفاهیم آن و صدا البته با راهکارهای حفظ حریم خصوصی خود و دیگران در این فضا، موجب می‌شود به شدت صدمه ببینیم. در این فصل به مفاهیم اولیه حریم خصوصی در شبکه‌های اجتماعی و فضای مجازی می‌پردازیم. پیش از هر چیز باید دانست شبکه اجتماعی چیست و چه انواعی دارد.

شبکه‌های اجتماعی

شبکه‌های اجتماعی را می‌توان مجموعه‌ای از تکنولوژی‌های کامپیوتری دانست که از طریق آن‌ها افراد مختلف می‌توانند با استفاده از اینترنت، به تعامل با یکدیگر بپردازند و به وسیله آن، اطلاعات خود را با دیگران به اشتراک بگذارند. شبکه‌های اجتماعی با وجود نوظهور بودن، به سرعت رشد می‌کنند. امروزه صدها و شاید هزاران شبکه اجتماعی مختلف در دنیا فعال می‌باشند. همین امر موجب شده تا تعریف دقیق و واحدی برای شبکه‌های اجتماعی مجازی وجود نداشته باشد. با وجود این، تمام این شبکه‌ها اشتراکاتی دارند. برای مثال همه آن‌ها بر بستر اینترنت هستند و محتوای این شبکه‌ها را کاربران تولید می‌کنند (جلالی، ۱۳۹۵). نقش اصلی را در هر شبکه اجتماعی، کاربران ایفا می‌کنند.



اساسی‌ترین ویژگی همهٔ این شبکه‌ها، ایجاد و به‌اشتراک‌گذاری پروفایل شخصی است. صفحهٔ پروفایل عموماً شامل بخش‌هایی؛ مانند عکس، اطلاعات شخصی (مانند اسم، سن، جنس، محل زندگی)، فضایی برای افزودن علایق و فعالیت‌ها (مانند کتاب‌های خوانده‌شده، فیلم‌های دیده‌شده، تفریح‌ها و وب‌سایت‌های موردعلاقهٔ کاربر) است. بسیاری از شبکه‌های اجتماعی به شما امکان می‌دهند عکس، موزیک، ویدئو و مطالب شخصی خود را روی صفحهٔ پروفایلتان قرار دهید. پروفایل درواقع بخشی از حریم خصوصی فرد است که آن را با دیگران به اشتراک می‌گذارد (مهران‌فر و رستگارپور، ۱۳۹۵). در هریک از این شبکه‌ها ممکن است این بخش از حریم خصوصی حفظ یا نقض شود. این کاربران هستند که تعیین می‌کنند به چه نحو از آن استفاده شود.

در شبکه‌های مختلف، میزان آزادی کاربران متفاوت است. در بعضی از این شبکه‌ها می‌توانید افراد دیگر را جست‌وجو و با آن‌ها ارتباط برقرار کنید. چنین افرادی ممکن است رابطهٔ دوری با شما داشته باشند یا اینکه کاملاً غریبه باشند. البته همان‌طور که گفته شد، این کار منوط به این است که درخواستان را قبول کنند (اکبری‌تبار و اسکندری‌پور، ۱۳۹۲).

حریم خصوصی

یکی از اصلی‌ترین مفاهیم در شبکه‌های اجتماعی، حریم خصوصی است. علی‌رغم اینکه حق حفظ حریم خصوصی، به‌عنوان یکی از پرکاربردترین حقوق، برای هر فردی شناخته شده است، هنوز صاحب‌نظران برجسته دنیا نتوانسته‌اند بر سر تعریفی واحد به توافق برسند؛ زیرا تعریف حریم خصوصی در جوامع مختلف، به عواملی مثل فرهنگ و زمینه‌های اجتماعی و محیطی که شخص در آن قرار دارد، وابسته است. گستردگی این مفهوم تا حدی است که گفته‌اند: «تمامی موارد حقوق بشر، جنبه‌ها و ابعادی از حریم خصوصی هستند» (فخار، ۱۳۹۵).



اما دانشمندان به‌دلیل سختی کار و پیچیدگی موضوع، آن را رها نکرده‌اند. ایشان به این نتیجه رسیده‌اند که می‌شود گفت حریم خصوصی تقریباً همان محرمانگی است: یعنی حق پنهان کردن بعضی چیزها از دیگران، حق

ناشناخته‌ماندن و حمایت از کرامت انسان. این تعریف یعنی هرکس حق دارد انتخاب کند چه چیزهایی را دیگران درباره او بدانند و چه چیزهایی را نه.

به‌طور کلی، می‌شود گفت در همه نقاط جهان، حریم خصوصی ارزشی مهم است و می‌شود آن را زیربنای توجه به شأن و منزلت انسان و بقیه ارزش‌های مهم (مثل آزادی اجتماعی و آزادی بیان) دانست (فخار، ۱۳۹۵).

درواقع، محرمانگی و حریم خصوصی، مفهومی نیست که با ظهور شبکه‌های اجتماعی به وجود آمده باشد؛ بلکه یکی از اساسی‌ترین حقوق هر فرد در فرهنگ‌ها و ادیان مختلف است. برای نمونه، در دین اسلام، حریم خصوصی بسیار محترم شمرده شده است؛ تا جایی که خداوند متعال در سوره حجرات، آیه ۱۲ می‌فرماید:

«يَا أَيُّهَا الَّذِينَ آمَنُوا اجْتَنِبُوا كَثِيرًا مِّنَ الظَّنِّ إِنَّ بَعْضَ الظَّنِّ إِثْمٌ وَلَا تَجَسَّسُوا
وَلَا يَغْتَبَ بَعْضُكُم بَعْضًا»

«ای کسانی که ایمان آورده‌اید، از بسیاری از گمان‌ها بپرهیزید که پاره‌ای از گمان‌ها گناه است و جاسوسی نکنید و بعضی از شما غیبت بعضی نکند.»

پیشوایان دینی هم در اسلام درباره حفظ حریم خصوصی افراد توصیه‌های فراوانی کرده‌اند؛ از جمله امام علی(ع) در نامه ۵۳ نهج‌البلاغه از مالک اشتر می‌خواهد که از تجسس در احوال مردم خودداری کند.

اینترنت و حریم خصوصی

امروزه اینترنت یکی از پرکاربردترین ابزارهای بشر است و در کنار نقش‌های متعددی که دارد، به نوعی رسانه نیز تبدیل شده است. سه ویژگی اساسی که این رسانه را از تلویزیون، رادیو و... متمایز می‌کند، قابلیت تعامل، سرعت عمل و نامحدودبودن فضای آن است. در اینترنت کاربران با یکدیگر تعامل می‌کنند و رابطه‌ای کاملاً دوسویه دارند. برخلاف تلویزیون و رادیو که مخاطبان مجبورند هرچه را پخش می‌شود، ببینند یا بشنوند. افراد به کمک اینترنت می‌توانند هم مخاطب و هم پخش‌کننده باشند. شاید به همین دلیل است که اینترنت به عنوان «بزرگ‌ترین شکل مشارکتی گفتار جمعی که تاکنون شناخته شده» معرفی شده است. اینترنت مانند فضایی مجازی برای ملاقات همه مردم جهان با یکدیگر و نیز شبکه شبکه‌ها و بزرگ‌ترین شبکه جهانی کامپیوتر است (عقیلی و پوری، ۱۳۹۰).



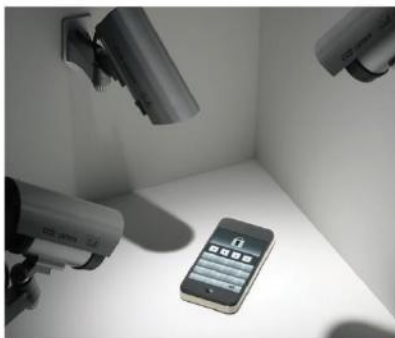
دلیل اصلی موفقیت اینترنت تبادل اطلاعات در سراسر جهان است؛ اما این آزادی، اغلب باعث ایجاد مشکل برای کسانی می‌شود که اطلاعات بازرشی را در آن ردوبدل می‌کنند. بنابراین، یکی از نگرانی‌های اساسی درباره اینترنت، حفظ حریم شخصی افراد است.

برای هر فرد ممکن است اطلاعات خاصی حریم شخصی او حساب شود که اگر از طریق اینترنت یا هر روش دیگری فاش شود، ضررهای هنگفتی به شخصیت، موقعیت، مال یا آبروی او وارد شود. اطلاعاتی مانند مسائل خانوادگی یا مالی یا پزشکی از این نوع اطلاعات است.



به هر حال، با ظهور شبکه‌ها و اینترنت، نسبت به قدیم، خطرات جدی‌تری متوجه همه است. یکی از مشکلات در این زمانه دردسترس بودن در هر مکان و زمان است؛ به این معنی که می‌توان در بیشتر جاها ردونشان اکثر افراد را پیدا کرد و اطلاعاتی از زندگی شخصی، تحصیلی و کاری‌شان به دست آورد (فخار، ۱۳۹۵).

فصل دوم: تهدیدات حریم خصوصی کاربران شبکه‌های اجتماعی



- **جاسوسی از کاربران**
- **ردیابی کاربران بر اساس سیستم موقعیت‌یابی**
- **نفوذ در شبکه‌های اجتماعی**
- **انتشار بدافزارها و باج‌افزارها در میان کاربران شبکه‌های اجتماعی**
- ...

تهدیدات حریم خصوصی کاربران شبکه‌های اجتماعی

مقدمه

همان‌طور که پیش از این نیز گفته شد، با وجود نوظهور بودن شبکه‌های اجتماعی مجازی، امروزه صدها شبکه اجتماعی متنوع به وجود آمده است. هر کدام از این شبکه‌ها فرصت‌ها و تهدیدهای خاص خود را دارد.

همه‌روزه تعداد کاربران شبکه‌های اجتماعی رو به افزایش است و از آنجاکه بیشتر آن‌ها چیزی از حفاظت محرمانگی نمی‌دانند، اطلاعات شخصی و حساس خود را به راحتی در اختیار دیگران قرار می‌دهند. نگرانی اصلی زمانی به وجود می‌آید که علی‌رغم ایجاد برخی سیاست‌های محرمانگی^۱ از سوی شبکه‌های اجتماعی مختلف، همچنان این شبکه‌ها آسیب‌پذیرند. در اینجا ذکر این نکته ضروری است که در اکثر مواقع، این نفوذها با استفاده از غفلت کاربران و بی‌احتیاطی در استفاده از این شبکه‌ها صورت می‌گیرد. آزمون‌های مختلف که به بررسی کاربران شبکه‌های اجتماعی پرداخته‌اند و نیز آماری که از آن‌ها به دست آمده است، نشان می‌دهد که بیشتر کاربران، بسیاری از اطلاعات مهم و شخصی خود

¹ Privacy Policy

را در این شبکه‌ها قرار می‌دهند و بدون هیچ شناخت و تحقیقی پیشنهادهای دوستی را می‌پذیرند و پس از آن اشخاص ناشناس می‌توانند به راحتی به این اطلاعات دست پیدا کنند. برای محافظت از محرمانگی، برنامه‌های کاربردی مختلفی عرضه شده است که به کاربران برای محدود کردن دسترسی دوستانشان کمک کنند (اسلامی، ۱۳۹۱). به این قبیل برنامه‌ها در ادامه خواهیم پرداخت.

در این فصل تلاش شده است مسائلی که در شبکه‌های اجتماعی، حریم خصوصی افراد را به خطر می‌اندازند، شناسایی شود.

جاسوسی از کاربران

متأسفانه بسیاری از مردم، زمانی که نرم‌افزارهای ارتباطی را بر روی سیستم خود نصب می‌کنند، معمولاً اصول امنیتی مربوط به آن‌ها را در نظر نمی‌گیرند و به این طریق به تولیدکنندگان این نرم‌افزارها امکان می‌دهند تا به اطلاعاتشان دسترسی پیدا کنند. چند نمونه از راه‌های دسترسی‌ای که خود کاربران مجوز آن را به تولیدکنندگان می‌دهند و سبب جاسوسی اطلاعات می‌شوند، در ادامه آورده شده است.



مجوز سطح دسترسی

هر نرم‌افزاری که بر روی سیستم افراد نصب می‌شود، به میزانی از اطلاعات دسترسی پیدا می‌کند؛ اما پیش از این دسترسی، از خودِ کاربر در این باره سؤال می‌کند. توافق‌نامه‌ای که کاربران غالباً بدون مطالعه موقع نصب نرم‌افزارها تأیید می‌کنند، حاوی بندهایی است که این قبیل دسترسی‌ها در آن‌ها ذکر شده است. بسیاری از این‌گونه برنامه‌ها زمینه‌ای مناسب برای سوءاستفاده از اطلاعات شخصی کاربران و طبیعتاً نقض حریم خصوصی آن‌ها فراهم می‌آورد. حتماً برای شما هم بارها پیش آمده که وقتی برنامه‌ای روی گوشی یا کامپیوتر خود نصب می‌کنید یا در سایتی عضو می‌شوید، با این پرسش مواجه شوید: «آیا با شرایط و قوانین ما موافقید؟» و بی‌درنگ گزینه «بله» را زده و به مرحله بعد رفته‌اید. در این حالت انگار زیر کاغذی سفید را امضا کرده‌اید که طرف مقابل هر چیزی دلش بخواهد، در آن می‌نویسد!

برای مثال، برخی از دسترسی‌هایی که نرم‌افزار پیام‌رسان تلگرام به‌هنگام نصب بر روی گوشی، از کاربران درخواست می‌کند، در زیر نمایش داده شده است.

دوربین	خواندن وضعیت تلفن و شناسه	خواندن کارت تماس شما	اصلاح و خواندن مخاطبان شما	یافتن حساب‌ها در دستگاه	خواندن کارت حافظه
تغییر یا حذف محتویات کارت حافظه	دریافت پیام‌های نوشتاری (پیامک)	مشاهده اتصالات Wi-Fi	مشاهده اتصالات شبکه	ضبط صدا	دسترسی کامل به اینترنت
نوشتن گزارش تماس	خواندن گزارش تماس	تماس مستقیم با شماره‌تلفن‌ها	موقعیت مکانی دقیق (مبتنی بر GPS و شبکه)	دسترسی به بلوتوث	دسترسی سرویس بر بستر وب گوگل

این مسائل ذکر شده، برای زمانی است که کاربر به‌علت کم‌دقتی چنین دسترسی‌هایی را به نرم‌افزار می‌دهد؛ در حالی که نرم‌افزارهای بسیاری وجود دارد که بدون اطلاع کاربر شروع به کپی‌برداری از اطلاعات وی می‌کنند؛ یعنی دیگر کسی در این باره حتی سؤالی هم از کاربر نمی‌پرسد. این مورد دربارهٔ نرم‌افزارهای بسیار مفیدی که به‌صورت رایگان ارائه می‌شوند، بسیار بیشتر اتفاق می‌افتد.

ذخیرهٔ اطلاعات در سرورها و امکان شنود اطلاعات

وقتی در قرارداد نرم‌افزار قید می‌شود که اطلاعات کاربر به‌مدت ۳۰ ماه در سرورهای آن‌ها ذخیره می‌شود، مشخص است که اطلاعات کاربران برای مدت طولانی در سرورهای مربوط به این نرم‌افزارها نگهداری می‌شود. البته این اطلاعاتی است که به‌صورت علنی به کاربران گفته می‌شود. نرم‌افزارهای بسیاری وجود دارند که خدماتی را در اختیار کاربران قرار می‌دهند و در مقابل (بدون اطلاع کاربر) اطلاعاتی را از کاربران دریافت می‌کنند. اطلاعات به‌دست‌آمده از کاربران (که در نگاه اول به نظر بسیاری از آن‌ها ساده و غیرمفید می‌آیند) برای برخی از سازمان‌ها (ازجمله سازمان‌های جاسوسی) به‌قدری ارزشمند است که حاضرند برای دسترسی به آن‌ها چندین میلیارد دلار هزینه کنند و حتی حاضر به سوءاستفاده از ابزارهای قانونی شوند. برای مثال، سازمان امنیت ملی آمریکا (NSA) از سال ۲۰۱۵ به‌بهانهٔ امنیت ملی، تمام سرویس‌های اینترنتی مستقر در آمریکا را مجبور به ارائهٔ اطلاعات کاربران کرده است. یا شرکت فیس‌بوک علاوه بر ارائهٔ تمام اطلاعات کاربران خود به NSA، یک کارشناس داده نیز در اختیار آن‌ها قرار داده تا در تحلیل داده‌های کاربران با NSA همکاری کند.



البته بسیاری از سازندگان نرم‌افزارهای رایگان، اهدافی تجاری دارند که با رسیدن به آن‌ها نیازی ندارند اطلاعات به‌دست‌آمده از کاربران را بفروشند. برای نمونه، شرکت گوگل با استفاده از داده‌های شخصی کاربران و شخصی‌سازی تبلیغات ارائه‌شده به آن‌ها، سالانه میلیاردها دلار سود کسب می‌کند.

امکان پشتیبان‌گیری از اطلاعات

نرم‌افزارهای پیام‌رسان معمولاً یک کپی از اطلاعاتی مانند ارتباطات، مخاطبان، مدت تماس و نوع ارتباط (پیامک، صوتی، تصویری) کاربران را، با توجیه پشتیبان‌گیری، پیش خود نگه می‌دارند که بیشتر برای ارتقای کیفیت سیستم‌هایشان از آن استفاده می‌کنند. بسیاری از نرم‌افزارها چنین بک‌آپی را با درخواست کاربر، به خودش نیز می‌دهند. مثلاً وقتی شما از واتساپ استفاده می‌کنید، می‌توانید از اطلاعات و چت‌های خود بک‌آپ بگیرید و نرم‌افزار را پاک کنید.



به این ترتیب، بعد از نصب مجدد برنامه، واتساپ تمام آن‌ها را به شما برمی‌گرداند. اینکه شرکتی تا این حد به اطلاعات شخصی افراد دسترسی داشته باشد، بحث‌برانگیز و البته کمی نگران‌کننده است. براساس اطلاعات جمع‌آوری شده می‌توان هویت کاربر و نوع فعالیت و طبقه اجتماعی وی را شناسایی کرد و اطلاعات متنوعی درباره او به دست آورد.

ردیابی کاربران براساس سیستم موقعیت‌یابی

تمام تلفن‌های هوشمند و وسایل ارتباطی امروزی دارای GPS¹ هستند. بسیاری از نرم‌افزارهای ارائه‌شده نیز از این ابزار برای دستیابی به اهداف خود استفاده می‌کنند. این تکنولوژی اگرچه بسیار مفید است، اما به وسیله آن بسیاری از نرم‌افزارها قادرند مسیر حرکت، مکان‌های موردعلاقه، مسیرهای پُرتردد و موارد مشابه مربوط به تمام کاربران را ثبت کنند. امروزه تقریباً اکثر نرم‌افزارهای پیام‌رسان با استفاده از دسترسی‌هایی که از کاربر می‌گیرند، به سادگی به GPS کاربران دسترسی دارند و در صورتی که بخواهند، می‌توانند به تمام اطلاعات مکانی کاربران دست پیدا کنند. این یعنی اینکه در هر لحظه از مکان آن‌ها و مسیرهای رفت‌وآمدشان آگاهی پیدا می‌کند و حتی می‌تواند این اطلاعات را برای مصارف بعدی خود ذخیره کند. استفاده از GPS در کنار مزیت‌های بسیاری که دارد، ممکن است واقعاً انسان را دچار دردسر کند. مثلاً در شبکه‌هایی مانند اینستاگرام

¹ Global Positioning System

می‌تواند خطر سرقت را افزایش دهد. فرض کنید به مسافرت رفته‌اید و در حین سفر از خود مرتباً عکس‌هایی با موقعیت مکانی خود منتشر می‌کنید. از این طریق مستقیماً به سارقان اعلام می‌کنید که در خانه نیستید و خانه شما برای سرقت آماده است (Tu و همکاران، ۲۰۰۸).



بسیاری از این نرم‌افزارهای رایگان، از رفتار، گفتار، موقعیت و عکس‌های ارسالی شما اطلاعاتی جمع‌آوری می‌کنند که می‌توانند از آن‌ها برای اهداف جاسوسی و تجاری و تبلیغاتی خود استفاده کنند (بیشتر نرم‌افزارها این تأیید اولیه را از کاربر می‌خواهند). این امر یکی از بارزترین نمونه‌های نقض حریم خصوصی افراد است که البته خود کاربران اجازه‌اش را صادر می‌کنند!

نفوذ در شبکه‌های اجتماعی

یکی از مخرب‌ترین پدیده‌های دنیای دیجیتال و البته یکی از اصلی‌ترین ناقضان حریم خصوصی، هکرها هستند. هک کردن^۱ در تعریف کلی عبارت است از استفاده از نرم‌افزاری

^۱ Hack

مخرب برای ایجاد مشکل در یک سیستم یا دزدیدن اطلاعات؛ اما وقتی مردم دربارهٔ هک و شبکه‌های اجتماعی صحبت می‌کنند، به تعریف اصلی آن اشاره نمی‌کنند. هک کردن شبکه‌های اجتماعی با داشتن کمی اطلاعات فنی، شدنی است. منظور از هک کردن در شبکه‌های اجتماعی این است که بر مبنای اطلاعات پروفایل شخصی فردی غریبه، اعتمادش جلب شود. این نوع هک کردن، مهندسی اجتماعی نامیده می‌شود. مهندسی اجتماعی از تکنیک‌های روانی متقاعدکننده استفاده می‌کند تا از ضعیف‌ترین عضو در سیستم امنیتی اطلاعات، که در اینجا انسان‌ها هستند، بهره‌برداری کند.



هنگامی که مردم در شبکه‌های اجتماعی صفحه‌ای ایجاد می‌کنند، معمولاً احتمال خطرهای امنیتی و نقض حریم خصوصی خود را نادیده می‌گیرند. هرچه از اطلاعات شخصی بیشتری در پروفایل عمومی خود استفاده کنید، هکرها راحت‌تر می‌توانند با استفاده از چنین اطلاعاتی از اعتماد شما سوءاستفاده کنند (باطنی و ترک، ۱۳۹۵).

مزیت امنیتی عمدهٔ شبکه‌های اجتماعی این است که فقط دوستان یا اعضای شبکه اجازه دارند تمام اطلاعات پروفایل شخصی را مشاهده کنند. البته این زمانی کاملاً مؤثر

است که در انتخاب اعضا یا دوستان خود احتیاط لازم را به خرج داده باشید. اگر هر درخواست دوستی یا کاری را قبول کنید، این احتمال وجود دارد که یکی از آن‌ها هکر باشد.

متأسفانه یکی از مشکلات شبکه‌های اجتماعی آنلاین این است که هیچ راهکاری برای تشخیص هویت واقعی افرادی که در آن پروفایل می‌سازند، وجود ندارد. در چنین وضعیتی هر هکری می‌تواند به راحتی پروفایلی رایگان در یکی از شبکه‌های اجتماعی ایجاد کند و علاقه‌مندی‌هایش را برحسب آن افرادی ثبت کند که مطابق هدفش هستند. اگر فرد هدف، درخواست ارتباط را قبول کند، هکر حتی به اطلاعات دیگر اعضای شبکه او نیز دسترسی پیدا می‌کند. راه مبارزه با مهندسی اجتماعی، آگاهی و هوشیاری کاربران شبکه‌های اجتماعی است.

جعل هویت

سارقان و مجرمان اینترنتی بسیاری از اوقات از طریق کپی کردن حساب کاربری دیگران یا ساختن حساب‌های کاربری غیرواقعی به اعمال مجرمانه خود می‌پردازند و باعث نقض حریم خصوصی دیگران می‌شوند. شاید بتوان یکی از بزرگ‌ترین معضلات فضای مجازی را، به خصوص در ایران، هویت نامشخص بسیاری از کاربران و به تعبیری هویت جعلی آنان دانست. با هویت‌های جعلی، ارتباطات جعلی شکل می‌گیرد. این کار خطر بزرگی برای امنیت جامعه مجازی است.

انتشار بدافزارها و باج‌افزارها در میان کاربران شبکه‌های اجتماعی

شبکه‌های اجتماعی، به دلیل فراگیربودن در همه جامعه، زمینه مناسبی را برای پخش هرزنامه‌ها و بدافزارهای مختلف فراهم آورده‌اند. از این رو، انتشار بدافزارها در شبکه‌های

اجتماعی افزایش یافته و معمولاً از کاربران شبکه‌های اجتماعی برای انتشارشان استفاده می‌شود. یکی از این بدافزارها، "بات"^۱ است که از شبکه‌های اجتماعی به‌عنوان مختلف سوءاستفاده می‌کند و حریم خصوصی افراد را به‌طور گسترده نقض می‌کند. آسان‌بودن گسترش بات‌ها در این شبکه‌ها و استفاده از این بستر به‌عنوان کانال فرمان و کنترل، سبب شده که طراحان بات‌ها تمایل زیادی به استفاده از شبکه‌های اجتماعی پیدا کنند (مودی و همکاران، ۱۳۹۵).



همچنین با استفاده از شبکه‌های اجتماعی، باج‌افزارها می‌توانند اطلاعات کاربران را رمز کنند و برای رمزگشایی آن‌ها هزینه‌هایی از کاربران بگیرند؛ یعنی ممکن است شما اطلاعات مهمی داشته باشید و آن را در گوشی یا کامپیوتر خود بدون تدابیر امنیتی نگه دارید. در اینجاست که ممکن است هکری آن اطلاعات را بردارد و آن را برایتان غیرقابل‌استفاده یا دسترسی‌ناپذیر کند و از شما بخواهد که برای دستیابی به آن اطلاعات مبلغی را پرداخت کنید یا کاری انجام دهید که مطابق میلان نیست.

^۱ Bot



ایجاد مزاحمت و هرزنگاری

مزاحمت و هرزنامه‌نگاری (اسپم‌کردن) آنلاین، سوءاستفاده رایجی است که برای آزار یا تهدید یا ایجاد هراس انجام می‌شود و ویژگی آن، قابلیت تکرار شونده‌اش است؛ یعنی این کار بارها و بارها انجام می‌شود. گاهی افراد با تبلیغات دروغین اینترنتی قربانی فریب و کلاهبرداری می‌شوند (مثل وقتی که عضو صفحات دوست‌یابی جعلی می‌شوند)؛ به نحوی که براساس موقعیت، بی‌آنکه بدانند، اطلاعات شخصی خود را در اختیار دیگران می‌گذارند. سوءاستفاده رایج دیگر، انتشار و توزیع بدخواهانه اطلاعات تصویری، به‌منظور جریحه‌دار کردن افراد است. درواقع، مزاحمت و هرزنامه‌نگاری که از طریق اینترنت یا تلفن همراه یا دوربین برای آسیب‌رساندن یا اذیت و آزار انجام می‌شود، ممکن است به‌شکل گسترده‌ای منتشر شود. به همین دلیل، این کار بسیار خطرناک و مضر است و ممکن است تبعات جبران‌ناپذیری را برای فرد و حریم شخصی او داشته باشد.

قلدری اینترنتی

«قلدری اینترنتی (سایبری)» زمانی اتفاق می‌افتد که یک کاربر اینترنت را، کاربری دیگر (حتی یک کودک پیش‌دبستانی یا نوجوان) با استفاده از فناوری‌های دیجیتال یا تلفن‌های همراه مورد آزار و اذیت، تهدید و تحقیر قرار دهد و حریم خصوصی‌اش را نقض کند. ممکن است قربانی مزاحمت سایبری یا زورگیری اینترنتی، با خطر ابتلا به اختلالات عاطفی و عوارض روانی روبه‌رو شود و نتواند به دوستان هم‌مدرسه‌ای، همکاران یا همسایه‌ها اعتماد کند. افراد گروه سنی ۱۵ تا ۲۹ سال اکثر قربانیان احتمالی آزار و اذیت اینترنتی را تشکیل می‌دهند. از این میان، یک‌سوم اعتراف کرده‌اند که قربانی قلدری اینترنتی شده‌اند. یک‌سوم دیگر ادعا کرده‌اند که قربانی زورگیری مجازی شده و یک‌سوم نیز مدعی شده‌اند که هر دو مورد را تجربه کرده‌اند.



اغفال کودکان در این نوع از ارتباطات

از مهم‌ترین آسیب‌های فرهنگی و اجتماعی شبکه‌های اجتماعی، به‌خصوص در شبکه‌های اجتماعی موبایل، می‌توان به روابط نامناسب بین کودکان اشاره کرد. این روابط که به‌دلیل کاهش توان نظارتی والدین در این فضا به وجود می‌آید، بعد از مدتی باعث دورشدن اعضای خانواده از یکدیگر می‌شود و درنهایت، اساس خانواده را از بین می‌برد. افزایش مزاحمت و هرزنامه‌نگاری، نقض حریم خصوصی، امکان بک‌آپ‌گیری از اطلاعات شخصی، اختلال در بسیاری از فعالیت‌های اجتماعی که ناشی از اعتیاد به این نرم‌افزارهاست، به‌مخاطره‌افتادن ارتباطات چهره‌به‌چهره، اغفال کودکان و اتلاف زمان از جمله آسیب‌هایی است که از این طریق پدید می‌آید. به‌گفتهٔ محققان، دانش‌آموزان و دانشجویانی که درگیر شبکه‌های اجتماعی می‌شوند، به‌دلیل اتلاف چندین ساعت از وقت خود در این شبکه‌ها، تمرکزشان بر درس کاهش می‌یابد و دچار افت تحصیلی می‌شوند.



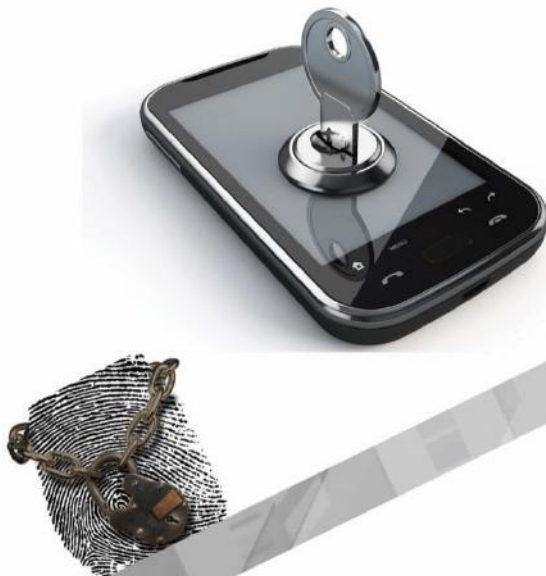
استفاده از VPN و پروکسی

باتوجه به محدودیت‌های موجود در برخی از شبکه‌های اجتماعی در کشور، بسیاری از کاربران، به خصوص نوجوانان، برای استفاده از این شبکه‌ها و عبور از این محدودیت‌ها، از سرویس VPN و پروکسی‌های مختلف استفاده می‌کنند. آنچه این ابزارها انجام می‌دهند (حداقل آنچه ادعا می‌کنند)، این است که داده‌های شما را رمزنگاری می‌کنند و به مقصد می‌رسانند؛ بدون اینکه کسی بتواند این داده‌ها و حتی خود شما را به عنوان کاربر، ردیابی کند. اما واقعیت این است که تمام داده‌های شما به صورت رمز نشده توسط فراهم کننده VPN قابل مشاهده است. به عبارت دیگر، هنگام استفاده از VPN، داده‌های شما ابتدا به سرور VPN منتقل می‌شود و سپس از آنجا به مقصد مدنظر شما انتقال می‌یابد. پاسخ از مقصد نیز مجدداً از همین مسیر به دست شما خواهد رسید. درواقع، سرور VPN (یا پروکسی) مانند یک واسط میان شما و مقصدتان عمل می‌کند. واضح است که اگر فراهم کننده VPN اراده کند، به سادگی می‌تواند به تمام اطلاعات شخصی شما که از طریق VPN او منتقل شده، دست یابد و در صورت نیاز حتی آن‌ها را برای خود ذخیره کند. بنابراین، در صورتی که به حریم خصوصی خود اهمیت می‌دهید، بهتر است از این گونه سرویس‌ها پرهیز کنید یا در استفاده از VPN‌ها و Proxy‌ها (به خصوص نسخه‌های رایگان آن‌ها) بسیار احتیاط کنید.



در سال‌های اخیر، اپراتورهای شبکه‌های اجتماعی، شرکت‌های امنیتی و محققان دانشگاهی تلاش کرده‌اند که راه‌حل‌هایی برای مقابله با خطرات بالا ارائه کنند. در بخش آخر این کتاب راه‌حل‌هایی را که ممکن است در برابر این خطرات، به کاربران کمک کنند، ارائه داده‌ایم؛ اما فراموش نکنیم که همه این روش‌ها فقط زمانی کارا خواهند بود که هوشمندی لازم در استفاده از شبکه‌های اجتماعی را داشته باشیم.

فصل سوم: راهبردهای حفظ حریم خصوصی در شبکه‌های اجتماعی



- اصول استفاده از شبکه‌های اجتماعی
- سازوکارهای تأیید هویت شبکه‌های اجتماعی
- روش‌های حفظ حریم خصوصی در شبکه‌های اجتماعی و پیام‌رسان‌ها

راهبردهای حفظ حریم خصوصی در شبکه‌های اجتماعی

مقدمه

همان‌طور که در فصل‌های قبل گفته شد، امروزه اینترنت و شبکه‌های اجتماعی تبدیل به بخشی از نیازهای اساسی انسان (مانند آب و غذا) شده‌اند و به‌هیچ‌وجه نمی‌شود آن را از زندگی مردم جدا کرد. هریک از ما روزانه به‌طور متوسط چندین ساعت از زمان خود را در این شبکه‌ها سپری می‌کنیم و به تعامل و تبادل اطلاعات با دیگران می‌پردازیم. با در نظر گرفتن این وضع، لازم است همه به‌طور دقیق به حریم خصوصی خود حساس باشیم و کارهای لازم را برای افزایش امنیت حریم خصوصی و امنیت دیجیتال خود به کار بندیم. هدف این فصل از کتاب، آشنایی با سازوکارهای امنیتی در شبکه‌های اجتماعی و روش‌های حفظ حریم خصوصی فرد و اطرافیان است. در انتهای فصل نیز تنظیمات مربوط به حریم خصوصی در شبکه‌های اجتماعی پرکاربرد بررسی شده و روش‌های موجود در این شبکه‌ها برای افزایش امنیت کاربری نمایش داده شده است (کینکوف و همکاران، ۱۳۸۹).



اصول استفاده از شبکه‌های اجتماعی

هنگام استفاده از شبکه‌های اجتماعی با رعایت فقط چند نکته ساده به راحتی می‌توان از وقوع بسیاری از اتفاقات بد جلوگیری کرد و تا حد زیادی از آسیب‌های ممکن این شبکه‌ها، در امان ماند. در ادامه برخی از این اصول به طور خلاصه ذکر می‌شوند (بشیر، ۱۳۹۲).

- فراموش نکنید که اینترنت همیشگی است. داده‌ای که شما در فضای آنلاین منتشر می‌کنید، برای همیشه آنجا می‌ماند. مهم نیست شما آن داده را پاک کنید، حتی پاک کردن حساب کاربری نیز منجر به پاک شدن آن نخواهد شد. آنچه منتشر می‌کنید، همیشه در دسترس دیگران خواهد بود. بنابراین، همواره دقت کنید که چه اطلاعاتی را در اینترنت منتشر می‌کنید؛ چون راه بازگشتی وجود ندارد.

- همیشه در کلیک کردن بر روی لینک‌ها احتیاط کنید. مهم نیست چه کسی لینک را ارسال کرده باشد. حتی اگر آن فرد دوستانه باشد، بدون احتیاط بر روی لینک‌ها کلیک نکنید. دزدان اینترنتی از شبکه‌های اجتماعی برای دزدیدن اطلاعات شما استفاده می‌کنند؛ چون در این فضاها فریب دادن راحت‌تر است. آن‌ها

از حساب کاربری دوستانتان استفاده می‌کنند تا لینک‌های خطرناک برایتان ارسال کنند. کافی است بر روی لینک‌ها کلیک کنید تا اطلاعات خصوصی تان به دست آن‌ها بیفتد. بنابراین، همیشه مواظب لینک‌های دریافتی باشید.



- در پذیرفتن دوستی افراد بسیار دقت کنید. هرگز به عکس و اسم افرادی که به شما درخواست دوستی می‌دهند، اعتماد نکنید. هیچ معلوم نیست که آن اطلاعات واقعی باشد. در شبکه‌های اجتماعی استفاده از عکس و نام دروغین بسیار ساده و مرسوم است. فقط دوستی کسانی را بپذیرید که آن‌ها را در دنیای واقعی می‌شناسید و به آن‌ها اعتماد دارید.



- مرتباً تنظیمات مربوط به حریم خصوصی خود را چک کنید.
همهٔ شبکه‌های اجتماعی تنظیماتی برای حریم خصوصی دارند. مطمئن شوید که این تنظیمات به‌گونه‌ای قرار داده شده که اطلاعاتتان را فقط با دوستان و خانواده‌تان در میان می‌گذارد. همچنین در بازه‌های زمانی مشخص، این تنظیمات را مجدداً بررسی کنید تا در صورت تغییر آن‌ها در اسرع وقت متوجه شوید.
- هرگز اطلاعات شخصی خود را منتشر نکنید.
در انتشار اطلاعات شخصی (مانند آدرس خانه، شماره‌تلفن، شماره‌ملی و شناسنامه) بسیار دقت کنید. هرگز این اطلاعات را در محیط مجازی منتشر نکنید. اگر کسی این اطلاعات را از شما پرسید، به او شک کنید. این اطلاعات می‌تواند به‌سادگی به دزدان اینترنتی امکان دزدیدن اطلاعات شما را بدهد.
- رمز عبور خود را مرتباً عوض کنید.
هرگز رمز عبورهایی را انتخاب نکنید که به‌سادگی می‌شود آن‌ها را حدس زد. رمز عبوری انتخاب کنید که حداقل ۸ نویسه داشته باشد و متشکل از عدد و حروف و علامت‌ها باشد. رمزهای عبور خود را در بازه‌های زمانی (مثلاً هر شش ماه) عوض کنید. برای حساب‌های کاربری مختلف هرگز رمز عبور یکسان استفاده نکنید.



- مراقب باشید اطلاعات شما در کجا منتشر می‌شود. دقت کنید که ممکن است حساب‌های کاربری شما در شبکه‌های مختلف به هم متصل باشند؛ مثلاً ممکن است عکسی که در توییتر منتشر می‌کنید، به‌طور خودکار در فیس‌بوک نیز منتشر شود.

- هرگز در سفر، موقعیت جغرافیایی خود را به اشتراک نگذارید. در مواقعی که به مسافرت می‌روید، هرگز مکان جغرافیایی خود را به‌همراه عکس‌های خود به اشتراک نگذارید. این‌گونه به دزدان نشان می‌دهید که خانه‌تان آماده سرقت است. زمانی عکس‌ها و مناطق را به اشتراک بگذارید که به خانه بازگشته‌اید.



- برای ارتباطاتتان حدومرز قائل شوید.

همیشه در زندگی آنلاین، مانند زندگی واقعی، حدومرزی برای ارتباطاتتان قائل شوید. قبل از اینکه متنی را توییت کنید یا محتوایی را در فیس‌بوک منتشر کنید، کمی فکر کنید و ببینید آیا کسی از دیدن آن ناراحت نمی‌شود یا اینکه در آینده برایتان مشکلی ایجاد نمی‌کند. این اصل را مدام مدنظر قرار دهید: همیشه چیزی را منتشر کنید که کسی در آینده نتواند آن را دست‌مایه سوءاستفاده از شما قرار دهد.

- حواستان باشد که لیست دوستانتان شامل چه کسانی است.

حتی مراقب دوستان دوستانتان باشید. ممکن است آن‌ها هم برایتان مشکل‌ساز شوند. ممکن است شما تنها به دوستانتان اجازه دیدن پست‌ها و عکس‌های فیس‌بوکتان را داده باشید؛ اما وقتی دوستی برایتان کامنت می‌گذارد یا مطلبتان را لایک می‌زند، دوستان او هم قادر به دیدن مطلب شما باشند. برای مثال، عکسی خانوادگی را برای لیست خانواده خود به اشتراک می‌گذارید. هیچ‌کسی جز اعضای خانواده شما در این لیست قرار نداشته‌اند و قاعدتاً نباید کسی جز این افراد بتواند عکس را مشاهده کند. برادران که در لیست خانواده قرار دارد، عکستان را لایک می‌کند و این باعث می‌شود فردی غریبه که در لیست دوستان برادر شماست، از طریق همین لایک به عکس شما دسترسی پیدا کند. یا برای مثال، یک توییت را برای لیستی خصوصی از افراد منتشر می‌کنید؛ اما یکی از افراد لیست آن را ریتوییت یا عکسی از آن را منتشر می‌کند. این مشکلات یادآور اصلی مهم است؛ اصلی که همواره لازم است رعایت کنید تا دچار مشکل نشوید: هیچ‌گاه چیزی را که از انتشار آن در زندگی واقعی‌تان احساس امنیت و راحتی نمی‌کنید، در فضای مجازی منتشر نکنید؛ زیرا سرانجام کسانی که نباید، آن را خواهند دید.



در همه شبکه‌های اجتماعی امکان مشخص کردن دسترسی افراد مختلف به مشخصات فردی و محتوایی که منتشر می‌کنید، وجود دارد. در فیس‌بوک این امکان را دارید که بخش‌های مختلف حساب کاربری‌تان را برای دوستان، دوستان دوستان، شبکه و همه افراد قابل دیدن کنید.



هنگامی که فردی بدون اجازه و غیرقانونی به حساب کاربری‌تان وارد شود، می‌توانید ارتباط وی را قطع کنید. برای این منظور، روی گزینه Account در بالای صفحه پروفایل در سمت راست، کلیک کنید. از پنجره‌ای که باز می‌شود، گزینه Account Settings را انتخاب کنید. اطلاعات مربوط به فعالیتهای حسابتان را در گزینه Account Security

خواهید یافت. اگر فرد دیگری هم log in شده باشد، همین اطلاعات درباره او نوشته می‌شود و می‌توانید او را به عنوان ناشناس معرفی و ارتباطش را قطع کنید. حتی ممکن است کسی به حسابتان نفوذ نکرده باشد؛ بلکه از کامپیوتر مدرسه، کتابخانه یا کافی‌نت محله‌تان وارد حساب فیس‌بوکتان شده باشید، اما فراموش کرده باشید از آن خارج شوید. اینجا هم این کار بسیار برایتان سودمند است و از این طریق کاری می‌کنید تا بعد از رفتن شما کسی نتواند از حسابتان استفاده کند.



سازوکارهای تأیید هویت شبکه‌های اجتماعی

همان‌طور که قبلاً هم گفتیم، بسیاری از اپراتورهای شبکه‌های اجتماعی تلاش می‌کنند با فعال کردن اقدامات امنیتی (مانند سازوکار «تأیید هویت کاربر» یا «تنظیمات حریم خصوصی») کاربران خود را در برابر اتفاقات بدی که ممکن است برایشان بیفتد، محافظت کنند. تعدادی از این روش‌ها را در زیر توضیح می‌دهیم.



سازوکار احراز هویت

برای اینکه اطمینان حاصل شود کاربری که ثبت‌نام می‌کند، کاربر واقعی است، اپراتورهای OSN^۱ از سازوکار تأیید هویت استفاده می‌کنند (مانند شناسایی عکس دوستان، تصدیق هویت چند فاکتور، یا در بعضی مواقع درخواست از کاربر که یک کپی از نام کاربری خود را ارسال کند). در این میان، تلگرام هم دو عامل احراز هویت را به کار برده است. کاربر در زمان وارد شدن به تلگرام، نه تنها نیاز به وارد کردن رمز عبور دارد، بلکه لازم است کد تأییدی را که به تلفن همراهش ارسال می‌شود، درج کند. این راهکار باعث می‌شود از ورود کاربر با حساب کاربری جعلی و نیز از انتشار اطلاعات نادرست جلوگیری شود. همچنین از این طریق از برخی حوادث پیشگیری می‌شود؛ مثلاً اینکه هکری حساب تلگرام را برباید.



^۱ Orbit Showtime Network: اپراتوری که با شراکت چند شرکت عربی و آفریقایی تأسیس شده است.

تنظیمات امنیت و حریم خصوصی

بسیاری از شبکه‌های اجتماعی آنلاین از تنظیمات حریم خصوصی کاربر با قابلیت‌های مختلف پشتیبانی می‌کنند. کاربران فیس‌بوک می‌توانند تنظیمات حریم خصوصی خود را سفارشی کنند. به این ترتیب، می‌توانند مشاهده مطالب، تصاویر، نوشته‌ها و بقیه بخش‌ها را شخصی‌سازی کنند. از سوی دیگر در Google+ سفارشی‌کردن حریم خصوصی به این شکل است که کاربران می‌توانند دوستان خود را دسته‌بندی کنند (مانند «دایره بهترین دوستان»، «دایره دوستان مدرسه»، «دایره کار») و به هر گروه، دسترسی موردنیاز را بدهند. به هر حال، ممکن است نخواهید آن مطلبی را که برای دوستان صمیمی خود ارسال می‌کنید، کل بچه‌های مدرسه ببینند.



سازوکارهای حفاظت داخلی

بعضی از شبکه‌های اجتماعی کاربران خود را با اجرای سازوکارهای حفاظت داخلی اضافی در برابر اسپم، پروفایل‌های جعلی، کلاهبرداری و دیگر تهدیدات محافظت می‌کنند. برای مثال، فیس‌بوک از کاربران خود در برابر حملات مخرب و دزدی اطلاعات، به وسیله فعال کردن سیستم ایمنی فیس‌بوک¹ (FIS) محافظت می‌کند.

¹ Facebook Immune System



گزارش کاربران

یکی از روش‌هایی که اپراتورها می‌توانند به‌وسیله آن از کاربرانی مانند ما، یعنی کاربران جوان و نوجوان خود، در برابر آسیب‌ها محافظت کنند، دریافت گزارش است. اپراتورها در این روش، گزینه‌ای برای گزارش سوءاستفاده‌ها یا سیاست‌های نقض‌شده در شبکه خود قرار می‌دهند. کاربران می‌توانند در صورت مشاهده این موارد، بلافاصله به اپراتورها اطلاع دهند. حتماً شما هم دیده‌اید که وقتی در تلگرام فرد ناشناسی پیامی ارسال می‌کند، در بالای صفحه گزینه report spam وجود دارد. اگر فرد مزاحم بود یا حرف‌های نامناسب زد، کافی است برای حفظ حریم خصوصی خودتان گزینه ریپورت را بزنید تا دیگر نتواند برایتان پیامی بفرستد.



سازوکار تأیید هویت دومرحله‌ای

یکی دیگر از روش‌هایی که برخی پیام‌رسان‌ها و شبکه‌های اجتماعی برای امنیت کاربران خود ارائه می‌کنند، تأیید هویت دومرحله‌ای است. با استفاده از این تنظیمات کاربران می‌توانند اطمینان حاصل کنند که ورود به حساب کاربری‌شان برای افراد غیرمجاز ممکن نیست. این شیوه از احراز هویت در هر شبکه اجتماعی یا پیام‌رسانی متفاوت است؛ اما اکثر سامانه‌ها پیامی متنی ارسال می‌کنند که حاوی کد منحصر به فردی است و این کد در زمان ورود به سامانه در کنار نام کاربری و گذرواژه پیشین درخواست می‌شود. پیام‌های متنی محیط ایمنی برای ارسال کد فرض شده‌اند؛ چراکه اگر نفوذگر به گذرواژه شما نیز دسترسی یابد، احتمال اینکه تلفن همراه شما را نیز ربوده باشد، بسیار کم است. در بخش بعدی بیشتر درباره این سازوکار در هر شبکه یا پیام‌رسان صحبت خواهیم کرد.



روش‌های حفظ حریم خصوصی در شبکه‌های اجتماعی و پیام‌رسان‌ها

در هریک از شبکه‌های اجتماعی، پیام‌رسان‌ها، سایتهای اشتراک‌گذاری و صندوق‌های پست الکترونیکی، گزینه‌های متفاوتی برای حفظ حریم خصوصی به شرح زیر وجود دارد.

شبکه اجتماعی فیس‌بوک



تأییدنکردن درخواست دوستی افراد ناشناس

پس از مدت‌زمان کوتاهی که از حضور شما در فیس‌بوک می‌گذرد، احتمالاً چند پیام دوست‌یابی دریافت می‌کنید. در این پیام‌ها از شما می‌خواهند که با آن افراد «دوست» شوید. زمانی که چنین درخواست‌هایی را بپذیرید، می‌توانید هر چیزی را که آن افراد می‌فرستند، ببینید و آن‌ها نیز آنچه را شما برای دیگران ارسال می‌کنید، می‌بینند. اگر درخواست از سوی کسی باشد که به ادامه ارتباط با او تمایل داشته باشید، شاید قصد داشته باشید نام او را به لیست «دوستان» اضافه کنید. اما اگر او را در دنیای واقعی نشناسید یا به هر دلیل نخواهید که در محیط مجازی با او ارتباط برقرار کنید، می‌توانید روی عبارت Not Now کلیک کنید.



ارسال و دریافت پیام و صفحه پست‌ها

هرچه بگویید، به خودتان برمی‌گردد. دانستن این نکته به شما کمک می‌کند تا هرگاه خواستید به قسمت Wall کسی پیغامی ارسال کنید یا درباره اطلاعات به‌روز او اظهارنظر کنید یا آن را تأیید کنید یا حتی دلیلی ارائه دهید، به افراد حاضر در شبکه و تأثیر گفته‌های خود کمی فکر کنید. پیامتان شما را چگونه معرفی می‌کند؟ اگر می‌خواهید چیزی را صرفاً به یکی از دوستان خود بگویید، تنها یک پیغام خصوصی بفرستید یا از سرویس چت در فیس‌بوک استفاده کنید.

کنترل محتویات پروفایل

می‌توانید تعیین کنید که چه کسی صفحه پروفایلتان را ببیند. صرف‌نظر از اینکه چه چیزی در صفحه پروفایل وارد کرده باشید، در صفحه تنظیمات حریم خصوصی، می‌توانید تعیین کنید که چه کسانی می‌توانند به این اطلاعات دسترسی داشته باشند. توصیه می‌شود که حداکثر این اجازه را به کسانی بدهید که در لیست «فقط دوستان» قرار دارند (کینکوف، ۱۳۸۹).

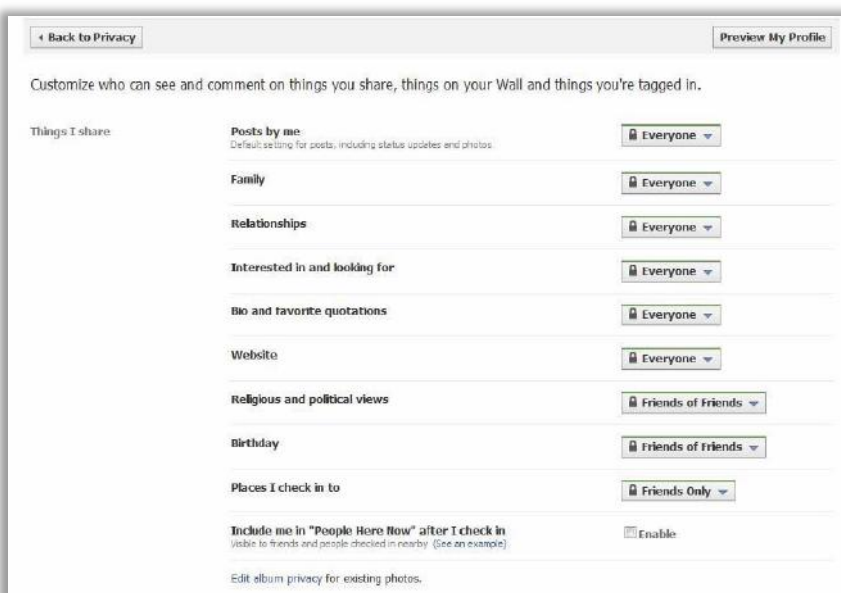
شخصی‌سازی تنظیمات حریم خصوصی

کاربران بسیاری از این تنظیمات پایه‌ای مطلع‌اند؛ ولی بسیاری از افراد نمی‌دانند که می‌توانند شخصی‌سازی بیشتری در این تنظیمات انجام دهند تا کنترل بیشتری بر روی اینکه چه کسانی بتوانند چه مطالبی را ببینند، داشته باشند. در قسمت پایینی صفحه «تنظیمات حریم خصوصی‌تان را انتخاب کنید»^۱ لینکی به بخش تنظیمات

^۱ Choose Your Privacy Settings

تهدیدات حریم خصوصی کاربران شبکه‌های اجتماعی

شخصی‌سازی^۱ وجود دارد. اگر روی این لینک کلیک کنید، به صفحه‌ای منتقل می‌شوید که امکانات کنترل جزئی امنیتی بسیاری را در اختیارتان می‌گذارد.



بخش «چیزهایی که به اشتراک می‌گذارم»^۲ در تنظیمات حریم خصوصی صفحه تنظیمات انتخابی به سه گروه تقسیم شده است: چیزهایی که به اشتراک می‌گذاریم، چیزهایی که دیگران به اشتراک می‌گذارند^۳، اطلاعات تماس^۴. در سمت راست هر آیتم در این صفحه یک کادر کشویی هست که به شما این امکان را می‌دهد تا مشخص کنید چه کسی به هریک از این آیتم‌ها دسترسی داشته باشد. برای مثال، پست‌های شما را به‌طور

^۱ Customize

^۲ Things I Share

^۳ Things Others Share

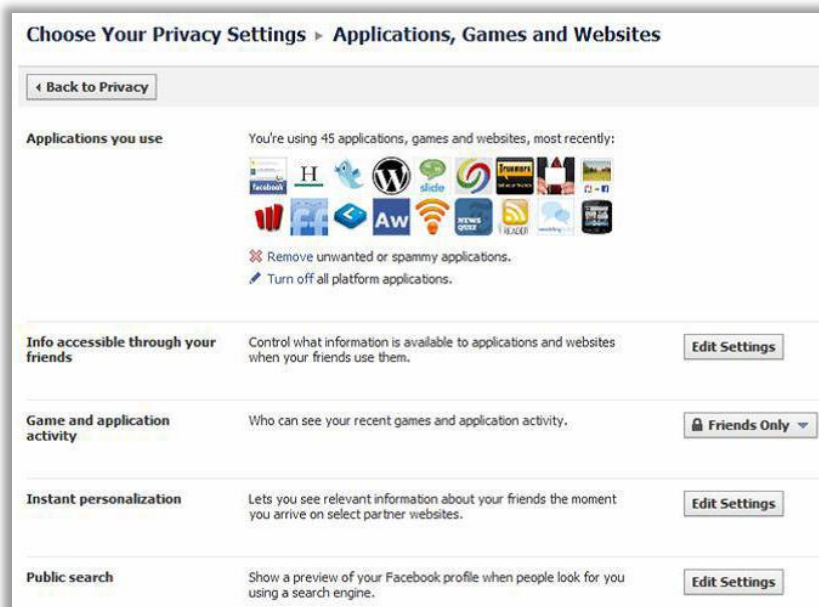
^۴ Contact Information

پیش‌فرض «همه» می‌توانند ببینند؛ ولی می‌توانید روی این کادر کلیک کنید و آن را به «دوستان دوستان»، «فقط دوستان» و «انتخابی» تغییر دهید.



کنترل برنامه‌های کاربردی

فیس‌بوک حاوی بسیاری از برنامه‌های کاربردی و تعدادی نرم‌افزار است که در داخل این سرویس کار می‌کنند. این برنامه‌های کاربردی می‌توانند شامل انواع بازی‌ها، خدمات اطلاع‌رسانی (خبررسانی)، آزمون‌ها و تقریباً هر چیز دیگری باشند که می‌تواند بر روی یک کامپیوتر برنامه‌ریزی شود. دانستن این نکته اهمیت دارد که سازندگان برنامه‌های کاربردی گاهی می‌توانند به داده‌های شما در فیس‌بوک دسترسی داشته باشند و بازی‌هایی وجود دارد که می‌توانند برخی از آن اطلاعات را با دوستان شما یا افراد دیگری که این بازی‌ها را انجام می‌دهند، به اشتراک بگذارند. اما درست مثل دیگر جنبه‌های فیس‌بوک، باید بر اینکه آن‌ها به چه اطلاعاتی می‌توانند دسترسی داشته باشند، نظارت کنید. می‌توانید با کلیک بر روی قسمت ویرایش تنظیمات خود که دقیقاً در پایین بخش برنامه‌های اجرایی و سایت‌های اینترنتی در پایین صفحه تنظیمات حریم خصوصی قرار دارد، به صفحه تنظیمات نرم‌افزارها، بازی‌ها و صفحات وب وارد شوید. در این مرحله صفحه‌ای را مشاهده می‌کنید که به شما اجازه می‌دهد تمام تنظیمات لازم برای برنامه‌های کاربردی، بازی و شبکه‌های اینترنتی (وب‌سایت‌ها) را مطابق کاربرد آن‌ها برای هر فرد، تنظیم کنید.



بلاک کردن کاربران فیس‌بوک

وقتی کسی را در فیس‌بوک بلاک می‌کنید، چه اتفاقی می‌افتد؟ با بلاک کردن هر کاربر، مانع این می‌شوید که فرد صفحه فیس‌بوکتان را ببیند. همچنین با این کار به‌طور خودکار با کاربر، unfriend می‌شوید.



افرادی که بلاک می‌شوند، نمی‌توانند:

- مطالبی را که در صفحه خود پست کرده‌اید، مشاهده کنند.
- شما را در پست‌ها یا نظرات یا عکس‌ها برچسب‌گذاری کنند.
- شما را به رویدادها یا گروه‌ها دعوت کنند.
- با شما گفت‌وگو کنند.
- شما را به‌عنوان یک دوست اضافه کنند.

برای بلاک کردن می‌توان از قسمت تنظیمات فیس‌بوک و گزینه Blocking اقدام کرد. در قسمت Blocking users باید دوستان مدنظر یا اشخاصی را که می‌خواهید، اضافه کنید.



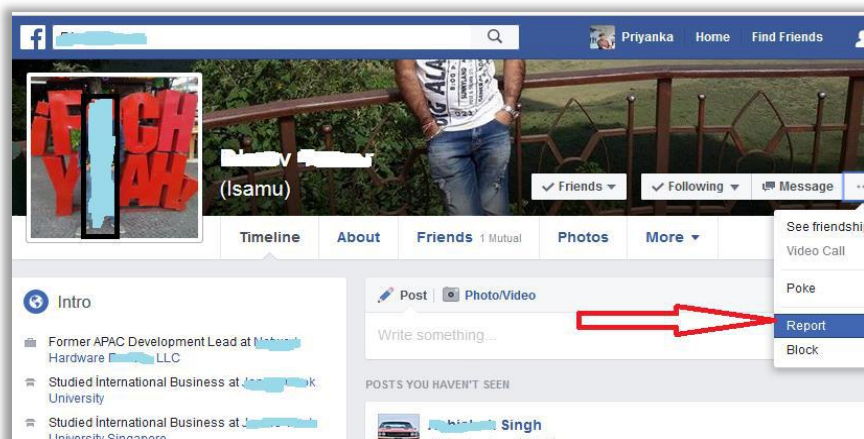
همچنین از طریق نمایه حساب کاربری می‌توانید شخص مدنظر را بلاک کنید.

تهدیدات حریم خصوصی کاربران شبکه‌های اجتماعی



ریپورت کاربران جعلی فیس‌بوک

به نمایه حساب کاربری جعلی بروید. اگر نمی‌توانید آن را پیدا کنید، سعی کنید نامی را که در نمایه مورد استفاده قرار می‌گیرد، جست‌وجو کنید یا اینکه از دوستانتان بخواهید پیوند آن را بفرستند.



بر روی عکس  کلیک کنید و Report را انتخاب کنید. دستورهای روی صفحه نمایش برای جعل هویت را برای Report دنبال کنید.

شبکه اجتماعی اینستاگرام



یکی دیگر از شبکه‌های اجتماعی که امروزه در میان ما بسیار محبوب شده، اینستاگرام است. این شبکه به دلیل جذابیت‌های زیاد، از جمله دسترسی بدون محدودیت و وجود طیف وسیعی از افراد جامعه (بازیگران، سیاست‌مداران، هنرمندان و...)، با اقبال زیادی در کشور روبه‌رو شده است. همچنین رشد سریع و چشمگیر استفاده از تلفن‌های هوشمند در میان افراد در سنین مختلف، تأثیر زیادی در رشد این شبکه اجتماعی داشته است. اما از طرف دیگر، این شبکه اجتماعی با توجه به ماهیت آن (که مبتنی بر محتوای تصویری است) بسیار ظرفیت آن را دارد که حریم خصوصی افراد را در معرض خطر قرار دهد. در ادامه به بررسی چند نکته ساده برای حفظ حریم خصوصی در این شبکه اجتماعی پرطرفدار و جذاب خواهیم پرداخت.

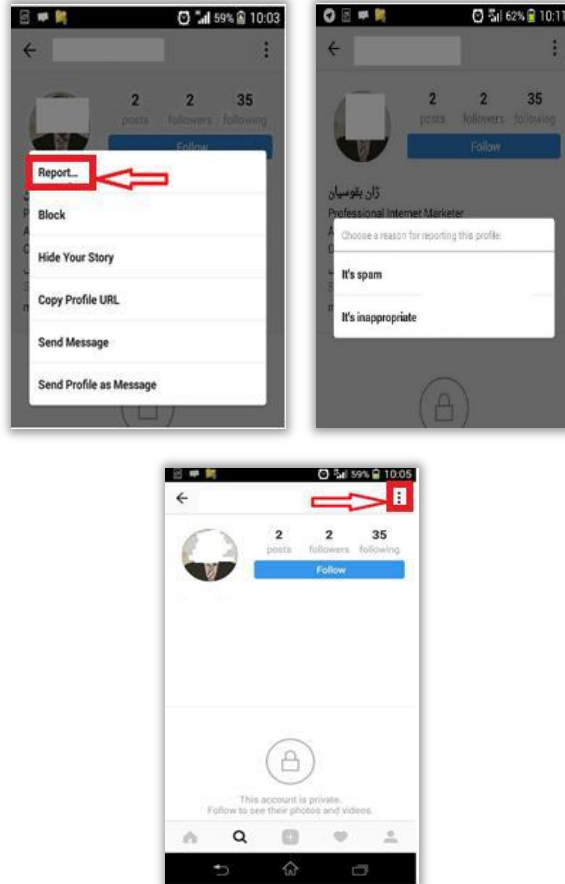
مسدودسازی کاربران مزاحم و مشکوک

کاربرانی را که به روش‌های مختلف مرتباً برایتان ایجاد مزاحمت می‌کنند یا کاربرانی را که حس خوبی به شما القا نمی‌کنند، مسدود کنید. با این کار تمام پست‌های آینده شما از دید آن‌ها مخفی می‌ماند و در نتیجه، آن‌ها از وضعیتتان اطلاع نخواهند داشت. برای مسدود کردن کاربر به صفحه پروفایل او بروید و پس از لمس سه نقطه بالای صفحه نمایش، گزینه Block User را انتخاب کنید.



ریپورت کردن کاربران

در اینستاگرام می‌توان کاربران، ویدئوها، تصاویر و کامنت‌ها را ریپورت کرد. برای ریپورت کردن کاربر یا صفحه اینستاگرام، طبق تصاویر زیر عمل کنید. ابتدا به صفحه موردنظر بروید و روی علامت سه نقطه کلیک کنید تا منویی به نمایش دربیاید. سپس عبارت Report را فشار دهید تا پنجره جدیدی نمایش داده شود و از شما دلالتان برای گزارش کردن آن کاربر را سؤال کند. دلیل خود را انتخاب کنید. سپس اینستاگرام از شما به دلیل گزارش کردن آن کاربر تشکر می‌کند و از طرف شما آن صفحه را بلاک می‌کند تا ارتباط آن با شما مسدود شود. با انجام دادن این مراحل می‌توانید کاربر خاطی را در اینستاگرام ریپورت کنید.



تأیید دستی پست‌های تگ‌شده

در تنظیمات اولیه اینستاگرام، وقتی کسی شما را در عکسی تگ می‌کند، آن عکس به‌صورت خودکار به پروفایل شما اضافه می‌شود. بهتر است این عکس‌ها را قبل از اضافه‌شدن به پروفایل خود بررسی و تأیید کنید.

حال می‌توانید تنظیمات را بر روی Add Manually قرار دهید و قبل از اضافه‌شدن عکسی به پروفایلتان، آن را تأیید کنید.

استفاده کمتر از هشتگ

زمانی که هشتگ‌ها را به یک پست عمومی اینستاگرام اضافه می‌کنید، در صفحه مربوط به آن هشتگ، عکس شما نمایش داده می‌شود. هشتگ برای دیده‌شدن عکس‌ها راهکار فوق‌العاده‌ای است؛ ولی اگر تمایل ندارید که عکس‌ها و فیلم‌هایتان را غریبه‌ها ببینند، بهتر است از هشتگ‌های کمتری استفاده کنید.



خصوصی‌سازی پروفایل

در نهایت اگر راهکارهای بالا به اندازه کافی به شما احساس امنیت نمی‌دهد، می‌توانید حساب کاربری خود را خصوصی کنید. پس از خصوصی‌سازی حساب کاربری، فقط دنبال‌کنندگان شما قادر به دیدن پست‌هایتان خواهند بود. اگر کاربر جدید قصد دنبال کردن مطالب شما را داشته باشد، ابتدا باید برای شما درخواستی ارسال کند و سپس با تأیید شما به لیست فالورهایتان اضافه شود. شما فقط از طریق نرم افزار رسمی اینستاگرام می‌توانید حساب کاربری خود را خصوصی‌سازی کنید.



پیام‌رسان تلگرام



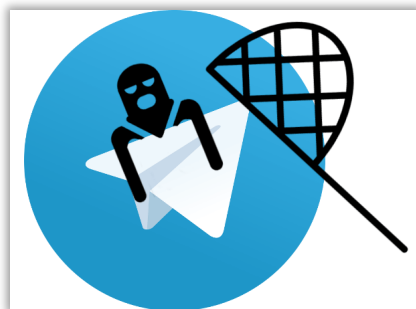
تلگرام نیز همچون اینستاگرام به دلایل مختلف در کشور ما بسیار محبوب شده است. محبوبیت این پیام‌رسان در ایران به حدی است که بیشتر تعداد کاربران تلگرام متعلق به ایران‌اند و امروزه عملاً این نرم‌افزار اولین انتخاب ایرانیان برای پیام‌رسانی است. از همین‌رو، بهتر است همه ما هنگام استفاده از این پیام‌رسان به حریم خصوصی خود بسیار دقت کنیم و از اطلاعات شخصی مهم خود، مراقبت کنیم. با وجود ادعای سازندگان تلگرام مبنی بر امنیت و رمزگذاری کامل اطلاعات، داشتن آگاهی از روش‌های افزایش میزان امنیت در هنگام استفاده از آن، ضروری است. دانستن تمام امکانات امنیتی و روش‌های حریم خصوصی مسئله‌ای است که نه تنها در این ابزار، بلکه در هر ابزار دیگری امری مهم است. بنابراین، در این بخش نیز به بررسی چند نکته برای افزایش امنیت این پیام‌رسان در حفظ حریم خصوصی خواهیم پرداخت.

ریپورت اسپم کردن کاربران

تعداد زیاد کاربران تلگرام در ایران، باعث شده که مزاحمت‌هایی نیز برای آنان پیش بیاید. برای مثال، اگر کسی شماره تلفن یا شناسه تلگرام شما را داشته باشد، به راحتی می‌تواند مزاحمتان شود. اما تلگرام هم برای جلوگیری از این‌گونه مزاحمت‌ها تدابیری

تهدیدات حریم خصوصی کاربران شبکه‌های اجتماعی

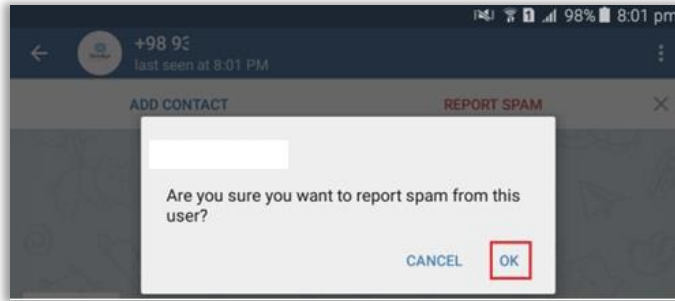
اندیشیده است. همان‌طور که قبلاً اشاره شد، می‌توانید کاربر مزاحم را ریپورت‌اسپم (ارسال گزارش مزاحمت به تلگرام) کنید. با انجام دادن ریپورت، گزارش فرد مزاحم به تلگرام ارسال می‌شود و کاربر ریپورت‌شده، تا مدت‌زمان معینی، نمی‌تواند به افراد ناشناس (کسانی که شماره‌اش را ندارند) پیام ارسال کند.



هنگامی که یک کاربر در تلگرام به شما پیام می‌دهد، در صورتی که شماره آن شخص را نداشته باشید، در بالای صفحه، دو گزینه با نام‌های ADD CONTACT و REPORT SPAM ظاهر می‌شود. برای ریپورت‌اسپم کردن آن شخص، بر روی گزینه REPORT SPAM ضربه بزنید.



سپس یک پنجره پاپ‌آپ با عنوان «آیا شما برای ریپورت‌اسپم کردن این کاربر مطمئن هستید؟» برایتان باز می‌شود. در صورت تأیید بر روی گزینه OK ضربه بزنید.



اکنون کار تمام است و کاربر مزاحم ریپورت شده است. کاربران ریپورت شده نمی‌توانند به کاربرانی که شماره آن‌ها را در لیست خود ندارند، پیام ارسال کنند و هنگامی که برای افراد ناشناس پیام ارسال کنند، با علامت قرمز رنگی در کنار پیام مواجه می‌شود. همچنین پیغامی برایشان ظاهر می‌شود که به آنان نشان می‌دهد ریپورت شده‌اند:

Sorry, you can only send messages to mutual contacts at the moment

متأسفیم. شما در حال حاضر قادر هستید تا تنها به مخاطبان متقابل خود پیام ارسال کنید.

در صورتی که کاربر مزاحم از طرف چند نفر ریپورت شود، تلگرام برای آن کاربر محدودیت‌هایی در زمینه اضافه شدن به گروه‌ها، برقراری تماس و... قائل می‌شود.

مسدود کردن کاربران

با استفاده از این امکان، کاربر می‌تواند افرادی را که برایش ایجاد مزاحمت می‌کنند یا شماره تماس‌های ناشناسی را که با ارسال تبلیغات ناخواسته و هرزنامه‌ها موجب اتلاف زمان و انرژی‌اش می‌شوند، انتخاب کند و نگذارد آن‌ها او را ببینند.

برای این کار کافی است روی اسم پروفایل کاربر موردنظر کلیک کنید (با انگشت ضربه بزنید) و بعد در بالاترین بخش سمت راست روی علامت سه‌نقطه عمودی ضربه بزنید. برای بلاک کردن کاربر، روی گزینه Block User ضربه بزنید. به این ترتیب، دسترسی کاربر مزاحم مسدود می‌شود. اگر پشیمان شدید، می‌توانید به بخش Block Users در بخش Setting و زیربخش privacy and policy وارد شوید. در آنجا لیست افرادی را که بلاک کرده‌اید، می‌توانید ببینید. اگر می‌خواهید کسی را از بلاک خارج کنید، دوباره روی اسمش کلیک کنید. روی علامت سه‌نقطه عمودی بروید و این بار گزینه Unblock را انتخاب کنید.



گفتنی است اگر حساب تلگرامتان را پاک کنید و دوباره بسازید، کسانی که شماره‌تان را در گوشی خود داشته‌اند و شما بلاکشان کرده بوده‌اید، از بلاک بودن خارج می‌شوند و می‌توانند دوباره با شما ارتباط بگیرند.

نمایش ندادن فعالیت‌ها

تلگرام به‌طور پیش‌فرض این امکان را می‌دهد که دیگران بتوانند فعال بودن یا نبودن کاربر را رصد کنند و وضعیت برخط بودن حساب کاربری فرد را مشاهده کنند. با استفاده از

امکان «مشاهده وضعیت فعالیت» می‌توان مشاهده وضعیت فعالیت کاربر، توسط دیگران را محدود کرد.

امکان افزودن به گروه‌ها

به‌طور پیش‌فرض، تنظیمات تلگرام به‌صورتی است که دیگران در صورت دسترسی به شماره تماس و مشخصات کاربر، می‌توانند او را به هر گروه تشکیل‌شده در فضای تلگرام، بیفزایند. این امر ممکن است مسائل و مشکلاتی را برای کاربران به وجود آورد و موجب ایجاد مزاحمت برای آنان شود. کاربر می‌تواند این وضعیت را محدود کند و اجازه ندهد به گروه‌هایی که افراد ناشناس ساخته‌اند، اضافه‌اش کنند. در شکل زیر صفحه تنظیمات مربوطه نشان داده شده است که در آن گزینه Everybody (حالت پیش‌فرض) امکان افزودن فرد به گروه‌ها را به همگان می‌دهد.

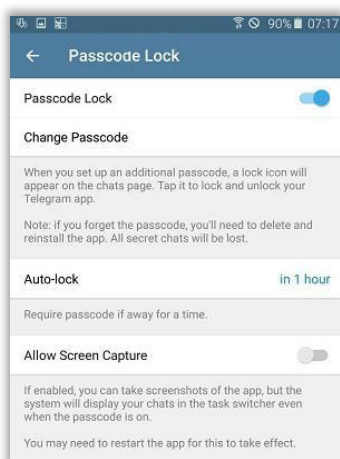
با انتخاب گزینه My Contacts فقط کسانی که در دفترچه تلفن کاربر هستند، این امکان را دارند. همچنین مشابه تنظیمات مربوط به مشاهده وضعیت فعالیت، با استفاده از افزودن استثنای در قسمت Add Exceptions، امکان اضافه‌شدن به گروه‌ها را می‌توان محدودتر کرد. با انتخاب Add Users در مقابل گزینه Always Allow می‌توان به افراد خاصی امکان افزودن کاربر به گروه‌ها را داد. در مقابل، گزینه Never Allow این امکان را می‌دهد که قابلیت اضافه‌کردن کاربر در گروه‌های مختلف را، از برخی افراد موجود در لیست تماس سلب کنیم.

تهدیدات حریم خصوصی کاربران شبکه‌های اجتماعی



رمز ورودی نرم‌افزار

با استفاده از این امکان، می‌توانید رمزی برای تلگرام فعال کنید تا میزان امنیت دسترسی به پیام‌ها را افزایش دهید:

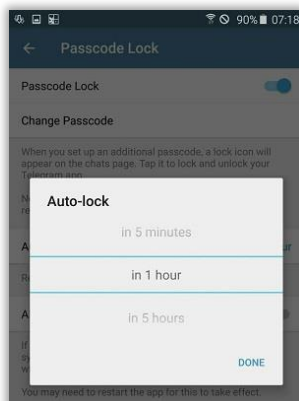


با انتخاب گزینهٔ Passcode Lock می‌توانید رمز ورود به تلگرام را مطابق عکس زیر که یک عدد چهاررقمی است، تعیین و تأیید کنید. با اضافه کردن رمز، علامت قفل در صفحهٔ

اصلی برنامه ظاهر می‌شود که نشان‌دهنده فعال بودن رمز ورودی است. در صورت نیاز به تغییر رمز ایجادشده می‌توانید از گزینه Change Passcode استفاده کنید.



همچنین در بخش Auto-Lock می‌توانید کاری کنید که نرم‌افزار به‌طور خودکار قفل شود. در شکل زیر تنظیمات این بخش را می‌بینید که در آن، زمان پیش‌فرض فعال شدن قفل، یک ساعت است؛ اما می‌توانید این زمان را تا پنج دقیقه هم کاهش دهید. با انتخاب Done فرایند تکمیل می‌شود.



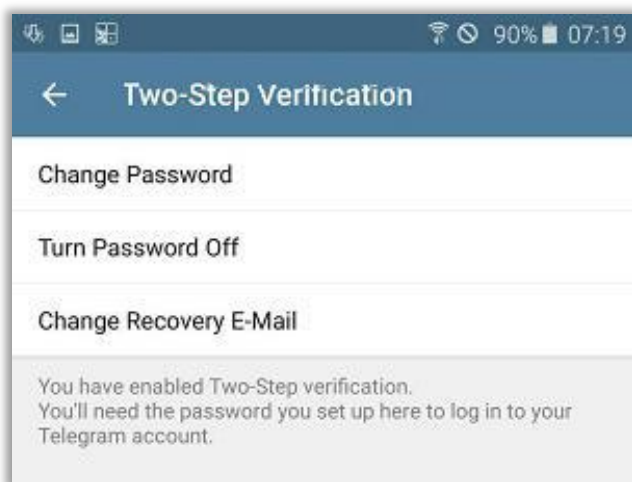
تأیید دومرحله‌ای

فعال‌سازی تلگرام در یک دستگاه دیگر نظیر تبلت یا رایانه شخصی، به این صورت است که کاربر شماره تماس خود را در دستگاه جدید وارد می‌کند و سرور تلگرام کدی چهار رقمی را برایش پیامک می‌کند. سپس کاربر باید کد پیامک‌شده را در دستگاه جدید وارد کند. به این ترتیب، نرم‌افزار در سیستم جدید فعال می‌شود.



با استفاده از این تنظیمات، می‌توانید ورود به حساب کاربری خود را امن‌تر کنید؛ یعنی علاوه بر وارد کردن کد ارسالی، رمز عبور نیز وارد کنید. با وارد شدن به بخش Two-Step

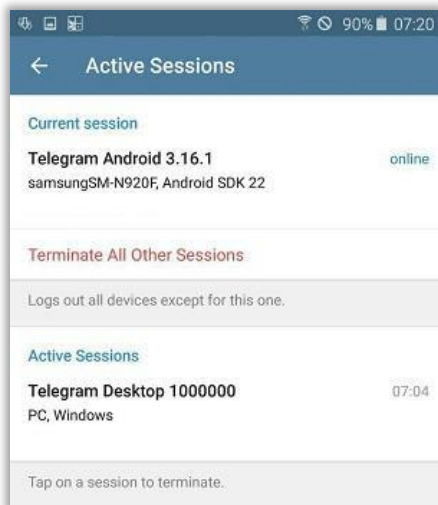
Verification و انتخاب گزینه Set Additional Password می‌توان رمز موردنیاز برای تأیید دومرحله‌ای را تنظیم کرد.



نمایش دستگاه‌های فعال بر روی نرم‌افزار

در بخش Active Sessions می‌توانید همه دستگاه‌هایی را که با حساب شما وارد شده‌اند، مشاهده کنید و در صورتی که با اطلاعات خودتان مطابقت نداشت، دسترسی دستگاه را حذف کنید.

با استفاده از گزینه Terminate All Other Sessions می‌توانید تمام دستگاه‌های دیگری را که از حساب کاربری‌تان استفاده می‌کنند، یکجا حذف کنید. اگر با دستگاه‌های عمومی و ناامن وارد تلگرام شده باشید، ممکن است به حساب کاربری‌تان دسترسی پیدا کنند.



گفت‌وگوی محرمانه

یکی از قابلیت‌های تلگرام، گفت‌وگوی محرمانه است. این گفت‌وگو برای محافظت از حریم خصوصی و امنیت کاربران است.



ویژگی‌های این گفت‌وگو به این شرح است:

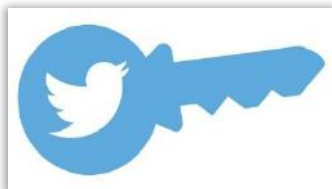
۱. گفت‌وگوها در هیچ‌جا ثبت نمی‌شود.
 ۲. کاملاً رمزگذاری می‌شود؛ به این معنا که پیام‌های ارسالی از ابتدای مسیر تا رسیدن به مقصد، رمزگذاری شده است.
 ۳. در دستگاه‌های دیگری که در آن‌ها از حساب تلگرامتان استفاده می‌کنید، پیام‌ها مشاهده نمی‌شود؛ یعنی مثلاً اگر تلگرام بر روی کامپیوترتان هم فعال باشد و با کسی Secret Chat کند، این چت در کامپیوتر قابل مشاهده نخواهد بود. اگر شک دارید که ممکن است کسی از کامپیوترتان پیام‌هایتان را بخواند، می‌توانید از این گزینه استفاده کنید.
 ۴. گفت‌وگوها بعد از مدتی معین حذف می‌شود.
 ۵. گفت‌وگوهای انجام‌شده دو طرف را به هیچ‌وجه نمی‌توان برای گروه‌ها یا افراد دیگر فرستاد.
- برای گفت‌وگوی محرمانه با یکی از افراد موجود در لیست مخاطبان، ابتدا نام وی را پیدا کنید. سپس قسمت بالای صفحه را که نام مخاطب یا شماره او همراه با تصویر نمایه‌اش قرار دارد، انتخاب کنید.
- بعد از انتخاب، مشخصات مخاطب را مشاهده می‌کنید. در این صفحه با انتخاب گزینه Start Secret Chat یک گفت‌وگوی محرمانه میان شما و مخاطب مدنظر ایجاد می‌شود. حالا در گفت‌وگوی ایجادشده، با کلیک روی نام یا شماره مخاطب، امکانات مرتبط با گفت‌وگوی محرمانه را مشاهده خواهید کرد:



شبکه اجتماعی توییتر

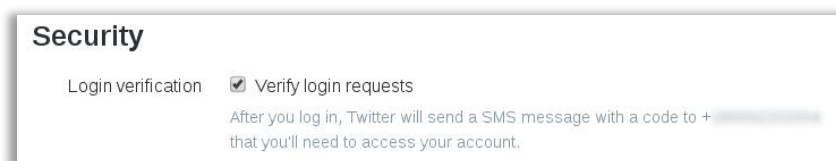


این روزها عضویت در شبکه اجتماعی توییتر، بیشتر از همیشه مورد توجه کاربران ایرانی قرار گرفته است. از این رو، دانستن نکات امنیتی پایه و برخی از تنظیمات برای ایمن‌سازی حساب‌های کاربری و حفظ حریم خصوصی از مهم‌ترین نکاتی است که کاربران پیش از شروع فعالیت جدی در این شبکه اجتماعی، باید آن‌ها را بدانند و رعایت کنند.



فعال‌سازی تأیید هویت دومرحله‌ای

فعال‌سازی تأیید هویت دومرحله‌ای به شما این امکان را می‌دهد که به همراه رمز ورود، هر بار از یک کد امنیتی جداگانه که به شماره موبایل‌تان پیامک می‌شود، استفاده کنید.



برای فعال‌سازی تأیید هویت دومرحله‌ای، از مسیر Settings > Account > Security بخش Login verification گزینه Verify login requests را در کامپیوتر انتخاب کنید. در موبایل نیز از مسیر Settings > Account > Security > Login verification گزینه Login verification را فعال کنید. دقت کنید که اگر تابه‌حال برای حساب کاربری تان از شماره‌تلفن استفاده نکرده‌اید، تویتر برای فعال‌سازی این قابلیت، از شما می‌خواهد تا در بخش تنظیمات مربوط به Mobile این کار را انجام دهید.

فعال‌سازی گزینه حفاظت از بازیابی رمز ورود

تویتر برای جلوگیری از هرگونه سوءاستفاده احتمالی از قابلیت بازیابی رمز عبور، تنظیماتی را در نظر گرفته است که با فعال‌سازی آن، موقع درخواست برای بازیابی حساب

تهدیدات حریم خصوصی کاربران شبکه‌های اجتماعی

کاربری، اطلاعات بیشتری (مانند ایمیل و شماره‌تلفن) از کاربر پرسیده می‌شود. این قابلیت باعث می‌شود برخی از تهدیدات متداول افراد سودجو و هکرها خنثی شود.

Password reset ☒ Require personal information to reset my password
When you check this box, you will be required to verify additional information before you can request a password reset with just your @username. If you have a phone number on your account, you may be asked to verify that phone number before you can request a password reset with just your email address.

برای فعال‌سازی این قابلیت از مسیر Settings > Account از زیرمجموعه security بخش Password reset گزینه Require personal information to reset my password را در کامپیوتر فعال کنید. نکته قابل توجه این است که برای فعال‌سازی این قابلیت حتماً باید از طریق مرورگر کامپیوتر اقدام کنید.

غیرفعال کردن موقعیت جغرافیایی

به‌صورت پیش‌فرض، تویتر این امکان را به کاربر می‌دهد که به‌همراه هر توییت، موقعیت جغرافیایی خود را نیز اعلام کند. اما از آنجاکه موقعیت جغرافیایی بعضی از کاربرها، به‌ویژه کاربران ایرانی، ممکن است جزء اطلاعات حساس آن‌ها محسوب شود، غیرفعال کردن کلی آن برای جلوگیری از هرگونه خطای کاربری و لورفتن موقعیت مکانی توصیه می‌شود.

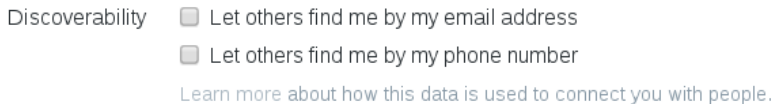
Tweet location ☐ Add a location to my Tweets
When you tweet with a location, Twitter stores that location. You can switch location on/off before each Tweet. [Learn more](#)
Delete location information

برای این کار، از مسیر **Setting > Privacy and safety** از زیرمجموعه Privacy به بخش **Tweet Location** بروید و گزینه **Add a location to my Tweets** را غیرفعال کنید.

غیرفعال کردن قابلیت شناسایی

یکی دیگر از قابلیت‌های توییتر، امکان شناسایی دوستان و آشنایان در این شبکه اجتماعی است. این قابلیت به افراد اجازه می‌دهد از طریق ایمیل و شماره‌تلفن، تنظیمات شناسایی را فعال کنند. افراد می‌توانند دوستان و آشنایان خود را از حضور در توییتر مطلع سازند و همچنین از طریق ایمیل و شماره‌تلفن، قابل جست‌وجو باشند.

اما این موضوع نیز برای بسیاری از کاربران ایرانی که تمایل دارند به‌صورت ناشناس در این شبکه اجتماعی فعالیت کنند، ممکن است دردسرساز شود. بنابراین، توصیه می‌شود این قابلیت را نیز غیرفعال کنید.



برای غیرفعال‌سازی این ویژگی از مسیر **Settings > Privacy and safety** از زیرمجموعه Privacy بخش **Discoverability**، گزینه‌های **Let others find me by my email address** و **Let others find me by my phone number** را غیرفعال کنید.

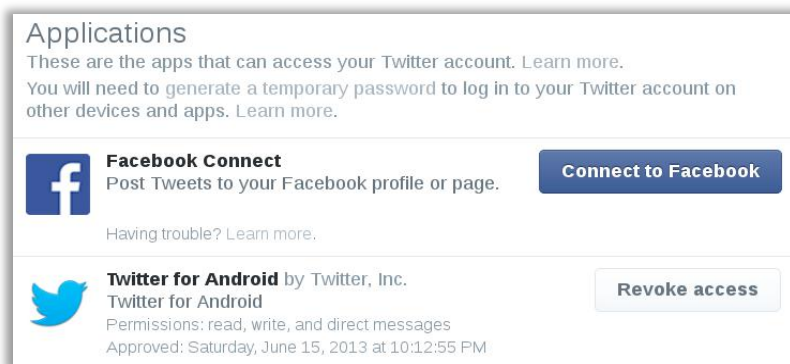
بررسی برنامه متصل به حساب کاربری

توییتر به‌عنوان یکی از شبکه‌های اجتماعی معتبر و شناخته‌شده این امکان را به کاربران خود می‌دهد که از طریق حساب کاربری توییتر در دیگر وب‌سایت‌ها ثبت‌نام کنند.

تهدیدات حریم خصوصی کاربران شبکه‌های اجتماعی

همچنین برای فعال‌سازی و استفاده از بسیاری از سرویس‌ها و برنامه‌های مرتبط با توییتر لازم است کاربران، به حساب کاربری توییتر متصل شوند.

این موضوع در عین کارایی‌هایی که دارد، در مواقعی ممکن است برای کاربرها مشکل‌ساز شود؛ به‌ویژه زمانی که کاربر دسترسی‌های مختلف حساب توییتر خود را به وب‌سایت و برنامه‌های ناشناس می‌دهد. به این ترتیب، هرگونه سوءاستفاده‌ای به راحتی امکان‌پذیر خواهد بود؛ مثلاً ارسال توییت‌های ناخواسته در زمان‌های مختلف، ارسال پیام‌های گوناگون و گروهی به دیگران که در مواردی با لینک‌های آلوده یا محتوای غیراخلاقی همراه است.



بنابراین، برای جلوگیری از بروز هرگونه مشکل، دسترسی‌های برنامه‌های متصل به حساب کاربری‌تان را از مسیر Settings > Apps بررسی کنید و دسترسی موارد ناشناس یا برنامه‌های قدیمی را که از آن‌ها استفاده نمی‌کنید، با کلیک روی Revoke access قطع کنید.

بررسی آخرین دسترسی‌ها

توییت‌ها با ثبت و ذخیره سوابق ورود و اتصال به حساب، امکان بررسی زمان و مکان آخرین دسترسی‌ها را به حساب کاربری، فراهم کرده است. بررسی آخرین سوابق، توجه به زمان دسترسی، مکان و IPها، می‌تواند در دوره‌های زمانی مختلف، شما را از دسترسی دیگران به حساب کاربری تان، مطلع سازد. برای مشاهده این بخش در کامپیوتر، از مسیر **Settings > Your Twitter data** اقدام کنید.

Login history		
If you see any suspicious activity from an app, go to the Apps tab to revoke its access. In some cases the IP location may differ from your physical location. Learn more		
APP	DATE & TIME	IP LOCATION
RapidMiner	Jan 30, 2017 2:09 PM	United States
Twitter.com	Jan 30, 2017 2:01 PM	United States
Twitter for Android	Jan 30, 2017 1:59 PM	United States

فراموش نکنید در صورت مشاهده موارد مشکوک در لیست سوابق ورود (Login history)، رمز ورود خود را بلافاصله تغییر دهید. همچنین دسترسی برنامه‌های ناشناس را قطع کنید. این کارها می‌تواند مانع از دست‌رفتن کنترل کامل حساب کاربری شما شود.

بلاک کردن کاربران در توییت‌ها

مسدود کردن یا بلاک کردن کاربران در توییت‌ها، به دو روش به شکل زیر اجرا می‌شود:

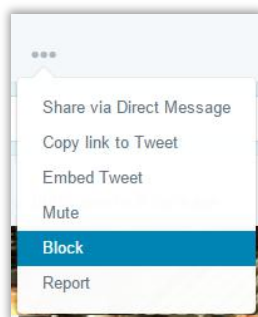
- مسدود کردن از طریق Tweet:

تهدیدات حریم خصوصی کاربران شبکه‌های اجتماعی



روی آیکن  در بالای صفحه کلیک کنید. روی گزینه Block کلیک کنید و سپس برای تأیید بازهم گزینه Block را انتخاب کنید.

- مسدود کردن از طریق نمایه:



به صفحه نمایه حساب موردنظر بروید. روی علامت سه‌نقطه کلیک کنید. گزینه Block را از منو، انتخاب و تأیید کنید.

ریپورت کاربران در توییتر



نمایه‌ای را که می‌خواهید گزارش دهید، باز کنید. بر روی علامت سه‌نقطه عمودی یا چرخ دنده (در بستر وب یا اندروید) کلیک کنید. ابتدا Report و سپس نوع موردی را که می‌خواهید گزارش دهید، انتخاب کنید.

اگر گزینه «سوءاستفاده» یا «مضر» را انتخاب کنید، از شما می‌خواهد که اطلاعات بیشتری درباره مسئله‌ای که گزارش می‌کنید، بدهید. همچنین ممکن است از شما بخواهد توییت اضافی را از حساب کاربری که گزارش می‌دهید، انتخاب کنید. بنابراین، زمینه بهتری برای ارزیابی گزارش شما وجود دارد.



Report Tweet

☒ **Spam**
This Tweet may be spam or from a spam account.

☐ **Compromised**
This user may not be in control of their account.

☐ **Abusive**
This Tweet may be in violation of the [Twitter Rules](#). In order to file a report you must still choose and complete a form. Select this option to continue.

☐ **Block and unfollow @megapenguinx**
Blocking will hide @megapenguinx's Tweets. Learn more about what [blocking](#) means.

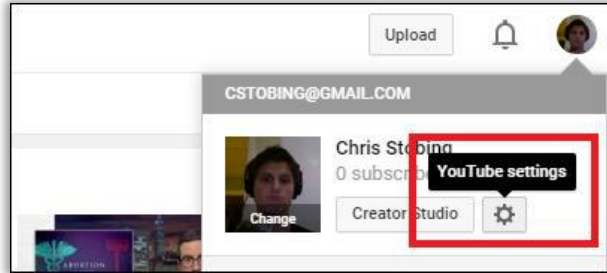
Submit

سایت اشتراک گذاری ویدئوی یوتیوب

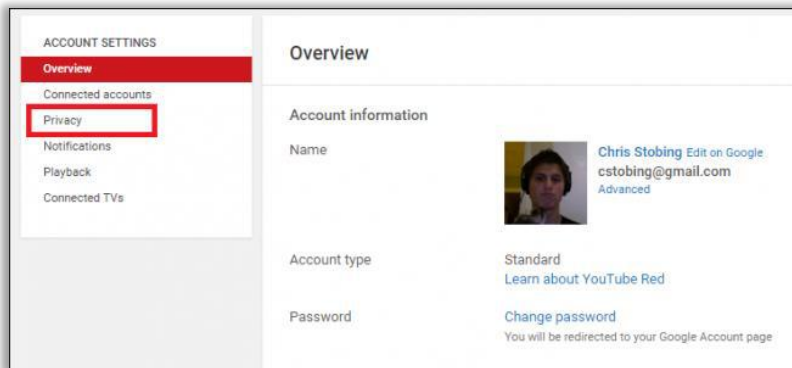


بعد از اینکه شرکت گوگل، سایت یوتیوب را خریداری کرد، حساب یوتیوب کاربران، به حساب جی‌میل آنها متصل شد. اگر کاربران روی حساب جی‌میل خود، نام و نام خانوادگی اصلیشان را تنظیم کرده باشند، حساب یوتیوبشان نیز نام اصلی آنها را نشان می‌دهد. به این ترتیب، مشخص می‌شود چه کسی در چه کانالی عضو شده یا چه ویدئوهایی را پسندیده است. خوشبختانه می‌توان با تنظیماتی از حریم شخصی خود در یوتیوب محافظت کرد.

برای این منظور، وارد صفحه اول یوتیوب شوید. سپس مانند شکل زیر، روی آیکن مشخص شده کلیک کنید تا وارد صفحه تنظیمات شوید.



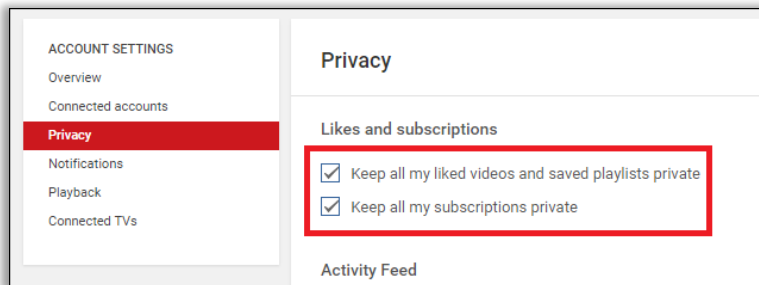
از منوی سمت چپ روی Privacy کلیک کنید.



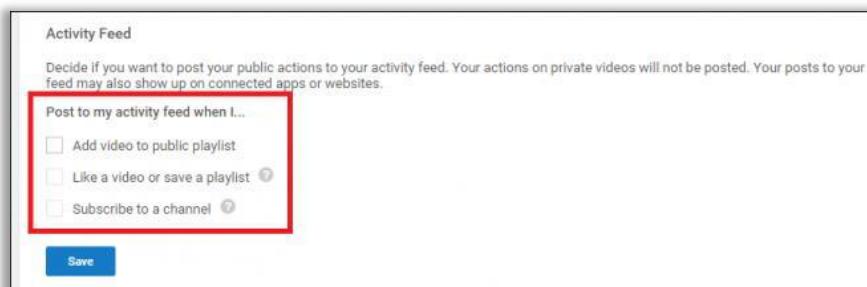
در این قسمت می‌توانید مشخص کنید چه اطلاعاتی از شما به‌صورت عمومی قابل‌رؤیت باشد.

برای اینکه لیست ویدئوهایی که شما لایک کرده‌اید و کانال‌هایی که عضوشان شده‌اید، از دید عموم مخفی بماند، مطمئن شوید که چک‌باکس‌های زیر را تیک زده‌اید.

تهدیدات حریم خصوصی کاربران شبکه‌های اجتماعی



برای مشخص کردن اینکه در بخش Activity Feed چه چیزی نشان داده شود هم گزینه‌هایی وجود دارد. Activity Feed فعالیت‌هایی از قبیل آپلود کردن ویدئوی عمومی و همچنین عضویت در کانال‌ها را شامل می‌شود.

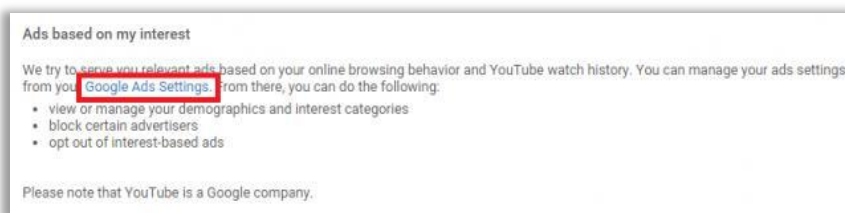


همان‌طور که می‌بینید، برخلاف قسمت قبل، اگر می‌خواهید فعالیت‌های خود را مخفی نگاه دارید، نباید هیچ‌کدام را تیک بزنید.

در پایین همین صفحه در بخش Ads based on my interest، تنظیمات Google's Ad Settings وجود دارد. این قسمت اطلاعات شما را به‌صورت عمومی نشان نمی‌دهد؛ اما در عوض مشخص می‌کند که گوگل بخشی از اطلاعات شما را ثبت می‌کند (مانند

علاقه‌مندی‌ها). گوگل از این اطلاعات برای شخصی‌سازی تبلیغات برای شما، استفاده می‌کند.

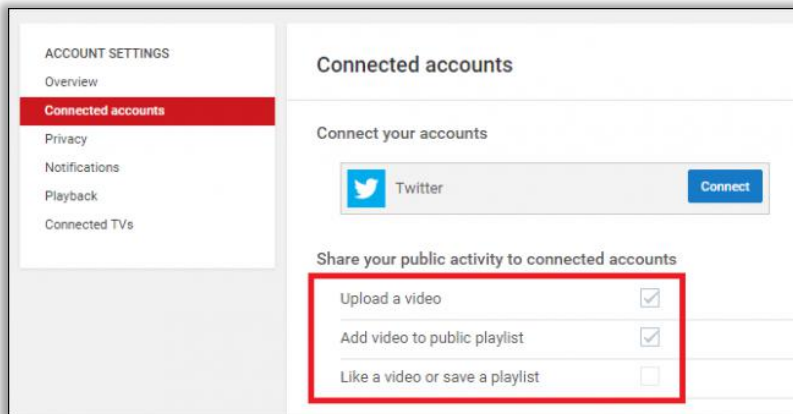
برای به‌روز کردن تنظیمات این قسمت روی لینک مشخص‌شده کلیک کنید.



برای اینکه این اطلاعاتتان ثبت نشود، در قسمت Ads Personalization می‌توانید نشانگر را روی off قرار دهید.

برای تنظیمات حساب‌های وصل‌شده به یوتیوب وارد بخش Connected Accounts شوید. از همان منویی که Privacy را انتخاب کرده بودید، گزینه Connected Accounts را انتخاب کنید.

در این قسمت می‌توانید حساب توئیترتان را به حساب یوتیوبتان وصل کنید و مشخص کنید چه فعالیت‌هایی در حساب توئیترتان منتشر شود. اگر حسابی را اضافه نکرده باشید، این قسمت غیرفعال خواهد بود.



شبکه اجتماعی واتس‌آپ



واتس‌آپ حاصل تلاش Brian Acton و Jan Koum، دو کارمند سابق شرکت یاهو، است. این شرکت ثروتمند را بیشتر از یک سال پیش فیس‌بوک با قیمت نجومی ۱۶ میلیارد دلار خرید. برنامه واتس‌آپ با وجود ده‌ها برنامه چت دیگر، همچنان از محبوب‌ترین برنامه‌های چت در جهان محسوب می‌شود و در اکثر گوشی‌های هوشمند از آن استفاده می‌کنند. این شرکت سال گذشته اعلام کرد که تعداد مشتریان این سرویس از مرز ۵۰۰ میلیون گذشته است. در حال حاضر برآورد می‌شود تعداد مشتریان واتس‌آپ بیش از یک میلیارد نفر باشد.

واتس‌آپ پس از واگذاری به فیس‌بوک دچار تحولاتی شد؛ مثلاً امکان دسترسی به آن از طریق وب فراهم شد و پس از مدتی وقتی فیس‌بوک احساس کرد دارد از سرویس‌های مشابه عقب می‌ماند، امکان تماس از طریق واتس‌آپ را نیز فعال کرد. این برنامه به‌طور چشمگیری ساده و آسان طراحی شده و هرکس به راحتی می‌تواند از آن استفاده کند.

باین همه، در عین سادگی، راهکارهایی امنیتی و قابلیت‌هایی کاربردی دارد. در ادامه برخی از ویژگی‌های امنیتی و کاربردهای این برنامه را ذکر می‌کنیم.



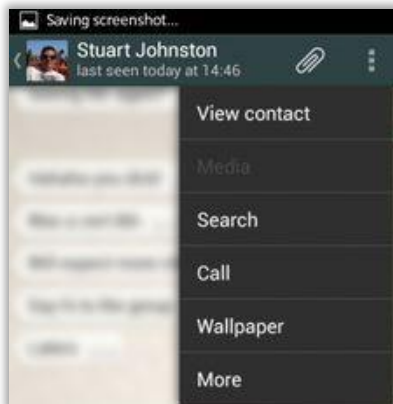
مسدود کردن افراد مزاحم

این نرم‌افزار در کنار سودمندی‌هایش، دردسرهایی دارد. یکی از این دردسرها این است که افرادی که قصد اذیت دارند، به راحتی می‌توانند با شما تماس بگیرند. در ادامه، روش بلاک کردن این افراد در واتس‌آپ در گوشی‌های اندروید را آموزش می‌دهیم.

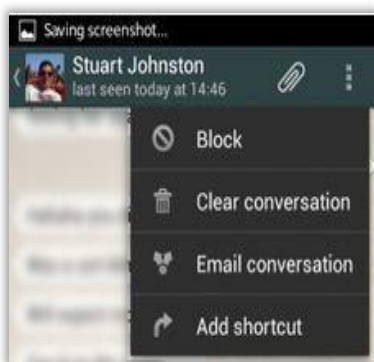
۱. نرم‌افزار واتس‌آپ را باز کنید و فردی را که می‌خواهید بلاک کنید، انتخاب کنید.

۲. در این مرحله باید روی علامت سه نقطه عمودی در گوشه بالای سمت راست صفحه کلیک کنید و گزینه More را انتخاب کنید.

تهدیدات حریم خصوصی کاربران شبکه‌های اجتماعی



۳. سپس روی Block کلیک کنید و OK را بزنید.



بعد از این مراحل، فرد مزاحم در واتس‌آپ بلاک شده است. برای خارج کردن فرد از حالت بلاک، کافی است این مراحل را برعکس انجام دهید.

غیرفعال کردن حالت ذخیره خودکار فایل‌های مدیا

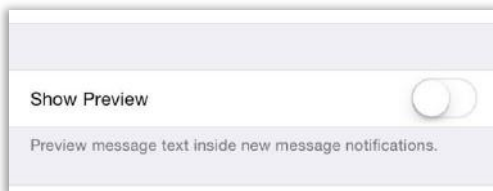
پیام‌رسان واتس‌آپ به‌طور خودکار تمام عکس‌ها و ویدئوهایی را که دریافت می‌کنید، در گوشی‌تان ذخیره می‌کند. معمولاً همه دوست‌دارند عکس‌ها و ویدئوها را در داخل خود برنامه ببینند و کسی علاقه ندارد حافظه گوشی‌اش به‌سرعت پر شود و سرعت گوشی افت کند. اگر عضو گروهی شده باشید که روزانه صدها فیلم و عکس در آن منتشر می‌شود، در مدت کمی حافظه گوشی پر خواهد شد. برای غیرفعال کردن این قابلیت باید ابتدا به منوی تنظیمات برنامه بروید و سپس با وارد شدن به قسمت Chat Settings گزینه Save Incoming Media را غیرفعال کنید.



غیرفعال کردن قابلیت پیش‌نمایش پیام‌ها

فرقی نمی‌کند واتس‌آپ را روی چه نوع سیستم‌عاملی نصب کرده‌اید. این برنامه به‌طور پیش‌فرض پس از نصب، پیام‌های دریافتی را در قالب یک اعلانیه نمایش می‌دهد. خیلی‌ها دوست ندارند دیگران بتوانند حتی اتفاقی این پیش‌نمایش‌ها را بخوانند. برای همین، این قابلیت را غیرفعال می‌کنند.

برای غیرفعال کردن پیش‌نمایش پیام‌های دریافتی در پیام‌رسان واتس‌آپ، به قسمت تنظیمات برنامه بروید و بعد از ورود به بخش Notifications، گزینه Show Preview را خاموش کنید.



نمایش ندادن موقعیت مکانی

یکی از قابلیت‌های اصلی در پیام‌رسان واتس‌آپ امکان مکان‌یابی کاربران است؛ به این معنا که اعضای این شبکه می‌توانند مکان دیگر اعضا را در زمان حضور در این شبکه مجازی پیدا کنند. به این ترتیب، بسیاری از اعضا بدون اینکه خود اطلاع داشته باشند، تحت تعقیب چشم‌های تجسس‌گری هستند که قصد ورود به حریم خصوصی‌شان را دارند. البته ناگفته نماند که تا خود کاربر گزینه نمایش مکان‌یابی و جی‌پی‌اس دستگاه خود را فعال نکند، این قابلیت فعال نمی‌شود.



هنگام چت کردن با کلیک بر روی آیکون فلش و سپس Share Location، این ویژگی فعال می‌شود؛ اما اگر این مسیر طی نشود، مکان فعلی شما با هیچ‌کس به اشتراک گذاشته نخواهد شد.



نمایش‌ندادن آخرین بازدید

واتس‌آپ به‌طور پیش‌فرض آخرین زمان مراجعه شما به این پیام‌رسان را برای دوستانتان نمایش می‌دهد. برای غیرفعال کردن این قابلیت به منوی تنظیمات برنامه بروید و بعد مسیر **Account > Privacy > Last Seen** را طی کنید. در این قسمت می‌توانید شخصی‌سازی‌های لازم را برای نمایش آخرین بازدیدتان انجام دهید یا تعیین کنید که هیچ‌یک از دوستانتان نتوانند آخرین بازدیدتان را ببینند.



پشتیبان‌گیری مداوم

واتس‌آپ به‌طور خودکار از تمام فعالیت‌های شما در سرورهای خود، فایل پشتیبان تهیه می‌کند. برای غیرفعال کردن این قابلیت باید مسیر Settings > Chat Settings > Chat Backup را دنبال و سپس تعیین کنید که فایل پشتیبان خودکار، هر چند وقت یک بار تهیه شوند.

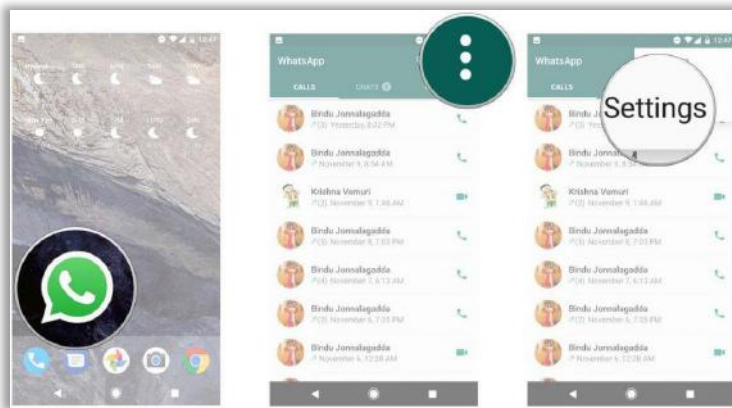


افزایش امنیت واتس‌آپ با استفاده از سیستم ورود دومرحله‌ای

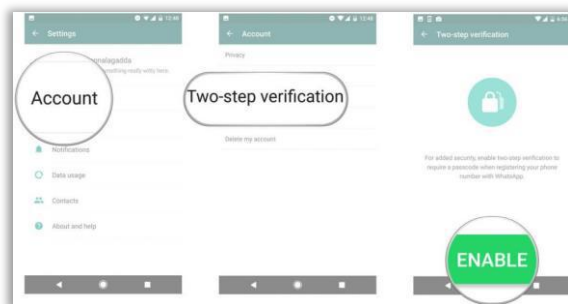
واتس‌آپ برای افزایش امنیت کاربران، فرایندی دومرحله‌ای را برای ورود به حساب کاربری فراهم کرده است. این سیستم امنیتی اختیاری، ورود اشخاص ثالث و کاربران غیرمجاز را به حساب کاربری، بسیار دشوارتر از قبل می‌کند. فعال کردن قابلیت تأیید هویت دومرحله‌ای واتس‌آپ می‌تواند تأثیر بسزایی بر افزایش ضریب امنیت حساب کاربری بگذارد. هنگام استفاده از این ویژگی، کاربران باید علاوه بر شماره‌تلفن و پیغام متنی یا صوتی تأییدی حساب، از یک کد امنیتی شش‌رقمی نیز استفاده کنند. همچنین از آن‌ها خواسته می‌شود که هر هفته کد امنیتی خود را مجدداً وارد کنند. لازم است کاربران یک آدرس ایمیل صحیح در سیستم ثبت کنند تا در صورت فراموشی کد امنیتی، بتوانند با استفاده از آن، ورود دومرحله‌ای را غیرفعال کنند. درغیراین‌صورت، برای ورود به حساب کاربری بدون استفاده از کد امنیتی، باید یک هفته منتظر بمانند و پس از ورود نیز تمام پیغام‌های مشاهده‌نشده آن‌ها حذف می‌شود. فعال کردن تأیید هویت دومرحله‌ای واتس‌آپ

کارچندان پیچیده‌ای نیست. برای این منظور کافی است یک آدرس ایمیل داشته باشید؛ چرا که کد شش‌رقمی تأیید هویت در مرحله دوم به آدرس ایمیلی ارسال می‌شود که ثبت می‌کنید. برای فعال کردن تأیید هویت دومرحله‌ای واتس‌آپ، مراحل زیر را طی کنید:

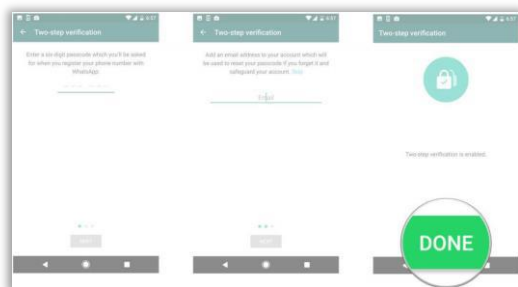
- ابتدا برنامه واتس‌آپ را اجرا کنید.
- آیکن منوی موجود در بخش بالا و سمت راست صفحه را کلیک کنید. این آیکن با علامت سه‌نقطه عمودی نمایش داده می‌شود.
- سپس گزینه Settings را انتخاب کنید.



- حال گزینه Account را کلیک کنید.
- گزینه Two-Step Verification را کلیک کنید. این گزینه مربوط به قابلیت تأیید هویت دومرحله‌ای واتس‌آپ است.
- در مرحله بعد باید گزینه سبز رنگ Enable را کلیک کنید.



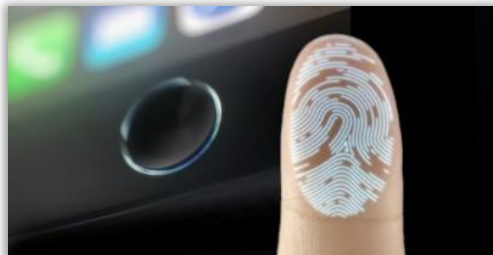
- حال باید یک کد شش‌رقمی دلخواه را وارد نمایید. دقت کنید که این کد را باید به خاطر بسپارید. پس از وارد کردن کد شش‌رقمی، گزینه Next را کلیک کنید. احتمالاً برای تأیید کد شش‌رقمی وارد شده، لازم است یک بار دیگر آن را وارد کنید.
- در مرحله بعد باید آدرس ایمیل مدنظرتان را وارد کنید. دقت کنید که باید برای فعال کردن قابلیت تأیید هویت دومرحله‌ای واتس‌آپ، حتماً به این ایمیل دسترسی داشته باشید. پس از وارد کردن آدرس ایمیل، گزینه Next را کلیک کنید.
- در مرحله آخر با پیام Two-Step Verification is now enabled مواجه می‌شوید. این پیغام از فعال شدن قابلیت تأیید هویت دومرحله‌ای واتس‌آپ خبر می‌دهد. گزینه Done را کلیک کنید.



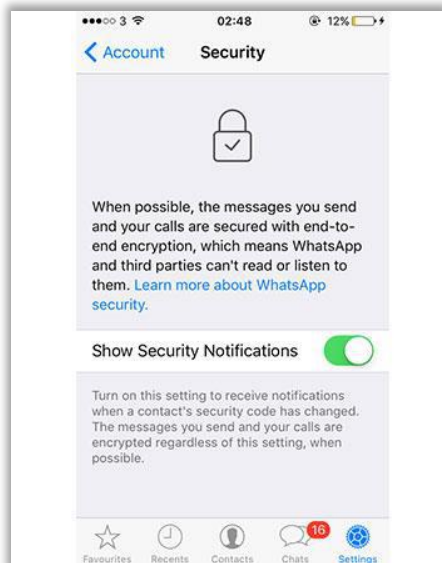
با طی کردن مراحل ساده بالا به راحتی قابلیت تأیید هویت دومرحله‌ای واتس‌آپ فعال می‌شود. اگر بخواهید این قابلیت را غیرفعال کنید، می‌توانید از طریق ایمیل ثبت‌شده خود، این کار را انجام دهید. برنامه واتس‌آپ به صورت دوره‌ای از شما می‌خواهد رمز عبور خود را وارد کنید. به این ترتیب، رمز خود را فراموش نخواهید کرد. با فعال کردن قابلیت تأیید هویت دومرحله‌ای واتس‌آپ، هرکس بخواهد به حساب کاربری تان وارد شود، باید از لایه امنیتی دوم هم عبور کند و از طریق ایمیل هم هویت خود را تأیید نماید. باتوجه به اینکه فقط شما به آدرس ایمیل واردشده، دسترسی دارید، کس دیگری نمی‌تواند به حساب کاربری تان وارد شود و سوءاستفاده‌ای از آن نکند.

فعال‌سازی تأیید کلید

به گفته مهندس رمزگذاری شرکت CloudFlare، در نرم‌افزار واتس‌آپ نکته‌ای مهم برای احراز هویت مخاطب وجود دارد. برای ضمانت رمزنگاری و اینکه کسی در میانه راه پیام‌ها را ن‌دزدد، لازم است که حتماً شخص موردنظرمان امکان رمزگشایی پیام‌ها را داشته باشد؛ اما ضرورت دارد مخاطب نیز ثابت کند همان کسی است که باید باشد.



برای این کار، واتس‌آپ و بقیه ابزارهایی که از امکان رمزنگاری دوطرفه استفاده می‌کنند، امکان بررسی کلیدهای منحصر به فرد خود را به یکدیگر می‌دهند. این کلیدها با نام Key Fingerprint شناخته می‌شوند. این کلیدها در واقع نسخه کوتاه‌شده کلیدهای منحصر به فردی هستند که واتس‌آپ برای شناسایی هویت کاربر ذخیره می‌کند. اما مشکل اینجاست که تنظیمات پیش فرض واتس‌آپ، هنگام تغییر Key Fingerprint مخاطب، آن را به شما اعلام نمی‌کند. اگر کلید عمومی مخاطبی تغییر کند، معانی مختلفی ممکن است داشته باشد. احتمالاً او گوشی جدیدی خریده یا واتس‌آپ را از گوشی‌اش پاک کرده و دوباره نصب کرده است. به هر حال، در صورتی که کلید به واسطه عملکرد کاربر تغییر کرده باشد، ناآگاهی از این تغییر، مشکلی ایجاد نمی‌کند. اما وضع ممکن است بدتر باشد. اگر شما از تغییر کلیدها آگاه نشوید، ممکن است کسی از طریق حمله Man-in-the-middle تلاش کند خود را دوست یا همکار شما جا بزند و به این ترتیب، امکان رمزگشایی پیام‌ها پیش از رسیدن به مخاطب مدنظر برایش ممکن می‌شود.



خوشبختانه در واتس‌آپ امکانی تحت عنوان Security Notification وجود دارد که با فعال کردن آن، در صورتی که کلید کاربری تغییر کند، مسئله به صورت خودکار به اطلاع شما می‌رسد. برای فعال‌سازی این قابلیت، در تنظیمات واتس‌آپ و در بخش Accounts، گزینه Security را انتخاب و گزینه Show Security Notifications را فعال کنید. توجه داشته باشید که بدون فعال کردن این گزینه، در صورت تغییر کلیدهای مخاطبانتان در واتس‌آپ، شما مطلع نمی‌شوید و این مسئله ممکن است امنیت و حریم شخصی شما را، با وجود رمزنگاری دوطرفه، به راحتی به خطر بیندازد (Greenberg, 2016).

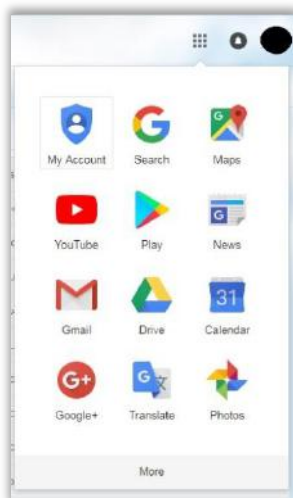
پست الکترونیکی جی‌میل



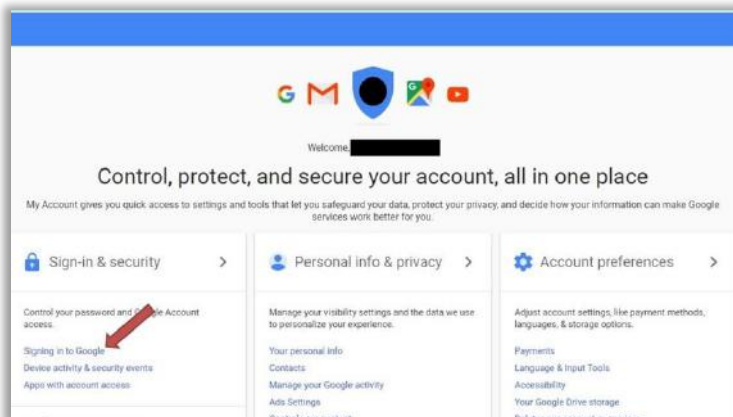
زمانی که ما قصد ثبت‌نام یا استفاده از شبکه‌های اجتماعی یا پیام‌رسان‌ها را داریم، عموماً از ما آدرس ایمیل یا در بیشتر مواقع جی‌میل (Gmail) را می‌خواهند تا

تهدیدات حریم خصوصی کاربران شبکه‌های اجتماعی

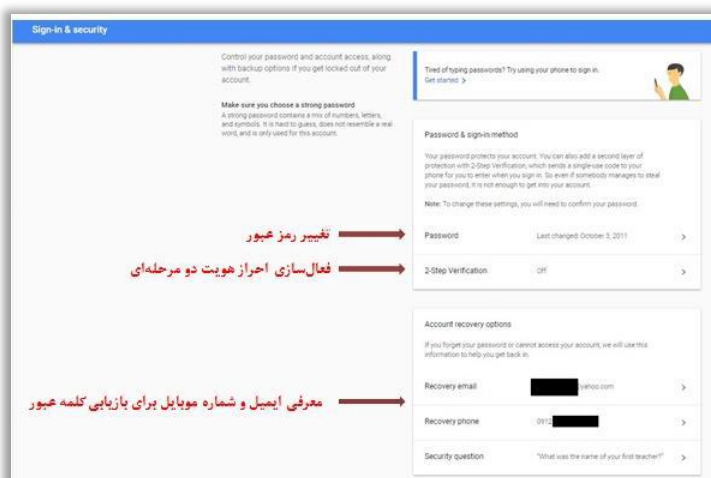
برای احراز هویت از آن استفاده کنند. یا زمانی که رمز عبورمان را گم یا فراموش کرده‌ایم، به کمک آن بتوانیم رمز عبور و درواقع حساب کاربری خود را بازیابی کنیم. با این تفاسیر، امنیت جی‌میل نکته‌ی حائز اهمیت است که بی‌توجهی به آن می‌تواند علاوه بر خود ایمیل، حساب‌های کاربری ما در شبکه‌های اجتماعی یا پیام‌رسان‌ها را نیز مختل کند. جی‌میل هم مانند شبکه‌های اجتماعی از راهکارهای امنیتی متفاوت استفاده می‌کند که استفاده از رمز عبور پیچیده، تغییر دوره‌ای آن، استفاده از شماره‌موبایل برای دریافت کدهای امنیتی و تأیید هویت دومرحله‌ای، از جمله مهم‌ترین و کاربردی‌ترین آن‌هاست. برای فعال‌سازی این روش‌ها یا تغییر رمز عبور و اعلام شماره تماس و آدرس ایمیل پشتیبان، ابتدا باید وارد حساب کاربری جی‌میل خود شوید. داخل صفحه‌ی جی‌میل شما، در بالای صفحه، سمت راست علامتی وجود دارد که به Google apps معروف است. روی آن کلیک کنید تا منویی به شکل زیر برایتان باز شود.



با کلیک بر روی گزینه My Account وارد صفحه‌ی حساب کاربری خود می‌شوید؛ درست به شکل زیر:



در این صفحه روی گزینهٔ signing to google که در شکل با فلش قرمز نشان داده شده، کلیک کنید تا، مطابق شکل زیر، وارد صفحهٔ sign-in & Security حساب کاربری خود شوید.



در این صفحه، همان‌طور که در شکل بالا نشان داده شده، می‌توانید رمز عبورتان را تغییر دهید. سعی کنید در فواصل زمانی معین این کار را انجام دهید؛ خصوصاً اگر در جای

نامطمئنی مانند کافی نت به حساب خود وارد شده‌اید و مطمئن نیستید که آیا از حساب خود خارج شده‌اید یا نه. یکی دیگر از مواقعی که باید بلافاصله رمز عبور خود را تغییر دهید، زمانی است که تلفن همراه، تبلت یا لپ‌تاپتان دزدیده شده است. در این مواقع توصیه اکید می‌شود بلافاصله رمزهای عبور خود را تغییر دهید. همان‌طور که در شکل نشان داده شده، در این صفحه می‌توانید تأیید هویت دومرحله‌ای را نیز فعال کنید. در قسمت پایین هم می‌توانید شماره تلفن و ایمیل پشتیبانی را معرفی کنید تا اگر خواستید کلمه عبور خود را بازیابی کنید، از طریق آن‌ها این کار انجام گیرد. توجه داشته باشید که در این مرحله و برای فعال‌سازی تمام این قابلیت‌ها نیاز به وارد کردن رمز عبور خود دارید.

سخن پایانی



شبکه‌های اجتماعی آنلاین می‌توانند خدمات سودمند و سرگرم‌کننده‌ای به کاربران بدهند و فضایی را مهیا کنند که افراد، بدون محدودیت‌های جغرافیایی، با دوستان و آشنایان ارتباط برقرار کنند و مطالبی را که دوست دارند، با آن‌ها به اشتراک بگذارند. در عین حال، این شبکه‌ها می‌توانند کاربر را در معرض خطر جدی امنیت سایبر قرار دهند. همان‌طور که اشاره شد، اخیراً تعداد کاربران این شبکه‌ها افزایش یافته است. این امر باعث جلب توجه هکرها شده است. درک روشن از مسائل امنیتی در شبکه‌های اجتماعی می‌تواند به کاربر کمک کند تا چگونگی کاهش خطرات امنیتی را بیاموزد.

امروزه دیگر گشت‌وگذار در وب، سفر یک‌نفره و مکاشفه در تنهایی نیست؛ زیرا شبکه‌های اجتماعی، از قبیل فیس‌بوک و تلگرام، به بخش جدایی‌ناپذیری از زندگی آنلاین تبدیل شده‌اند. در کنار آن، هرچا تعداد کاربر زیاد می‌شود، توجه هکرها و افراد سوءاستفاده‌گر هم جلب می‌شود. از این رو، این شبکه‌ها در حال تبدیل شدن به حفره‌های مهم امنیتی‌ای هستند که هر روز کاربران زیادی را در کام خود فرومی‌برند.

همان‌طور که همه‌روزه استفاده از شبکه‌های اجتماعی از قبیل فیس‌بوک، اینستاگرام و تلگرام بیشتر و بیشتر می‌شود، حفظ حریم خصوصی نیز اهمیت بیشتری پیدا می‌کند. عضویت در شبکه‌های اجتماعی همواره برای عده زیادی با نگرانی و اضطراب همراه بوده است و در مواقعی نیز منجر به مشکلاتی شده است. کم نیستند افرادی که از برچسب خوردن عکس‌هایشان توسط دیگران یا دیده شدن عکس‌های خصوصی‌شان توسط دوستانِ نه‌چندان صمیمی شاکی‌اند. در برخی جوامع این مشکل به‌اندازه‌ای زیاد شده که کلماتی مانند Facebook Friend به فرهنگ لغات راه یافته است.



توصیه ما برای کاربران شبکه‌های اجتماعی این است که اطلاعات غیرضروری را حذف کنند و حریم خصوصی و امنیتی خود را به درستی تنظیم کنند. بهتر است که کاربران شبکه‌های اجتماعی مانند فیس‌بوک تنظیمات لازم را انجام دهند و اطلاعات خود را فقط در معرض نمایش

خود و دوستانشان قرار دهند. بهتر است که درخواست دوستی افراد ناشناس را رد کنند. حداقل یکی از نرم‌افزارهای امنیتی تجاری را نصب نمایند. والدین نیز باید همواره بر فعالیت‌های فرزندان خود نظارت داشته باشند.

منابع و مأخذ

- [۱] اقتصاد آنلاین، (۱۳۹۶)، «اسکرین‌شات می‌تواند جرم باشد»، <http://www.eghtesadonline.com/بخش-عمومی-۱۸۸۴۴۴/۳۰-اسکرین-شات-می-تواند-جرم-باشد>
- [۲] فخار، فاطمه (۱۳۹۵)، حفاظت از حریم شخصی در شبکه‌های اجتماعی، تهران: انتشارات ناقوس.
- [۳] بشیر، حسن، رفیعی، الهام، مرادی، علیرضا و افراسیابی، محمدصادق (۱۳۹۲)، مطالعات شبکه‌های اجتماعی و سبک زندگی جوانان، تهران: سیمای شرق.
- [۴] اکبری‌تبار، علی‌اکبر، اسکندری‌پور، ابراهیم (۱۳۹۲)، رسانه‌های اجتماعی و شبکه‌های اجتماعی مجازی. تهران: شبکه ملی فرهنگ.
- [۵] جلالی، مهدی (۱۳۹۵)، آشنایی با شبکه‌های اجتماعی، فرصت‌ها و تهدیدها.
- [۶] سالمی، نجمه، فدایی، غلامرضا و عصاره، فریده (۱۳۹۳)، «به‌کارگیری معیارهای تحلیل شبکه‌های اجتماعی در ارزیابی‌های کتاب‌سنجی»، فصل‌نامه دانش‌شناسی (علوم کتابداری و اطلاع‌رسانی و فناوری اطلاعات)، ۷(۲۵)، ۸۱-۸۸.
- [۷] مهرانفر، آتوسا و مریم رستگارپور (۱۳۹۵)، سیستم‌های پیشنهاددهنده در شبکه‌های اجتماعی، اهواز: انتشارات علوم و فنون پزشکی.
- [۸] شبانین، مؤگان، امنیت اطلاعات در شبکه‌های اجتماعی (۱۳۹۴)، تیم مقاله آی‌تی <http://it-research.ir>

- [۹] کینکوف، گانتر شری، صدیق‌نواز، ندا و خدابنده، هنگامه (۱۳۸۹)، آموزش استفاده از شبکه‌های اجتماعی، ناشر: طاهریان.
- [۱۰] عقیلی سیدوحید و پوری، احسان (پاییز ۱۳۹۰)، «تأثیر شبکه‌های اجتماعی مجازی بر ارتباطات بین‌فردی کاربران»، نشریه فرهنگ ارتباطات، ۱(۳)، ۲۵-۴۲.
- [۱۱] ترک، مولود و باطنی، مهدی (۱۳۹۵)، «افزایش دقت تشخیص پست‌های اسپم در شبکه‌های اجتماعی با استفاده از سیستم ایمنی مصنوعی»، دومین همایش ملی پژوهش‌های مهندسی رایانه، همدان.
- [۱۲] مؤدی، مهدی؛ مهدیه قزوینی؛ محمد علانی و حسین مودی، (۱۳۹۵)، «تشخیص بات‌نت‌های شبکه‌های اجتماعی»، دومین کنفرانس بین‌المللی وب‌پژوهی، تهران: دانشگاه علم و فرهنگ.
- [13] Liu, C. C., Tao, S. Y., & Nee, J. N. (2008). Bridging the Gap between Students and Computers: Supporting Activity Awareness for Network Collaborative Learning with GSM Network. *Behaviour & Information Technology*, 27(2), 127-137.
- [14] Tu, Chih-Hsiung, Michael Blocher, and Joshua Ntoruru. "Integrate Web 2.0 Technology to Facilitate Online Professional Community: EMI Special Editing Experiences." *Educational Media International* 45.4 (2008): 335-341.
- [15] <http://www.internetlvestats.com/>
- [16] <http://familyweb.ir>
- [17] Greenberg, Andy, 2016, "Two Tips to Keep Your Phone's Encrypted Messages Encrypted", <https://www.wired.com/2016/04/tips-for-encrypted-messages/>



فناوران توسعه امن ناجی
Naji Secure Development
Technologist co