مقدمه

با واژهٔ حریم خصوصی غریبه نیستیم. مدافع‌های زیادی داره، اهمیت و نیازش هنوز برای عموم روشن نیست، و از دید بسیاری برابره با پنهان‌کردن چیزهای بد. جوامع و حکومت‌های مدرن مدام درتلاشن این تصویر دورازحقیقت رو در ذهن افراد نهادینه کنن. اینجا لازمه از خودتون بپرسید چرا.

این فهرست، تهیه‌شده توسط 6102bitcoin، برای اون دسته از افراده که به اهمیت موضوع واقفن و دوست دارن آگاهانه‌تر، با دغدغهٔ کمتر نسبت به نقض حریم خصوصی و آزادی‌شون، در عصر دیجیتال زندگی کنن. راجع به هر مورد و دلیل وجودش در لیست فکر کنید. دوست دارید یک مرحله فراتر برید؟ بسیار عالی؛ راجع به هرکدوم جداگونه تحقیق کنید.

۱. از لینوکس استفاده کنید

مشاهدهٔ ویدئوی معرفی سیستم عامل Tails در توئیتر؛ کاری از استودیو ویویدو، با همکاری نیما فاطمی

۲. از گوگل اجتناب کنید (چرا؟)

درعوض، از DuckDuckGo استفاده کنید.

۳. از تلفن‌های burner استفاده کنید

این مورد به سادگی خرید یک تلفن ارزون‌قیمت و سیم‌کارت بدون‌هویت نیست. نحوهٔ خرید و پرداخت شما—در کنار عوامل دیگه—مهمه. این ویدئو، با ته‌مایهٔ طنز، شما رو با ذهنیت موردنیاز برای این کار آشنا می‌کنه، و می‌تونه الهام‌بخش باشه.

۴. از مسدودکنندهٔ تبلیغات (ad blocker) استفاده کنید

هدف تنها این نیست که کمتر تبلیغ ببینید. افزونهٔ uBlock Origin رو پیشنهاد می‌کنم. جلوتر درمورد ابزارها و افزونه‌های دیگه‌ای که می‌تونید همراه با مرورگرتون استفاده کنید صحبت خواهیم کرد.

👈 نصب افزونهٔ فایرفاکس

۵. از وی‌پی‌ان استفاده کنید

در وهلهٔ اول، اطمینان حاصل کنید از وی‌پی‌انی استفاده می‌کنید که قابل‌اعتماده. اگه از سایت‌های فارسی‌زبان داخلی اشتراک تهیه می‌کنید، نیازه در این تصمیم بازبینی کنید.

آیا وی‌پی‌ان‌ها/فیلترشکن‌هایی که در ایران فروخته می‌شوند، قابل‌اطمینان هستند؟ 👈

سرویس‌دهندهٔ وی‌پی‌ان شما می‌تونه ببینه از چه سایت‌هایی بازدید می‌کنید. (تصویر: ProtonVPN) 👇

در وهلهٔ دوم، اطمینان حاصل کنید وی‌پی‌انی که استفاده می‌کنید نشت (leak) نداره. درضمن، درنظر داشته باشید منطقهٔ زمانی شما به‌راحتی قابل‌تشخیصه.

- 👈 بررسی نشت آی‌پی
- 👈 بررسی نشت WebRTC؛ اطلاعات بیشتر
- 👈 بررسی منطقهٔ زمانی

۶. از تور استفاده کنید

معرفی سرویس تور در یوتیوب

معرفی و آموزش راه‌اندازی سرویس تور در یوتیوب

در ویدئوی بالا، کاری از استودیو کج‌آرت با همکاری نیما فاطمی، از اعضای اصلی تیم پروژهٔ تور، کوتاه با کاربرد این سرویس ارزشمند آشنا می‌شید. من هم در ویدئویی مفصل‌تر به معرفی و استفاده ازش می‌پردازم.

۷. اگه از شخص ناشناسی لینک دریافت کردید، بازش نکنید

اینترنت جای خطرناکیه. با احتیاط بیشتری رفت‌وآمد کنید. درمقابل، اگه در موقعیت ارسال پیام هستید و شخص مقابل شما رو نمی‌شناسه، تاحدامکان از قراردادن لینک و ضمیمه اجتناب کنید. به‌قولی، آداب و رسوم اینترنتی (netiquette) رو رعایت کنید.

۸. به تماس‌های ناشناس جواب ندید

به‌شخصه، سال‌هاست که این روش رو پیش گرفته‌م. یک ادب خوب، از دید من، اینه که همیشه خودتون رو در نقطهٔ مقابل هم قرار بدید. اگه قراره با کسی تماس بگیرید که شما رو نمی‌شناسه، مؤدبانه‌ست که قبلش خبر بدید، حتی با یک پیام. اون شخص موظف به پاسخ‌دادن به تماس شما نیست.

۹. از روش‌های مناسب برای برقراری ارتباط استفاده کنید

از Keybase، Signal، و نرم‌افزارهایی استفاده کنید که رمزنگاری سرتاسر (end-to-end encryption) دارن. بیشتر مکالمه‌های روزمرهٔ من در فضای E2EE اتفاق می‌افته. درمورد اهمیت رمزنگاری در مکالمه‌ها اینجا بخونید.

برای مثال، توئیتر مکان مناسبی برای داشتن یک مکالمهٔ مهم نیست. پیام‌های ردوبدل‌شده نه E2EE هستن و نه ازبین می‌رن. اطلاعاتی که در پیام خصوصی با دوستی به‌اشتراک می‌ذارید یا عکسی که برای یک غریبه می‌فرستید نه‌تنها قابل‌حذف نیستن بلکه درصورت دسترسی شخص سومی به حساب شما یا دیگری می‌تونن خطرناک هم باشن.

درنتیجه، همیشه سعی کنید مکالمه رو به کانال امن‌تری سوق بدید.

یکی از روش‌هایی که کنترل بیشتری روی مکالمه در توئیتر (و پلتفرم‌های دیگه) به شما می‌ده استفاده از ابزار Pastebin است. می‌تونید پیامی رو نوشته و انقضای اون رو burn after read قرار بدید تا یک‌بارمصرف باشه.

۱۰. از شبکه‌های اجتماعی با نام و هویت واقعی‌تون استفاده نکنید

شبه‌ناشناسی (pseudonymity) مزیت‌های خودش رو داره—اگه به‌درستی پیاده بشه—و می‌تونه در حفظ حریم خصوصی شما بسیار مؤثر باشه.

ممکنه براتون جالب باشه که «مقاله‌های فدرالیست» با نام مستعار پوبلیوس (Publius) امضا و منتشر شدن.

۱۱. حواستون به میکروفون‌های همیشه‌فعال (always-on) باشه

شاید همه خونهٔ هوشمند نداشته باشن، اما خیلی‌ها از Siri، Google Assistant، و ابزارهای مشابه استفاده می‌کنن. همیشه نمی‌شه سهولت و حریم خصوصی رو درکنارهم داشت. این موضوع که همهٔ دستگاه‌هامون می‌تونن به ما گوش بدن واقعیتی ترسناک اما درحال‌اتفاقه.

۱۲. تاحدامکان از پول نقد استفاده کنید

«حریم خصوصی این روزها یک کالای لوکس است که هر روز گران‌تر می‌شود.» —کتاب کوچک بیت‌کوین

درمورد پول، کارکردش، و ضعف‌هاش در فصل اول این کتاب فوق‌العاده بخونید یا بشنوید.

۱۳. عکس آپلود نکنید

هوشمند عمل کنید. قبل از ارسال هر چیزی روی اینترنت به عواقب احتمالی‌اش فکر کنید. چیزی رو نشر ندید که در آینده بخواید به حذفش فکر کنید.

۱۴. از گذرواژه‌های قوی استفاده کنید

از چیزهایی مثل 1Password و LastPass—یا iCloud Keychain درصورتی‌که کاربر آی‌اواس هستید—دوری کنید. درمقابل، از نرم‌افزارهای متن‌باز و آزادی مثل KeePassXC یا Bitwarden استفاده کنید.

👈 اطلاعات بیشتر درمورد نرم‌افزارهای مدیریت گذرواژه

۱۵. از احراز هویت دوعاملی (two-factor authentication) استفاده کنید

در فعال‌کردن 2FA شک نکنید. لزومی به استفاده از Google Authenticator نیست؛ جایگزین‌های متن‌باز رو امتحان کنید، مثل andOTP. هرگز از روش پیامک (SMS) استفاده نکنید چون از امنیت کافی برخودار نیست.

۱۶. وب‌کم (یا دوربین) رو پوشونده، غیرفعال کرده، یا درصورت‌امکان دربیارید؛ میکروفون رو قطع یا غیرفعال کرده یا به‌کلی جدا کنید

برای اینکه اهمیت این موضوع رو بهتر درک کنید، مستند کوتاه State of Surveillance (دولت نظارت) رو ببینید.

فرقی نمی‌کنه اگه دسترسی‌های موقعیت مکانی رو غیرفعال کرده باشید، فرقی نمی‌کنه به اینترنت و وای‌فای متصل باشید یا نه؛ تا زمانی که تلفن همراه شما روشنه، در شبکه حضور دارید.

۱۷. از اینترنت عمومی استفاده نکنید

دفعهٔ بعد که خواستید به وای‌فای مجانی کافهٔ موردعلاقه‌تون وصل بشید، بیشتر فکر کنید.

مشاهدهٔ ویدئو در توئیتر

۱۸. اطلاعات شخصی خودتون رو دراختیار عموم قرار ندید

علاوه‌براینکه لزومی نداره افراد، به‌خصوص غریبه‌ها، راجع به جزئی‌ترین چیزهای زندگی شما بدونن، با به‌اشتراک‌گذاری (یا درز ناخواستهٔ) چنین اطلاعاتی شما یکی از بزرگ‌ترین ریسک‌های آنلاین رو متحمل می‌شید.

مشاهدهٔ ویدئو در توئیتر

اگه غریبه‌ای رو در خیابون ببینید و از شما درمورد اطلاعات شخصی‌تون سؤال کنه، چه جوابی بهش می‌دید؟ آیا نام کامل، تاریخ تولد، شماره، محل سکونت، و سابقهٔ کاری‌تون رو دراختیارش می‌ذارید، یا مردد می‌شید و قبلش فکر می‌کنید؟ به همین ترتیب، اگه چیزی در اینترنت منتشر می‌کنید، هرکسی می‌تونه اون رو ببینه.

این می‌تونه امتدادی از نکتهٔ بالاتر درمورد انتشار عکس باشه: حتی اگه عکس یا اسکرین‌شاتی به‌اشتراک می‌ذارید، توجه داشته باشید که اطلاعات مهم رو از معرض دید پاک کنید. اطمینان حاصل کنید که این کار رو درست انجام داده‌اید. این مقاله تلنگر خوبیه.

قبل از پرداختن به موضوع بعدی و برای اینکه استراحت کوتاهی هم کرده باشیم، می‌خوام اشاره کنم که من می‌دونم از دید کسی که دغدغهٔ مشابهی نداره، این‌ها ممکنه شعارگونه به‌نظر بیان، اما من به همهٔ موارد لیست معتقدم، و تلاش کرده‌م و می کنم بهشون پایبند باشم.

این‌ها همه پیشنهادن؛ اجباری در انجام هیچ‌کدوم نیست. هرکسی آزاده هرطور که علاقه داره زندگی کنه، و من به تصمیم همهٔ افراد احترام می‌ذارم. اگه دوست دارید آزادانه در شبکه‌های اجتماعی سیر کنید، بدون دغدغه عکس و ویدئو منتشر کنید، و نگران موضوع‌های مطرح‌شده در این مقاله نباشید، تشویقتون هم می کنم.

به اعتقاد من، از دو چیز باید به‌دور بود: حاشیه و تعصب. همه عاقل و بالغ هستیم، و می‌تونیم برای خودمون تصمیم بگیریم. ضمن اینکه تجربهٔ من نشون داده شما نمی‌تونید کسی رو مجبور به انجام کاری بکنید. اون شخص خودش باید به درک از اون نیاز برسه. تا اون زمان، کاری از دست شما ساخته نیست.

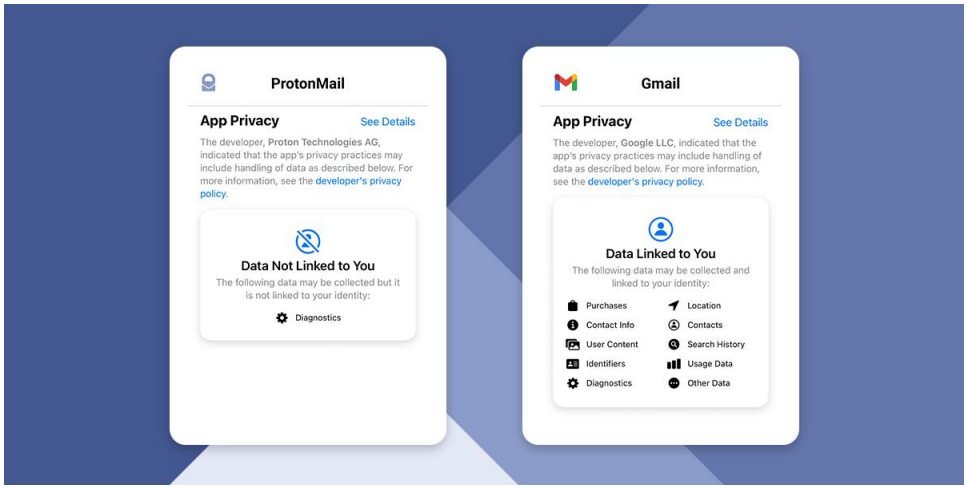
۱۹. از ایمیل‌های موقت استفاده کنید

ایمیل واقعاً راه ارتباطی امنی نیست. جلوتر بعد به نشت داده اشاره می‌کنم، و خواهید دید که درز اطلاعات چطور می‌تونه امنیت و حریم خصوصی شما رو به‌خطر بی‌اندازه.

👈 سرویس Temp Mail یا Email on Deck

می‌تونید سرویس‌های دیگه رو جستجو کنید.

اما اگه به آدرس ایمیل نیاز دارید، از سرویس‌هایی استفاده کنید که به حریم خصوصی شما احترام می‌ذارن. جی‌میل، یاهو، و غیره رو کنار بذارید. (اگه نیازه، تحقیق کنید چرا باید کنارشون بذارید.) پروتون‌میل یکی از گزینه‌های خوبه که می‌تونید بهش مهاجرت کنید.



مقایسهٔ حریم خصوصی اپ‌های پروتون‌میل و جی‌میل در آی‌اواس (تصویر: ProtonMail)

در مقاله‌ای مجزا به معرفی و بررسی سرویس پروتون‌میل پرداخته شده. اگه قصد دارید بررسی‌اش کنید، می‌تونه شروع خوبی باشه. اینجا مطالعه‌ش کنید.

۲۰. از فایرفاکس استفاده کنید

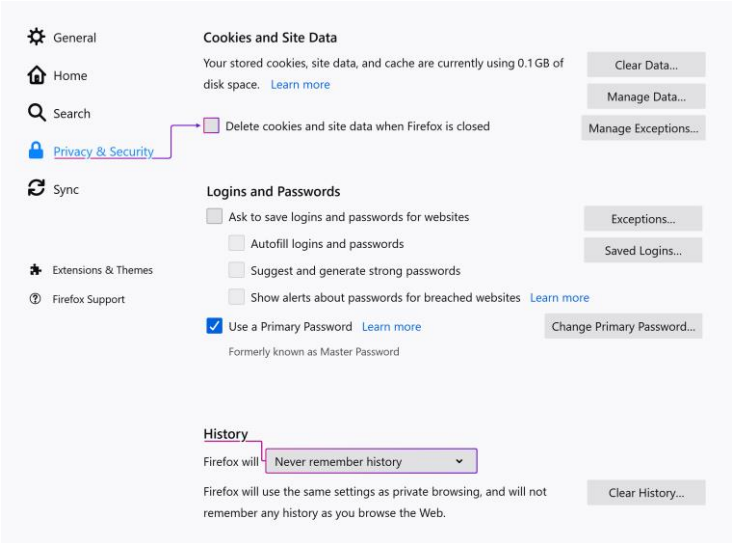
مهاجرت سخت اما ضروریه. فرقی نمی‌کنه کاربر ویندوز هستید، مک، یا لینوکس؛ فایرفاکس برای هر سه موجوده. نگران بوکمارک‌ها و لاگین‌هاتون هستید؟ به‌راحتی می‌تونید از هر مرورگری به فایرفاکس انتقال بدید. اگه هنوز از کروم و سافاری استفاده می‌کنید، وقتشه قدم بعدی رو بردارید.

نرم‌افزارهای جایگزین برای حفظ بهتر و بیشتر حریم خصوصی (تصویر: ₿itcoin Q+A)

در مقاله‌ای مجزا به معرفی نکات حریم خصوصی، ابزارها، و ترفندهای فایرفاکس پرداخته شده. اینجا مطالعه‌ش کنید.

۲۱. تاریخچهٔ وبگردی و کوکی‌ها رو خودکار پاک کنید

درمورد کوکی‌ها بخونید. کارشون؟ به‌خاطرسپردن تنظیمات، اطلاعات ورود، اطلاعات واردشده در فرم‌ها، و غیره. به‌لطف کوکی‌ها، با بستن و بازکردن مرورگر نیازی به ورود دوباره در سایت‌ها نیست. اما کوکی‌هایی هم هستن که شما رو دنبال (track) می‌کنن.



افزونهٔ Cookie AutoDelete می‌تونه کار شما رو راحت کنه.

پیشنهاد می‌کنم سری به تنظیمات حریم خصوصی و امنیت مرورگر هم بزنید.

۲۲. اگه قدیمیه و امتحان خودش رو پس داده، مثل PGP، ازش استفاده کنید؛ اگه تازه‌ست و پرطرفدار، احتیاط کنید

در دو مقالهٔ مجزا به رمزنگاری کلید عمومی RSA و آموزش جامع نرم‌افزار PGP پرداخته شده. مقالهٔ اول پیش‌نیاز دومیه. پیشنهاد می‌شه مطالعه کنید.

۲۳. به‌طور مداوم سیستم عامل دستگاهتون رو حذف و دوباره نصب کنید

هارد دیسک‌ها و اس‌اس‌دی‌ها رو قبل از دورانداختن حتماً به‌صورت فیزیکی ازبین ببرید.

سکانسی در سریال مستر ربات؛ الیوت، شخصیت اصلی، تمام حافظه‌های ذخیره‌سازی خودش رو ازبین می‌بره

۲۴. تلفن همراهتون رو در کشو قرار بدید

خاموش‌بودن به‌معنای خاموشی کامل نیست.

۲۵. هرگز حافظه‌های فلش ناشناخته رو به دستگاهتون وصل نکنید

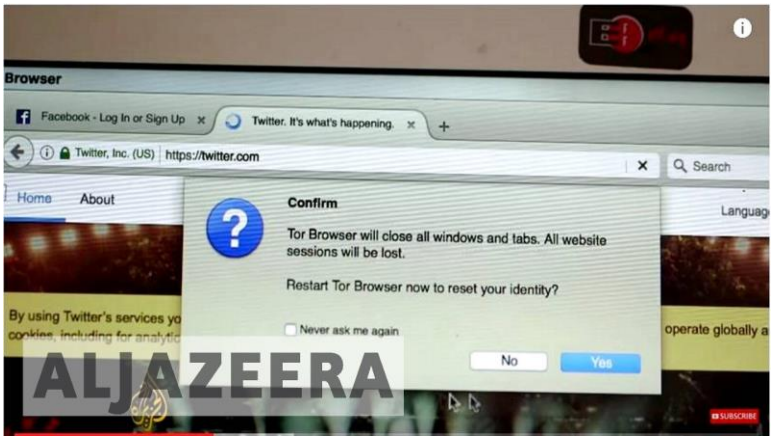
روشی جالب جهت محافظت از حافظه‌های فلش (تصویر: توئیتر)

۲۶. کتاب بخونید (ترجیحاً فیزیکی تا دیجیتال)

کتاب و مقاله بخونید، و سعی کنید مدام به دانشتون در این زمینه (و هر زمینهٔ مهم دیگه‌ای) اضافه کنید. این مهم‌ترین اصله.

۲۷. تاحدامکان از پیامک و تلفن استفاده نکنید

یکی از نکات جالبی که در ویدئوی زیر بهش اشاره می‌شه استفاده از دستگاهی مثل آی‌پاد به جای تلفن همراهه. از امکانات یک گوشی هوشمند بهره‌مندید، منهای قابلیت برقراری تماس و ارسال پیامک. ویدئو رو برای اطلاعات بیشتر ببینید.



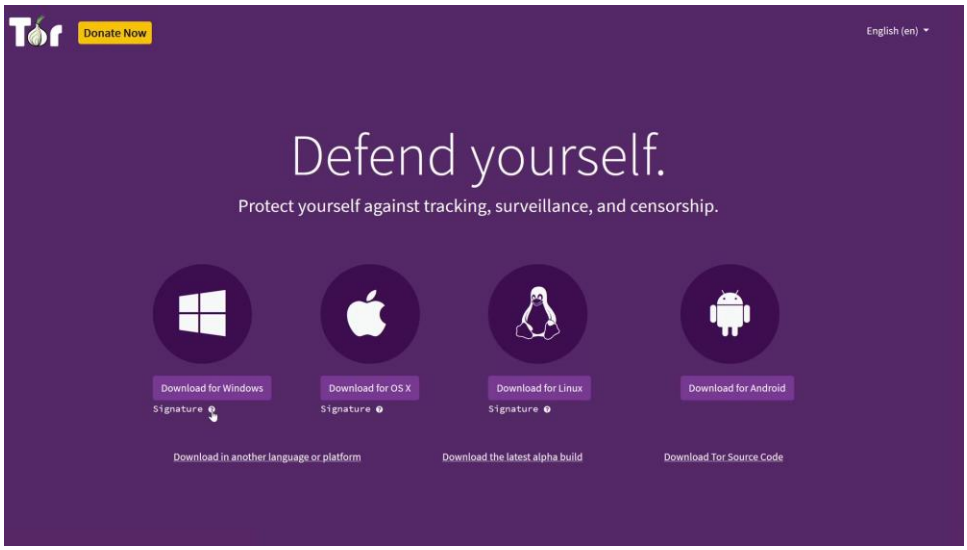
مشاهده در یوتیوب

۲۸. فرض کنید همه‌چیز ثبت (log) می‌شه

وقتی با این ذهنیت پیش می‌رید، آگاهانه‌تر عمل می‌کنید، می‌نویسید، و حرف می‌زنید. این مقاله رو برای اطلاعات بیشتر بخونید.

۲۹. نرم‌افزارهای ناشناخته رو نصب نکنید

حتماً صحت امضای نرم‌افزار رو درصورت وجود احراز و، البته، قبل از واردکردن کلید سازندهٔ نرم‌افزار از اصالت اون اطمینان حاصل کنید. به‌قولی، "don't trust, verify" اینجا بسیار حائزاهمیته. برای اطلاعات بیشتر درمورد احراز و اصالت‌سنجی نرم‌افزارها به راهنمای جامع PGP رجوع کنید.



آموزش تصویری اصالت‌سنجی فایل‌ها در یوتیوب

۳۰. نرم‌افزارهای ناشناخته رو در محیط ماشین مجازی (virtual machine) اجرا کنید

اجرای نرم‌افزارها در محیط ماشین مجازی امکان بروز خطر رو تا حد زیادی کاهش می‌ده. مفهوم sandbox و ابزارهایی مثل Sandboxie هم بسیار کارآمدن. درموردشون بخونید.

۳۱. قانون رو زیرپا نذارید

انجام کارهای غیرقانونی توجه افراد و سازمان‌ها رو به شما جلب می‌کنه—به همین سادگی.

۳۲. نسخهٔ پشتیبان (backup) تهیه کنید؛ صحت نسخهٔ پشتیبان رو بررسی کنید

توجه کنید که نسخهٔ پشتیبانی که بررسی و صحت‌سنجی نشده، درواقع نسخهٔ پشتیبان نیست.

۳۳. و به‌عنوان نکته‌های آخر . . .

دیرباور باشید، هرچیزی رو تا زمانی که اصالتش رو احراز نکرده‌اید قبول نکنید، برنامه‌نویسی یاد بگیرید، و سؤال بپرسید. حتماً سؤال بپرسید.

راهنماهای مرتبط

رمزنگاری کلید عمومی RSA

راهنمای جامع نرم‌افزار PGP

فایرفاکس: حریم خصوصی، ابزارها، و ترفندها

معرفی ProtonMail: حریم خصوصی و امنیت