ایمن‌سازی دستگاه‌های خود

این منبع برخی از گام‌های عملی اولیه را برای ایمن‌سازی دستگاه‌ها در برابر انواع رایج ردیابی دستگاه ارائه می‌دهد و اقداماتی مانند خاموش کردن Bluetooth، WiFi و اشتراک‌گذاری موقعیت‌مکانی؛ تغییرنام دستگاه‌هایتان؛ بررسی وجود جاسوس‌افزار و مجوزهای برنامه‌ها؛ و انجام بازنشانی به تنظیمات کارخانه را پوشش می‌دهد.

این‌ها نکات کلی برای ایمن نگه داشتن دستگاه‌های شما هستند. ممکن است مراحل دقیق برای دستگاه‌های مختلف متفاوت باشد و با گذشت زمان تغییر کند.

در iPhone و iPad، معمولاً می‌توانید با ضربه زدن روی آیکون "تنظیمات" در صفحه اصلی و سپس کشیدن انگشتتان به سمت پایین برای نمایش نوار جستجو، تنظیمی را پیدا کنید. (جهت یافتن راهنما، به http://tiny.cc/iphonesearch مراجعه کنید.)

در دستگاه‌های Android، انگشتتان را از صفحه اصلی به سمت بالا بکشید: نوار جستجویی ظاهر می‌شود که می‌گوید "جستجوی تلفن خود و موارد بیشتر". تنظیمی را که به دنبال آن هستید در نوار جستجو تایپ کنید.

در زمان عدم استفاده از Bluetooth و WiFi، آن‌ها خاموش کنید.

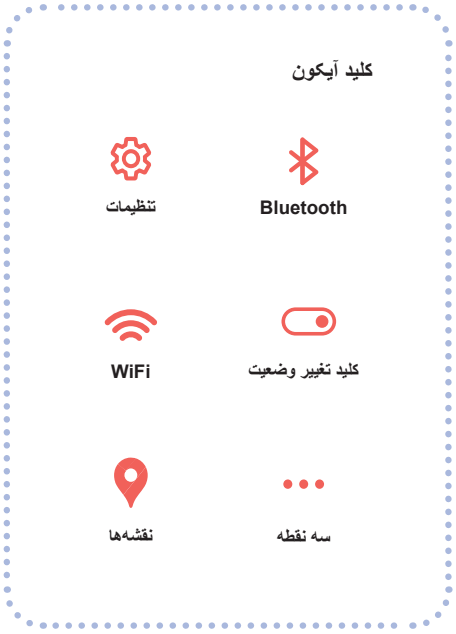
Bluetooth و WiFi دستگاهتان را برای دستگاه‌های دیگر قابل مشاهده می‌کنند. در زمان عدم استفاده از آن‌ها، با رفتن به **تنظیمات** یا ضربه زدن روی آیکون‌های **Bluetooth** و **WiFi** آن‌ها را خاموش کنید.

همچنین می‌توانید به تنظیمات Bluetooth خود بروید (**تنظیمات > Bluetooth**) و به دنبال دستگاه‌هایی بگردید که با تلفن شما جفت شده‌اند. اگر دستگاهی را نمی‌شناسید، آن را از حالت جفت‌سازی خارج کنید.

خاموش کردن اشتراک‌گذاری موقعیت‌مکانی

اشتراک‌گذاری موقعیت‌مکانی و برنامه‌هایی مانند "یافتن تلفن من" حتی اگر تلفن شما خاموش باشد همچنان کار می‌کنند، بنابراین باید آنها را در تنظیمات خاموش کنید. در iPhone، **تنظیمات** > حریم خصوصی > سرویس‌های موقعیت‌مکانی را باز کنید یا "سرویس‌های موقعیت‌مکانی" را جستجو کنید و اشتراک‌گذاری موقعیت‌مکانی را خاموش نمایید.

در دستگاه Android، **نقشه‌ها** را باز کنید، روی عکس پروفایل خود و سپس اشتراک‌گذاری موقعیت‌مکانی ضربه بزنید. روی عکس پروفایل هر کسی که *نباید* موقعیت‌مکانی شما را ببیند ضربه بزنید و سپس گزینه "توقف" را انتخاب کنید.



ایمن‌سازی دستگاه‌های خود

تغییرنام دستگاه‌های خود

حتی اگر هرگز نام تلفن خود را تغییر نداده باشید، باز هم نامی دارد که با آن شناسایی می‌شود. در iPhone، روی "**تنظیمات** > عمومی > درباره > نام" ضربه بزنید، یا "نام" را جستجو کنید، سپس نام جدیدی وارد کنید و روی "انجام شد" ضربه بزنید.

در دستگاه Android، روی **تنظیمات** > درباره تلفن > نام دستگاه ضربه بزنید، یا "نام" را جستجو کنید، سپس نام جدیدی وارد کنید و روی "تأیید" ضربه بزنید.

بررسی جاسوس‌افزار

"جاسوس‌افزار" به برنامه‌هایی گفته می‌شود که به شخص دیگری اجازه می‌دهند روی دستگاه شما جاسوسی کند. بررسی کنید برنامه‌هایی وجود دارند که شما آن‌ها را نمی‌شناسید یا خیر. در iPhone، انگشت‌تان را در صفحه اصلی به سمت راست بکشید تا کتابخانه برنامه‌ها (App Library) را ببینید.

روی کادر جستجو در بالای صفحه‌نمایش ضربه بزنید، سپس در فهرست برنامه‌ها پیمایش کنید و هر چیزی را که نمی‌شناسید حذف کنید.

در دستگاه Android، به **تنظیمات** > برنامه‌ها و اعلان‌ها > مشاهده همه برنامه‌ها بروید یا "برنامه‌ها" را جستجو کنید.

همچنین برنامه‌هایی مانند *Certo* و *Incognito* وجود دارند که می‌توانید از آن‌ها استفاده کنید تا دستگاه‌هایتان را برای وجود جاسوس‌افزار اسکن کنند، اما باید بدانید که همیشه احتمال دارد جاسوس‌افزاری همچنان روی تلفن شما باقی بماند.

بررسی مجوزهای برنامه

همچنین می‌توانید از جمع‌آوری یا اشتراک‌گذاری اطلاعاتی مانند موقعیت مکانی توسط هر برنامه‌ای جلوگیری کنید. در iPhone، روی **سه نقطه** > حریم خصوصی و امنیت > گزارش حریم خصوصی برنامه ضربه بزنید تا ببینید هر برنامه چه چیزی به اشتراک می‌گذارد یا "گزارش حریم خصوصی" را جستجو کنید. روی هر برنامه ضربه بزنید تا تنظیمات را تغییر دهید.

کلید آیکون


تنظیمات

سه نقطه

کلید تغییر وضعیت

در دستگاه Android، برنامه *DuckDuckGo* را از Play store دانلود و سپس آن را باز کنید. روی **تنظیمات** > محافظت از ردیابی برنامه ضربه بزنید و سپس **کلید تغییر وضعیت** را به سمت راست بکشید.

بازنشانی به تنظیمات کارخانه

اگر همه چیز را امتحان کرده‌اید و هنوز فکر می‌کنید کسی ممکن است تلفن شما را ردیابی کند، می‌توانید بازنشانی به تنظیمات کارخانه را انجام دهید. بااین‌حال، با این کار همه داده‌ها، شامل هرگونه شواهد روی تلفن شما حذف خواهد شد. اگر تلفن خود را بازنشانی کنید، نمی‌توانید از نسخه پشتیبان ذخیره‌شده بازیابی کنید زیرا هر چیزی که شما را ردیابی می‌کرده است ممکن است دوباره بارگذاری شود: باید کاملاً از نو شروع کنید.

اگر از انجام این کار اطمینان دارید، در iPhone می‌توانید روی **تنظیمات** > عمومی > انتقال یا بازنشانی iPhone، سپس "پاک کردن همه محتوا و تنظیمات" ضربه بزنید. می‌توانید عبارت "بازنشانی" را جستجو کنید تا این تنظیم را بیابید.

اگر iPhone دارید، همچنین می‌توانید حالت محافظت شدید (Lockdown Mode) را روشن کنید که از شما در برابر بیشتر انواع جاسوس‌افزارها محافظت می‌کند. این حالت همچنین میزان استفاده شما از برنامه‌هایی مانند FaceTime و Safari را محدود می‌کند. جهت کسب اطلاعات بیشتر در مورد حالت محافظت شدید، به https://support.apple.com/en-ca/HT212650 مراجعه کنید.

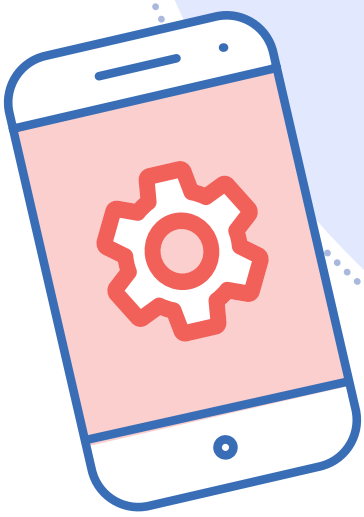
در دستگاه اندرویدی، با رفتن به **تنظیمات** شروع کنید، سپس "بازنشانی" را جستجو نمایید. به دنبال نتیجه‌ای مانند "بازنشانی به تنظیمات کارخانه" یا "پاک کردن همه داده‌ها" بگردید و روی آن ضربه بزنید.

Financial contribution from

Public Health Agency of Canada | Agence de la santé publique du Canada

برقراری ارتباط ایمن

این منبع چند گام عملی اولیه برای برقراری ارتباط ایمن آنلاین ارائه می‌دهد تا از انواع رایج ردیابی آنلاین جلوگیری کند و اقداماتی مانند خروج از حساب‌های کاربری، خاموش کردن اشتراک‌گذاری موقعیت‌مکانی، بررسی تنظیمات حریم خصوصی و تغییر رمزهای عبور را پوشش می‌دهد.



این‌ها نکات کلی برای ایمن نگه داشتن دستگاه‌های شما هستند. ممکن است مراحل دقیق برای دستگاه‌های مختلف متفاوت باشد و با گذشت زمان تغییر کند.

در iPhones وiPads، معمولاً می‌توانید با ضربه زدن روی آیکون "تنظیمات" در صفحه اصلی و سپس کشیدن انگشت‌تان به سمت پایین برای نمایش نوار جستجو، تنظیمی را پیدا کنید. (جهت یافتن راهنما، به http://tiny.cc/iphonesearch مراجعه کنید.)

در دستگاه‌های Android، انگشت‌تان را از صفحه اصلی به سمت بالا بکشید: نوار جستجویی ظاهر می‌شود که می‌گوید "جستجوی تلفن خود و موارد بیشتر". تنظیمی را که به دنبال آن هستید در نوار جستجو تایپ کنید.

خروج از همه حساب‌های کاربری

ممکن است در برخی از برنامه‌ها روی بیش از یک دستگاه وارد شده باشید. در اینجا نحوه خروج از *Facebook* در همه دستگاه‌ها آمده است: روی **سه نقطه** و سپس **تنظیمات**، سپس "رمزعبور و امنیت" و بعد "مرکز حساب‌های کاربری" ضربه بزنید. روی "رمز عبور و امنیت" و سپس "جایی که وارد شده‌اید" ضربه بزنید.

حالا همه حساب‌های کاربری *Facebook*، *Instagram* یا *WhatsApp* خود را خواهید دید. روی هرکدام ضربه بزنید تا ببینید در کدام دستگاه‌ها وارد شده‌اید، سپس برای هرکدام که تلفن شما نیست روی "خروج" ضربه بزنید.

برقراری ارتباط ایمن

خاموش کردن اشتراک‌گذاری موقعیت‌مکانی در رسانه‌های اجتماعی

این نکته مهم است که بدانید در صورتی که از *Snapchat* استفاده می‌کنید، مکان شما را روی نقشه نشان می‌دهد. برای انجام این کار، *Snapchat* را باز کنید و روی آیکون پروفایل خود ضربه بزنید. سپس روی **سه نقطه عمودی** در بالا سمت راست ضربه بزنید و به سمت پایین به بخش "چه کسی می‌تواند..." پیمایش کنید. اگر روی "مشاهده موقعیت‌مکانی من" ضربه بزنید، پنجره بازشویی ظاهر می‌شود که "حالت شبح" را نشان می‌دهد. **وضعیت** آن را به "روشن" تغییر دهید.

در *Facebook* یا *Instagram*، می‌توانید موقعیت‌مکانی را با ضربه زدن روی **تنظیمات** > حریم خصوصی > سرویس‌های موقعیت مکانی و سپس ضربه زدن روی **کلید تغییر وضعیت** کنار آن خاموش کنید. بیشتر شبکه‌های اجتماعی دیگر آن را در مکان‌های مشابه در تنظیمات مانند "حریم خصوصی" یا "ایمنی" قرار می‌دهند.

بررسی تنظیمات حریم خصوصی

همه حساب‌های کاربری شبکه اجتماعی شما دارای تنظیمات حریم خصوصی هستند که معمولاً با ضربه زدن روی **تنظیمات** و سپس چیزی مانند "حریم خصوصی"، "حریم خصوصی و امنیت" یا "مخاطبان" قابل دسترسی است. مطمئن شوید که این مورد به گونه‌ای تنظیم شده باشد که فقط آنچه پست می‌کنید برای دوستان نمایش داده شود.

تغییر رمزهای عبور در ذخیره‌سازی ابری

اگر از ذخیره‌سازی ابری، مانند *iCloud* یا *Google Drive*، برای عکس‌ها یا ویدیوهای خود استفاده می‌کنید؛ مطمئن شوید که رمزعبور را تغییر داده‌اید تا هیچکس دیگری نتواند به آن دسترسی پیدا کند.

Financial contribution from

Public Health Agency of Canada
Agence de la santé publique du Canada

MediaSmarts

مرور ایمن

این منبع چند گام عملی اولیه برای مرور ایمن آنلاین ارائه می‌دهد تا از انواع رایج ردیابی آنلاین جلوگیری کند و اقداماتی مانند استفاده از مرورگرهای متمرکز بر حریم خصوصی، مرور خصوصی/ناشناس، پاک کردن تاریخچه و ورود با ایمیل‌های ناشناس و رمزهای عبور قوی را پوشش می‌دهد.

این‌ها نکات کلی برای ایمن نگه داشتن دستگاه‌های شما هستند.
ممکن است مراحل دقیق برای دستگاه‌های مختلف متفاوت باشد و با گذشت زمان تغییر کند.

در iPhones وiPads، معمولاً می‌توانید با ضربه زدن روی آیکون "تنظیمات" در "صفحه اصلی" و سپس کشیدن انگشت‌تان به سمت پایین برای نمایش نوار جستجو، تنظیمی را پیدا کنید. (جهت یافتن راهنما، به http://tiny.cc/iphonesearch مراجعه کنید.)

در دستگاه‌های Android، انگشتتان را از "صفحه اصلی" به سمت بالا بکشید: نوار جستجویی ظاهر می‌شود که می‌گوید "جستجوی تلفن خود و موارد بیشتر". تنظیمی را که به دنبال آن هستید در نوار جستجو تایپ کنید.

استفاده از مرورگر متمرکز بر حریم خصوصی

مرورگرهایی مانند *Firefox* و*DuckDuckGo* با در نظر گرفتن حریم خصوصی طراحی شده‌اند، بنابراین تا حد امکان شما را ردیابی نمی‌کنند. سعی کنید به جای مرورگری که با دستگاه شما ارائه شده است، از یکی از آن‌ها استفاده کنید.

مرور خصوصی یا ناشناس

اکثر مرورگرها دارای حالت **خصوصی** یا **ناشناس** هستند. این حالت باعث می‌شود خود مرورگر سایت‌هایی را که بازدید کرده‌اید ثبت نکند، اما مانع از ثبت فعالیت‌های شما توسط آن سایت‌ها (یا ارائه‌دهنده اینترنت شما، یا برنامه‌های دیگر روی دستگاه‌تان) نمی‌شود.

کلید آیکون

حالت خصوصی یا ناشناس

تنظیمات

مرور ایمن

پاک کردن تاریخچه خود

"تاریخچه" را جستجو کنید. اگر حساب *Google* دارید، می‌توانید تاریخچه *Google* و *YouTube* خود را نیز پاک کنید. به **myactivity.google.com** بروید و "فعالیت وب و برنامه"، "تاریخچه موقعیت‌مکانی" و "تاریخچه YouTube" را خاموش کنید.

برای پاک کردن تاریخچه مرورگر در Safari، روی تنظیمات سپس Safari > پاک کردن تاریخچه و داده‌های وب‌سایت ضربه بزنید یا "داده‌های وب‌سایت" را جستجو کنید.

ورود با ایمیل ناشناس

بسیاری از وب‌سایت‌ها و سرویس‌ها از شما می‌خواهند که برای ثبت‌نام آدرس ایمیل ارائه دهید. اگر نیازی به کلیک روی لینک تأیید ندارید، می‌توانید از یک آدرس ایمیل جعلی که در **Sharklasers.com** ایجاد شده است، استفاده کنید.

همچنین می‌توانید یک آدرس *Protonmail* رایگان، خصوصی و امن ایجاد کنید تا مجبور نباشید از آدرسی استفاده کنید که ممکن است شخص دیگری آن را شناسایی کند.

استفاده از رمزعبورهای قوی

می‌توانید رمز عبوری بسازید که با عبارتی به‌یادماندنی (مثلاً "I like bananas") شروع شود و سپس برخی از حروف را به اعداد یا نویسه‌ها (مانند ستاره یا علامت تعجب تغییر دهید تا به !L1keBan@nas تبدیل شود).

اما از یک رمزعبور یکسان برای حساب‌های مختلف استفاده نکنید. بسیار مهم است که برای حساب ایمیل اصلی خود رمزعبوری قوی و متفاوت استفاده کنید، زیرا ایمیل‌های بازیابی حساب به آن ارسال خواهند شد. همچنین می‌توانید از یک مدیر رمزعبور مانند *1Password* استفاده کنید. اگر از آن استفاده می‌کنید، مطمئن شوید که رمزعبوری که برای آن استفاده می‌کنید قوی و متفاوت از همه رمزعبورهای دیگرتان باشد.

کلید آیکون

Financial contribution from

Public Health Agency of Canada
Agence de la santé publique du Canada