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