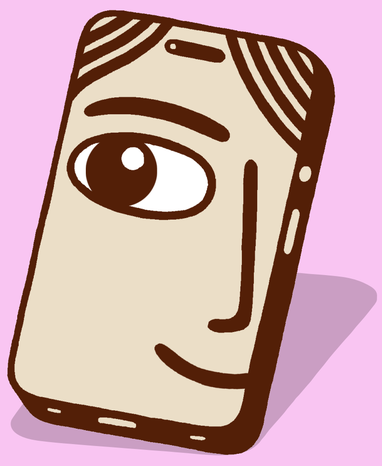
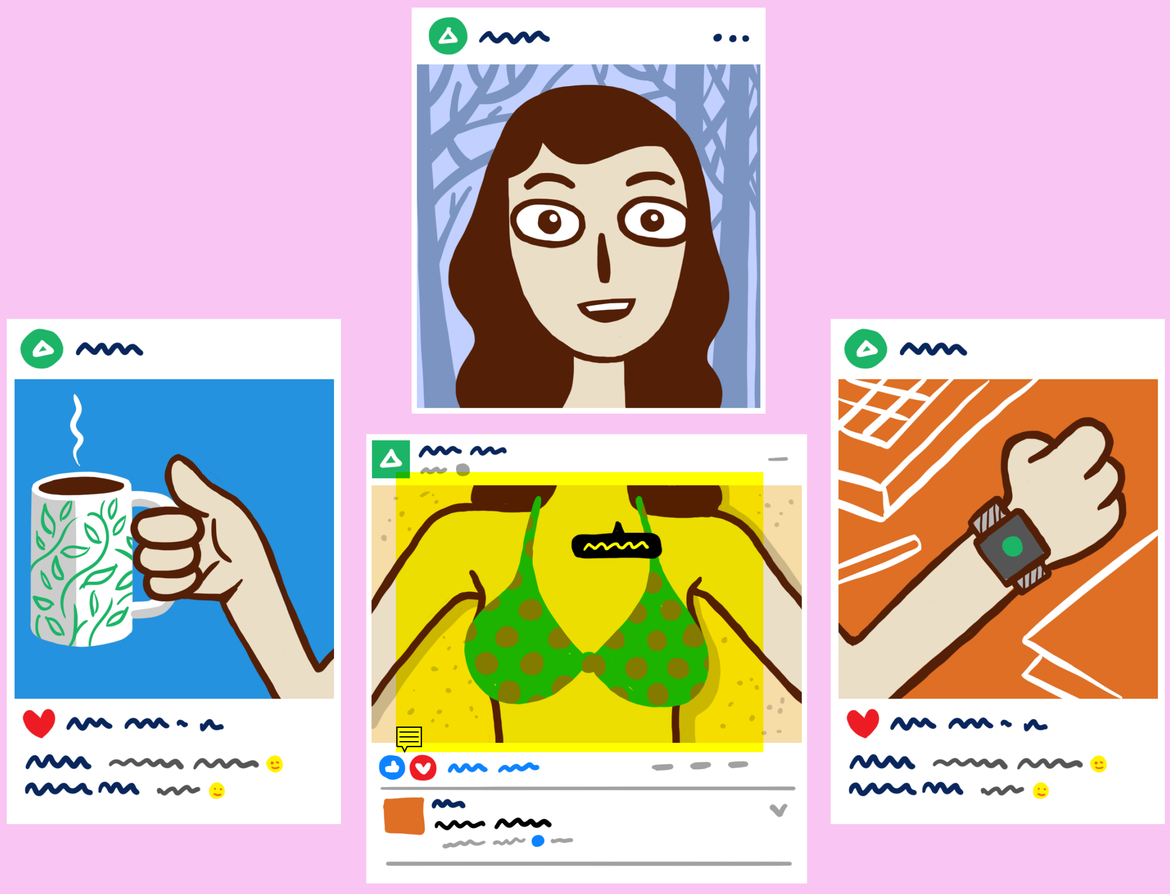
امنیت در فضای مجازی

حواس‌جمعی در استفاده از شبکه اجتماعی



نبض‌ایران
تقویت صدای ایرانیان



دسترسی به پلاتفرم‌ها

تصاویری که آپلود می‌کنید، دوستانی که تگ می‌کنید، پست‌هایی که می‌نویسید، این‌ها همه تصویری اینترنتی از شما ایجاد می‌کند.

اولین چیزی که باید بدانید این است که پلاتفرمی که در آن هستید دسترسی راحتی به بسیاری اطلاعات راجع به شما دارد.

اگر کاربر فیس‌بوک، اینستاگرام، توئیتر و حتی تلگرام هستید، بدانید که اکثریت پیغام‌های آن‌ها رمزگذاری نشده. آن‌ها در ضمن می‌توانند نموداری اجتماعی از شما بر اساس فعالیت‌هایتان، محل حضورتان، دوستان‌تان و چیزهایی که «لایک» کردید ایجاد کنند.

خطر متوجه شما چیست؟

اما پیشنهاد ما این است که برگردید به «تشخیص خطر» تا بفهمید در اینترنت باید نگران چه کسی یا چه چیزی باشید. این‌که شرکتی آمریکایی دنبال داده‌هایتان باشد؟ یا کسی یا چیزی که بتواند به صورت عمومی به اطلاعات‌تان دسترسی پیدا کنید.

عمومی در مقابل خصوصی

اولین نکته‌ای که باید به آن آگاه باشید «عمومی» در مقابل «خصوصی» است.

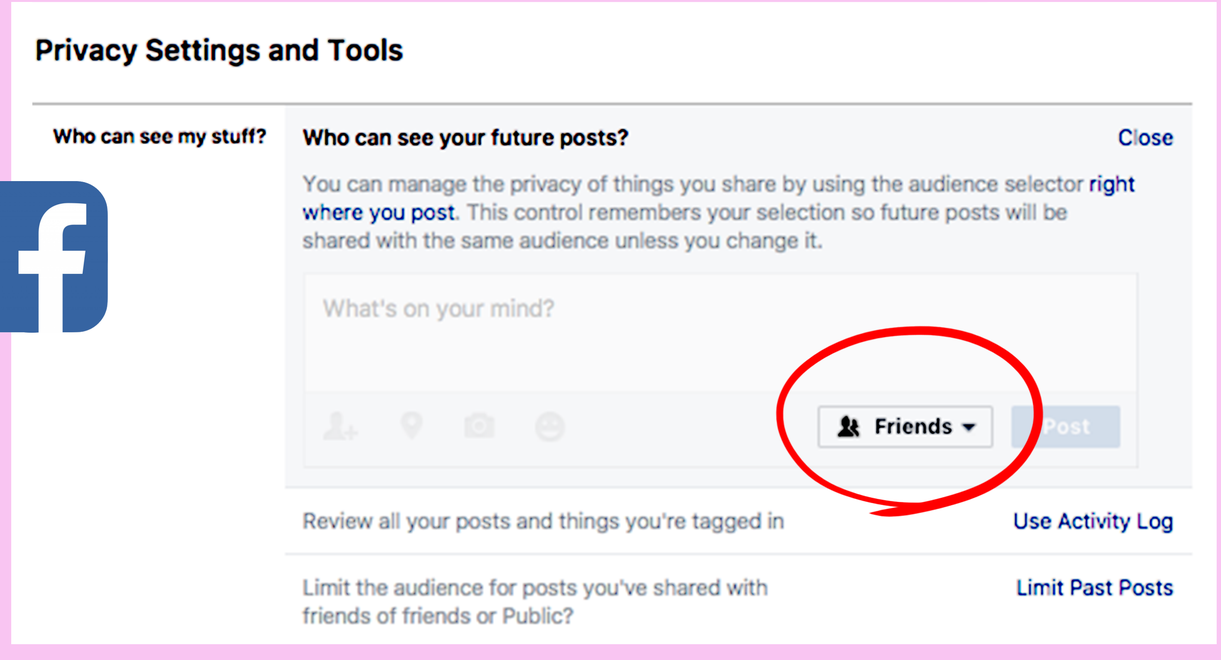
آیا دارید مقاله‌ای راجع به پیوستن به راه‌پیمایی غرور هم‌جنس‌گرایان هنگام بازدید از اقوام‌تان در تورنتو پست می‌کنید؟

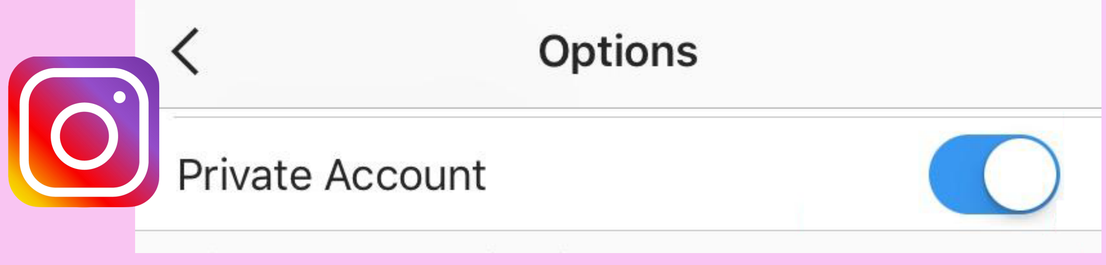
اگر این پست عمومی باشد شاید بخواهید به این فکر کنید که دولت ایران یا کارفرمایتان چه واکنشی به دیدن آن خواهد داشت. این امکان هست که اگر این اطلاعات به صورت عمومی قابل دسترسی باشد، کسی که بخواهد برای اطلاعات موجود راجع به شما جستجو کند بتواند به آن دسترسی پیدا کند.

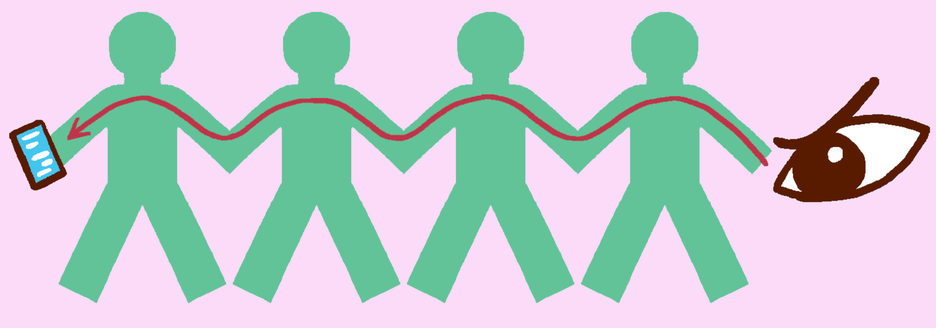
برای خصوصی کردن پست‌هایتان در فیس‌بوک می‌توانید قبل از انتشار آن‌ها کاری کنید که فقط «دوستان»تان آن‌ها را ببینند.

اگر این پست خصوصی باشد آیا مطمئنید که تمام کسانی که حساب‌تان را دنبال می‌کنند می‌شناسید؟ می‌توانید فهرست افرادی را که مورد اعتمادتان هستند برای بعضی پست‌ها ایجاد کنید.

در اینستاگرام هم همین‌طور حواس‌تان به آن‌چه پست می‌کنید و این که صفحه‌تان خصوصی است یا عمومی، باشد.

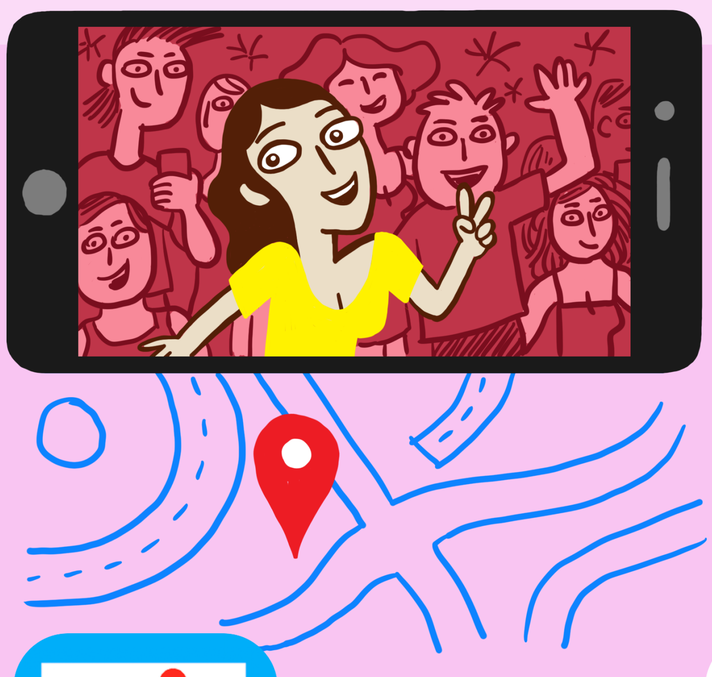






امنیت شما نه تنها به تنظیمات شبکه‌های اجتماعی خود، بلکه به عملکرد هر فرد دیگری که اجازه دسترسی یا مشاهده پیام‌ها، گروه‌ها یا پست‌های شما را دارد نیز بستگی دارد. به عنوان مثال آیا همه دوستان شما در فیسبوک از رمز عبور قوی و برنامه احراز هویت برای تصدیق دو مرحله‌ای استفاده می‌کنند؟

فراداده (متادیتا)



جدا از این‌که تگ «لوکیشن» را روی عکس‌هایتان نگذارید خوب است بدانید که عکس‌هایی که در فیس‌بوک و اینستاگرام پست می‌کنید حاوی «فراداده» است، یعنی اطلاعات مشخصی مثل لوکیشن و زمان. مثلا آیا در مهمانی‌ها یا گردهمایی‌هایی شرکت می‌کنید که می‌دانید مامورین پلیس نظر مثبتی به آن‌ها ندارند؟ شاید با رفتارتان اطلاعاتی حیاتی در اختیار مقامات بگذارید تا بر اساس این اطلاعات مکان‌های خاص و زمان‌های جلسات منظم را راحت‌تر تحت نظارت قرار دهند.

اولا می‌توانید عکس‌هایی که حاوی اطلاعات شخصی باشند منتشر نکنید. اما به غیر از این می‌توانید با نرم‌افزارهای مختلف فراداده‌ها را از روی عکس‌هایتان حذف کنید.

Exif Eraser (Android)

Metapho (iOS)