



بخش دوم

نکات مهم برای استفاده از شبکه های اجتماعی و
برنامه های دوست یابی



OUTRIGHT
ACTION INTERNATIONAL



Every day around the world, LGBTIQ people's human rights and dignity are abused in ways that shock the conscience. The stories of their struggles and their resilience are astounding, yet remain unknown—or willfully ignored—by those with the power to make change. OutRight Action International, founded in 1990 as the International Gay and Lesbian Human Rights Commission, works alongside LGBTIQ people in the Global South, with offices in six countries, to help identify community-focused solutions to promote policy for lasting change. We vigilantly monitor and document human rights abuses to spur action when they occur. We train partners to expose abuses and advocate for themselves. Headquartered in New York City, OutRight is the only global LGBTIQ-specific organization with a permanent presence at the United Nations in New York that advocates for human rights progress for LGBTIQ people.

hello@OutRightInternational.org
<https://www.facebook.com/outrightintl>
<http://twitter.com/outrightintl>
<http://www.youtube.com/lgbthumanrights>
<http://OutRightInternational.org/iran>

OutRight Action International
80 Maiden Lane, Suite 1505, New York, NY 10038 U.S.A.
P: +1 (212) 430.6054 • F: +1 (212) 430.6060

This work may be reproduced and redistributed, in whole or in part, without alteration and without prior written permission, solely for nonprofit administrative or educational purposes provided all copies contain the following statement:

© 2018 OutRight Action International. This work is reproduced and distributed with the permission of OutRight Action International. No other use is permitted without the express prior written permission of OutRight Action International. For permission, contact hello@OutRightInternational.org.



بخش دوم

نکات مهم برای استفاده از شبکه های اجتماعی و
برنامه های دوست یابی



OUTRIGHT
ACTION INTERNATIONAL





جدول محتوا

I مقدمه

- ۱..... امنیت خریدنی نیست.....
- ۲..... راهنمای حاضر با فرض موارد زیر نگاشته شده است:
- ۲..... امنیت دیجیتال را عادت خود کنید
- ۲..... هر چه سرمایه ی اجتماعی ای که از طریق جلب اعتماد در شبکه خود کسب کرده باشید بیشتر باشد، خط دفاعی امنیت شما نیز بیشتر خواهد بود.....
- ۲..... انواع شبکه های اجتماعی.....
- ۳..... گردآوری اطلاعات توسط شبکه های اجتماعی.....
- ۳..... گردآوری فعال اطلاعات.....
- ۳..... اطلاعات غیرفعال
- ۴..... گرد آوری اطلاعات توسط شخص سوم
- ۵..... چرا باید درباره ی گردآوری اطلاعات بدانیم؟
- ۵..... حکایت زیر نشان می دهد چگونه می توان از گردآوری غیر فعال اطلاعات برای گردآوری فعال اطلاعات استفاده کرد.
- ۵..... در حکایت بالا چه اطلاعاتی گردآوری شده است؟.....
- ۶..... امنیت وسایلی که برای اتصال به شبکه های اجتماعی و برنامه های دوست یابی استفاده می شود.....
- ۶..... آدرس IP خود را چگونه مخفی کنم؟.....
- ۷..... Virtual Private Networks (VPNs).....
- ۸..... در پایین چند نمونه از VPN هایی که با توجه به موارد ذکر شده، مناسب هستند، آمده است:
- ۸..... محافظت از خود در شبکه های اجتماعی
- ۱۰..... پیام رسان و اپلیکیشن های ارتباطی.....
- ۱۱..... مشکیت (MeshKit).....
- ۱۱..... حفاظت از خود در اپلیکیشن های دوست یابی

۱۴ منابع و مآخذ

IV واژه نامه



مقدمه

نوشته حاضر، بخش دوم راهنمای امنیت دیجیتال است. تمرکز این بخش بر امنیت شخصی و حرفه ای و محافظت از اطلاعات در شبکه های اجتماعی و برنامه های دوست یابی است. امیدواریم مطالعه این بخش، آگاهی شما را نسبت به تاثیر ردپای دیجیتال بر امنیت شخصی و حرفه ای، بالا ببرد.

امنیت خریدنی نیست

حملات و تهدیدات دیجیتال، همواره نقاط ضعف امنیتی شما را هدف قرار می دهند. برای همین تمرکز برنامه های امنیتی بر کاهش خطر این نوع تهدیدات و حملات است.

چه از رایانه شخصی استفاده کنید یا از رایانه مشترک (محل کار، منزل، کافی نت) یا اینکه بیشتر فعالیت های اینترنتی خود را روی تبلت یا گوشی هوشمند انجام دهید، راهنمای حاضر شما را در برآوردن نیازها، انتخاب ابزارهای امنیتی و به کارگیری عادت های ایمنی و تضمین امنیت شخصی و حرفه ای برخط و برون خط (آنلاین و آفلاین)، یاری خواهد کرد.

این راهنما به دو بخش تقسیم شده است:

- تمرکز **بخش اول** بر امنیت دیجیتال از منظر شخصی و حرفه ای است. این بخش کمک می کند تا شبکه و جوامع دیجیتالی خود را شناسایی و بازبینی کرده و بر امنیت و راهکارهای پیشگیرانه تمرکز کنید.
- تمرکز **بخش دوم** بر امنیت و پیشگیری از تهدیدات متوجه وسایل الکترونیکی، گردآوری اطلاعات از طریق اینترنت، شبکه های اجتماعی و اپلیکیشن های دوست یابی است.

تعریف امنیت دیجیتال

امنیت دیجیتال به حفاظت از اطلاعات و منابع دیجیتالی در برابر تهدیدات داخلی، خارجی، عمدی و تصادفی گفته می شود. برای نهادها و افراد، امنیت دیجیتال به معنی شناسایی، پیشگیری و پاسخگویی به تهدیدات از طریق اعمال سیاست های امنیتی، استفاده از نرم افزار و خدمات فناوری اطلاعات است

راهنمای حاضر با فرض موارد زیر نگاشته شده است:

- شما به صورت روزمره از رایانه و تلفن همراه برای ارتباطات یا کار استفاده می کنید.
- تلاش ما بر پیشنهاد راهکارهای موثر و کم هزینه است اما توجه داشته باشید که برخی از راهکارهای رایگان، پر مخاطره هستند. بیشتر تمرکز ما بر سیستم عامل های مایکروسافت و اندروید است که رواج بیشتری در سطح جهانی دارند.
- از آنجا که تکنولوژی (فناوری) همواره در حال تغییر است، تلاش ما بر آن بوده که این مجموعه را به صورت انعطاف پذیر تنظیم کنیم (تا در شرایط مختلف قابل استفاده باشد) زیرا باید به طور مستمر در عادات امنیتی خود بازنگری کنید.



امنیت دیجیتال را عادت خود کنید

بازنگری -----> برآورد -----> بکارگیری

این سه مرحله را به صورت ماهانه، هر دوماه یک بار، فصلی، هر شش ماه یک بار یا سالانه تکرار کنید.

استفاده از شبکه های اجتماعی بر روی رایانه شخصی و تلفن همراه

شبکه های اجتماعی ابزاری است که به کاربران اجازه می دهد تا از طریق تبادل پیام یا ایجاد و به اشتراک گذاری محتوا با یکدیگر ارتباط برقرار کنند. سرمایه اجتماعی با استفاده از شبکه های اجتماعی (برخط و برون خط/آنلاین و آفلاین) به دست می آید.

هر چه سرمایه ی اجتماعی ای که از طریق جلب اعتماد در شبکه خود کسب کرده باشید بیشتر باشد، خط دفاعی امنیت شما نیز بیشتر خواهد بود.

انواع شبکه های اجتماعی



- اپلیکیشن های ارتباطی -- Telegram, Signal, Facebook, Twitter, Zello, FireChat
- (تلگرام، سیگنال، فیسبوک، توئیتر، زیلو، فایر چت)
- اپلیکیشن های مدیریت محتوا و به اشتراک گذاری -- Instagram, YouTube, Tumblr, Squarespace
- (اینستاگرام، یوتیوب، تامبلر، اسکوائر اسپیس)

- اپلیکیشن های پیگیری اخبار و اطلاعات - Reddit, wikis
- (ردیت، ویکی ها)
- وقایع و موقعیت مکانی -- Foursquare, Glympse, Yelp
- (فوراسکوئر، گلیمپس، یلپ)
- مکان یاب اپلیکیشن های اجتماعی و دوست یابی -- Bumble, Tinder, Grindr, Scruff
- (فازکسا، ردنی ارگ، ردنی تی، لبماب)

گردآوری اطلاعات توسط شبکه های اجتماعی

نمونه های شبکه های اجتماعی دو نوع داده گردآوری می کنند: داده فعال و داده غیر فعال. لازم است بدانید که اشخاص سوم هم می توانند اطلاعات شبکه های اجتماعی شما را گردآوری کنند.

گردآوری فعال اطلاعات

اطلاعات فعال، اطلاعاتی است که به صورت عمدی و توسط خود کاربر از طریق فرم در اختیار اپلیکیشن و سایت قرار داده می شود. اینها اطلاعاتی است که شما شخصا در اختیار شرکت سازنده شبکه اجتماعی قرار می دهید. مثال این نوع داده ها حساب کاربری شبکه های اجتماعی است که در آن نام کاربری، موقعیت مکانی، علایق، اطلاعات پرداخت یا اطلاعات جستجوی خود را افشا می کنید.

نمونه ی گردآوری اطلاعات فعال در فیسبوک، اطلاعاتی است که از پروفایل شما جمع آوری می شود. شما می توانید این اطلاعات را از طریق زیر دانلود کنید: Facebook.com > Login > Settings : The screen will look like below:

General Account Settings

To download your information, go to Your Facebook Information .		
Name	Yousef Fahrad	Edit
Username	https://www.facebook.com/yousef.fahrad	Edit
Contact	Primary: yousef.fahrad@gmail.com	Edit
Ad account contact	yousef.fahrad@gmail.com	Edit
Temperature	Fahrenheit	Edit
Manage Account	Modify your Legacy Contact settings or deactivate your account.	Edit

General

Security and Login

Your Facebook Information

اطلاعات غیرفعال

اطلاعات غیرفعال، اطلاعاتی است که از شما درخواست نشده ولی برای کارایی ذخیره می شود. نمونه های این اطلاعات: ساعت ارسال پیام ها، آدرس IP، موقعیت مکانی بر اساس آدرس IP، اطلاعات ثبت ورود، کوکی ها، نوع دستگاهی که استفاده می کنید، مانند تلفن همراه یا رایانه و غیره.

نمونه ی اطلاعات غیر فعالی که فیسبوک گردآوری می کند، سابقه مرور شماست که می توان از طریق زیر آن را دریافت کرد: Facebook.com > Login > Settings >

Access Your Information

Here is a list of your Facebook information that you can access at any time. We've categorized this information by type so you can easily find what you're looking for. Our [Data Policy](#) has more information about how we collect and use your information, how it's shared and how long we retain it. It also outlines your rights and how you can exercise them, and how we operate and transfer your information as part of our global services.

You can choose to [download your information](#) if you'd like a copy of it.

Information About You ⓘ Expand all

**Ads**
Your interests, interactions, and existing relationships you have with advertisers that...

**About You**
Information associated with your Facebook account

**Search History**
A history of the words, phrases and names you've searched for

**Location History**
A history of precise locations received through Location Services on your device

**Calls and Messages**
Logs of your calls and messages that you've chosen to share in your device settings

**Security and Login Information**
Your login history, session length, and other security-related information. For all of your...

گرد آوری اطلاعات توسط شخص سوم

گرد آوری اطلاعات توسط شخص سوم هنگامی اتفاق می افتد که کاربران به افزونه ها، بر افزارها، نرم افزار ها و اپلیکیشن های دیگر اجازه دسترسی به حساب کاربری خود را می دهند. به عنوان مثال، استفاده از فیسبوک برای وارد شدن به یک اپلیکیشن دوست یابی.

برای یافتن سایت ها و اپلیکیشن هایی که به اطلاعات شما در فیسبوک دسترسی دارند، به مسیر زیر مراجعه کنید:

Facebook.com > Login > Settings > Apps and Websites

- General
- Security and Login
- Your Facebook Information
- Privacy
- Timeline and Tagging
- Location
- Blocking
- Language
- Face Recognition
- Notifications
- Mobile
- Public Posts
- Apps and Websites**
- Business Integrations
- Ads
- Payments
- Support Inbox

Apps and Websites

Logged in With Facebook

Active 1 Expired Removed

Data Access Allowed

These are active apps and websites. This means you recently logged into them with Facebook, and they can request info you chose to share with them. [Learn More](#)

Use this list to:

- View and update the info they can request
- Remove the apps and websites you no longer want

Active Apps and Websites Remove

**Seed&Spark L...**
[View and edit](#)

☐

چرا باید درباره ی گردآوری اطلاعات بدانیم؟

تبادل اطلاعات دیجیتال اشکال مختلفی به خود گرفته است و هر روز ابزارهای جدیدی به شبکه‌های اجتماعی اضافه می‌شود. بنابراین داشتن آگاهی اجمالی از نوع اطلاعاتی که این اپلیکیشن‌ها گردآوری می‌کنند برای امنیت شخصی و حرفه ای افرادی که از این شبکه‌های اجتماعی استفاده می‌کنند، ضروری است.

حکایت زیر نشان می‌دهد چگونه می‌توان از گردآوری غیر فعال اطلاعات برای گردآوری فعال اطلاعات استفاده کرد.

ریغ یروآدرگ زا ناوت یم ه‌نوگچ دهد ل‌اعف یروآدرگ یارب تا‌عالطا ل‌اعف درک هدافتسا تا‌عالطا:

دوست یکی از دوستان شما به صورت پابلیک (public) افرادی را تگ (tag) کرده تا آنها را از یک وب سایت خبری جدید درباره حقوق جامعه دگرباشان مطلع کند. یکی از دوستان این مطلب را دیده و روی آن کلیک می‌کند. مدیر وب سایت خبری متوجه می‌شود یکی از آی پی آدرس‌هایی که وارد سایت شده، از طریق این پست در شبکه اجتماعی هدایت شده است. مدیر وب سایت کدی می‌نویسد که بر اساس اطلاعات آدرس IP و آن پست، هشدار (نوتیفیکیشن) دریافت کند. مراحل نوتیفیکیشن به شرح زیر می‌باشد:

زیر می‌باشد:

اگر شخصی با یک آدرس IP بیش از سه بار در هفته از سایت بازدید کند، پنجره ای جدید باز شده و از فرد درخواست می‌شود که آدرس ایمیل خود را وارد کرده تا آخرین اخبار را از طریق پست الکترونیکی دریافت کند.

دوست نامبرده، بیش از سه بار در هفته از این وب سایت بازدید کرده، صفحه درخواست ایمیل را دیده و آدرس ایمیل خود را وارد کرده است.

در حکایت بالا چه اطلاعاتی گردآوری شده است؟

ی‌لصا تسپ زا ی‌عامرتجا هکبش هب طوبرم یاه هداد

- « تمام مشارکت‌ها (engagements) با پست - چه کسی like کرده، unlike کرده، نظرات دیگران و غیره.
- « اطلاعات عمومی هر حساب کاربری که به نوعی با این پست مشارکت داشته است.
- « برچسب‌ها (tags) - که پروفایل‌های افراد را به نظرات زیر پست مرتبط می‌کند.
- « تاریخ و زمان ارسال اطلاعات.
- « تبدیل‌ها - تعداد کاربرانی که برای مشاهده وب سایت روی لینک موجود در پست کلیک کرده اند.

داده‌های تحلیلی فرا افزار و اپلیکیشن‌های شخص سوم که ممکن است برای ردیابی بیشتر اطلاعات (ترافیک وب سایت) استفاده شوند.

- « آدرس IP و هر گونه اطلاعات مربوط به آدرس IP مانند حامل و موقعیت مکانی.
- « دستگاه مورد استفاده (تلفن همراه یا رایانه رومیزی)
- « دسترسی - از طریق برنامه یا مرورگر و یا موارد دیگر
- « مدت زمان حضور و تعداد دفعات بازدید هر آدرس IP منحصر به فرد از وب سایت

اطلاعات مربوط به فرم های اینترنتی ارسال شده

- « ایمیل
- « زمان و تاریخ پر شدن و ارسال فرم
- « دستگاه (تلفن همراه یا رایانه رومیزی)
- « نرم افزار مورد استفاده (مرورگر یا اپلیکیشن)
- « آدرس IP و هر گونه اطلاعات مربوط به آدرس IP

فهرست فوق کامل نیست ولی اصل مطلب را می‌رساند: اطلاعات بسیار زیادی را می‌توان از طریق کوچکترین مشارکت در اینترنت گردآوری کرد. این اطلاعات گردآوری شده به افرادی که شما را تحت نظر دارند و تحلیلگران اطلاعاتی نشان می‌دهند که کجاها دنبال اطلاعات بیشتر در مورد یک کاربر خاص بگردند.

برای همین به یک خط دفاعی دیجیتالی و امنیت الکترونیکی نیاز است که مرتب باید به روز رسانی شود. هرچه بیشتر مسیر دسترسی به اطلاعات را مسدود کنید، امنیت تان بالاتر رفته، و خطر کشف شدن توسط افراد ناشناس، دولت و شرکت های دیگر کمتر می‌شود. نکته مهم: در حوزه امنیت، هیچ چیز صددرصد امن نیست.

یکی از راه های کم کردن خطر این است که هیچ اطلاعاتی را در فضای مجازی پخش نکرده و همه چیز را خاموش کنید. مثلاً همه چیز را از برق بکشیم و همه حساب های کاربری خود را ببندیم. البته چنین کاری در عصر ارتباطات واقع گرایانه نیست. زیرا دوربین های امنیتی در ایستگاه قطار، فرودگاه، گذرگاه های مرزی و مخصوصاً در مناطق شهری با اجرای نرم افزار های شناساگر چهره، همواره در حال گردآوری اطلاعات غیر فعال هستند.

بهترین گزینه شما بالا بردن سطح دانش و استفاده از این دانش برای تغییر عادت های قدیمی است تا بتوانید در مسیر امنیت دیجیتال گام برداشت.

امنیت وسایلی که برای اتصال به شبکه های اجتماعی و برنامه های دوست یابی استفاده می شود

امنیت وسایلی که برای اتصال به شبکه های اجتماعی و برنامه های دوست یابی استفاده می شود. دستگاه هایی که از آن ها برای اتصال به شبکه های اجتماعی و اپلیکیشن های دوست یابی استفاده می کنید، باید از بالاترین امنیت ممکن برخوردار باشند. باید به دقت لایه های امنیتی خود را افزایش داده و چیزی را از قلم نیندازید.

برخی از نکات زیر تکرار نکاتی است که قبلاً مطرح شده است. آنچه بیشتر به عادت ها و کارهای روزمره شما مربوط است را انتخاب کرده و به کار گیرید.

آدرس PI خود را چگونه مخفی کنم؟

سه روش متداول برای مخفی کردن آدرس IP عبارتند از:

- **TOR چیست؟** - یک شبکه پیازی (onion router) یا چند لایه است که ترافیک اینترنت را از طریق یک شبکه همپوشان داوطلب و رایگان جهانی و دارای بیش از ۷ هزار رله (رایانه هایی که اجزا کوچک اطلاعات از آنها عبور می کنند)، هدایت می کند. این شبکه پیازی مکان و محتوای اطلاعات کاربران را از هر کسی که نظارت شبکه یا تجزیه و تحلیل ترافیک انجام می دهد، پنهان می کند.
- **سرور پراکسی** - (سیستم رایانه ای یا اپلیکیشن) سروری است که بین رایانه کاربر و سرور های دیگر قرار گرفته و درخواست ها را از یکی به دیگری منتقل می کند.
- **شبکه خصوصی مجازی یا VPN - VPN** با گسترش برد شبکه خصوصی به کاربران اجازه می دهد تا از طریق شبکه های مشترک یا عمومی به تبادل اطلاعات بپردازند. فعالیت VPN بگونه ای است که انگار رایانه ها به طور مستقیم به یک شبکه خصوصی وصل هستند. برنامه هایی که تحت VPN اجرا می شوند می توانند از کارکرد، امنیت و مدیریت شبکه خصوصی بهره مند شوند

برای رایانه : مرورگر Tor مانند کروم، فایرفاکس و سافاری نرم افزاری رایگان است که می توانید با نصب آن بر روی رایانه خود، IP خود را مخفی کرده و به صورت ناشناس از اینترنت استفاده کنید. این راهکار رایگان با استفاده از لایه های رمزنگاری سنگین، داده ها را در چند لایه مختلف پنهان کرده و امنیت و حریم خصوصی شما را تامین می کند. تور بردی torbirdy راهکار دیگری است که دکمه ای را به مرورگر حاضر شما اضافه کرده و می توانید با آن برای آدرس IP خود را مخفی کنید.

برای تلفن همراه : اپلیکیشن رایگان orbot اوربات به شما اجازه می دهد تا در یک محیط بسیار امن از اینترنت استفاده کنید. اوربات برای رمزنگاری اطلاعات از Tor استفاده کرده و ترافیک اینترنتی را از رایانه های پراکنده در سراسر دنیا عبور می دهد.

اپلیکیشن های پروکسی: outline اپلیکیشن جدیدی است که توسط گوگل طراحی شده و استفاده از VPN را آسان می کند. Outline هیچگونه اطلاعاتی در مورد کاربران جمع آوری نمی کند. برای راهنمای دانلود و استفاده از outline به بخش منابع رجوع کنید.

Virtual Private Networks (VPNs)

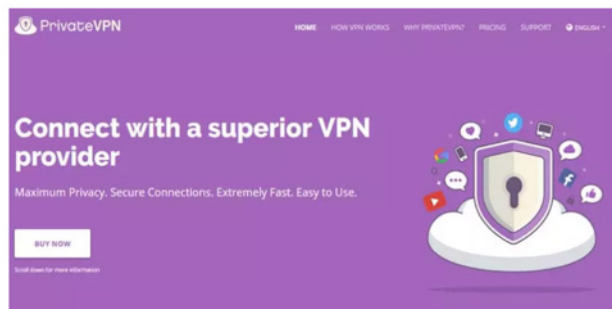
در بخش اول وی پی ان را مطرح کرده و به تشریح آن پرداختیم. شبکه های VPN به پل ارتباطی بین دستگاه و اینترنت تبدیل می شوند. با هر وسیله الکترونیکی که به WiFi وصل می شوید، پیشنهاد می شود از VPN استفاده کنید.

دو دلیل اصلی برای لزوم استفاده از VPN در ایران وجود دارد. دلیل اول: حفاظت از حریم شخصی خود در فضای مجازی و جلوگیری از دسترسی دولت و هکرها به ترافیک اینترنتی. دلیل دوم: دسترسی به سایت های سانسور شده بدون ترس از مجازات شدن به خاطر دور زدن فیلترینگ. در ایران مردم بنا به دلایل مختلفی از جمله همجنسگرایی، استفاده از سایت های دوست یابی و قمار، مجازات می شوند. VPN به همه در ایران اجازه می دهد که به صورت کاملاً محرمانه به محتوایی که در حالت عادی در دسترس ساز است، دسترسی پیدا کنند.

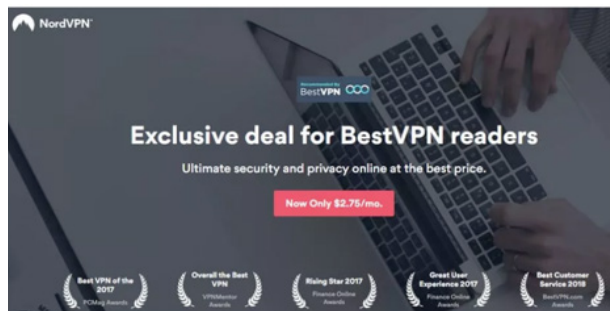
بسیار مهم VPN با ختنه دروم ردی تاکن

- مطمئن شوید شرکت فراهم کننده ی سرویس VPN، فعالیت های اینترنتی شما را تحت نظر قرار نمی دهد و اطلاعات شما را به هر کسی که با یک نامه حقوقی در شرکت را میزند، نمی دهد. شرایط استفاده از خدمات و سیاست های مربوط به حریم شخصی شرکت را مطالعه کرده و در این رابطه سوال بپرسید.
- بدانید که شرکت فراهم کننده ی VPN چه اطلاعاتی را ذخیره و نگهداری می کند. آیا ممکن است از این اطلاعات بر علیه خود شرکت استفاده شود، یا به شخص سومی فروخته و یا برای بازاریابی استفاده شود؟ آیا این شرکت اطلاعات شما را برای روز مبادا نگه داشته که در صورت نیاز در اختیار شخص دیگری بگذارد؟ تکرار می کنیم، شرایط استفاده از خدمات و سیاست های مربوط به حریم شخصی شرکت را مطالعه کرده و در این رابطه سوال بپرسید.
- VPN های رایگان یا VPN های ارزان محلی را استفاده نکنید. چرا؟ شرکت هایی که VPN رایگان در اختیار افراد می گذارند باید بالاخره از طریق پول در بیاورند. اگر از طریق فروش اشتراک کسب درآمد نکنند، حتماً درآمد خود را از طریق اطلاعات کاربران کسب می کنند، چه با فروش اطلاعات و چه با استفاده کردن از این اطلاعات برای بازاریابی. کاربران به هیچ وجه نباید از VPN های ارزان ایرانی استفاده کنند. دولت ایران از این VPN ها به عنوان دام استفاده می کند. لطفاً فقط از شرکت های VPN بین المللی استفاده کنید که از حریم خصوصی کاربران حمایت می کنند. اگر امکانات مالی محدودی دارید در این باره خوب فکر کنید.
- امنیت و حریم خصوصی VPN. به دنبال VPN هایی بگردید که در سیاست های حریم شخصی خود قید کرده اند هیچ سابقه ای نگه نمی دارند، و یا فقط بطور محدود سابقه اتصال را نگه نمی دارند. اگر شرکتی سابقه نگه ندارد، حتی اگر مقامات با حکم قضایی آن را مجبور کنند تا اطلاعات شما را در اختیارشان قرار دهد، چیزی برای تحویل دادن نخواهد داشت.
- علاوه بر این، برای ایران VPN ها باید رمزنگاری OpenVPN که بهترین روش رمزنگاری موجود در بازار است، داشته باشند. این یعنی احتمال هک شدن ترافیک اینترنتی کاهش می یابد، و هر قدر هم کسی بخواهد بداند در اینترنت چه می کنید نمی تواند به اطلاعات شما دسترسی پیدا کند.
- به فناوری توجه کنید. راه اندازی VPN کار سختی نیست. فقط کافی است چند دوست در شهرها و کشور های مختلف داشته باشید که حاضر باشند ترافیک شما را از روی سرور های خود عبور دهند. با این حال اگر شرکتی فاقد فناوری بک اند (back-end) قوی باشد، حریم خصوصی و امنیت خود و کاربران را به خطر انداخته و ممکن است قربانی دزدیده شدن اطلاعات، هک، و جاسوسی شوند. در رابطه با فناوری مورد استفاده شرکت فراهم کننده VPN تحقیق کنید.

در پایین چند نمونه از VPN هایی که با توجه به موارد ذکر شده، مناسب هستند، آمده است:



PrivateVPN یک سرویس دهنده سوئدی است که هیچ سابقه ای را ذخیره نمی کند. این برنامه با داشتن بیش از 80 سرور در 52 کشور جهان، هم از قابلیت سیستم مبتنی بر فایروال و هم خاموش کننده ی فوری یا کیل سوئیچ (kill switch) برخوردار است.



NordVPN دارای ویژگی های امنیتی اضافی است. دارای دکمه خاموش کننده ی فوری (kill switch)، محافظت در برابر فاش شدن DNS، سرورهای غیر قابل ردیابی، اتصال خودکار، VPN به Tor، و رمزنگاری دو مرحله ای (دوباره، دوگانه) VPN است.



VyprVPN برای امنیت بیشتر یک حالت «پنهان» عالی دارد. از رمزنگاری قوی OpenVPN استفاده می کند و سیاست حفظ حریم خصوصی آن غیر قابل نفوذ است (هر چند استفاده از P2P در این VPN مثلاً در برنامه های پیام رسان، توصیه نمی شود).



استفاده از نرم افزار CyberGhost آسان است. از رمزنگاری بسیار قوی استفاده می کند. محل شرکت سازنده آن در کشور رومانی است. سابقه مهمی را نگهداری نمی کند و مزیت دیگر این نرم افزار پذیرش پرداخت به صورت بیت کوین (Bitcoin) است.

محافظت از خود در شبکه های اجتماعی

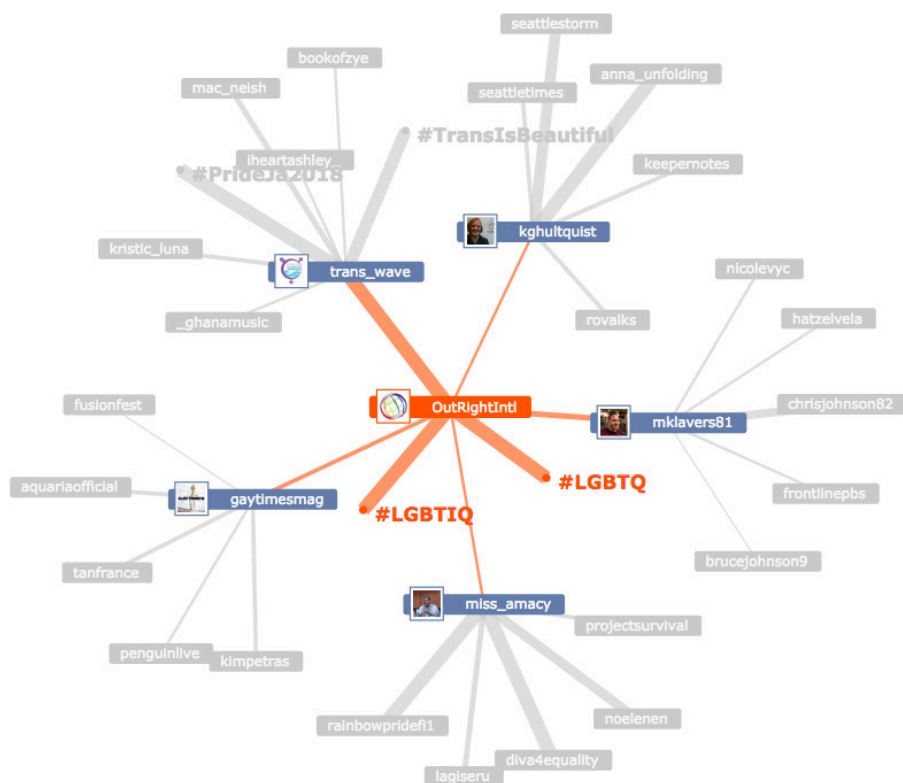
به خاطر دارید اولین باری که حساب کاربری در اینستاگرام باز کردید کی بود؟ خیر؟ اینستاگرام به یاد دارد. اینستاگرام حتی می داند که شما در چه ساعت و تاریخی با چه ایمیل و نامی حساب کاربری خود را باز کره اید. علاوه بر این، اینستاگرام سابقه تمامی پست ها و تغییراتی که در حساب کاربری خود داده اید را نیز دارد. اینها اطلاعاتی است که اینستاگرام درباره خود می داند، حال اگر حساب توییتر خود را نیز به اینستاگرام وصل کنید، اینستاگرام این اطلاعات را درباره ی توییتر شما هم خواهد دانست.

چرا این را مطرح کردیم؟ چون باز کردن حساب کاربری در شبکه های اجتماعی، کاری نیست که سرسری انجام داد. بلکه تصمیمی است که باید بعد از تفکر و تفحص گرفت. قبل از عضویت در شبکه های اجتماعی باید سوال های زیر را از خود پرسید:

- چرا می خواهید در این شبکه اجتماعی عضو شوید؟ کار، دلایل شخصی، تفریح، غیره.
- آیا سیاست های حریم شخصی را خوانده اید؟ خیر؟ در این صورت حداقل مقاله ای که حاوی چند نکته در رابطه با سیاست های حریم شخصی این شبکه اجتماعی باشد، پیدا کرده و بخوانید.
- آیا عضویت در این شبکه پرمخاطره به نظر می رسد؟ اگر پرمخاطره به نظر می رسد، چرا هنوز هم می خواهید عضو آن شوید؟ حاضرید تبعات این تصمیم را به جان بخرید؟

- حتما هنگام عضویت در شبکه های اجتماعی از VPN استفاده کنید تا آدرس IP شما در شبکه ثبت نشود. توجه کنید که در این صورت اپلیکیشن، موقعیت مکانی VPN را شناسایی می کند (نه موقعیت مکانی خود شما) و ممکن است اطلاعات دیگری از شما بخواهد و یا بر اساس قوانین کشوری دیگر (مثل قوانین کلی حفاظت اطلاعات اتحادیه اروپا) با شما رفتار کند.
 - آیا می خواهید از اسم واقعی خود استفاده کنید؟ توجه داشته باشید که برخی شبکه های اجتماعی سیاست استفاده از اسم واقعی دارند، این سیاست ها با مرور زمان کم رنگ تر شده اند. اگر علاقه ندارید اسم واقعی خود را هنگام عضویت در شبکه های اجتماعی استفاده کنید، از اسم واقعی خود استفاده نکنید.
 - هنگام عضویت فقط اطلاعات ضروری را وارد کنید و اطلاعات اضافی وارد نکنید.
 - اگر می خواهید هویت خود را مخفی نگه دارید، از ایمیلی غیر از ایمیل شخصی و کاری خود استفاده کنید. مطمئن شوید ایمیلی که استفاده می کنید، به حساب های کاربری دیگر تان متصل نباشد. مثلاً به قابلیت چند حسابی گوگل متصل نباشد. در صورت امکان یک حساب ایمیل رمزنگاری شده مثل Protonmail باز کنید.
 - توجه داشته باشید که ممکن است پاسخ برخی سوالات مربوط به بازیافت گذرواژه، با کمی تحقیق قابل کشف باشد. مثلاً در چه شهری متولد شده اید و یا نام سگ و گربه تان چیست؟ شاید بد نباشد برای برخی از این سوال ها پاسخ های غلط انتخاب کنید.
 - گزینه احراز هویت دو مرحله ای را فعال کنید مخصوصاً اگر نگران موارد فوق هستید. (برای اطلاعات بیشتر در این زمینه به بخش اول این راهنما مراجعه کنید).
 - به محض تایید شدن حساب کاربری خود، تنظیمات پیش فرض حریم خصوصی خود را بررسی کرده و تغییر دهید. همچنین هر وقت نرم افزار یک شبکه اجتماعی به روز رسانی می شود مجدداً تنظیمات حریم خصوصی خود را بررسی کنید.
- توجه کنید که هر زمان وارد اپلیکیشن می شوید، اطلاعاتی مربوط به شما ارسال می شود.** اپلیکیشن های مورد استفاده خود را خوب بشناسید. بعنوان مثال توییتر فقط ۲ تنظیم دارد: حساب کاربری خصوصی و حساب کاربری عمومی. توییتر حد وسط ندارد.

به یاد داشته باشید که تنها شما نیستید که می تواند اطلاعات حساس تان را افشا کند. دوستان می توانند شما را در عکس های مختلف تگ (tag) کرده، موقعیت مکانی شما را اعلام و ارتباطشان با شما را به نحوی علنی (public) کنند. با دوستان خود در رابطه با حریم خصوصی و اطلاعاتی که نمی خواهید درباره ی شما در شبکه های اجتماعی پخش شود صحبت کنید. **خطوط قرمز خود را واضح ترسیم کنید چرا که حریم خصوصی را نمی توان عطف به ماسبق کرد.**



هنگام استفاده از شبکه های اجتماعی، حریم خصوصی باید به طور مداوم مدیریت شود. نکات پایین جهت یادآوری ذکر می شوند:

- برای وصل شدن به حساب کاربری خود از VPN استفاده کنید.
- همیشه پس از هر به روز رسانی نرم افزار، تنظیمات حریم خصوصی خود را بررسی کرده تا مطمئن شوید چیزی عوض نشده و تنظیمات به حالت پیشفرض باز نگشته است.
- بدانید چه کسی را دنبال (follow) می کنید و چه کسی شما را دنبال می کند. چرا که همه ی ارتباطات توسط نرم افزار شبکه های اجتماعی ثبت می شود.
- به عنوان مثال دوستان شما می توانند تمامی صفحات و مقالات مربوط به دگرباشان که شما لایک کرده اید را ببینند.
- « برای احتیاط بیشتر قبل از دنبال کردن افرادی که نمی شناسید، حساب کاربری آنها را بررسی کنید. بیوگرافی و آخرین پست های آنها را مطالعه کرده و نام کاربری آنها را در موتورهای جستجو، جستجو کنید. اگر به چیزی شک کردید، آن فرد را دنبال نکنید.
- قبل از انتشار مطالب (پست کردن)، نوشته خود را مجدداً بخوانید. اگر نسبت به انتشار مطلبی شک دارید، دکمه ارسال (send) را ننزید و مطلب را برای زمان دیگری بگذارید. اگر بعداً هم شک داشتید این مطلب را ارسال نکنید.

پیام رسان و اپلیکیشن های ارتباطی

پیام رسان های بسیار مختلفی وجود دارند که از سیستم همتا به همتا peer-to-peer استفاده می کنند. تلگرام، WhatsApp و سیگنال پیام رسان هایی هستند که از طریق WiFi و یا داده همراه (دیتا) ارتباط شخص به شخص برقرار کرده و از شماره تلفن و یا آدرس ایمیل به عنوان شناسه استفاده می کنند. تلگرام در ایران به تازگی فیلتر شد.

نکاتی که باید در مورد پیام رسان ها بدانید:

- تمامی این اپلیکیشن ها از رمزنگاری end-to-end استفاده می کنند. یعنی محتوا در مبدا کد گذاری شده و در مقصد برای باز کردن این کد به کلید نیاز است. نکته: افرادی که می خواهند از راه پیام رسان با هم در ارتباط باشند، همگی باید از یک اپلیکیشن استفاده کنند، در غیر این صورت این فرآیند دیگر end-to-end نخواهد بود.
- تنظیمات را بررسی کنید! این نوع اپلیکیشن ها داده های فعال و غیرفعال را گردآوری می کنند. تلگرام و WhatsApp هر دو سابقه و محتوای اطلاعات را ذخیره می کنند. با مراجعه به تنظیمات این برنامه ها می توانید ذخیره سازی اطلاعات را غیر فعال کنید. هرچا عبارت «به اشتراک گذاری اطلاعات حساب من» (Share my account information...) را دیدید، آن را غیر فعال کنید. به یاد داشته باشید که WhatsApp متعلق به فیس بوک است و از اطلاعات غیر فعال شما برای تبلیغات استفاده می کند. از بین این سه اپلیکیشن، سیگنال از همه محرمانه تر است چون فقط اطلاعات پروفایل شما را ذخیره می کند. درست ماند VPN هر چه این اپلیکیشن ها اطلاعات کمتری در مورد شما ذخیره کنند برای حریم خصوصی شما بهتر است.
- ذخیره کردن داده ها و دانلود اتوماتیک فایل های رسانه ای. این قابلیت را خاموش کنید. این قابلیت را می توانید در منوی تنظیمات اپلیکیشن یافت.
- پیام رسان ها به صورت خودکار سابقه مکالمات شما را ذخیره می کنند. این قابلیت را خاموش کنید. تنظیمات خود را به گونه ای تغییر دهید تا بعد از مدتی مکالمات شما به صورت خودکار پاک شود. با این کار حتی اگر کسی بدون اجازه به تلفن شما دسترسی پیدا کند، نمی تواند سابقه گفتگوهای گذشته شما را ببیند.
- به صورت پیش فرض نوتیفیکیشن ها فعال هستند. این قابلیت را خاموش کنید. در این صورت حتی اگر کسی که نمی شناسید یا مورد اعتماد تان نیست تلفن شما را ببیند، نمی تواند اطلاعات نوشته شده در هشدار پیام روی صفحه شما را به طور تصادفی بخواند. برای مکالماتی که نمی خواهید در آینده پیدا شوند از گزینه ی چت مخفی (secret chat) و نابودی خودکار (self-destruct) استفاده کنید. نکته: این کار مانع از عکس (اسکرین شات) گرفتن افراد از پیام های شما نمی شود. تا زمانی که پیامی پاک نشده باشد، قابلیت باز پخش آن وجود دارد.
- استفاده از شبکه های توری (Mesh Networks) راهکار دیگری است که می تواند برای شما یک لایه امنیتی اضافی فراهم کند. این نوع شبکه ها دستگاه های الکترونیکی را بطور مستقیم به یکدیگر وصل کرده و از WiFi، اینترنت، و دیتا برای اتصال استفاده نمی کنند.

مشکیت (MeshKit)

یک راهکار ساده برای ساختن چنین شبکه‌هایی استفاده از اپلیکیشن فایر چت (FireChat) است که با مشکیت (MeshKit) ساخته شده است. مشکیت به کسانی که نمی‌توانند از اینترنت یا دیتا استفاده کنند، قابلیت اتصال می‌دهد. این شبکه‌ها چگونه کار می‌کنند؟ داده‌ها با یا بدون اتصال به اینترنت، بطور مستقیم بین تلفن‌های هوشمند iOS و اندروید، حرکت می‌کنند.

فناوری مشکیت این قابلیت را دارد که در کلود هم استفاده شود. ولی نکته کلیدی این فناوری قابلیت استفاده از آن به عنوان شبکه همتا به همتا (peer-to-peer) است. برای اطلاع بیشتر از طرزکار این فناوری به منبع زیر مراجعه کنید:

<https://medium.com/@shalunov/how-many-people-do-you-need-to-build-a-network-out-of-phones-fewer-than-you-think>

۷۲۹fe۵dcdf۲

استفاده از برنامه‌های رادیوی Wifi برای برقراری ارتباط و یا ارسال پیام در موارد اضطراری یا فاجعه‌های طبیعی، مرسوم شده است. استفاده از برنامه

حفاظت از خود در اپلیکیشن‌های دوست‌یابی

هنگام استفاده از شبکه‌های اجتماعی و برنامه‌های دوست‌یابی، خوب است که وب‌سایت و اطلاعات توسعه‌دهندگان آن را برای یافتن جزئیات شیوه کارشان درباره: گردآوری داده، راهنمایی‌های ایمنی، اطلاعات مکانی، تنظیمات، شرایط استفاده از خدمات، حریم خصوصی، تحریم کشورها و برنامه‌های پرداخت خدمات کاربری، بررسی کنید. برای تصمیم‌گیری درباره انتخاب اپلیکیشن، از وب‌سایت‌هایی که کار مقایسه انجام می‌دهند استفاده کنید یا خودتان جدول تهیه کرده و برنامه‌های مختلف را با هم مقایسه کنید. تعدادی از برنامه‌های دوست‌یابی در جدول زیر به عنوان نمونه مقایسه شده اند: Zello پس از فصل طوفان سال گذشته شایع شد. متأسفانه این برنامه فقط با اتصالات WiFi یا تلفن همراه کار می‌کند.

GRINDR	برنامه دوست‌یابی
دستورالعمل‌های ایمنی عمومی درباره افشا اطلاعات شخصی. اگر با فردی قرار ملاقات دارید، به یکی از دوستان خود بگویید. اگر فردی که با او ملاقات می‌کنید، به شما آزار رساند با پلیس تماس بگیرید، و غیره. لینک‌ها و منابع مخصوص کاربران تراجنسیتی (لینک‌های مخصوص ایالات متحده).	راهنمای امنیتی
از GPS برای نشان دادن موقعیت دقیق مکانی شما استفاده می‌کند. تنظیمات مربوط به مخفی کردن محل دقیق در پروفایل است.	فاصله و موقعیت مکانی
امنیت سلامت: وضعیت اچ‌آی‌وی تاریخ آخرین آزمایش. به مردان همجنسگرا اجازه استفاده از کلمات توصیفی و انتشار سن، قد، وزن، قومیت و غیره می‌دهد. فیلتر سنی دارد.	تنظیمات
کسانی که خارج از ایالات متحده از خدمات این برنامه استفاده می‌کنند، موظف به رعایت قوانین محلی بوده و مسئولیت رفتارشان با خودشان است.	شرایط استفاده از خدمات
گفته‌اند که امنیت اطلاعات شخصی را نمی‌توانند تضمین کنند. توضیحاتی درباره هویت جنسی، تراجنسیتی، و غیره دارد.	حریم خصوصی
ترکیه، ایران، عربستان سعودی، اندونزی. پلیس مصر از این برنامه استفاده می‌کند.	کشورهای تحریمی
ابتکارات: از موقعیت جغرافیایی برای مرتبط ساختن افرادی که از خشونت علیه دگرباشان جنسی فرار می‌کنند با سازمان MOSAIC استفاده می‌کند. به تازگی توسط شرکت Beijing Kunlun خریداری شده و این شرکت به اعضا اطمینان داده است که دولت چین به اطلاعاتشان دسترسی نخواهد داشت.	سایر

برنامه دوست یابی	TINDER
راهنمای امنیتی	راهنمای مخصوص اولین ملاقات، ارایه تلفن تماس برای گزارش سوءاستفاده، امنیت در زمان ملاقات با افراد جدید.
فاصله و موقعیت مکانی	اطلاعات مکانی شما را گردآوری می کند و تنها زمانی که بخواهید دیگر از این برنامه استفاده نکنید، می توانید این قابلیت را غیر فعال کنید. فواصل را به مایل نشان می دهد، نه موقعیت دقیق مکانی.
تنظیمات	می توانید مشخصات فردی که دنبال او می گردید را انتخاب کنید. در بيو می توانید گرایش جنسی و سن را مشخص کنید. فیلتر سنی دارد.
شرایط استفاده از خدمات	در قبال رفتار افراد در خارج از برنامه مسئولیت نمی پذیرد. انتشار هر نوع مطلب که دیگران را به خشونت فیزیکی، کوته بینی و نژاد پرستی تشویق کند، ممنوع است.
حریم خصوصی	هنگام استفاده از این برنامه می پذیرید که اطلاعات مربوط به گرایش جنسی، ملیت، قومیت، مذهب و ... را افشا کنید.
کشورهای تحریمی	نامعلوم اما ظاهراً در ایران فیلتر شده است.
سایر	سیستم شان را برای امنیت سایبری مورد بازبینی مداوم قرار می دهند.

برنامه دوست یابی	COFFEE MEETS BAGEL
راهنمای امنیتی	فاقد راهنمای مخصوص اولین ملاقات ولی در صورت جستجو یا رجوع به وبلاگ سازنده این برنامه می توانید نکات ایمنی پیدا کنید، چارچوب مبهم
فاصله و موقعیت مکانی	هنگام استفاده از برنامه، اطلاعات مکانی شما را گردآوری می کند.
تنظیمات	می توانید مشخصات فردی که دنبال او می گردید را انتخاب کنید. باید اطلاعات مربوط به دین، محل کار، و قومیت خود را وارد کنید. قابلیت مرور کردن ندارد و روزی بیش از یک نفر به شما پیشنهاد نمی شود.
شرایط استفاده از خدمات	می پذیرید که هیچ کار خطرآفرین، نژاد پرستانه یا تبعیض آمیز انجام ندهید.
حریم خصوصی	تمام تلاش خود را برای محرمانه نگه داشتن اطلاعات شما می کنند.
کشورهای تحریمی	ممکن است در بعضی کشورها ممنوع یا مسدود باشد.
سایر	تلاش دارد به شما در برقراری ارتباط های معنی دار کمک کند. قابلیت انتخاب رابطه مرد با مرد یا زن با زن دارد. مانند پنج منبع برای جامعه دگرباشان

برنامه دوست یابی	CHAPPY
راهنمای امنیتی	مراقب مطالبی که منتشر می کنید باشید، نکاتی برای ملاقات های حضوری و برون خط، اگر با فردی قرار ملاقات دارید به یکی از دوستان خود بگویید، در روز قرار ملاقات بگذارید، اول طرف خود را بشناسید.
فاصله و موقعیت مکانی	می توان موقعیت مکانی را فعال یا غیر فعال کرد
تنظیمات	بخش درباره من:عکس، سن، شغل، تحصیلات و غیره
شرایط استفاده از خدمات	مسائل معمول، از اطلاعات محافظت کنید و غیره
حریم خصوصی	اطلاعات مربوط به حساب کاربری فیسبوک را گردآوری می کند.
کشورهای تحریمی	نامعلوم
سایر	

HORNET	برنامه دوست یابی
از سلامت خود مطلع باشید. کاربران را از وضعیت HIV اعضا مطلع می کند.	راهنمای امنیتی
موقعیت مکانی شما به صورت داوطلبانه و فقط به کاربران برنامه اعلام می شود.	فاصله و موقعیت مکانی
	تنظیمات
تمرکز راهنمای این اپلیکیشن بر مواردی است که مجاز به نمایش در حساب کاربری خود هستید یا نه (مثلا مطالب نژادپرستانه ممنوع است). به نظر می رسد بیشتر امنیت خود برنامه Hornet مهم باشد تا کاربران.	شرایط استفاده از خدمات
	حریم خصوصی
ظاهرا در ایران فیلتر نشده است. - نامعلوم	کشورهای تحریمی
به دنبال یافتن راهکارهایی برای توانمندسازی جامعه دگرباشان جنسی است. این فقط یک اپلیکیشن نیست بلکه یک شبکه اجتماعی مخصوص جامعه دگرباشان است.	سایر

SCRUFF	برنامه دوست یابی
دستورالعمل های ایمنی را در وب سایت زیر منتشر کرده https://support.scruff.com/hc/en-us/articles/203102124-Location-Security-Privacy-An-Inside-Look و به نظر می رسد تیم پشتیبانی خوبی داشته باشد	راهنمای امنیتی
این برنامه بر اساس موقعیت مکانی فعالیت می کند و براساس موقعیت مکانی اطلاعات می دهد.	فاصله و موقعیت مکانی
اپلیکیشن شبکه ارتباطی که دارای ویژگی های ربات سخنگو یا چت بات chatbot است	تنظیمات
تمرکز راهنمای این اپلیکیشن بر کارهای مجاز و غیر مجاز در آن می باشد. قوانین سختگیرانه درباره جعل هویت.	شرایط استفاده از خدمات
فهرست اطلاعاتی که جمع آوری می کند در لینک زیر آمده است: https://www.scruff.com/en/info/privacy	حریم خصوصی
ظاهرا در ایران فیلتر نشده است. - نامعلوم	کشورهای تحریمی
به امنیت توجه دارد و صفحه ای حاوی فهرستی از قوانین و اطلاعات دارد: https://www.scruff.com/en/resources/trave	سایر

برنامه های دوست یابی وسیله ای برای ارتباط و آشنایی با گروهی از افراد همفکر است. برنامه های دوست یابی تنها یکی از ابزارهای دیجیتالی موجود برای آشنایی با دیگران هستند. برخی افراد از گروه های ملاقات مخصوص علایق مشترک مانند ورزش، مجله کامیک، مسافرت، آشپزی، فیلم و ... استفاده می کنند. در زیر فهرستی از نکات که به ایجاد آگاهی در زمینه امنیت عمومی هنگام تداخل زندگی برخط و برون خط (آنلاین و آفلاین) (به ویژه اگر استفاده از هر یک از این برنامه ها به خودی خود خطرناک است) کمک می کند، آورده ایم.

اگر امکانش را دارید، توصیه می شود که از نسخه پولی اپلیکیشن که به ویژگی های امنیتی پیشرفته تری به شما دسترسی می دهد، استفاده کنید. مخصوصا اگر از طریق VPN به این برنامه ها وصل می شوید.

- از سایت ها و برنامه هایی که به هر کسی اجازه می دهند به شما پیام دهد، اجتناب کنید.
- به تنظیمات موقعیت جغرافیایی برنامه های دوست یابی و یا هر نوع اپلیکیشن شبکه اجتماعی توجه کنید. بسیاری از برنامه های دوست یابی

از موقعیت مکانی شما استفاده می کنند. اما افراد غریبه نباید بتوانند به اطلاعاتی که یافتن محل زندگی شما را ممکن می سازد، دسترسی داشته باشند - در بعضی موارد برای جلوگیری از این امر ممکن است مجبور به خرید ویژگی های اضافه ی برنامه شوید.

- **از سیستم پیام رسان برنامه دوست یابی استفاده کنید.** ممکن است به اندازه ارسال پیامک با سیستم پیام رسان پیش فرض گوشی راحت نباشد، اما از نظر امنیتی برای شما بهتر است.
- **از یک شماره تلفن اینترنتی (VoIP) برای دوست یابی استفاده کنید.** بهتر است قبل از ملاقات حضوری، با فرد مورد نظر صحبت کنید. به جای دادن شماره تلفن واقعی خود به کسی که نمی شناسید، بهتر است از یک شماره تلفن اینترنتی استفاده کرده و تماس را به تلفن خود منتقل کنید. استفاده از Google Voice می تواند یک گزینه مناسب باشد. البته VPN یا سرویس VPN شما هم ممکن است برای شماره های VoIP (چندین سرویس رایگان هست) گزینه هایی داشته باشد .
- **دوستان مشترک خود را پیدا کنید.** گاهی اپلیکیشن های دوست یابی به شما نشان می دهند که با فردی که در حال صحبت با او هستید، دوستان مشترک دارید. با این دوستان صحبت کنید و نظرشان را درباره ی فرد مورد نظر خود جویا شوید. اگر به دوست مشترکتان زیاد اعتماد ندارید، ممکن است بهتر باشد ارتباط تان را زودتر قطع کنید.
- **جستجو کردن افراد، علامت بدبینی و کژانگاری نیست - هوشمندانه است.**
 - « جستجوی نام کاربری - هم از طریق موتور جستجو و هم در شبکه های اجتماعی.
 - « عکس نمایه فرد را جستجوی معکوس کنید. این کار به شما نشان می دهد این تصویر چند بار و کجاها در اینترنت استفاده شده است (مثلا <https://www.tineye.com>).
 - « اگر حساب کاربری مد نظر جعلی باشد، تعداد عکس هایی که می توانید برای جستجوی معکوس استفاده کنید، محدود خواهد بود. در این صورت از فرد مورد نظر عکس های بیشتری بخواهید (که صورتش در آن معلوم باشد) تا بهتر بتوانید وی را بسنجید.
 - « اگر قرار است حضوری ملاقات کنید، سعی کنید نام واقعی او را بررسی کنید یا هر دو توافق کنید که از نام مستعار استفاده کنید. در هر صورت، درباره چارچوبی که برای ایمنی خود تعیین کرده اید، صریح باشید.
- **از انتشار اطلاعاتی که منجر به شناسایی شما می شود، خودداری کنید.**
 - « از افشای جزئیات بپرهیزید - به آنچه در پس زمینه تصاویر تان دیده می شود - مانند نام خیابان، کافه ها، افراد و غیره- توجه کنید.
 - « از عکس های غیر تکراری و منحصر به فرد برای حساب کاربری سایت های دوست یابی استفاده کنید. جستجوی معکوس تصاویر کاری بسیار آسان است . اگر برای حساب کاربری سایت های دوست یابی از عکسی استفاده کنید که در حساب کاربری اینستاگرام یا فیسبوک هم موجود باشد، پیدا کردن شما در شبکه های اجتماعی برای دیگران دشوار نخواهد بود.
- **اطلاعات شخصی خود را به افراد غریبه ندهید -** کلی گویی کنید - آیا این فرد واقعا لازم است بداند از کجا فارغ التحصیل شده اید یا اینکه خواهر و برادر دارید؟ مواردی وجود داشته که از این نوع اطلاعات برای اخاذی استفاده شده است. همیشه هنگام اشتراک گذاری و صحبت با دیگران این نکته را مد نظر داشته باشید.
- **به حس درونی خود اعتماد کنید -** اگر چیزی به شما می گویند یک جای کار اشکال دارد، آن را جدی بگیرید.
 - « **نیروهای انتظامی و گشت امنیت اخلاق برای به دام انداختن دگرپاشان در برنامه های دوست یابی فعالیت می کنند.** بنابراین، اگر در جستجوی خود اطلاعات کمی در مورد شخصی به دست آورده اید، یا سوالات او زیادی خصوصی است و یا چیزی مشکل دار به نظر می رسد، سریع مکالمه را قطع کنید. نمونه این مورد اتفاقی است که به تازگی در مصر افتاد.
 - « **از بستن حساب های کاربری واهمه نداشته باشید.**
- **درباره انتظارات خود قبل از قرار ملاقات توافق کنید.** این کار در هر شرایطی خوب است. مشخص کنید که این دیدار یک قرار ملاقات یا ارتباط کوتاه مدت یا مورد خاص تری است -- بعد ببینید طرف مقابل هم همین درک را دارد یا نه. اگر هدف، برقراری رابطه جنسی است، ترجیحا از قبل درباره خواسته های خود توافق کنید. اگر به چیزی حس خوبی نداشته باشید، گفتگو را قطع کنید.
- **چند قرار اول خود را در مکان های عمومی بگذارید (یا قبل از یک ارتباط hook-up).**

- « این کار ممکن است اولویت شما نباشد و حتی ممکن است زیاده روی به نظر برسد - اما هدف این کار تضمین ایمنی است و این اقدام اضافی ممکن است شما را از یک خطر بالقوه نجات دهد.
- « زودتر سر قرار بروید و چند دقیقه قبل از ورود به محل قرار از بیرون آن را زیر نظر بگیرید.
- « میزی را انتخاب کنید که در وسط رستوران یا کافی شاپ قرار دارد و نسبت به تمام خروجی ها اشراف داشته باشد. حتی بهتر است میزی را انتخاب کنید که به درب خروج دسترسی سریع داشته باشد.
- **به یک نفر بگویید کجا هستید و بهانه ای برای پایان دادن به ملاقات آماده باشید.**
- « یک نفر را در شماره گیری سریع گوشی خود داشته باشید یا قرار بگذارید که در یک زمان معین با شما تماس بگیرد.
- « سعی کنید حتی یک گام فراتر رفته و از دوستی بخواهید در نزدیکی محل شما باشد.
- « برخی افراد حتی یک سرویس مسافری را از قبل رزرو می کنند تا در صورت نیاز بتوانند سریع از محل دور شوند.
- **پول نقد دم دست داشته باشید.**
- « کمی پول در لباس یا لوازم خود مخفی کنید که اگر کیف پولتان گم شد، بدون پول نمانید.
- **اگر حوصله ندارید از پیچاندن قرار تترسید.**
- « پس از اینکه به کسی گفتید مایل به برقراری رابطه نیستید، دیگر هرگز به تماس ها یا ایمیل های وی پاسخ ندهید.

**هرگز از اولویت دادن به ایمنی خود،
خجالت نکشید، حتی اگر لازم باشد
بی ادبانه برخورد کنید.**



منابع و مآخذ

اطلاعات برخط (آنلاین) درباره امنیت دیجیتال

<https://iran.outrightinternational.org/interview-article/safety-security-guide-p2>

امنیت دیجیتال و سلامت روان

https://iran.outrightinternational.org/interview-article/mental_security

محافظت از وسایل الکترونیکی

<https://iran.outrightinternational.org/interview-article/safety-security-guide>

حفاظت از وسایل الکترونیکی در برابر حملات

<https://iran.outrightinternational.org/interview-article/digisecurity>

برای ساختن یک شبکه از تلفن ها به چند نفر نیاز است؟ کمتر از آن که فکر می کنید

<https://medium.com/@shalunov/how-many-people-do-you-need-to-build-a-network-out-of-729fe5dcd2-phones-fewer-than-you-think>



واژه نامه

ردپای دیجیتال

مجموعه ای منحصر به فرد از فعالیت های دیجیتال، اقدامات، مشارکت ها و ارتباطات قابل پیگیری است که در اینترنت و یا دستگاه های دیجیتال نمایان می شود. دو طبقه بندی اصلی برای ردپاهای دیجیتال وجود دارد: غیرفعال و فعال.

ردپای دیجیتال غیر فعال

اشاره به داده هایی دارد که ناخواسته از خود در فضای مجازی به جای می گذارید . به عنوان مثال، هنگام بازدید از یک وب سایت، سرور وب ممکن است آدرس IP شما را ثبت کند. این مساله شرکت رساننده خدمات اینترنت و موقعیت تقریبی مکانی شما را افشا می کند.

ردپای دیجیتال فعال

به داده هایی گفته می شود که به طور آگاهانه در فضای مجازی افشا می کنید . به عنوان مثال، حساب های کاربری شبکه های اجتماعی.

رمزنگاری

به معنی مخدوش کردن پیام یا اطلاعات به گونه ای است که فقط طرفین مجاز، به آن دسترسی داشته و افراد غیر مجاز به آن دسترسی نداشته باشند.

داده های حسگر

داده هایی است که توسط حسگر هایی مانند دوربین و میکروفون در مکان های عمومی، خانه های خصوصی و دستگاه های تلفن همراه ایجاد می شود.

فراداده یا متادیتا

اطلاعات ذخیره شده در فایل هایی است که توسط حسگرها ایجاد شده اند.

شبکه خصوصی مجازی یا VPN

VPN با گسترش برد شبکه خصوصی، به کاربران اجازه می دهد تا از طریق شبکه های مشترک یا عمومی به تبادل اطلاعات بپردازند. فعالیت VPN بگونه ای است که انگار رایانه ها به طور مستقیم به یک شبکه خصوصی وصل هستند. برنامه هایی که تحت VPN اجرا می شوند می توانند از کارکرد، امنیت و مدیریت شبکه خصوصی بهره مند شوند.

شبکه همپوشان داوطلب و رایگان جهانی هدایت می کند. این شبکه دارای بیش از ۷ هزار رله (رایانه هایی که اجزا کوچک اطلاعات از آنها عبور می کند) است. این شبکه پیازی مکان و محتوای اطلاعات کاربران را از هر کسی که نظارت شبکه یا تجزیه و تحلیل ترافیک انجام می دهد، پنهان می کند.	TOR چیست؟ یک شبکه پیازی (onion router) یا چند لایه است که ترافیک اینترنت را از طریق یک
به معنی استفاده از لایه سوکت های امن (Secure Socket Layer- SSL) یا پروتکل امنیتی لایه انتقال (Transport Layer Security-TLS) تحت HTTP است. HTTPS درخواست های صفحه کاربر و نیز صفحاتی که مرورگر از سرور وب دریافت کرده را رمزنگاری و رمزگشایی می کند. استفاده از HTTPS مانع از استراق سمع و حملات مرد میانی می شود.	HTTPS (HTTP over SSL or (HTTP Secure
یک پروتکل استاندارد باز است. این پروتکل برای ارائه دادن رابط ارتباطی انعطاف پذیر داده جهت انتقال اطلاعات بین وسایل الکترونیکی در قالب پیام کوتاه، طراحی شده است.	پیام کوتاه همتا به همتا (SMPP)
رادیو WiFi یک شبکه بی سیم است که درست مانند تلفن همراه، تلویزیون و رادیو امواج رادیویی استفاده می کند. در حقیقت، برقراری ارتباط درون یک شبکه بی سیم بسیار شبیه ارتباطات رادیویی دو طرفه است.	WiFi
یک برنامه پیام رسان رایگان برای ارتباطات عمومی و خصوصی است که حتی بدون دسترسی به اینترنت یا داده همراه (دیتا) کار می کند. FireChat با MeshKit ساخته شده است.	FireChat
یک ماژول نرم افزاری است که توسعه دهندگان را قادر می سازد تا اتصال مشبک همتا به همتا peer to peer را به برنامه یا دستگاه خود اضافه کنند. داده ها به طور مستقیم بین گوشی های هوشمند (iOS و Android) و بدون نیاز به اتصال به اینترنت، جریان می یابد. Open Garden کار دشوار بهینه سازی بلوتوث، Bluetooth LE، Wi-Fi Direct، ANT، و دیگر پروتکل های بی سیم را در تمامی نسخه های مختلف اندروید و iOS انجام داده است. در حال حاضر برخی سازمان ها می توانند از «جادوی مش» بهره مند شوند.	MeshKit
رمزنگاری End-to-End از مشاهده مکالمه توسط شخص سوم جلوگیری می کند. این کار با ارسال کلید رمزگشایی پیام از طرف گیرنده انجام می شود، بنابراین فقط گیرنده می تواند پیام را مشاهده کند. این روش نوعی رمزنگاری است که در آن پیام ها کد گذاری می شوند و برای باز کردن آنها کلید لازم است.	رمزنگاری End-to-End

77B134

1 36 40

2

0

294A

A21BE E F

5

A85B

A 05E2



2

E7

26B22 BB1DE24F8
83C64064F
5 AC44A4684902
55095BFBC5605076
73532277B
AA7F8F089
3C2E6C4E90
C4A21BE4E7F
A85BECCB
CAA05F28B2
7229247687363
77BC25E3
15565C90ABAA
0704D6422501200D

64

AB1D
D608C16
B7E92DFE
4680605
97C4B6423
46F2F4
DD 2573375
118107
66C42CC
CD128D5
C84EE5DE909
B513

BAA3

