

حفظ امنیت دیجیتال هنگام قطع اینترنت

TECH توانا TAWANA

حفظ امنیت دیجیتال
هنگام قطع اینترنت

توانا
TAVAANA
آموزشکده آنلاین
برای جامعه مدنی ایران
e-collaborative
for civic education

توانا‌تک را دنبال کنید!

tech.tavaana.org

@tavaanatech
@/tavaanatech
@Tavaanatech
@TavaanaTech

پشتیبانی سریع در زمینه امنیت دیجیتال

@Tech_admin_b
@tavaanatech
tech@tavaana.org

انواع ابزارهای امن و رایگان عبور از فیلترینگ در بشکن

@beshkan.tt
@beshkan

یک ایمیل خالی به آدرس beshkan@tavaana.org بفرستید تا نسخه به‌روز ابزارهای رایگان و امن و عبور از فیلترینگ برایتان فرستاده شود.

www.tech.tavaana.org

پروژهٔ

e-collaborative
for civic education

www.eciviced.org

حفظ امنیت دیجیتال
هنگام قطع اینترنت

ناشر: E-Collaborative for Civic Education

پاییز ۱۴۰۵

© E-Collaborative for Civic Education 2026

e-collaborative
for civic education

ECCE (E-Collaborative Civic Education) یک سازمان غیرانتفاعی در ایالات متحده آمریکا تحت 501c3 است که از فناوری اطلاعات و ارتباطات برای آموزش و ارتقای سطح شهروندی و زندگی سیاسی دموکراتیک استفاده می‌کند.

ما به عنوان بنیان‌گذاران و مدیران این سازمان اشتیاق عمیق مشترکی داریم که شکل‌دهنده ایده‌های جوامع باز است. همچنین برای ما، شهروند، دانش شهروندی، مسئولیت و وظیفه شهروندی یک فرد در محافظت از جامعه سیاسی دموکراتیک پایه و اساس کار است؛ همان‌طور که حقوق عام بشر که هر شهروندی باید از آن‌ها برخوردار باشد، اساسی و بنیادی هستند. ECCE دموکراسی را تنها نظام سیاسی قادر به تأمین طیف کاملی از آزادی‌های شهروندی و سیاسی برای تک‌تک شهروندان و امنیت، برابری و عدالت می‌داند. ما دموکراسی را مجموعه‌ای از ارزش‌ها، نهادها و فرایندها می‌دانیم که مبشر صلح، توسعه، تحمل و مدارا، تکثرگرایی و جوامعی شایسته‌سالار است که به کرامت انسانی و دستاوردهای انسانی ارج می‌گذارند.

ما پروژه اصلی ECCE یعنی «آموزشکده توانا: آموزشکده مجازی برای جامعه مدنی ایران» را در سال ۲۰۱۰ تاسیس کردیم. آموزشکده توانا در ارائه منابع و آموزش در دنیای مجازی در ایران، یک نهاد پیشرو است. توانا با ارائه دوره‌های آموزشی زنده در حین حفظ امنیت و با ناشناس‌ماندن دانشجویان، به یک جامعه آموزشی قابل اعتماد برای دانشجویان در سراسر کشور تبدیل شده است. این دروس در موضوعاتی متنوع مانند نهادهای دموکراتیک، امنیت دیجیتال، حقوق زنان، وب‌نویسی، جدایی دین و دولت و توانایی‌های رهبری ارائه می‌شوند. آموزشکده توانا آموزش زنده دروس و سمینارهای مجازی را با برنامه‌هایی مثل مطالعات موردی در جنبش‌های اجتماعی و گذارهای دموکراتیک، مصاحبه با کنشگران و روشنفکران، دستورالعمل‌های خودآموز، کتابخانه مطالب توصیفی، ابزارهای کمکی و راهنمایی برای آموزشگران ایرانی و حمایت مداوم و ارائه مشاوره آموزشی برای دانشجویان تکمیل کرده است.

تلاش ما برای توسعه توانایی‌های آموزشکده توانا متوجه گردآوردن بهترین متفکران ایران و صداهای حذف‌شده است. به همین ترتیب، به دنبال انتشار و ارتقای آثار مکتوب روشنفکران ایرانی هستیم که ایده‌های آنان در جمهوری اسلامی ممنوع شده است.

یکی از نقاط تمرکز تلاش توانا، ترجمه متون کلاسیک دموکراسی و مقالات معاصر در این باره و نیز ترجمه آثار مرتبط با جامعه مدنی، حقوق بشر، حاکمیت قانون، روزنامه‌نگاری، کنشگری و فناوری اطلاعات و ارتباطات است. امید ما این است که این متون بتواند سهمی در غنای فردی هم‌وطنان ایرانی و برساختن نهادهای دموکراتیک و جامعه‌ای باز در ایران داشته باشد.

سپاسگزار بازتاب نظرات و پیشنهادهای شما!

فهرست

مقدمه	۷
امنیت دستگاه‌های هوشمند	۹
شبکه‌های اجتماعی در ایران: خطرات احتمالی واقعی	۱۴
چرا ایمیل هنوز اهمیت دارد؟	۲۳
رمزهای عبور: ساده اما حیاتی	۲۵
امنیت وی.پی.ان و انتخاب سرویس مطمئن	۲۷
امنیت دیجیتال در تجمعات و اعتراضات	۳۰
امنیت خانواده و نزدیکان: چک‌لیست اضطراری مشترک	۳۲
مواجهه با بازرسی دستگاه	۳۴
اقدامات و مراقبت‌های امنیتی در زمان قطع اینترنت	۳۶
جمع‌بندی	۴۳
منابع برای مطالعه بیش‌تر	۴۵

مقدمه

دسترسی به اینترنت در ایران همواره پایدار و بدون وقفه نبوده است. قطعی‌های گسترده، محدودیت‌های ناگهانی و نظارت روزافزون دیگر پدیده‌ای استثنایی به شمار نمی‌روند، بلکه بخشی از واقعیت روزمره میلیون‌ها شهروند ایرانی محسوب می‌شوند. در چنین شرایطی، عدم آگاهی از یک اصل ساده امنیتی می‌تواند پیامدهای جدی در پی داشته باشد؛ از جمله از دست رفتن دسترسی به حساب‌های کاربری، در معرض خطر قرار گرفتن مخاطبان فرد، یا استفاده از محتوای گوشی همراه علیه صاحب آن.

این کتابچه با هدف ارتقای امنیت دیجیتال کاربرانی تدوین شده است که بدون نیاز به دانش فنی تخصصی خواستار برقراری حداقل استانداردهای امنیتی در فضای دیجیتال خود هستند. زبان این اثر ساده و توضیحات آن کاربردی است و هر نکته بر اساس تهدیدهایی نگاشته شده که کاربران ایرانی به طور مستمر با آن مواجه‌اند.

این کتابچه هشت موضوع اصلی را در بر می‌گیرد:

- **امنیت تلفن هوشمند**: قفل صفحه، رمزنگاری، به‌روزرسانی سیستم‌عامل، مدیریت اپلیکیشن‌ها و تهیه نسخه پشتیبان.
- **شبکه‌های اجتماعی**: تنظیمات حریم خصوصی در اینستاگرام، تلگرام، واتس‌اپ و ایکس، و خطرات مرتبط با متادیتای عکس.
- **ایمیل**: انتخاب سرویس امن، فعال‌سازی تایید دو مرحله‌ای و مدیریت رمز عبور.

- **وی.پی.ان:** معیارهای انتخاب یک سرویس مطمئن و پرهیز از گزینه‌های رایگان و فاقد شفافیت.
- **امنیت در تجمعات و اعتراضات:** آماده‌سازی پیش، حین و پس از حضور در تجمعات عمومی.
- **امنیت خانواده و نزدیکان:** چک‌لیست هماهنگی مشترک به منظور کاهش ریسک جمعی.
- **مواجهه با بازرسی:** اقدامات لازم پیش، حین و پس از بازرسی احتمالی گوشی همراه.
- **اقدامات و مراقبت‌ها در زمان قطعی اینترنت:** دلایل پرهیز از پیام‌رسان‌های داخلی، شیوه مقابله با کلاهبرداری‌های فروش VPN، روش‌های شناسایی اپلیکیشن‌های جعلی و مخرب، جایگزین‌های پیامک برای تایید هویت حساب‌های کاربری، آماده‌سازی نقشه‌ها و ابزارهای آفلاین، و تهیه نسخه پشتیبان از اسناد مهم پیش از قطعی.

مطالعه تمامی بخش‌ها به ترتیب یا در یک نشست الزامی نیست؛ شما می‌توانید بر اساس نیاز فعلی خود، مطالعه را از هر بخش که نیاز دارید آغاز کنید. هر بخش به گونه‌ای مستقل تدوین شده است تا در هر لحظه، از جمله در شرایط اضطراری، امکان دستیابی سریع به پاسخ مورد نظر فراهم باشد.

امنیت دستگاه‌های هوشمند

چرا امنیت دستگاه‌های هوشمند مهم‌ترین اولویت است؟

دستگاه‌های هوشمند (گوشی - تبلت) دیگر فقط یک وسیله ارتباطی نیستند. امروز دستگاه‌های هوشمند شما حاوی تاریخچه مکان‌هایی است که به آن‌ها رفته‌اید، پیام‌هایی که ارسال کرده‌اید، عکس‌هایی که گرفته‌اید، فهرست مخاطبانتان و حتی بخشی از عادت‌ها و الگوهای رفتاری روزمره شماست. در شرایطی که ممکن است دستگاه‌ها بازرسی یا ضبط شوند، یک دستگاه هوشمند محافظت‌نشده، مخصوصا گوشی هوشمند می‌تواند به منبع گسترده‌ای از اطلاعات درباره شما و اطرافیانتان تبدیل شود.

قفل گوشی؛ اولین و مهم‌ترین خط دفاعی

قفل صفحه مانند در ورودی خانه است. اگر این در به اندازه کافی محکم نباشد، سایر لایه‌های امنیتی نیز تاثیر چندانی نخواهند داشت. در حقیقت اولین قدم برای محافظت از اطلاعات گوشی، انتخاب یک قفل صفحه امن است. روش‌های مختلفی مثل کد (PIN)، رمز عبور، اثر انگشت و تشخیص چهره وجود دارد، اما همه آن‌ها از نظر امنیت و شرایط استفاده یکسان نیستند. در ادامه، مزایا و محدودیت‌های هر کدام را بررسی می‌کنیم.

کد عددی (PIN) شش‌رقمی یا بیش‌تر

یکی از بهترین گزینه‌ها برای استفاده روزمره است. یک پین شش‌رقمی یک میلیون ترکیب

ممکن دارد، در حالی که یک پین چهار رقمی تنها ۱۰ هزار ترکیب ایجاد می‌کند.

رمزعبورترکیبی

استفاده از حروف، اعداد و نمادها امنیت بیش‌تری فراهم می‌کند، هرچند واردکردن آن ممکن است زمان بیش‌تری ببرد.

اثرانگشت

استفاده از آن آسان و سریع است، اما در برخی شرایط ممکن است فرد مجبور شود اثر انگشت خود را برای بازکردن دستگاه ارائه کند.

تشخیص‌چهره

این روش نیز راحت است، اما مانند اثر انگشت ممکن است در برخی شرایط بدون نیاز به دانستن رمز عبور، برای باز کردن دستگاه مورد استفاده قرار گیرد.

رمزگذاری (Encryption)؛ محافظت از داده‌ها حتی در صورت دسترسی فیزیکی

رمزگذاری دستگاه باعث می‌شود داده‌های ذخیره‌شده روی حافظه گوشی به شکلی نگهداری شوند که بدون مجوز لازم، خواندن آن‌ها دشوار یا غیرممکن باشد. این قابلیت از عکس‌ها، فایل‌ها و داده‌های برنامه‌ها روی خود دستگاه محافظت می‌کند و یکی از لایه‌های مهم امنیت گوشی است.

آیفون

در نسخه‌های iOS 8 و بالاتر، رمزگذاری به صورت پیش‌فرض فعال است؛ به شرط آنکه برای دستگاه رمز عبور یا کد (PIN) تعیین شده باشد.

اندروید

در بیش‌تر دستگاه‌های دارای اندروید ۱۰ و نسخه‌های جدیدتر، رمزگذاری به صورت پیش‌فرض فعال است. در نسخه‌های قدیمی‌تر ممکن است لازم باشد وضعیت آن را در بخش Security بررسی یا فعال کنید.

نکته‌مهم

فراموش نکنید که رمزگذاری دستگاه با رمزگذاری سرتاسری پیام‌ها یکسان نیست. رمزگذاری دستگاه از داده‌های ذخیره‌شده روی گوشی محافظت می‌کند، در حالی که رمزگذاری سرتاسری از محتوای ارتباطات در مسیر ارسال و دریافت محافظت می‌کند.

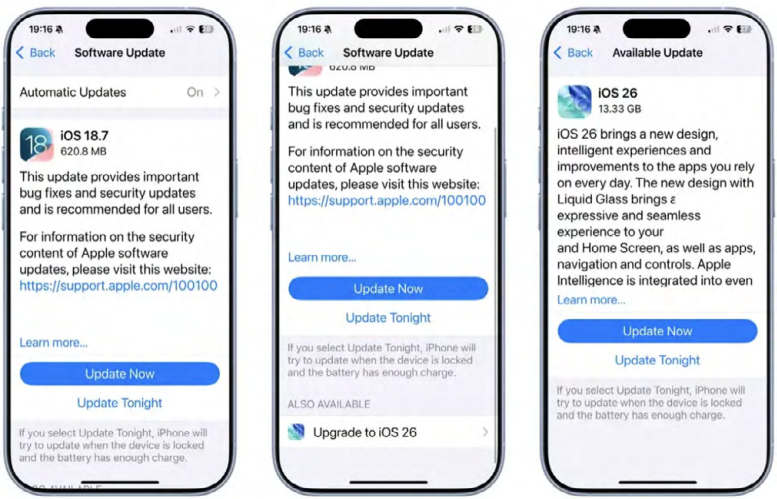
همچنین فعال‌بودن رمزگذاری به این معنی نیست که همه اطلاعات در هر شرایطی امن هستند؛ امنیت دستگاه به عواملی مانند قفل صفحه، به‌روزبودن سیستم‌عامل و امنیت برنامه‌ها نیز بستگی دارد.

به‌روزرسانی سیستم‌عامل؛ نه فقط یک توصیه، بلکه یک ضرورت

بسیاری از حملات سایبری از آسیب‌پذیری‌هایی سوءاستفاده می‌کنند که در نسخه‌های جدید سیستم‌عامل برطرف شده‌اند. به همین دلیل، به‌روزرسانی منظم سیستم‌عامل و برنامه‌ها یکی از ساده‌ترین و موثرترین اقدامات امنیتی است.

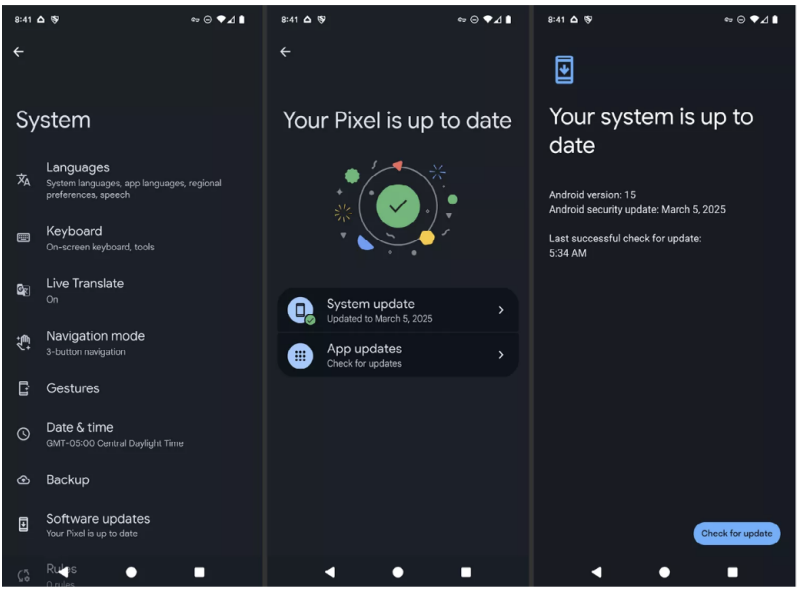
آیفون از این مسیر:

Settings > General > Software Update



اندروید از این مسیر:

Settings > Software Update یا Security Update.

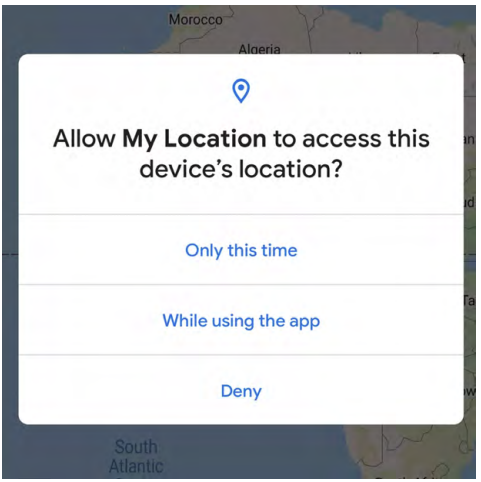


- برنامه‌های نصب‌شده را نیز از طریق App Store یا Google Play حتما به‌روز نگه دارید.

مدیریت اپلیکیشن‌ها؛ هر اپلیکیشن یک سطح دسترسی است

هر برنامه‌ای که روی گوشی نصب می‌کنید، ممکن است به بخش‌هایی مانند مکان، دوربین، میکروفون، مخاطبان یا حافظه دستگاه دسترسی داشته باشد. به همین دلیل، مرور دوره‌ای مجوزهای دسترسی اهمیت زیادی دارد.

- دسترسی‌های برنامه‌ها را به طور منظم بررسی کنید.
- برنامه‌هایی را که استفاده نمی‌کنید حذف کنید.
- برای اپلیکیشن‌هایی که به موقعیت مکانی نیاز دارند، در صورت امکان گزینه «فقط هنگام استفاده» را انتخاب کنید.



پشتیبان‌گیری (Backup)؛ آماده‌بودن برای بدترین سناریو

اگر گوشی شما گم شود، آسیب ببیند یا به هر دلیلی اطلاعاتتان را از دست دهید، داشتن نسخه پشتیبان می‌تواند جلو ازدست‌رفتن اطلاعات مهم را بگیرد.

- اطلاعات مهم را در فضای ابری امن ذخیره کنید.
- از لیست مخاطبان مهم نسخه پشتیبان تهیه کنید.
- نسخه دیجیتال اسناد ضروری را در محلی امن و ترجیحا رمزگذاری‌شده نگه دارید.
- از عکس‌ها و فایل‌های ارزشمند خانوادگی در بیش از یک محل نسخه پشتیبان داشته باشید.

شبکه‌های اجتماعی در ایران: خطرات احتمالی واقعی

شبکه‌های اجتماعی در ایران فقط ابزار ارتباطی نیستند؛ در بسیاری موارد به منابع اطلاعاتی قابل دسترس برای نهادهای مختلف تبدیل می‌شوند. گزارش‌های متعددی نشان می‌دهد که پست‌های قدیمی، لایک‌ها، عضویت در گروه‌ها و حتی تعاملات ساده کاربران می‌تواند در شرایط خاص مورد استناد قرار بگیرد.

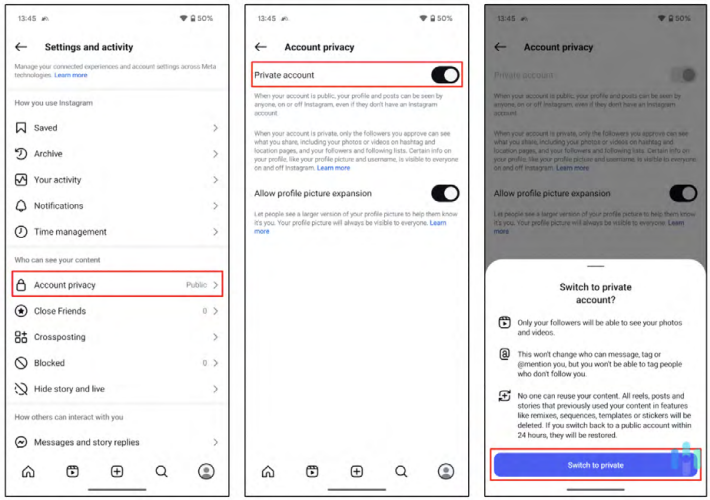
اینستاگرام: پرکاربردترین شبکه اجتماعی

اینستاگرام بخش بزرگی از زندگی آنلاین ما را در خود جای داده است؛ از عکس و ویدیو گرفته تا اطلاعات شخصی، ارتباطات و فعالیت‌های روزمره. به همین دلیل، بررسی و تنظیم حریم خصوصی حساب می‌تواند به کاهش میزان اطلاعاتی که دیگران درباره شما می‌بینند یا جمع‌آوری می‌کنند کمک کند.

تنظیمات مهم حریم خصوصی

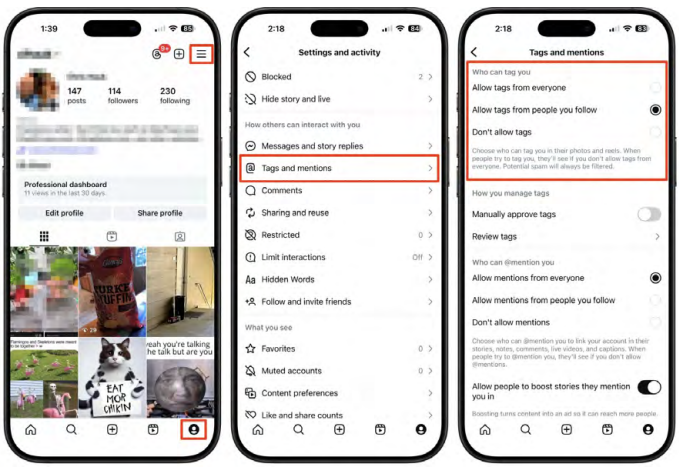
برای کاهش ریسک:

- حساب خود را خصوصی (Private) کنید. از این مسیر:
  Settings > Account Privacy > Private Account.



- لیست دنبال‌کنندگان را بررسی کنید (افراد ناشناس را حذف کنید).
- تگ‌شدن را به حالت تایید دستی تغییر دهید. از این مسیر:

Settings > Tags.



- اطلاعات شخصی (شماره، آدرس، محل کار) را از بخش معرفی (Biography) حذف کنید.

پیش‌ازموقعیت‌های حساس

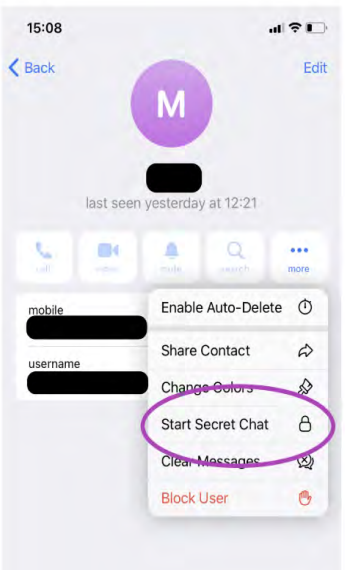
- پست‌ها و استوری‌های قدیمی را بایگانی (Archive) کنید (حذف نکنید).
- لایک‌ها و کامنت‌های مرتبط با موضوعات حساس را در صورت نیاز بررسی و پاک کنید.
- عضویت‌ها و تعامل با صفحات سیاسی را بازبینی کنید.

تلگرام: محبوب اما با برداشت اشتباه از امنیت

تلگرام امکانات امنیتی مختلفی دارد، اما همه گفت‌وگوها و قابلیت‌های آن به یک شکل محافظت نمی‌شوند. شناخت تفاوت این قابلیت‌ها و تنظیم درست حریم خصوصی می‌تواند به محافظت بهتر از حساب و اطلاعات شما کمک کند.

نکات مهم امنیتی

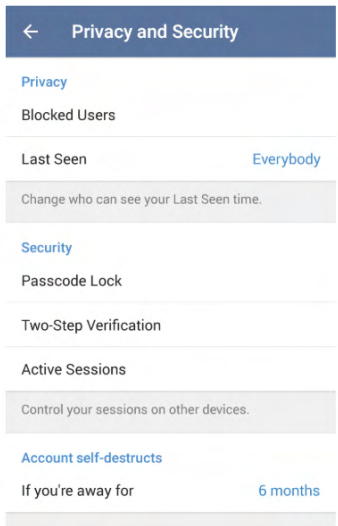
- چت‌های معمولی (Cloud Chats) رمزگذاری سرتاسری ندارند و روی سرور ذخیره می‌شوند.
- فقط گفت‌وگوی خصوصی (Secret Chat) رمزگذاری سرتاسری (End-to-End) دارد و روی دستگاه ذخیره می‌شود.

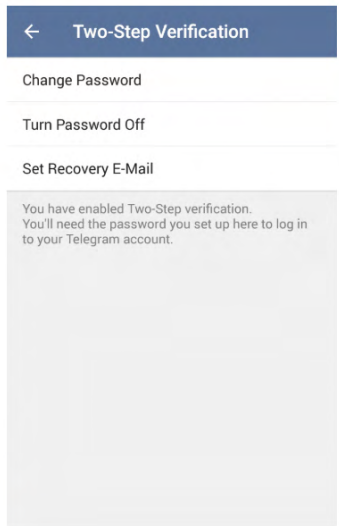


- اعضای گروه‌ها و کانال‌ها در صورت دسترسی به گوشی قابل مشاهده‌اند.

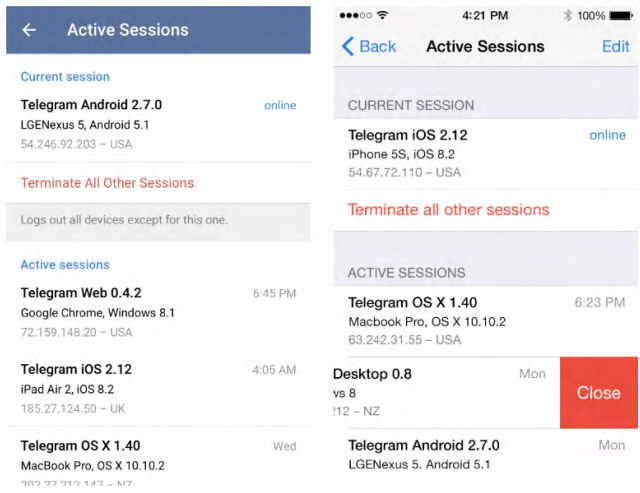
اقدامات امنیتی پیشنهادی برای تلگرام

- فعال‌سازی تایید هویت دو مرحله‌ای (Two- Step Verification)، از این مسیر: Settings > Privacy and Security.





- فعال‌کردن قفل اپ (Passcode / Face ID)
- بررسی دستگاه‌های فعال (Active Sessions)



- استفاده از گفتگوی خصوصی (Secret Chat) برای گفت‌وگوهای حساس.
- فعال‌کردن پیام‌های خود نابودشونده.

واتس‌اپ: رمزگذاری قوی اما متادیتای قابل تحلیل

واتس‌اپ از رمزگذاری سرتاسری برای پیام‌ها و تماس‌ها استفاده می‌کند، اما اطلاعاتی مانند زمان و نحوه استفاده از سرویس، جدا از محتوای پیام‌ها هستند و موضوع حریم خصوصی را مهم می‌کنند.

نکات‌مهم

- محتوای پیام‌ها و تماس‌ها با رمزگذاری سرتاسری محافظت می‌شود اما برخی اطلاعات مربوط به استفاده از سرویس، مانند زمان و الگوی ارتباط، ممکن است در قالب متادیتا ثبت شود یا قابل دسترسی باشد. میزان و نوع این اطلاعات به

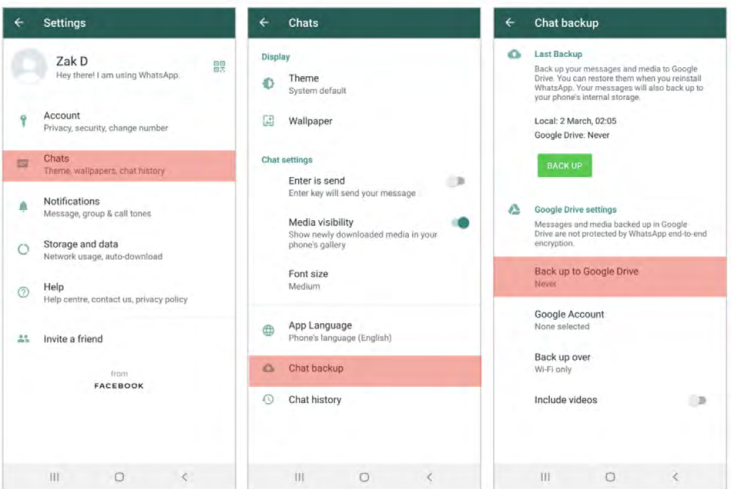
داده‌هایی که سرویس نگهداری می‌کند و شرایط دسترسی به آن‌ها بستگی دارد.

- نسخه پشتیبان گفت‌وگوها (Backup chats) به صورت پیش‌فرض رمزگذاری سرتاسری ندارند (مگر فعال شود).

تنظیمات مهم امنیتی

- فعال‌کردن Two-Step Verification.
- فعال‌کردن End-to-End Encrypted Backup، از این مسیر:

Settings > Chats > Chat Backup.

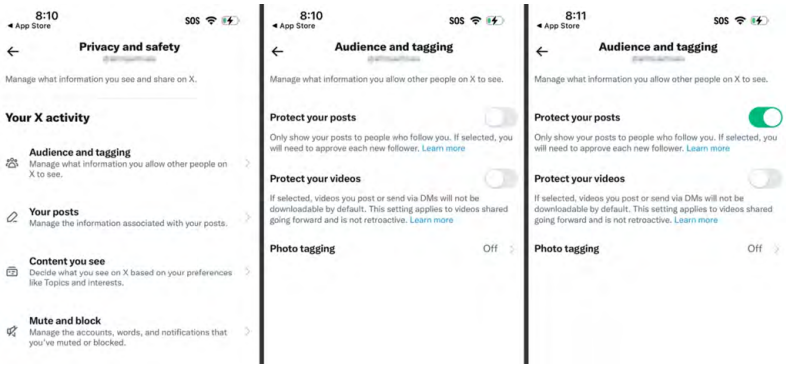


X (توییتر سابق): قدرتمند اما حساس

X امکان انتشار سریع محتوا و برقراری ارتباط با مخاطبان گسترده را فراهم می‌کند، اما فعالیت‌های عمومی، اطلاعات حساب و تعاملات شما می‌تواند تصویر قابل‌توجهی از فعالیت آنلاینتان ایجاد کند. بنابراین، بررسی تنظیمات حریم خصوصی و دقت در اطلاعاتی که منتشر می‌کنید اهمیت زیادی دارد.

تنظیمات‌مهم‌امنیتی

- خصوصی‌کردن حساب در صورت انتشار محتوای حساس.



- غیرفعال‌کردن موقعیت مکانی (Location) در توییت‌ها.
- استفاده از FA2 مبتنی بر اپ (، نه SMS).
- بررسی اپلیکیشن‌های متصل به حساب.

نکته‌مهم

استفاده از نام واقعی، عکس واقعی یا اشاره به محل زندگی می‌تواند به شناسایی هویت کمک کند.

فراداده (Metadata) عکس: اطلاعات پنهان

- هر عکس شامل داده‌های پنهان Exif است، مانند:
- موقعیت دقیق GPS
- زمان و تاریخ ثبت تصویر
- مدل گوشی و تنظیمات دوربین.

این اطلاعات ممکن است همراه عکس ذخیره شوند و در صورت انتشار یا ارسال عکس در شبکه‌های اجتماعی، موقعیت مکانی شما را فاش کنند.

حذف فراداده (Metadata) از عکس‌ها پیش از انتشار یا ارسال

عکس‌ها ممکن است اطلاعاتی مانند موقعیت مکانی، تاریخ و زمان ثبت، مدل گوشی و مشخصات دوربین را در خود ذخیره کنند. رفتار برنامه‌ها با این اطلاعات یکسان نیست و به روش ارسال عکس نیز بستگی دارد.

وضعیت فراداده در برنامه‌های پرکاربرد

- **اینستاگرام:** هنگام بارگذاری عکس، اینستاگرام معمولا تصویر را پردازش می‌کند و فراداده‌هایی مانند مختصات GPS را از نسخه‌ای که نمایش داده می‌شود حذف می‌کند. با این حال، نباید فرض کرد که پلتفرم پیش از پردازش به اطلاعات فایل دسترسی ندارد.
- **فیس‌بوک:** عکس‌های بارگذاری‌شده معمولا برای نمایش دوباره پردازش می‌شوند و بیش‌تر فراداده‌های EXIF از نسخه منتشرشده حذف می‌شوند. این موضوع لزوما به معنی حذف اطلاعات از تمام نسخه‌های ذخیره‌شده در زیرساخت پلتفرم نیست.
- **تلگرام:** اگر عکس را به شکل معمولی و به صورت Photo بفرستید، برنامه معمولا آن را فشرده یا پردازش می‌کند و ممکن است فراداده‌های اصلی حذف شوند. اما اگر عکس را به شکل File ارسال کنید، احتمال حفظ فراداده‌های فایل اصلی بیشتر است.
- **واتس‌اپ:** ارسال عکس به شکل معمولی معمولا باعث پردازش تصویر و حذف بیش‌تر فراداده‌های EXIF می‌شود. در مقابل، ارسال همان عکس به شکل Doc-ument ممکن است اطلاعات فایل اصلی، از جمله موقعیت مکانی، را حفظ کند.
- **سیگنال:** هنگام ارسال عکس به شکل تصویر، معمولا اطلاعات فراداده از نسخه ارسالی حذف می‌شود؛ با این حال، بهتر است برای اطلاعات حساس، حذف فراداده را پیش از ارسال بررسی کنید. رمزگذاری سرتاسری سیگنال به‌تنهایی به معنی حذف فراداده از فایل نیست.
- **ایکس** (X): عکس‌هایی که از مسیر معمول انتشار بارگذاری می‌شوند، عموما پردازش می‌شوند و فراداده‌های EXIF آن‌ها از نسخه نمایش‌داده‌شده حذف می‌شود. با این حال، برای عکس‌های حساس بهتر است به این مسئله اتکا نکنید.

چطور پیش از ارسال، فراداده عکس را حذف کنیم؟

- **اندروید:** می‌توانید از ابزار Scrambled Exif برای حذف فراداده عکس پیش از به‌اشتراک‌گذاری آن استفاده کنید.
- **آیفون:** هنگام به‌اشتراک‌گذاری عکس از برنامه Photos، وارد بخش Options شوید و گزینه Location را غیرفعال کنید. برای مدیریت دقیق‌تر فراداده‌ها نیز می‌توانید از برنامه Metapho استفاده کنید.

نکته‌امنیتی

اگر موقعیت مکانی یا اطلاعات دیگری که ممکن است هویت یا محل حضور شما را آشکار کند اهمیت دارد، پیش از ارسال یا انتشار، حتما فراداده عکس را حذف کنید. این کار به‌ویژه هنگام ارسال عکس به شکل File یا Document مهم است. حذف فراداده نیز همه خطرهای حریم خصوصی را برطرف نمی‌کند؛ خود تصویر ممکن است نشانه‌هایی از محل، افراد یا شرایط ثبت عکس داشته باشد.

مدیریت اطلاعات دیجیتال فقط یک انتخاب نیست؛ یک عادت امنیتی است. حتی اقدامات ساده مثل بررسی تنظیمات یا حذف متادیتا می‌تواند نقش مهمی در کاهش ریسک داشته باشد.

چرا ایمیل هنوز اهمیت دارد؟

در دنیایی که پیام‌رسان‌ها مثل واتس‌اپ و تلگرام غالب شده‌اند، ایمیل هنوز یکی از مهم‌ترین ابزارهای دیجیتال است. ایمیل فقط برای ارسال پیام نیست؛ بلکه برای بازیابی حساب‌ها، ارتباطات رسمی و مستند و ارتباط امن با سازمان‌ها استفاده می‌شود. ازدست‌دادن ایمیل، یعنی ازدست‌دادن دسترسی به بسیاری از حساب‌های دیگر.

Protonmail: چرا انتخاب می‌شود؟

Proton Mail در سوئیس میزبانی می‌شود و تحت قوانین سخت‌گیرانه حریم خصوصی فعالیت می‌کند. این سرویس از رمزگذاری سرتاسری (End-to-End Encryption) استفاده می‌کند؛ یعنی حتی خود شرکت هم قادر به خواندن محتوای ایمیل‌ها نیست.

روش استفاده

- به em.noprot مراجعه کنید و حساب بسازید (بدون نیاز به شماره تلفن).
- اگر برای ارتباطات حساس استفاده می‌کنید، از نام واقعی در ایمیل استفاده نکنید.
- تایید دو مرحله‌ای (AF2) را از ابتدا فعال کنید.
- اپلیکیشن Proton Mail را روی تلفن همراهتان نصب کنید.

تایید دو مرحله‌ای (2FA): لایه دوم امنیت

2FA یعنی حتی اگر رمز عبور شما لو برود، ورود بدون کد دوم ممکن نیست.

روش‌های موجود، به ترتیب از ضعیف به قوی

- SMS: ناامن (قابل رهگیری و آسیب‌پذیر در SIM Swap)

  نکته مهم: استفاده از SMS برای امنیت توصیه نمی‌شود، مخصوصا در حساب‌های حساس.
- ای‌میل بازیابی: متوسط
- اپلیکیشن Authenticator: امن (کدهای ۳۰ ثانیه‌ای)
- کلید امنیتی فیزیکی: بسیار امن (مثل YubiKey)

اپلیکیشن‌پیشنهادی

Aegis Authenticator

- متن‌باز و رایگان
- امکان تهیه نسخه پشتیبان رمزنگاری‌شده
- قابل انتقال بین دستگاه‌ها

امنیت ایمیل فقط به انتخاب سرویس وابسته نیست؛ بلکه ترکیبی از رمز قوی، احراز هویت دومرحله‌ای، و مدیریت درست دسترسی‌ها است.

اگر ایمیل از دست برود، معمولا بخش بزرگی از هویت دیجیتال هم از بین می‌رود.

رمزهای عبور: ساده اما حیاتی

رمز عبور یکی از مهم‌ترین لایه‌های محافظت از حساب‌های شماست. استفاده از رمزهای کوتاه، قابل حدس یا تکراری می‌تواند امنیت چندین حساب را هم‌زمان به خطر بیندازد.

روش ساخت رمز عبور قوی

- یک عبارت طولانی و غیرقابل‌حدس انتخاب کنید.
- از ترکیبی از حروف، اعداد و نمادها استفاده کنید.
- از اطلاعات شخصی مثل نام، تاریخ تولد یا شماره تلفن استفاده نکنید.
- برای هر حساب یک رمز عبور کاملا متفاوت داشته باشید.
- برای مدیریت رمزهای متعدد، از یک مدیر رمز عبور استفاده کنید.

نکته: طول و منحصربه‌فرد بودن رمز معمولاً از پیچیده‌کردن یک رمز کوتاه مهم‌تر است.

مدیر رمز عبور: راه‌حل حرفه‌ای

مدیر رمز عبور (Password Manager) برنامه‌ای است که رمزهای عبور شما را به صورت امن نگهداری می‌کند و می‌تواند برای هر حساب، رمز عبوری قوی و متفاوت ایجاد کند. به این ترتیب، لازم نیست رمزهای پیچیده را حفظ کنید یا برای چند حساب از یک

رمز استفاده کنید.

- Bitwarden: رایگان، متن‌باز و امن
- KeePassXC: کاملا آفلاین و امن

این ابزارها برای هر حساب یک رمز قوی و متفاوت تولید و ذخیره می‌کنند.

امنیت وی.پی.ان و انتخاب سرویس مطمئن

VPN ترافیک اینترنت شما را از طریق یک سرور واسط رمزگذاری می‌کند و مسیر می‌دهد. در این روند دو کار مهم انجام می‌شود: عبور از فیلترینگ و مخفی‌کردن این‌که چه سایت‌هایی را از کجا باز می‌کنید.

نکته مهم: VPN محتوای پیام‌های شما را در اپ‌هایی مثل سیگنال یا تلگرام امن‌تر نمی‌کند (آن‌ها خودشان رمزگذاری دارند)، بلکه بیش‌تر فراداده (Metadata) اتصال (این‌که شما به کدام سرویس‌ها وصل می‌شوید) را از دید ناظر شبکه پنهان می‌کند.

چطور یک VPN مطمئن انتخاب کنیم؟

سیاست عدم ثبت لاگ (No-Log Policy)

سرویس باید صراحتا اعلام کند که فعالیت یا اتصال کاربران را ذخیره نمی‌کند. بهتر است این ادعا با بررسی کارشناسان مستقل (Independent Audit) هم تایید شده باشد، نه این‌که فقط به ادعای خود شرکت اکتفا شود.

کشورمیزبان

سرویس‌هایی که در کشورهایی با قوانین سخت‌گیرانه حریم خصوصی مستقر هستند و

خارج از توافق‌های اشتراک اطلاعاتی بین دولتی هستند، خطر کم‌تری دارند.

پروتکل‌های امن

پروتکل‌هایی مثل WireGuard و OpenVPN امن و قابل‌اعتماد شناخته می‌شوند. از وی.پی.ان‌های رایگان ناشناس که پروتکل خود را اعلام نمی‌کنند دوری کنید.

کلید قطع اضطراری (Kill Switch)

این قابلیت در صورت قطع ناگهانی اتصال VPN، به طور خودکار اینترنت دستگاه را قطع می‌کند تا داده شما بدون محافظت به بیرون درز نکند. برای کاربران ایرانی که با قطعی‌های ناگهانی مواجه‌اند، این ویژگی حیاتی است.

خطرات وی.پی.ان‌های رایگان و ناشناس

بسیاری از وی.پی.ان‌های رایگانی که به صورت گسترده در ایران دست‌به‌دست می‌شوند:

- ترافیک کاربران را جمع‌آوری و به تبلیغ‌دهندگان یا اشخاص ثالث می‌فروشند.
- برخی به طور خاص مشغول هدف‌گیری کاربران ایرانی هستند و ممکن است بدافزار یا کد جاسوسی درون خود داشته باشند.
- اغلب فاقد Kill Switch و رمزگذاری واقعی‌اند و فقط یک واسط ساده بدون محافظتند.
- معمولا شرکت‌های سازنده نامعتبر دارند.

قبل از نصب هر VPN، به خصوص نسخه‌های APK که خارج از Google Play دست‌به‌دست می‌شوند، منبع را بررسی کنید و در صورت امکان از نسخه رسمی سایت سرویس دانلود کنید.

وی.پی.ان‌های شناخته‌شده برای کاربران ایرانی

- **Psiphon**: رایگان، متن‌باز و طراحی‌شده برای دورزدن فیلترینگ گسترده.
- **Outline VPN**: ساخته Google Jigsaw و با امکان راه‌اندازی سرور اختصاصی توسط خود کاربر.

- **ProtonVPN**: دارای نسخه رایگان محدود، مستقر در سوئیس و با no-log تاییدشده.
- **Lantern** : تمرکز بر عبور از سانسور با پهنای باند تطبیقی.

چندنکته‌عملی

- همیشه بیش از یک وی.پی.ان نصب داشته باشید تا در صورت مسدودشدن یکی، جایگزین در دسترس باشد.
- فایل نصب (APK) سرویس‌های مورد اعتماد را از قبل و به صورت آفلاین ذخیره کنید (همان‌طور که در بخش قطعی اینترنت اشاره شد).
- از واردکردن اطلاعات پرداخت واقعی در وی.پی.ان‌های ناشناس خودداری کنید؛ در صورت امکان از روش‌های پرداخت ناشناس استفاده کنید.
- به‌روزرسانی منظم اپ VPN را فراموش نکنید؛ نسخه‌های قدیمی ممکن است آسیب‌پذیری امنیتی داشته باشند.

امنیت دیجیتال در تجمعات و اعتراضات

آماده‌سازی پیش از حضور

پیش از حضور در تجمع، بهتر است علاوه بر توجه به امنیت فیزیکی، برای محافظت از اطلاعات شخصی و ارتباطات خود نیز آماده باشید. رعایت چند نکته ساده درباره گوشی، اطلاعات شخصی، عکس و فیلم و نحوه ارتباط با همراهان می‌تواند در کاهش خطرهای احتمالی، پیش از تجمع، هنگام آن و پس از پایان تجمع کمک‌کننده باشد.

گوشی ساده یا حالت محدود

در صورت امکان، گوشی دوم و ساده با اطلاعات محدود همراه ببرید. اگر فقط یک گوشی دارید، پیش از رفتن اپلیکیشن‌های حساس را حذف یا اطلاعات ورود به آن‌ها را از حافظه مرورگر و اپ پاک کنید.

عکس یا فیلم منتشر نکنید اگر چهره حاضران مشخص و شناسایی‌شدنی است

انتشار عکس یا فیلمی که چهره افراد دیگر در آن مشخص است، می‌تواند آن‌ها را در معرض شناسایی قرار دهد، حتی اگر خودتان قصد آسیب نداشته باشید. در صورت لزوم، چهره‌ها را تار یا سانسور کنید.

لباس و ظاهر خنثی

از پوشیدن لباس یا حمل وسایلی که به‌راحتی قابل تشخیص و بازشناسی در فیلم و عکس باشد (رنگ خاص، لوگو، طرح منحصربه‌فرد) خودداری کنید.

در طول تجمع

- موقعیت مکانی (Location) گوشی را کاملا خاموش کنید، نه فقط برای یک اپ خاص.
- Wi-Fi و بلوتوث را در صورت عدم نیاز خاموش کنید تا امکان ردیابی از طریق شبکه‌های اطراف کاهش یابد.
- در صورت امکان از حالت هواپیما استفاده کنید و فقط در مواقع لازم آن را خاموش کنید.
- از یک کلمه یا علامت با دوستان همراه برای هماهنگی در صورت جدا افتادن توافق کنید.

در صورت وقوع بازداشت جمعی

- خونسردی خودتان را حفظ کنید و از درگیری فیزیکی با ماموران یا کلامی بپرهیزید.
- اگر گوشی همراه‌تان است و امکانش را دارید، آن را خاموش کنید (نه فقط قفل).
- کد یا رمز از پیش توافق‌شده را در صورت امکان به نزدیک‌ترین فرد مطلع اطلاع دهید.

بعد از تجمع

پیگیری کنید که آیا عکس یا فیلمی از شما در فضای مجازی منتشر شده که نیاز به حذف یا گزارش داشته باشد، و در صورت شک به دسترسی احتمالی مشکوک به گوشی، همان مراحل گفته‌شده در بخش «بعد از بازرسی» (تغییر رمزها و بررسی Active Sessions) را انجام دهید.

امنیت خانواده و نزدیکان: چک‌لیست اضطراری مشترک

این بخش به‌ویژه برای افرادی اهمیت دارد که به دلیل فعالیت حرفه‌ای، اجتماعی یا مدنی، روزنامه‌نگاری، فعالیت آنلاین یا دسترسی به اطلاعات حساس، ممکن است با خطرات بیشتری روبرو باشند. در چنین شرایطی، امنیت فقط به گوشی و حساب‌های خود فرد محدود نمی‌شود؛ اعضای خانواده، دوستان و همکاران نزدیک نیز ممکن است ناخواسته اطلاعاتی مهم درباره فرد در اختیار داشته باشند.

برای مثال، ذخیره عکس‌ها و اطلاعات حساس، به‌اشتراک‌گذاری رمز عبور یا استفاده از یک حساب مشترک می‌تواند در صورت دسترسی دیگران به دستگاه یا حساب یکی از اعضای خانواده، خطر بیش‌تری ایجاد کند.

به همین دلیل، بهتر است افراد نزدیک درباره چند اصل ساده با هم توافق داشته باشند: چه اطلاعاتی را ذخیره یا به اشتراک نگذارند، از رمزهای مشترک استفاده نکنند و در شرایط اضطراری بدانند چگونه از حساب‌ها و اطلاعات یکدیگر محافظت کنند.

امنیت دیجیتال در چنین شرایطی یک موضوع فردی نیست؛ امنیت هر فرد می‌تواند بر امنیت اطرافیانش و برعکس، تاثیر بگذارد.

توافق‌های پایه‌ای که باید از قبل انجام شود

یک کلمه یا جمله رمز (Code Word)

با نزدیکانتان از قبل بر یک کلمه یا جمله ساده توافق کنید که معنای مشخصی برای اقدام مشخصی داشته باشد. این روش می‌تواند در شرایط اضطراری، مثل زمانی که امکان صحبت‌کردن آزادانه ندارید، تماس بسیار کوتاه است یا نمی‌توانید جزئیات یک وضعیت را در پیام توضیح دهید، کمک‌کننده باشد. کلمه یا جمله توافقی باید ساده و طبیعی باشد و فقط افراد موردنظر معنای آن را بدانند.

فهرست تماس اضطراری فیزیکی

یک نسخه کاغذی از شماره‌های ضروری (وکیل، اعضای نزدیک خانواده، سازمان‌های حمایتی) با چند نفر مورد اعتماد در میان بگذارید، نه این‌که فقط در گوشی‌تان ذخیره کنید. در این صورت اگر بازداشت شوید این افراد می‌توانند اقدامات ضروری برای اطلاع‌رسانی و پیگیری را انجام بدهند.

توافق درباره این‌که چه کسی چه اقداماتی را انجام دهد

از قبل مشخص کنید اگر برای یکی از اعضای خانواده یا نزدیکان اتفاقی افتاد یا ارتباط با او قطع شد، چه کسی و در چه زمانی مسئول پیگیری، اطلاع‌رسانی و اقدامات ضروری برای پاک‌سازی دستگاه یا محل سکونت و... است تا چیزی از قلم نیفتد.

هماهنگی فنی بین اعضای خانواده و نزدیکان

- از پیام‌رسان مشترک امن (ترجیحا Signal) به عنوان کانال اصلی خانوادگی استفاده کنید
- پیام‌های خود نابودشونده را برای گفت‌وگوهای حساس در گروه خانوادگی فعال کنید.
- مطمئن شوید همه اعضا حداقل یک VPN نصب‌شده و تست‌شده دارند، نه فقط شما.
- از به‌اشتراک‌گذاری رمز عبور بین اعضا خودداری کنید؛ به جایش از مدیر رمز عبور با دسترسی اضطراری (Emergency Access در Bitwarden) استفاده کنید.

مواجهه با بازرسی دستگاه

بازرسی گوشی - چه در بازداشت، چه در ایست بازرسی و چه در مرز، یکی از پرخطرترین لحظات از نظر امنیت دیجیتال است. اقدامات پیشگیرانه تفاوت زیادی در میزان آسیب‌پذیری شما ایجاد می‌کند.

آماده‌سازی پیش از بازرسی

- هر اپلیکیشن حساس (پیام‌رسان، ایمیل، شبکه اجتماعی) را با قفل جداگانه محافظت کنید، نه فقط با قفل کلی گوشی.
- چت‌های حساس را در Secret Chat یا پیام‌های خود نابودشونده نگه دارید تا تاریخچه طولانی روی دستگاه باقی نماند.
- عضویت در گروه‌ها و کانال‌های حساس را به صورت دوره‌ای بازبینی کنید و در صورت نیاز از آن‌ها خارج شوید.
- یک ویجت یا میانبر برای خاموش‌کردن سریع گوشی روی صفحه اصلی قرار دهید.
- اگر امکانش هست، از فضای پنهان (Hidden Space) در برخی گوشی‌های اندروید یا از پروفایل کاری جداگانه برای اطلاعات حساس استفاده کنید.

حین بازرسی

- خونسردی خود را حفظ کنید و از درگیری فیزیکی یا کلامی با ماموران بپرهیزید.
- اگر ممکن است پیش از تحویل گوشی آن را خاموش کنید؛ گوشی خاموش و رمزگذاری‌شده دسترسی به داده را دشوارتر می‌کند.
- تحت فشار روانی، رمز عبور یا رمز بازکردن قفل Biometric (اثر انگشت/چهره) را می‌توان به شکل متفاوتی درخواست کرد؛ آگاه باشید که قفل کد (PIN)، عبور معمولا محافظت بیش‌تری نسبت به قفل Biometric (اثر انگشت یا چهره) دارد.
- از دادن اطلاعات اضافی درباره مخاطبین، گروه‌ها یا فعالیت‌های دیگران خودداری کنید

پس از بازرسی

- در اولین فرصت امن، تمام رمزهای عبور حساب‌های مهم (ایمیل، شبکه اجتماعی، پیام‌رسان) را تغییر دهید.
- Active Sessions یا دستگاه‌های فعال را در تلگرام، واتس‌اپ و ایمیل بررسی و دستگاه‌های ناشناس را حذف کنید.
- از تمام حساب‌ها در تمام دستگاه‌ها خارج شوید و دوباره وارد شوید.
- گوشی را از نظر نصب برنامه‌های ناشناس یا مشکوک بررسی کنید.

اقدامات و مراقبت‌های امنیتی در زمان قطع اینترنت

در زمان قطعی یا محدودیت گسترده اینترنت، نیاز فوری به ارتباط و دسترسی، فضای مناسبی برای سوءاستفاده ایجاد می‌کند؛ از پیام‌رسان‌های داخلی که ادعای امن‌بودن دارند، تا فروشندگان وی.پی.ان‌های ناامن و اپلیکیشن‌های مخربی که وعده «وصل‌کردن اینترنت» می‌دهند. دانستن این خطرها پیش از وقوع قطعی، مهم‌ترین راه پیشگیری است.

پیام‌رسان‌های داخلی

پیام‌رسان‌های داخلی را برای ارتباطات حساس استفاده نکنید. پیام‌رسان‌هایی مانند بله، روبیکا و سروش گاهی به عنوان جایگزین پیام‌رسان‌های جهانی در دوران قطعی معرفی می‌شوند، اما نگرانی‌های جدی درباره ساختار امنیتی آن‌ها وجود دارد: با وجود ادعای رمزگذاری، بسیاری از آن‌ها رمزگذاری سرتاسری واقعی ندارند و سرورهای مرکزی به محتوای پیام‌ها دسترسی دارند. برخی از این اپ‌ها داده‌های گسترده‌ای از کاربران (پیام، تصویر، فایل، اطلاعات تماس) جمع‌آوری می‌کنند. حتی اگر محتوای پیام خوانده نشود، متادیتا (چه کسی، چه زمانی، با چه کسی در ارتباط است) برای تحلیل شبکه‌های ارتباطی افراد ارزشمند است.

به همین دلیل، حتی در زمانی که این برنامه‌ها تنها ابزار در دسترس به نظر می‌رسند، توصیه نمی‌شوند. دسترسی‌های اپلیکیشن را بررسی کنید و از نصب برنامه‌هایی که

مجوزهای غیرضروری (تماس، پیامک، مکان) می‌خواهند خودداری کنید. اپ‌ها را فقط از منابع رسمی دانلود کنید.

فروش وی.پی.ان‌های تقلبی و ناامن

مراقب کلاهبرداری‌های فروش VPN باشید. همزمان با افزایش تقاضا برای VPN در دوران قطعی، تعداد کانال‌ها و صفحات فروش جعلی نیز افزایش می‌یابد. برخی کاربران پس از پرداخت هزینه، سرویسی دریافت نمی‌کنند یا سرویسی می‌گیرند که امنیت لازم را ندارد و حتی می‌تواند اطلاعاتشان را در معرض خطر بگذارد. برای کاهش این خطر: سابقه فعالیت کانال یا صفحه فروشنده را بررسی کنید؛ کانال‌های تازه‌ساز یا با سابقه کوتاه معمولا قابل‌اعتماد نیستند. نام یا آی.دی کانال را جست‌وجو کنید تا ببینید کاربران دیگر چه تجربه‌ای داشته‌اند.

به وعده‌های غیرواقعی مانند «VPN نامحدود و همیشه پایدار» یا «دسترسی تضمینی در همه شرایط» مشکوک باشید. از پرداخت به روش‌های غیرقابل پیگیری خودداری کنید. تا حد امکان از سرویس‌های شناخته‌شده‌ای استفاده کنید که پیش‌تر معرفی شدند (مانند Outline VPN، ProtonVPN، Psiphon و Lantern).

اپلیکیشن‌های مخرب و ناامن

در دوران قطعی، برخی افراد یا گروه‌ها با سوءاستفاده از نیاز فوری کاربران، اپلیکیشن‌های جعلی با وعده‌هایی مانند «وصل‌شدن اینترنت»، «دورزدن اختلال» یا «اینترنت رایگان» منتشر می‌کنند. این برنامه‌ها معمولا از طریق بلوتوث، ShareIt یا لینک‌های منتشرشده در شبکه‌های اجتماعی دست‌به‌دست می‌شوند و بدون شفافیت درباره سازنده یا عملکردشان توزیع می‌شوند. نصب چنین برنامه‌هایی می‌تواند به دسترسی غیرمجاز به مخاطبین و پیام‌ها، شنود تماس‌ها، سرقت حساب‌های کاربری، یا نصب بدافزار پنهان منجر شود.

توجه داشته باشید که قطع اینترنت مانع فعالیت بدافزار نیست؛ بسیاری از آن‌ها با اتصال مجدد یا حتی از طریق پیامک و بلوتوث فعال می‌شوند.

برای شناسایی این برنامه‌ها به این نشانه‌ها توجه کنید:

- درخواست مجوزهای غیرضروری (پیامک، تماس، حافظه، میکروفن)

- نداشتن وب‌سایت رسمی یا اطلاعات تماس مشخص
- اصرار بر نصب فوری و ایجاد حس اضطرار
- وعده غیرواقعی «وصل کردن اینترنت قطع‌شده».

هیچ اپلیکیشنی نمی‌تواند به تنهایی محدودیت‌های زیرساختی اینترنت را حذف کند؛ چنین ادعاهایی همیشه هشداردهنده‌اند. پیش از هر قطعی، اپلیکیشن‌های مطمئن (مانند فایل نصب وی.پی.ان‌های معرفی‌شده توسط منابع معتبر مثل تواناتک) را از قبل و به صورت آفلاین ذخیره کنید تا نیازی به جست‌وجوی اضطراری و پرخطر در آن لحظه نداشته باشید.

نگهداری از اسناد مهم؛ نسخه پشتیبان پیش از قطعی اینترنت

نیاز به یک سند مهم (کارت ملی، شناسنامه، مدارک پزشکی، اسناد ملکی، گواهی‌های شغلی) اغلب دقیقا در لحظه‌ای پیش می‌آید که دسترسی به اینترنت یا فضای ابری قطع است. فضای ذخیره‌سازی ابری (مانند گوگل درایو یا آی‌کلاود) فقط زمانی قابل دسترسی است که اینترنت برقرار باشد. در برخی موقعیت‌ها (ارائه مدرک هویتی به مراجع محلی، بیمارستان یا نیروی امدادی)، عدم دسترسی سریع به یک سند می‌تواند مشکل‌ساز شود.

تهیه نسخه دیجیتال

با اپلیکیشن‌های اسکنر (اسکنر داخلی گوشی‌های اندروید و آیفون یا Adobe Scan) مدارک کاغذی را به فایل PDF خوانا تبدیل کنید. فایل‌ها را با نام مشخص و قابل جست‌وجو ذخیره کنید، مثلا «کارت-ملی-نام-خانوادگی». برای مدارک حجیم مانند چند صفحه پزشکی، از فرمت PDF فشرده استفاده کنید تا انتقالشان در اتصال ضعیف هم سریع‌تر باشد.

ذخیره‌سازی امن

اسناد را در یک پوشه رمزگذاری‌شده روی گوشی یا لپ‌تاپ نگهداری کنید؛ BitLocker در ویندوز یا FileVault در مک این امکان را به صورت محلی و بدون نیاز به اینترنت

فراهم می‌کنند.

یک نسخه پشتیبان روی فلش مموری یا کارت حافظه جداگانه (ترجیحا رمزگذاری‌شده) نگه دارید تا در صورت ازکارافتادن یا مسدودشدن گوشی اصلی، اسناد همچنان در دسترس باشند.

در صورت دسترسی به اینترنت، نسخه‌ای از اسناد را در یک سرویس ابری معتبر و رمزگذاری‌شده هم بارگذاری کنید؛ این نسخه در دوران قطعی کامل به تنهایی کافی نیست، اما برای بازگشت اینترنت یا دسترسی از دستگاه دیگر مفید است.

نکات‌امنیتی

- هرگز اسناد هویتی حساس را بدون رمزگذاری روی گوشی ذخیره نکنید؛ در صورت گم‌شدن یا ضبط دستگاه، از این اطلاعات می‌تواند سوءاستفاده شود.
- برای پوشه یا فایل رمزگذاری‌شده، از رمزی متفاوت از رمزهای روزمره استفاده کنید و آن را جایی غیر از همان دستگاه هم به خاطر بسپارید.
- حداقل در دو مکان مجزا (مثلا گوشی و یک فلش مموری) نسخه پشتیبان را نگهداری کنید.
- در صورت صدور مدرک جدید (مثلا تمدید گذرنامه)، نسخه پشتیبان را به‌روز کنید.

نقشه‌ها و ابزارهای آفلاین؛ آمادگی پیش از قطعی اینترنت

بسیاری از اپلیکیشن‌ها، از نقشه‌ها گرفته تا دیکشنری‌ها و برخی پیام‌رسان‌ها، برای بارگذاری محتوای اولیه به اینترنت نیاز دارند. اگر این محتوا از قبل دانلود نشده باشد، در لحظه قطعی هیچ راهی برای دریافت آن نیست. آماده‌سازی ابزارهای آفلاین باید بخشی از یک روال منظم باشد، نه اقدامی که فقط هنگام احساس خطر قطعی انجام می‌شود.

گوگل مپس (Google Maps)

اپلیکیشن را باز کنید و منطقه مورد نظر (شهر یا محله) را در مرکز صفحه قرار دهید. روی عکس پروفایل یا آیکون منو بزنید و گزینه نقشه‌های آفلاین» (Offline maps) را انتخاب کنید. روی گزینه «انتخاب نقشه خودتان» (Select your own map) بزنید و محدوده

مورد نیاز را با کشیدن قاب انتخاب مشخص کنید. روی دانلود بزنید. نقشه‌های آفلاین معمولا پس از حدود ۳۰ روز منقضی می‌شوند و باید به‌روزرسانی شوند.

منابع اطلاعاتی و ترجمه آفلاین

Kiwix امکان دانلود نسخه کامل ویکی‌پدیا یا بخش‌هایی از آن (مانند مقالات پزشکی یا اورژانسی) را به صورت یک فایل فشرده و کاملا قابل جست‌وجوی آفلاین فراهم می‌کند. Google Translate نیز امکان دانلود زبان‌های مورد نیاز برای استفاده آفلاین را از بخش تنظیمات زبان دارد.

پیام‌رسانی بدون اینترنت

Briar با استفاده از بلوتوث یا Wi-Fi مستقیم، بدون نیاز به سرور یا اینترنت، امکان ارسال پیام میان دستگاه‌های نزدیک به هم را فراهم می‌کند. نصب و آشنایی اولیه با این اپلیکیشن باید پیش از وقوع قطعی انجام شود.

نکات تکمیلی نقشه‌ها و ابزارهای آفلاین را هر چند وقت یک‌بار به‌روز کنید؛ به‌ویژه نقشه‌های گوگل مپس که منقضی می‌شوند. پیش از دانلود نقشه‌های حجیم، فضای خالی گوشی را بررسی کنید. نحوه کارکرد این ابزارها را در حالت آفلاین (مثلا با خاموش‌کردن موقت دیتای موبایل) از قبل امتحان کنید تا در لحظه بحران با نحوه استفاده آشنا باشید. در صورت امکان، اطلاعات مهم را روی بیش از یک دستگاه ذخیره کنید.

نگهداری از حساب‌ها در دوران اختلال اینترنت؛ جایگزین‌های پیامک تایید هویت

در شرایط اختلال یا قطعی اینترنت، دسترسی به کدهای تایید پیامکی ممکن است با مشکل مواجه شود. به همین دلیل، بهتر است برای ورود و بازیابی حساب‌های مهم، فقط به پیامک وابسته نباشید.

در دوران قطعی، شبکه مخابراتی ممکن است با ترافیک سنگین یا اختلال مواجه شود و پیامک کد تایید با تاخیر برسد یا اصلا دریافت نشود. همچنین در صورت تعویض، مسدودشدن یا ازدست‌رفتن سیم‌کارت، دسترسی به پیامک‌های تایید نیز ممکن است از

بین برود.

برخی اطلاعات مربوط به پیامک نیز می‌تواند برای اپراتور یا نهادهای دارای دسترسی قانونی یا فنی قابل مشاهده باشد؛ بنابراین برای حساب‌های حساس، بهتر است از روش‌های امن‌تر و جایگزین برای احراز هویت استفاده کنید.

اپلیکیشن‌های احراز هویت دومرحله‌ای (Authenticator Apps)

اپلیکیشن‌های تایید هویت دومرحله‌ای مانند Google Authenticator و Aegis کدهای یک‌بارمصرف را کاملا آفلاین و مستقل از شبکه تلفن یا اینترنت تولید می‌کنند؛ این کدها بر پایه زمان ساخته می‌شوند و نیازی به پیامک یا اتصال اینترنت ندارند. برای فعال‌سازی، از بخش تنظیمات امنیتی هر سرویس (گوگل، ایمیل، شبکه اجتماعی) گزینه «احراز هویت دو مرحله‌ای با اپلیکیشن» را انتخاب کرده و کد QR نمایش داده‌شده را با اپلیکیشن اسکن کنید. اپلیکیشنی را انتخاب کنید که امکان پشتیبان‌گیری رمزگذاری‌شده و محلی داشته باشد، نه لزوما همگام‌سازی ابری، تا در صورت گم‌شدن یا تعویض گوشی، دسترسی از بین نرود.

کدهای پشتیبان (Backup Codes)

اکثر سرویس‌های مهم (گوگل، اینستاگرام، تلگرام، ایمیل و...) هنگام فعال‌سازی احراز هویت دو مرحله‌ای، مجموعه‌ای از کدهای پشتیبان یک‌بارمصرف ارائه می‌دهند؛ این کدها را از پیش، وقتی به اینترنت دسترسی دارید، دریافت و ذخیره کنید. بهترین شیوه نگهداری، چاپ یا نوشتن این کدها روی کاغذ و نگهداری در مکانی امن است؛ ذخیره در یک فایل متنی روی گوشی کافی نیست، چون در صورت مسدودشدن یا ضبط دستگاه در دسترس فرد دیگری قرار می‌گیرد.

کلید امنیتی فیزیکی و کلید عبور (Passkey)

کلیدهای فیزیکی مانند YubiKey برای حساب‌های حساس‌تر (مثل ایمیل اصلی) یک لایه امنیتی مستقل از شبکه موبایل فراهم می‌کنند و در برابر فیشینگ نیز مقاوم‌ترند. کلید عبور (Passkey) به جای رمز عبور و پیامک، از قفل تشخیص چهره یا اثر انگشت همان

دستگاه استفاده می‌کند و کاملا مستقل از شبکه مخابراتی عمل می‌کند.

نکات تکمیلی برای هر حساب مهم

- یک ایمیل بازیابی ثانویه که به شماره تلفن ایرانی وابسته نیست تنظیم کنید.
- پیش از وقوع قطعی اینترنت، یک بار روند ورود با کد پشتیبان یا اپلیکیشن احراز هویت را امتحان کنید تا در لحظه نیاز با مراحل آشنا باشید.
- حداقل از دو روش جایگزین (مثلا اپلیکیشن احراز هویت به علاوه کد پشتیبان) هم‌زمان استفاده کنید تا در صورت ازدست‌رفتن یکی، دیگری در دسترس باشد.

جمع‌بندی

امنیت دیجیتال، برخلاف تصور رایج، محصول یک اقدام یک‌باره نیست، بلکه نتیجه مجموعه‌ای از عادت‌های کوچک و مستمر است: قفل‌کردن گوشی با یک کد قوی، فعال نگه‌داشتن تایید دو مرحله‌ای، بررسی دوره‌ای مجوزهای اپلیکیشن‌ها و آمادگی از پیش برای شرایطی که دسترسی به اینترنت یا حتی گوشی همراه ممکن است در دسترس نباشد.

آنچه در این کتابچه ارائه شد، پوششی جامع بر هشت حوزه اصلی امنیت دیجیتال است؛ از محافظت از گوشی هوشمند و حساب‌های کاربری گرفته تا آمادگی برای بازرسی، تجمعات، و قطعی گسترده اینترنت. با این حال، تاکید می‌شود که هیچ یک از این اقدامات به تنهایی تضمین‌کننده امنیت کامل نیست؛ امنیت دیجیتال یک فرایند لایه‌ای است که هرچه بیش‌تر از پیش و به صورت پیشگیرانه اجرا شود، اثربخشی بیش‌تری خواهد داشت.

توجه به این نکته نیز ضروری است که امنیت فردی به تنهایی کافی نیست. همان‌گونه که در بخش امنیت خانواده و نزدیکان اشاره شد، خطر دیجیتال در میان نزدیکان منتقل و پخش می‌شود؛ به همین دلیل، هماهنگی و آگاهی‌بخشی به اعضای خانواده و نزدیکان، بخشی جدایی‌ناپذیر از یک رویکرد امنیتی مسئولانه است.

فناوری و روش‌های نظارتی به طور مداوم در حال تغییرند و به همین ترتیب، ابزارها و توصیه‌های امنیتی نیز نیازمند بازبینی و به‌روزرسانی دوره‌ای هستند. آنچه امروز یک راهکار

مطمئن تلقی می‌شود، ممکن است در آینده نیازمند بازنگری باشد؛ از این‌رو، پیگیری منابع معتبر و به‌روز در حوزه امنیت دیجیتال توصیه می‌شود.

در نهایت، هدف از تدوین این کتابچه، نه ایجاد نگرانی، بلکه توانمندسازی خواننده برای تصمیم‌گیری آگاهانه در فضای دیجیتال است. امید است این مجموعه بتواند گامی هرچند کوچک در جهت افزایش تاب‌آوری دیجیتال کاربران ایرانی در برابر قطعی‌های اینترنت، محدودیت‌ها و نظارت فزاینده باشد.

منابع برای مطالعه بیش‌تر

- راهنمای امنیت دیجیتال در زمان قطعی اینترنت
- ۵ اصل امنیت دیجیتال در خبررسانی
- امنیت دیجیتال در تبعید: توصیه‌هایی برای ایرانیان فعال در خبررسانی
- چک‌لیست امنیتی: امنیت دیجیتال برای کنشگران
- هشدار امنیتی هنگام خرید تجهیزات اینترنت استارلینک در ایران
- هشدار؛ پس از کلیک روی لینک مشکوک یا آلوده، چه باید کرد؟
- نگهداری از اسناد مهم: تهیه نسخه پشتیبان پیش از قطعی اینترنت
- نگهداری از حساب‌ها در دوران اختلال اینترنت: چهار جایگزین پیامک تایید هویت
- نقشه‌ها و ابزارهای آفلاین: آمادگی برای دوران قطعی اینترنت
- وی.پی.ان و کانفیگ: نکات امنیتی در دوران قطعی اینترنت
- هشدار امنیتی؛ کانفیگ‌های ناشناس VPN می‌توانند مستقیماً شما را به نهادهای امنیتی وصل کنند
- بازگشت از بازداشت؛ اولین قدم‌ها برای محافظت از اطلاعات شخصی
- وقتی فیلترشکن تله است؛ هشدار امنیتی برای فعالان و روزنامه‌نگاران
- پیام‌رسان‌های داخلی چگونه می‌توانند مسیر اتصال کاربران – از VPN تا استارلینک – را شناسایی کنند؟

- ایست بازرسی و گوشی‌های همراه؛ راهنمای سریع محافظت از حریم خصوصی
- از فیشینگ تا نفوذ حساب‌ها: چگونه در برابر حملات سایبری هدفمند ایمن بمانیم؟
- افزایش کلاهبرداری‌های فروش VPN در زمان قطع اینترنت؛ چگونه فریب نخوریم؟
- خطرات خرید کانفیگ‌های وی.پی.ان از منابع ناشناس
- چرا فعالان ایرانی خارج از کشور در شبکه‌های اجتماعی هدف شناسایی قرار می‌گیرند؟
- هشدار امنیتی: سوءاستفاده از قطع اینترنت برای نقض حریم خصوصی کاربران با اپ‌های مخرب
- افزایش امنیت با حذف اطلاعات پنهان عکس‌ها قبل از انتشار
- ۷ راه‌کار مهم برای حفظ حریم خصوصی، پیش از حضور در اعتراضات خیابانی