تو خیابان و قطعی‌ها

گوشی و حساب‌ها

گوشی‌تون رو طوری آماده کنید که اگه گرفتنش، نه شما لو برید نه بقیه.

مهم‌ترین سه کار

۱ **قفل اثر انگشت و تشخیص چهره رو قبل از بیرون رفتن خاموش کنید.**

۲ **حرف حساس رو فقط تو Signal با پیام‌های ناپدیدشونده بزنید.**

۳ **رمز و کد تأیید رو هیچ‌وقت تو صفحه‌ای که از لینک باز شده نزنید.**

این راهنما و همهٔ راهنماهای دیگه، رایگان، اینجاست:

iranuncensored.com/fa/ready/phone

یا این کد رو با دوربین گوشی اسکن کنید.

آخرین به‌روزرسانی: ۱ نوامبر ۲۰۲۶

۱ اصلاً گوشی ببرید؟



بی‌گوشی رفتن امن‌ترین حالته گوشی روشن، حتی بدون اینترنت، از راه دکل‌ها جاتون رو نشون می‌ده. اگه لازمش ندارید، خونه بذاریدش.



اگه می‌شه، یه گوشی دوم خالی یه گوشی ارزان یا قدیمی که توش ایمیل، شبکهٔ اجتماعی و عکس شخصی نیست. اگه گرفتنش، چیزی برای لو دادن نداره.



سیم‌کارت تازه شما رو پنهان نمی‌کنه سیم‌کارت‌ها با کد ملی ثبت می‌شن و اپراتور شمارهٔ سریال خود گوشی (IMEI) رو هم می‌بینه. سیم‌کارت تازه تو همون گوشی، همون گوشیه.



حالت هواپیما کافی نیست حالت هواپیما با وای‌فای، بلوتوث و موقعیت خاموش، ردیابی رو کم می‌کنه ولی صفر نمی‌کنه. مطمئن‌ترین راه نبردن گوشیه؛ بعدش خاموش کردن کامل.

۲ قفل و رمز گوشی



یه رمز قوی بذارید حداقل ۸ رقم، یا بهتر ترکیبی از حرف و عدد که حدس زدنش سخته. تاریخ تولد و ۱۲۳۴ رمز نیست.



اثر انگشت و چهره رو خاموش کنید انگشت یا صورت‌تون رو می‌شه به زور جلوی گوشی گرفت. قبل از بیرون رفتن، فقط باز کردن با رمز رو روشن بذارید.



رمز، رمزگذاری گوشی رو فعال می‌کنه آیفون و بیشتر گوشی‌های اندروید وقتی رمز دارن، اطلاعات رو رمزگذاری می‌کنن. ولی کارت حافظه معمولاً رمزگذاری نمی‌شه، پس چیز حساس روش نذارید.



از روی صفحهٔ قفل عکس بگیرید بیشتر گوشی‌ها دوربین رو بدون باز کردن قفل روشن می‌کنن. اینجوری اگه گوشی رو از دست‌تون قاپیدن، قفل می‌مونه.



قفل اضطراری رو یاد بگیرید آیفون: دکمهٔ کنار و یه دکمهٔ صدا رو ۲ ثانیه نگه دارید و Cancel بزنید؛ تا رمز نزنید چهره کار نمی‌کنه. بیشتر نگه ندارید، تماس اضطراری می‌گیره. اندروید: پاور رو نگه دارید و Lockdown رو بزنید. تو خیلی از گوشی‌ها، مثل سامسونگ، این گزینه اول باید از تنظیمات قفل صفحه (Show Lockdown option) روشن بشه؛ از قبل امتحانش کنید.



جای خطرناک، گوشی رو خاموش کنید گوشی‌ای که خاموش شده و هنوز رمزش زده نشده، اطلاعاتش کامل قفله و باز کردنش خیلی سخت‌تره. قبل از ایست بازرسی یا وقتی خطر بازداشت هست، خاموشش کنید.

۳ پیام‌رسان‌ها



Signal با پیام‌های ناپدیدشونده Signal پیام و تماس رو سرتاسری رمزگذاری می‌کنه. پیام‌های ناپدیدشونده و قفل ثبت‌نام (Registration Lock) رو روشن کنید تا کسی نتونه با شماره‌تون حساب‌تون رو بگیره. Signal تو ایران فیلتره؛ با فیلترشکن یا پراکسی Signal وصل بشید.



پیام ناپدیدشونده هم محدودیت داره فقط پیام‌های بعد از روشن کردنش پاک می‌شن. طرف مقابل می‌تونه اسکرین‌شات بگیره، و اگه گوشی اون رو زودتر بگیرن، پیام‌ها هنوز اونجاست.



چت معمولی تلگرام سرتاسری رمزگذاری نمی‌شه تو تلگرام فقط «چت مخفی» (Secret Chat) سرتاسریه. گروه‌ها و چت‌های معمولی روی سرور تلگرام می‌مونن. رمز دومرحله‌ای بذارید، چون کد ورود با پیامک از اپراتور رد می‌شه.



WhatsApp: پیام رمزگذاری‌شده، پشتیبان نه پیام‌ها و تماس‌های WhatsApp سرتاسری رمزگذاری می‌شن، ولی پشتیبانش تو Google Drive یا iCloud پیش‌فرض نه. تو بخش Chat backup، گزینهٔ End-to-end encrypted backup رو روشن کنید.

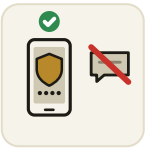


روبیکا، ایتا و بله رو زیر نظر بدونید این پیام‌رسان‌ها داخلی‌ان و روی شبکه‌ای کار می‌کنن که رژیم کنترلش رو داره. هیچ حرف حساسی اونجا نزنید.



اسم واقعی آدم‌ها رو ذخیره نکنید فعال‌ها و آدم‌های حساس رو با یه اسم مستعار ذخیره کنید که فقط خودتون بفهمید. دفترچهٔ تلفن از اولین جاهاییه که می‌گردن.

۴ حساب‌هاتون رو قفل کنید



تأیید دومرحله‌ای رو روشن کنید برای ایمیل، تلگرام، اینستاگرام و بقیه. اگه می‌شه برنامهٔ کدساز (Authenticator) رو به جای پیامک انتخاب کنید، چون پیامک از اپراتورهای وابسته به رژیم رد می‌شه.



از حساب‌های غیرلازم خارج بشید تو گوشی‌ای که بیرون می‌برید، فقط حساب‌هایی باشه که لازم دارید. اگه گوشی باز شد، همه چیزتون دست‌شون نمی‌افته.



گالری و چت‌ها رو مرتب پاک کنید عکس، فیلم و پیامی که نمی‌خواید کسی ببینه رو قبل از بیرون رفتن پاک کنید. سطل زبالهٔ گالری رو هم خالی کنید.



تاریخچهٔ موقعیت مکانی رو خاموش کنید تاریخچهٔ مکان گوگل و هر برنامه‌ای که جای شما رو ثبت می‌کنه، خاموش و پاک کنید. این فهرست دقیق رفت و آمدتونه.



قبلش پشتیبان بگیرید اگه گوشی رو گرفتن یا مجبور شدید پاکش کنید، عکس‌ها و شماره‌های لازم از بین نره. پشتیبان رو جای امن و رمزدار نگه دارید.

۵ لینک‌ها و برنامه‌های تقلبی



هکرهای وابسته به رژیم فعال‌ها رو هدف می‌گیرن گروهی به اسم APT42 یا Charming Kitten، که به سپاه نسبت داده می‌شه، تو ۱۴۰۱ با دعوت‌نامهٔ جعلی تو WhatsApp و صفحهٔ ورود تقلبی ایمیل فعال‌ها رو هک کرد.



رمز رو فقط تو سایتی که خودتون باز کردید بزنید صفحه‌های تقلبی شبیه گوگل و مایکروسافت ساخته می‌شن و حتی کد دومرحله‌ای رو هم می‌دزدن. روی لینک نزنید؛ خودتون آدرس سایت رو باز کنید.



VPN و برنامه رو فقط از منبع رسمی بگیرید برنامه‌ای که با لینک تو پیامک یا گروه دست‌به‌دست می‌شه ممکنه بدافزار باشه. فقط از فروشگاه رسمی یا سایت خود سازنده نصب کنید.

هیچ‌وقت کدی که براتون پیامک شده رو به کسی یا تو صفحه‌ای که از لینک باز شده ندید.

۶ اگه گوشی رو گرفتن



از قبل تصمیم بگیرید چی کار کنید تو بازداشت ممکنه رمز گوشی رو با تهدید بخوان و ندادنش فشار بیشتری بیاره. بهترین راه اینه که از قبل تو گوشی چیزی نباشه که کسی رو گرفتار کنه.



رمز حساب‌ها رو از یه دستگاه دیگه عوض کنید خودتون یا یه آدم مطمئن، از یه دستگاه دیگه رمز ایمیل و پیام‌رسان‌ها رو عوض کنید و از همهٔ دستگاه‌های وصل خارج بشید.



به آدم‌هایی که باهاشون حرف زدید خبر بدید اگه گوشی‌تون دست مأمورها افتاد، به کسایی که باهاشون در ارتباط بودید بگید تا مراقب باشن و پیام‌ها رو پاک کنن.

درست یا غلط؟

باور غلط **«سیم‌کارت تازه تو همون گوشی یعنی ناشناس شدم.»**
درستش نه. اپراتور شمارهٔ سریال خود گوشی رو هم می‌بینه و سیم‌کارت‌ها هم با کد ملی ثبت می‌شن.

باور غلط **«تلگرام کامل رمزگذاری شده.»**
درستش فقط «چت مخفی» سرتاسری رمزگذاری می‌شه. چت‌ها و گروه‌های معمولی روی سرور تلگرام هستن.

باور غلط **«تأیید دومرحله‌ای دارم، پس هک نمی‌شم.»**
درستش خیلی کمک می‌کنه، ولی صفحه‌های تقلبی کد رو هم می‌دزدن. کلید امنیتی سخت‌افزاری (Security Key) جلوی این ترفند رو می‌گیره. کد رو فقط تو برنامه یا سایتی بزنید که خودتون باز کردید.

باور غلط **«اثر انگشت از رمز امن‌تره.»**
درستش برای روزهای عادی راحته، ولی انگشت و صورت رو می‌شه به زور جلوی گوشی گرفت. برای بیرون رفتن، فقط رمز.

فهرست آماده‌شدن

- [ ] اثر انگشت و تشخیص چهره رو خاموش کردم
- [ ] رمز گوشی حداقل ۸ رقم یا حرف و عدده
- [ ] Signal نصبه و پیام‌های ناپدیدشونده روشنه

- [ ] تأیید دومرحله‌ای ایمیل، تلگرام و اینستاگرام روشنه
- [ ] اسم آدم‌های حساس تو گوشی مستعاره
- [ ] عکس‌ها و چت‌های حساس و سطل زباله رو پاک کردم
- [ ] تاریخچهٔ موقعیت مکانی خاموش و پاکه
- [ ] از اطلاعات لازم پشتیبان امن و رمزدار دارم
- [ ] از حساب‌هایی که بیرون لازم ندارم خارج شدم
- [ ] قفل اضطراری گوشی‌م رو یاد گرفتم و تمرین کردم

سه تمرین

جواب‌ها آخر فایله.

۱. یه پیام WhatsApp از یه «مؤسسهٔ پژوهشی» میاد که شما رو به یه همایش دعوت می‌کنه و برای دیدن برنامه، لینک ورود به جیمیل می‌ده. چی کار می‌کنید؟

الف) لینک رو باز می‌کنید، چون تأیید دومرحله‌ای دارید و مشکلی پیش نمیاد

ب) لینک رو نمی‌زنید و از یه راه مستقل، مثلاً سایت رسمی خودشون، درستیش رو چک می‌کنید

ج) از فرستنده می‌خواید برنامه رو فایل کنه و فایل رو باز می‌کنید

۲. فردا می‌خواید برید بیرون. گوشی‌تون با چهره باز می‌شه و توش عکس‌های تجمع‌های قبلیه. چی کار می‌کنید؟

الف) تشخیص چهره رو خاموش می‌کنید، عکس‌ها رو جای امن می‌فرستید و از گوشی و سطل زباله پاک می‌کنید

ب) فقط گوشی رو روی حالت هواپیما می‌ذارید

ج) عکس‌ها رو تو یه پوشهٔ مخفی گالری می‌ذارید

۳. دوستتون می‌خواد یه سیم‌کارت تازه تو گوشی خودش بذاره و با خیال راحت بره بیرون. چی کار می‌کنید؟

الف) بهش می‌گید فکر خوبیه، فقط سیم‌کارت به اسم یکی دیگه باشه

ب) بهش می‌گید خود گوشی هم شناسه داره؛ یا گوشی نبره یا یه گوشی دوم خالی ببره

ج) بهش می‌گید فقط وای‌فای رو خاموش کنه کافیه

منبع‌ها

EFF Surveillance Self-Defense, Attending a Protest
https://ssd.eff.org/module/attending-protest

Telegram FAQ (cloud chats vs Secret Chats encryption)
https://telegram.org/faq

Human Rights Watch, Iran: State-Backed Hacking of Activists, Journalists, Politicians (Dec 2022)
https://www.hrw.org/news/2022/12/05/iran-state-backed-hacking-activists-journalists-politicians

The Intercept, Hacked Documents: How Iran Can Track and Control Protesters' Phones (Oct 2022)
https://theintercept.com/2022/10/28/iran-protests-phone-surveillance/

Apple Support, About Face ID advanced technology (when a passcode is required)
https://support.apple.com/en-us/102381

Signal, Help users in Iran reconnect to Signal (proxy)
https://signal.org/blog/help-iran-reconnect/

How-To Geek, How to use Lockdown mode on Android
https://www.howtogeek.com/806113/how-to-use-lockdown-mode-on-android/

جواب تمرین‌ها

۱. ب) لینک رو نمی‌زنید و از یه راه مستقل، مثلاً سایت رسمی خودشون، درستیش رو چک می‌کنید. دقیقاً همین ترفند رو APT42 تو ۱۴۰۱ زد. صفحه‌های تقلبی کد دومرحله‌ای رو هم می‌گیرن. فایل ناشناس هم می‌تونه بدافزار باشه. فقط از راه مستقل چک کنید.

۲. الف) تشخیص چهره رو خاموش می‌کنید، عکس‌ها رو جای امن می‌فرستید و از گوشی و سطل زباله پاک می‌کنید. صورت‌تون رو می‌شه به زور جلوی گوشی گرفت. پوشهٔ مخفی رو هر کسی که گوشی دستشه پیدا می‌کنه. حالت هواپیما هم چیزی از توی گوشی پاک نمی‌کنه.

۳. ب) بهش می‌گید خود گوشی هم شناسه داره؛ یا گوشی نبره یا یه گوشی دوم خالی ببره. اپراتور شمارهٔ سریال گوشی رو می‌بینه، پس سیم‌کارت تازه تو همون گوشی ردش رو قطع نمی‌کنه. سیم‌کارت به اسم یکی دیگه هم اون آدم رو گرفتار می‌کنه.

ایران بدون سانسور

راهنمای ایمنی برای روزهای سخت

همهٔ راهنماهای «آماده باشیم»

همه‌شون رایگان و به فارسی. هر کدوم که لازم دارید رو بخونید و برای خانواده و دوست‌هاتون بفرستید.

اگه حمله شد

- نقشهٔ خانواده از همین امروز
- کیف اضطراری و ذخیرهٔ خونه
- وقت حمله کجا پناه بگیرید
- بعد از یه انفجار نزدیک
- رفتن از شهر، کی و چطور
- دود، مواد شیمیایی و تأسیسات هسته‌ای

تو خیابان و قطعی‌ها

- امن موندن تو تجمع
- **گوشی و حساب‌ها**
- وقتی اینترنت قطع می‌شه
- بازداشت: شما و خانواده
- فیلم گرفتن امن
- خبر درست، شایعهٔ دروغ

کمک‌های اولیه و زندگی

- کمک‌های اولیه برای نجات جان
- آتش، گاز و برق تو خونه
- آب، غذا و بهداشت وقت قطعی
- آرامش ذهن، بچه‌ها و سالمندها
- همسایه‌ها و ساختمان، با هم

همهٔ راهنماها، رایگان و به فارسی:

iranuncensored.com/fa/ready

یا این کد رو با دوربین گوشی اسکن کنید.