



Before You



THINK!

T - is it true?

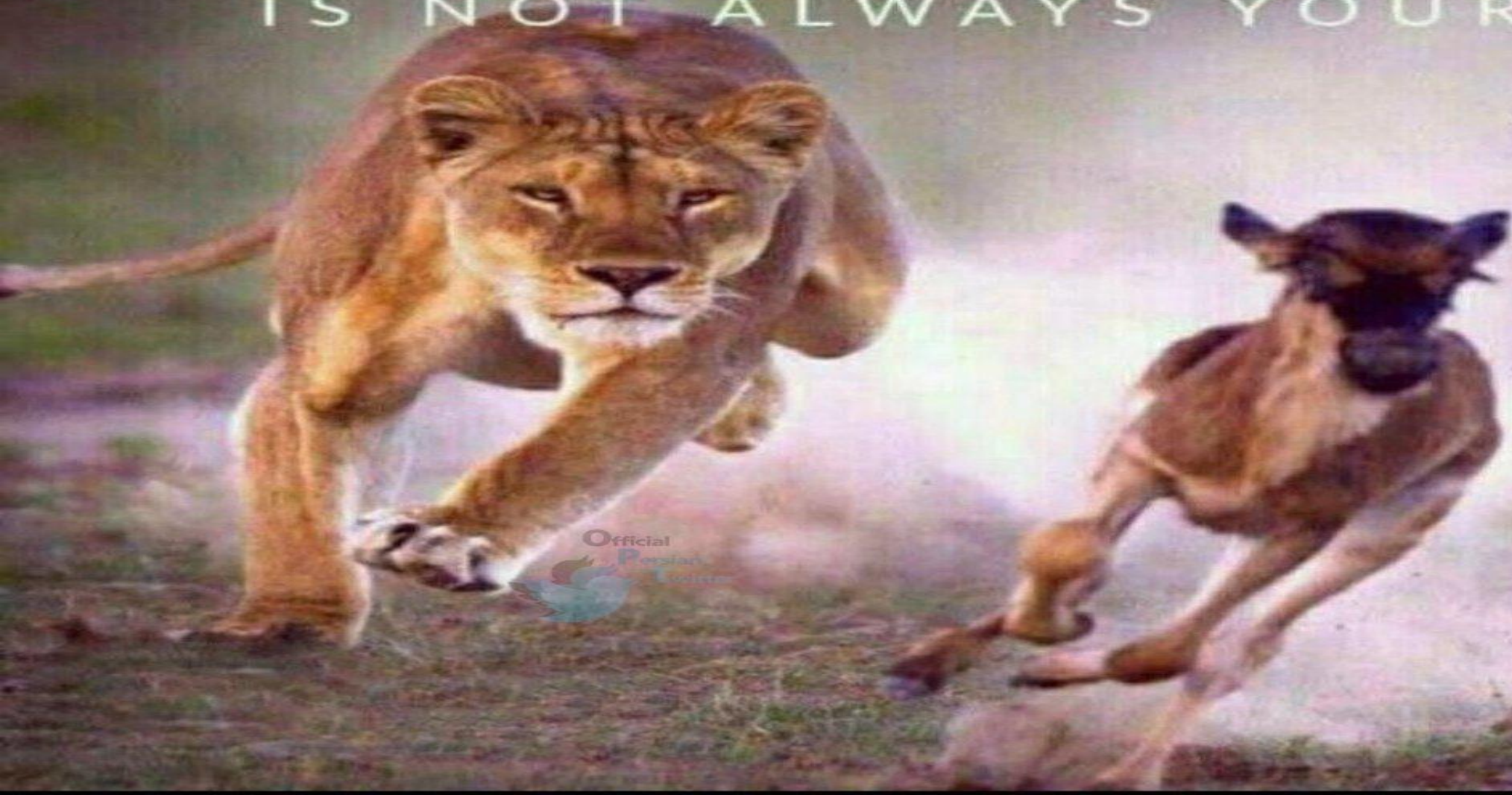
H - is it helpful?

I - is it inspiring?

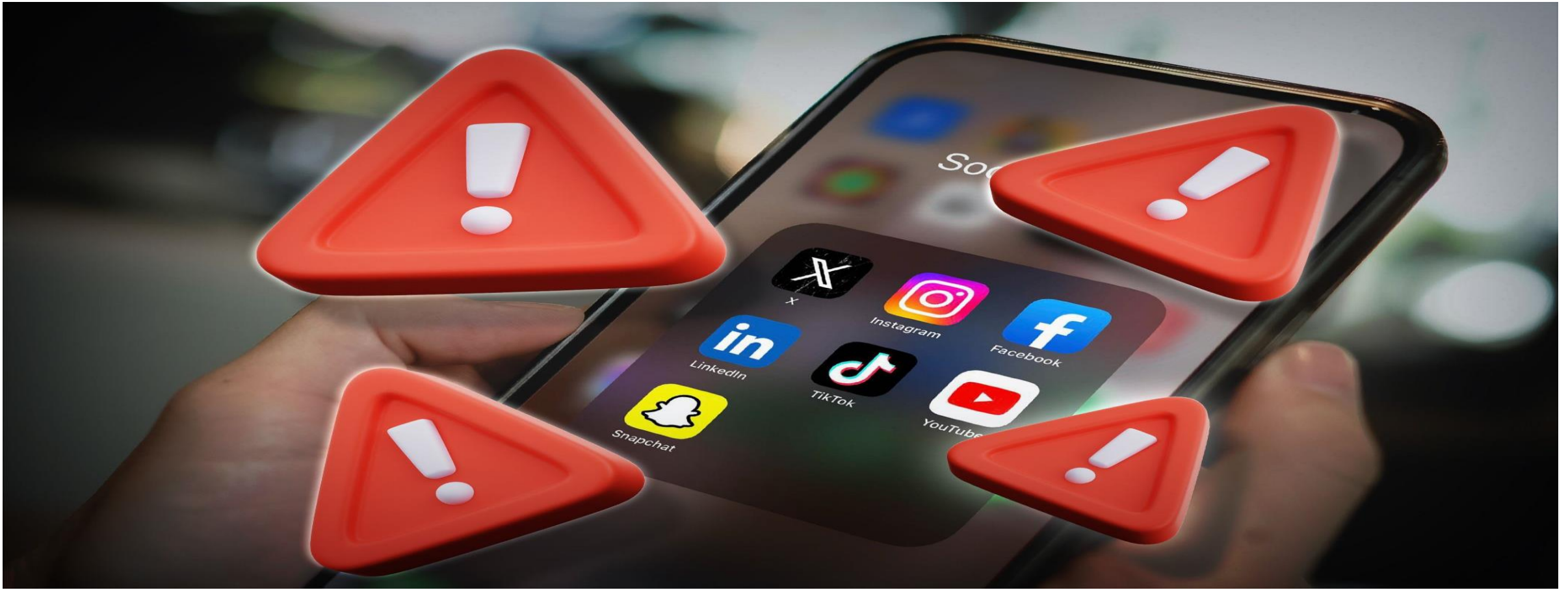
N - is it necessary?

K - is it kind?

YOUR
FOLLOWER
IS NOT ALWAYS YOUR FAN







Privacy and Protection Don't Mean Social Networks are Good for You

خیلی هالز هین قلمه عاشق زنده گیسولونو پیدا کردند



هیچی نلگو، سلت خورده
دوسالی بود که با عشق
تو واسر آشنا شده بود -
دیروز فهمید طرف ناصر
شاطر سرکوفه است

Does Social Media Do More Harm Than Good for Society?

Propaganda and Misinformation Spread on Social Media





Pros: Why is social media good?

Social media and technology offer us greater convenience and connectivity:

- staying connected with family and friends worldwide via email, text, FaceTime, etc.
- quick access to information and research
- banking and bill pay at our fingertips
- online learning, job skills, content discovery (YouTube)
- involvement in civic engagement (fundraising, social awareness, provides a voice)
- great marketing tools ابزار عالی بازاریابی
- opportunities for remote employment فرصت های شغلی از راه دور



Cons: Why is social media bad?

- Online vs Reality هویت جعلی
- Increased usage (time spent) صرف زمان زیاد
- Social Media is addicting. اعتیاد
- Fear of Missing Out. [FOMO](#) ترس از دست دادن مطالب و اخبار
- Self-image issues نیاز به تایید دیگران و کاهش اعتماد به نفس

social networks

10 negative effects of social media on society



- 
- Cyberbullying قلدری سایبری
 - Spread of misinformation اطلاعات نادرست
 - Addiction اعتیاد
 - The decline in face-to-face communication ارتباطات چهره به چهره
 - Self-esteem issues اعتماد به نفس
 - Social isolation انزوای اجتماعی
 - Polarization and echo chambers قطبی شدن — فقط دوست داریم به علایق توجه نماییم
 - Cyberstalking and harassment آزار و اذیت سایبری
 - Decrease in privacy کاهش فضای خصوصی
 - Comparison and envy مقایسه کردن



Misinformation vs. Disinformation: What Is the Difference?





What Is Misinformation?

اطلاعات غلط چیست

اطلاعات غلط صرفاً اطلاعات نادرستی است که بدون توجه به قصد منتشر می شود. کسانی که در گسترش آن دخیل هستند نمی دانند آنچه آنها به عنوان واقعیت در نظر گرفته اند، در واقع نادرست است.

این روزها، اطلاعات نادرست به دلیل رسانه های اجتماعی و اینترنت تأثیر گسترده تر و ویرانگری دارد، یعنی با سهولت اشتراک گذاری همه چیز تشدید می شود.

به عنوان مثال، اطلاعات نادرستی منتشر شده است که می گوید واکسن ها باعث ناباروری، اوتیسم و مرگ می شوند. این امر باعث شده است که بسیاری از جمله افراد مشهور از مصرف واکسن کووید-۱۹ امتناع کنند و دیگران را تشویق کنند که از این کار استفاده نکنند. در نتیجه، این واکسن در بخش های مختلف با مقاومت مواجه شده است



What Is Disinformation?

اطلاعات نادرست چیست؟

اطلاعات نادرست به انتشار عمدی اطلاعات نادرست برای فریب دادن، ایجاد هرج و مرج، گمراه کردن و دستکاری مردم اشاره دارد.

برخلاف اطلاعات نادرست که می تواند بدون قصد سوء منتشر شود، اطلاعات نادرست با هدف صریح فریب و اغلب با یک برنامه خاص منتشر می شود.

همچنین می تواند از منابع بسیاری از جمله انتشار اطلاعات نادرست توسط هوش

مصنوعی باشد. THIS PERSON DOES NOT EXIT.

6 Questions to Ask Yourself Before Joining Any Social Network

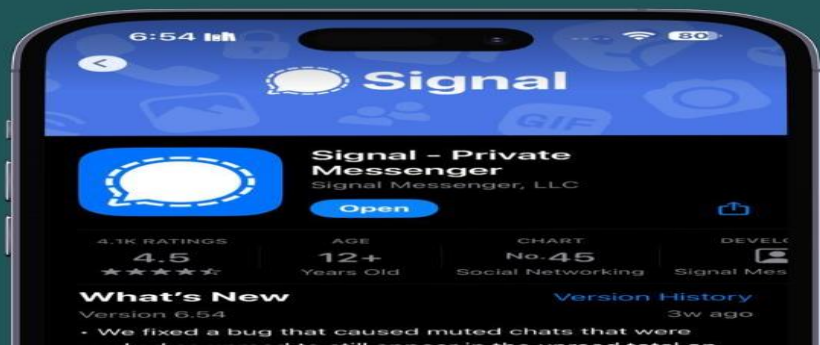


- How Does the Site Handle Privacy and Your Data?
- Does the App's Content Align with Your Interests?
- Will The App Merely Be a Distraction?
- Who Are You Likely to Connect With?
- What Features Does the App Offer?
- Is the Platform Future-Proof?

How Does the Site Handle Privacy and Your Data?

چگونه سایت با حریم خصوصی و داده های شما برخورد می کند؟

برخی از پلتفرم ها سیاست های حفظ حریم خصوصی مشکوک دارند. به عنوان مثال، WhatsApp ممکن است اطلاعات حساب شما از جمله شماره تلفن، استفاده از برنامه، آدرس IP و سایر اطلاعات را با متا و سایر ارائه دهندگان خدمات شخص ثالثی که برای بهبود خدمات خود با آنها همکاری می کند، به اشتراک بگذارد.



Does the App's Content Align with Your Interests?

آیا محتوای برنامه با علایق شما مطابقت دارد

امروزه، پلتفرم های رسانه های اجتماعی تمایل دارند بر یک نوع اصلی محتوا تمرکز کنند. به عنوان مثال، TikTok در درجه اول دارای ویدیوهای کوتاه است، در حالی که YouTube به شدت به سمت ویدیوهای طولانی تر متمایل است.

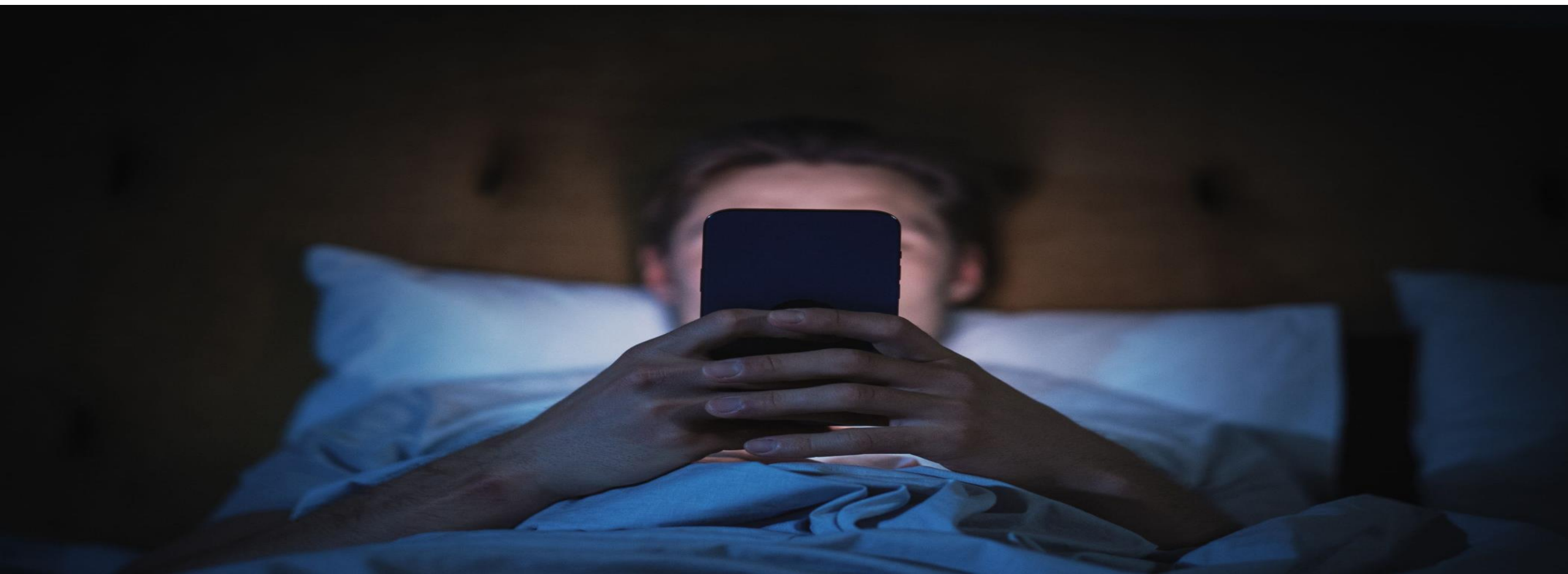
پلتفرم ایکس (توییتر سابق) بر روی پست های کوتاه متمرکز می باشد

Snapchat بر روی پست سریع و موقت متمرکز می باشد

اینستاگرام بر روی Reels و اشتراک گذاری عکس متمرکز می باشند

Will The App Merely Be a Distraction

آیا این برنامه صرفاً یک حواس پرتی خواهد بود



Who Are You Likely to Connect With

احتمال دارد با چه کسی ارتباط برقرار کنید

قبل از اینکه برای یک پلتفرم ثبت نام کنید، لحظه ای در مورد نوع افرادی که امیدوارید با آنها تعامل داشته باشید فکر کنید - دوستان و خانواده، تأثیرگذاران و سازندگان محتوا، یا حرفه ای ها؟ سپس، در مورد پایگاه کاربری پلتفرم تحقیق کنید تا ببینید آیا با مخاطب مورد نظر شما مطابقت دارد یا خیر؟

What Features Does the App Offer

برنامه چه ویژگی هایی ارائه می دهد

یک چیز مسلم است - پلتفرم های رسانه های اجتماعی همیشه در رقابت با یکدیگر هستند. اینستاگرام و فیسبوک Stories و Reels را برای رقابت با TikTok و snapchat راه اندازی کردند، TikTok Notes را برای رقیب اینستاگرام معرفی کرد و اگر دقت کنید نمونه های بی شماری ظاهر می شوند.

اگر پلتفرم های مستقر دائماً از یکدیگر استفاده می کنند، جای تعجب نیست که برنامه های جدیدتر سعی می کنند ویژگی های محبوب را نیز تکرار کنند. اما بسیاری از پلتفرم ها هنوز در مرحله رشد خود ممکن است فاقد ویژگی هایی باشند که شما به آنها تکیه می کنید

عمر پلتفرم

حالی که اگر برای یک شبکه اجتماعی ثبت نام می کنید که سال هاست وجود دارد، این موضوع نباید مشکلی ایجاد کند، اما طول عمر پلتفرم های جدیدتر اغلب غیر قابل پیش بینی است. تقریباً غیر ممکن است که بدانیم آیا یک برنامه واقعاً اجرا می شود یا خیر.



WHAT DO YOUR DEVICES KNOW ABOUT YOU?

Whether it's a computer on your desk or a phone in your pocket, your devices retain a lot of personal data. And all of that information may be vulnerable to cybercriminals.



WINDOWS PCs



MACS



ANDROID TABLETS



SMART PHONES

Passwords



Web browser autofill
Stored in the file system

Credit Card Numbers



Web browser autofill
Downloaded credit card statements

Social Security Number



Downloaded tax documents

Deleted Files



All deleted files, including ones no longer in recycle bin or trash, can be recovered until physical storage space overwritten.

Bank Account Info



Downloaded bank statements

Recent Files



List kept by operating system



Various applications keep their own recent file lists

Contacts



Windows Contacts



Address Book



Contact manager

Current Location



Readable off your GPS

Text Messages



Text log stored on phone

Phone Calls



Call log stored on phone

KNOWING WHAT INFORMATION YOUR DEVICE CONTAINS IS THE FIRST STEP TO PROTECTION.

Name and Address



Web browser autofill



Windows Contacts



Address Book



Contact manager

Recently Visited Sites



Browser's cache



Browser's history



Cookies

Recent Locations



Photos
Navigation apps

CYBER CRIME STATISTICS

Average monetary cost to victim of cyber crime:



Email scams sent daily:

75
MILLION



Daily victims of scam emails:

2,000



Percent of Americans who have experienced cyber crime:

73%



Percentage of Americans who believe that cyber-criminals will not be brought to justice:

78%

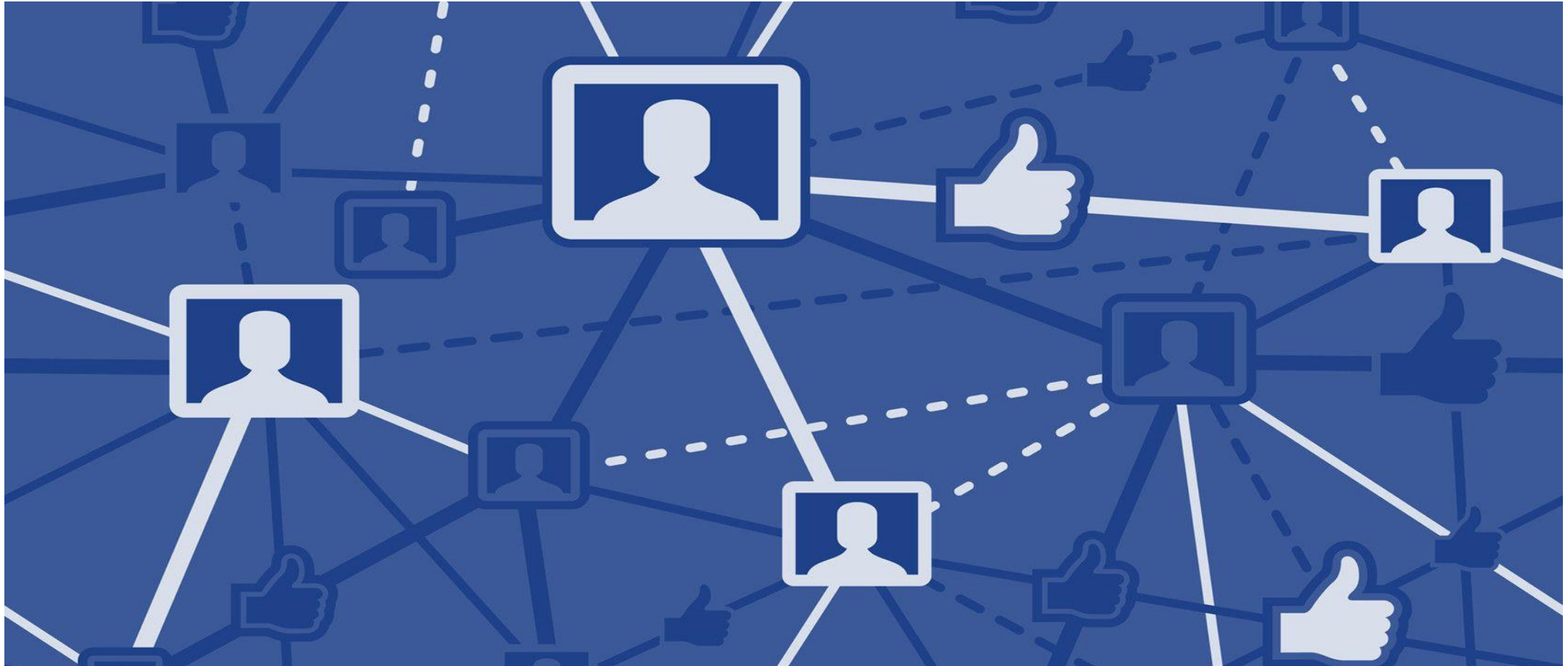


Percentage of Americans who expect to escape cyber crime in their lifetime:

2%

SOURCE: CYBER CRIME WATCH

How Do Social Networks Make Money?



Fundraisers

About

Explore

+ Raise Money



Create a Fundraiser

Facebook fundraisers make it easy to support friends, family and the causes that are important to you, such as:



No fees for donations to most non-profit fundraisers and low fees for personal fundraisers



Over 1 million non-profits on Facebook to support or raise money for a personal cause such as a medical or education cause



Quickly spread your story to build momentum and raise more money

Raise Money

Popular on Facebook



Fundraiser categories

- Animals
- Arts and culture
- Business
- Community and social action
- Crisis relief
- Education
- Environment
- Faith
- Funeral and loss
- Health and medical
- International
- Personal emergency
- Sport

- 1. Venture Capital سرمایه خطر پذیر
- 2. Advertising تبلیغات
- 3. User Data داده های کاربران
- 4. Premium Memberships عضویت های ممتاز
- 5. Transaction Fees and Virtual Products کارمزد تراکنش ها
- 6. Diversifying متنوع کردن

چند راه حل ساده برای ایمن ماندن در شبکه های اجتماعی

گمنام ثبت نام کنیم مراقب پیگانه ها باشیم واقع بین باشیم

تنظیمات حریم خصوصی خودمان را ارتقاء دهیم

در صورت نیاز از شناسه های مکان یابی استفاده کنیم

افرادی را که به عنوان دوست قبول می کنیم، با دقت انتخاب کنیم

اطلاعات شخصی خود را به اشتراک نگذاریم

از عکس ها و
آبرویمان محافظت
کنیم

از رمز عبورهای قوی استفاده کنیم



SOCIAL MEDIA SECURITY

4 TIPS TO KEEP YOUR PERSONAL INFORMATION SAFE ON SOCIAL MEDIA



1. THINK BEFORE YOU POST.

Do not post any personal information, such as your full birthdate, that could fall into the wrong hands and be used against you.

2. USE STRONG, DIVERSE PASSWORDS.

Information about you, such as your dog's name, is probably on the internet. Therefore, it should not be your password. You also should not reuse passwords for other sites.



3. USE PRIVACY SETTINGS.

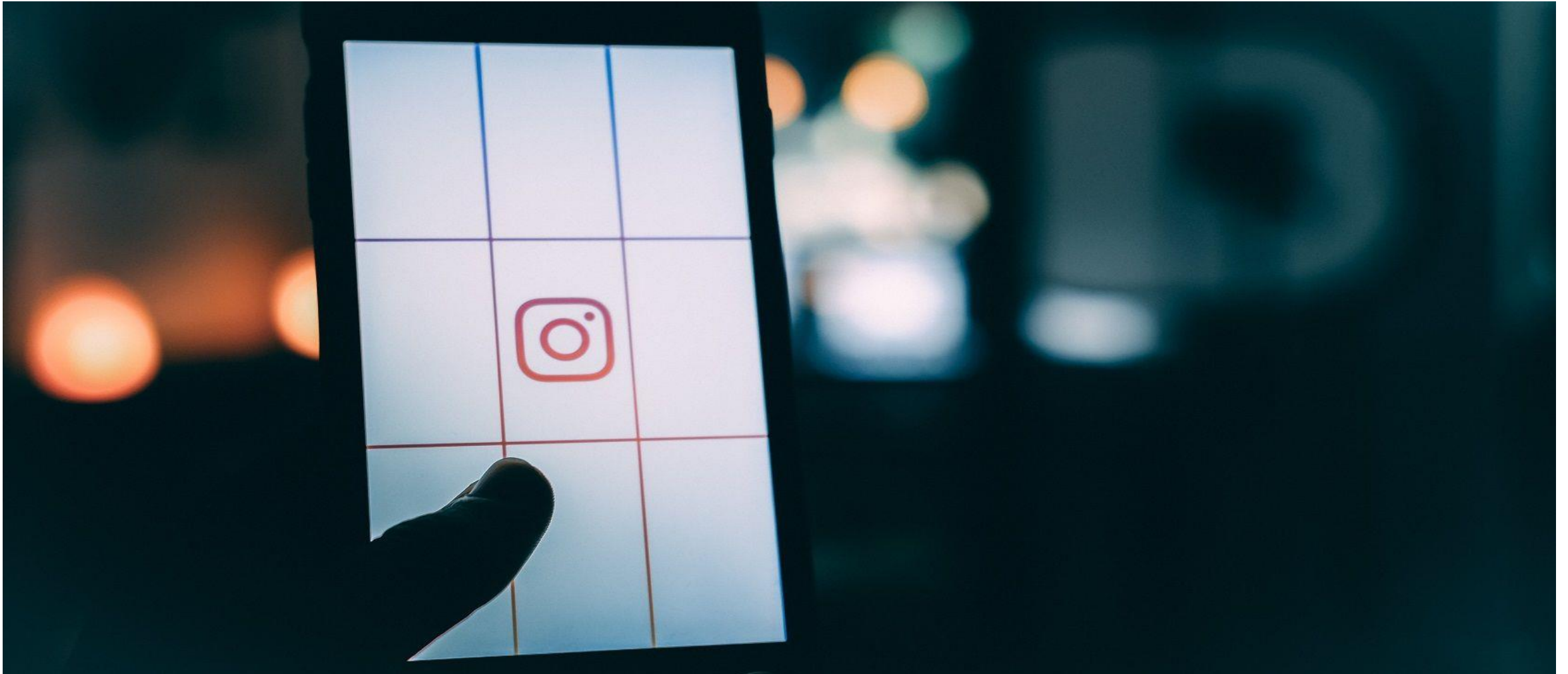
You should ensure that whatever you're posting is only shown to the friends and family if that's your preference (and it probably should be).

4. BE IMAGE CONSCIOUS.

Make sure your social media image is what you want it to be for future employers.

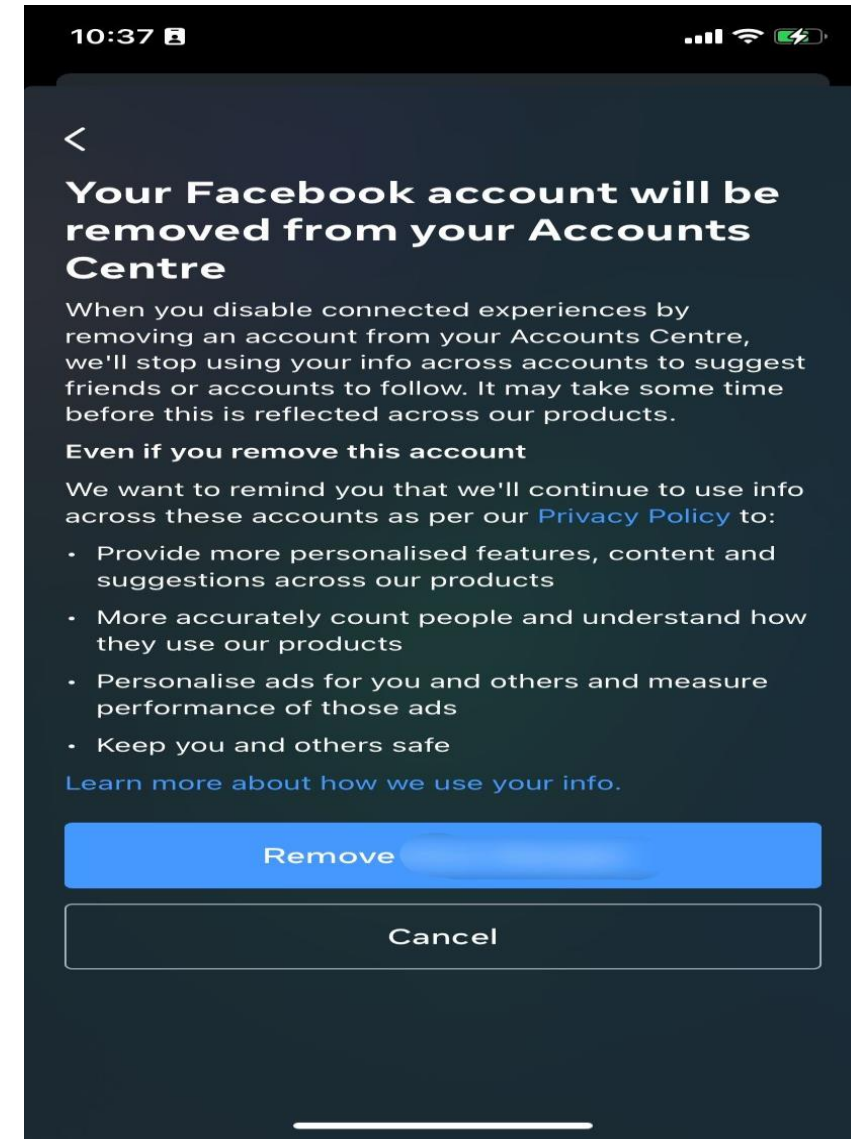
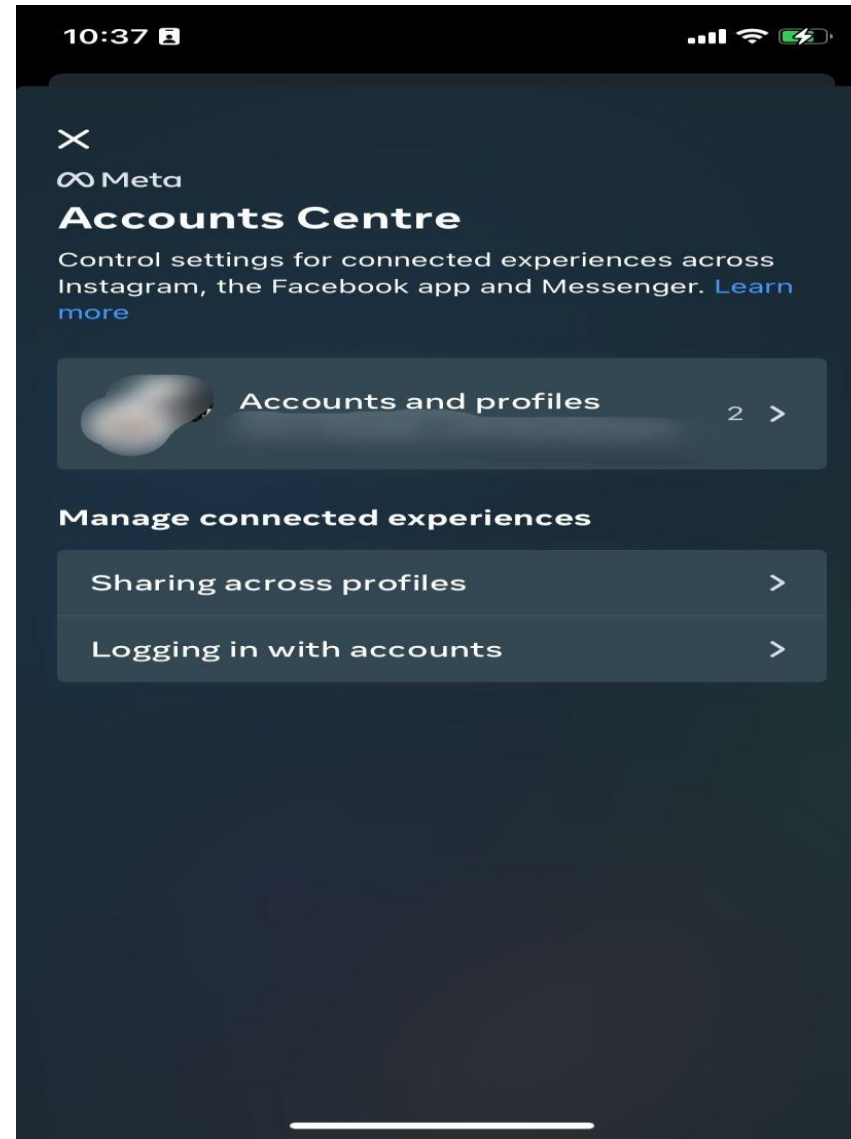
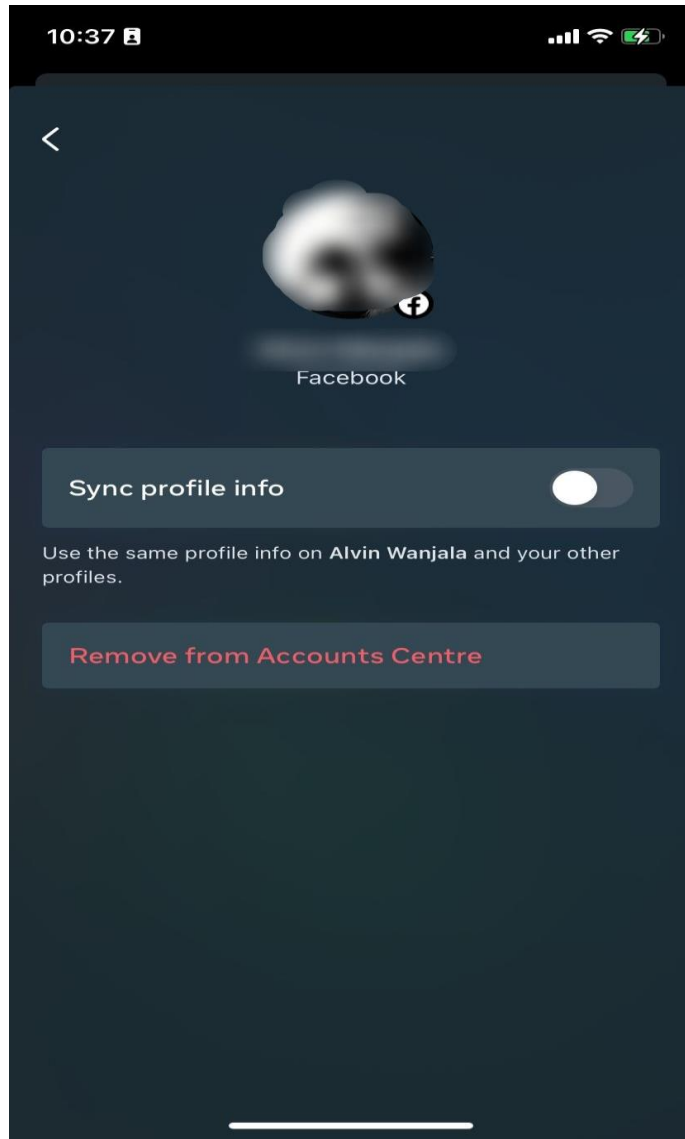


How to Make Your Instagram More Private



1. Unlink Your Facebook Profile

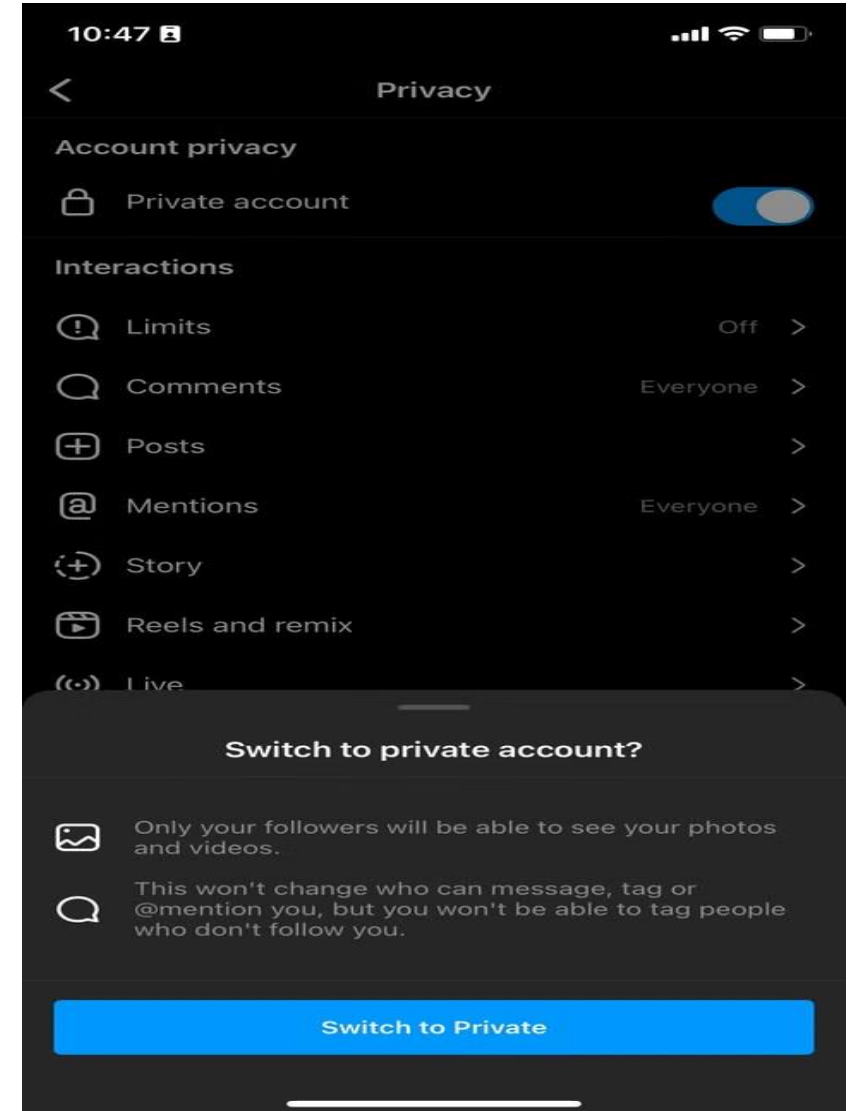
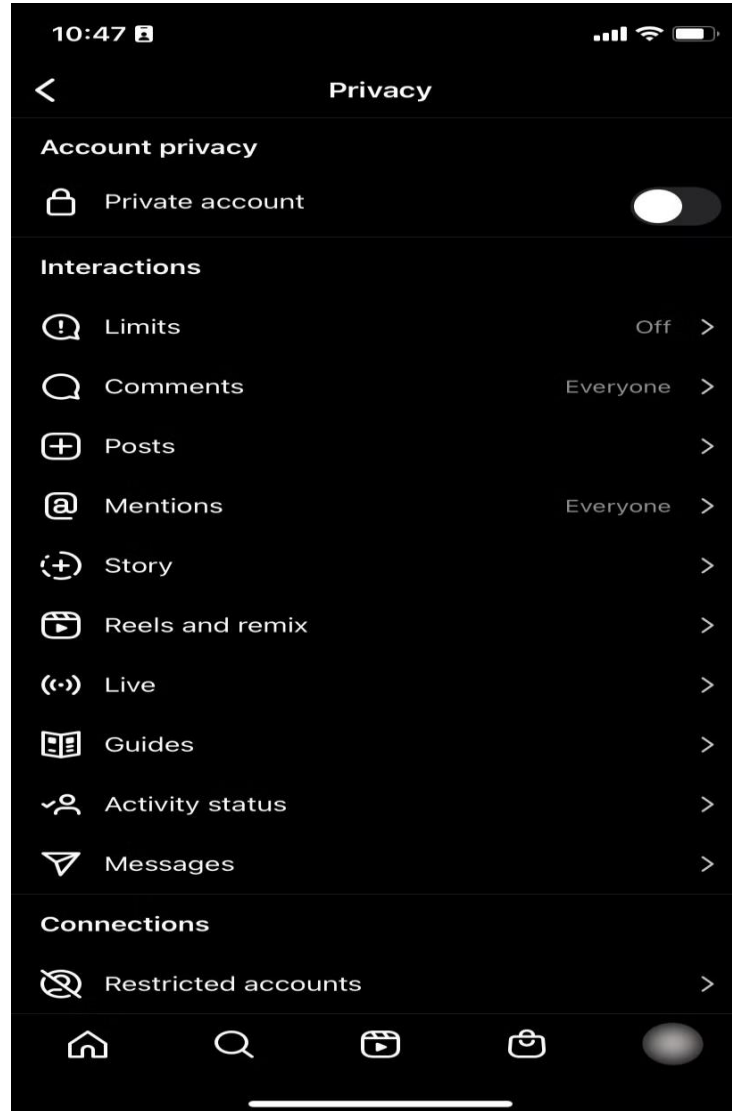
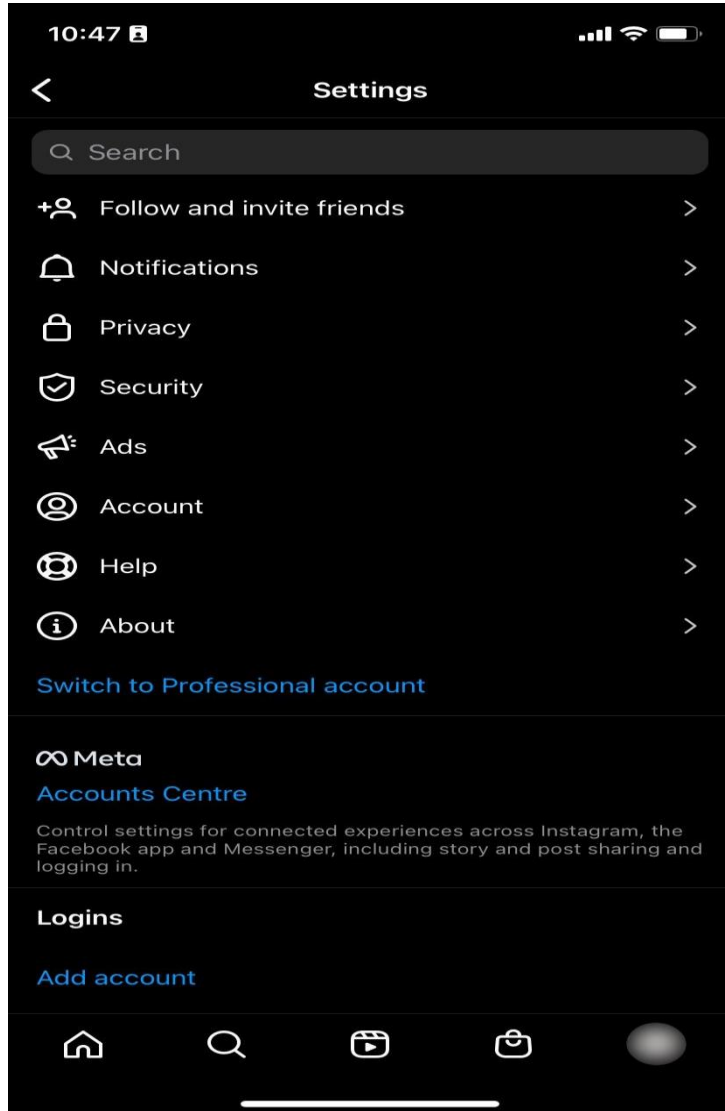
پیوند پروفایل فیسبوک خود را لغو کنید



برای جدا کردن حساب فیسبوک خود از اینستاگرام، به صفحه پروفایل اینستاگرام خود بروید. در آنجا، روی نماد همبرگر واقع در گوشه بالا سمت راست ضربه بزنید و وارد تنظیمات شوید. روی **Accounts Center > Accounts and profiles** ضربه بزنید و حساب فیسبوک پیوند شده خود را انتخاب کنید. روی **Remove from Accounts Center** ضربه بزنید و در صفحه بعد **Continue** را بزنید. در نهایت، روی **Remove [Facebook account account]** ضربه بزنید تا پیوند پروفایل فیس بوک خود را لغو کنید.

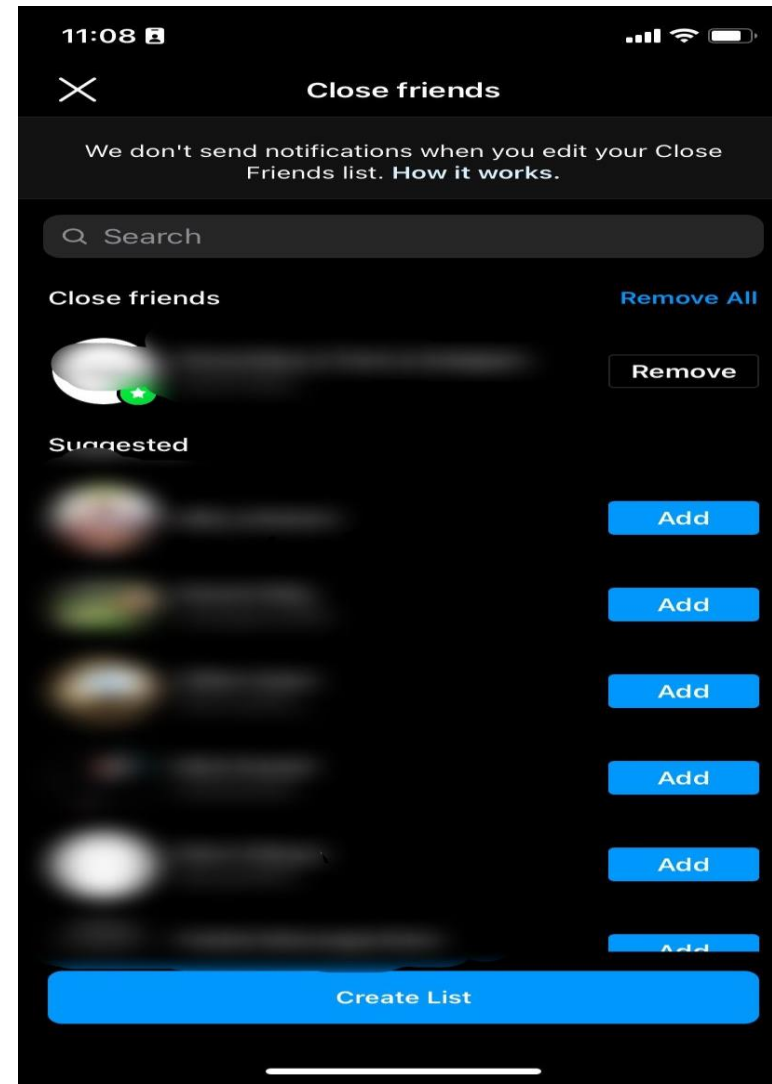
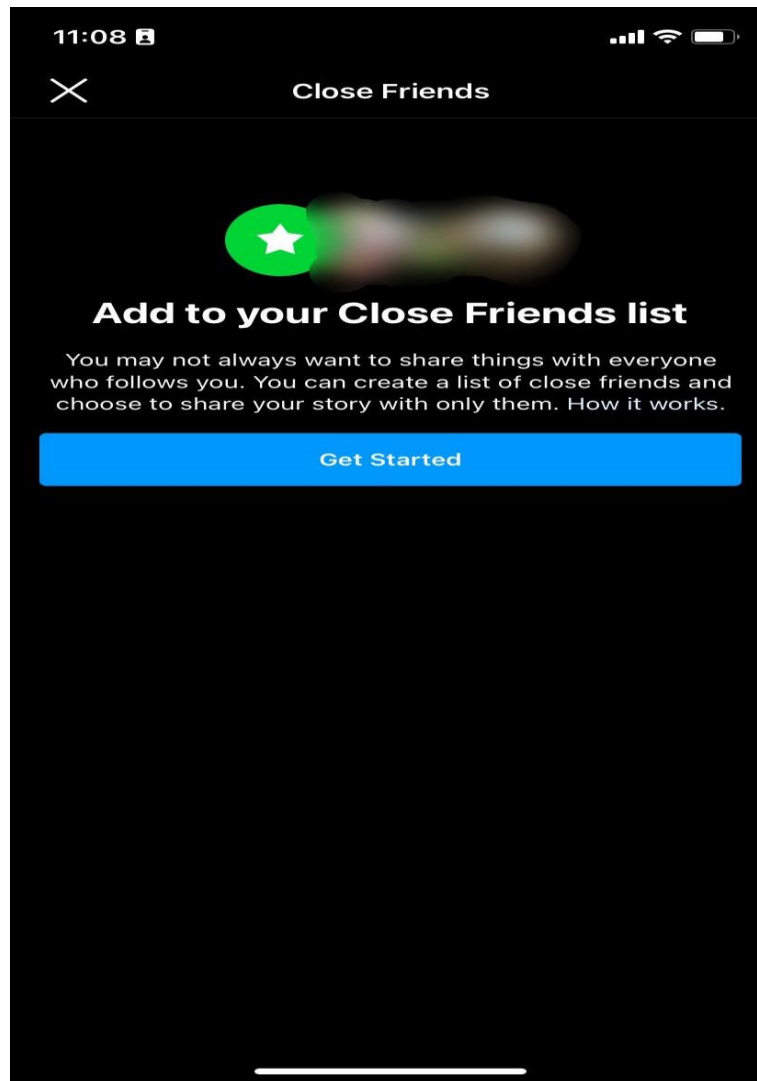
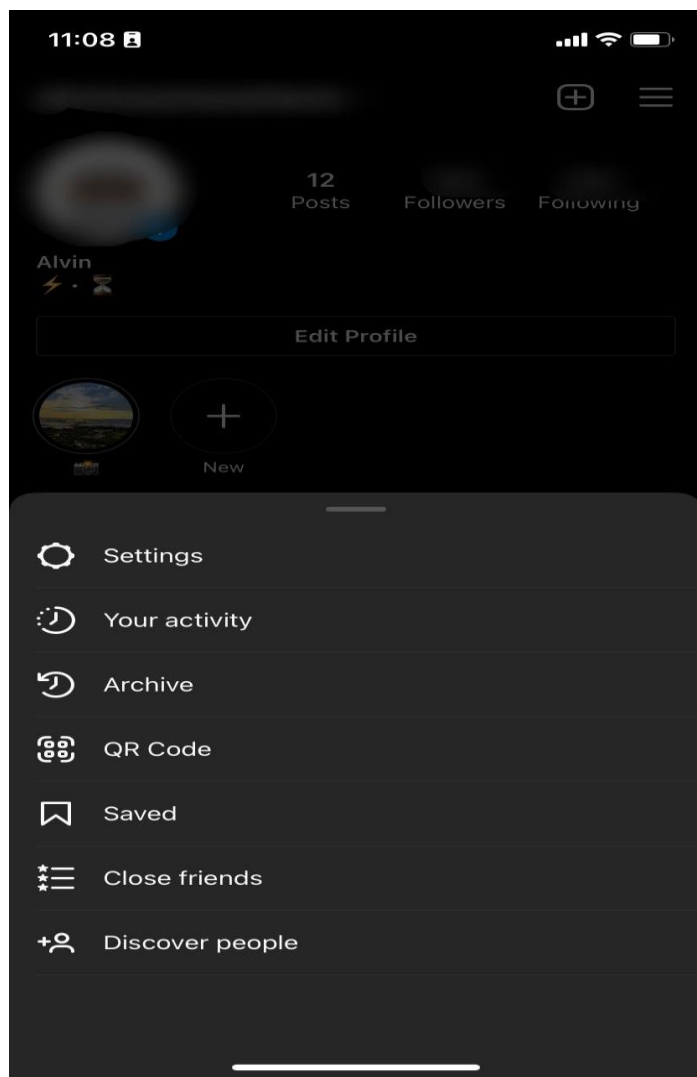
2. Set Your Instagram Account to Private

اکانت اینستاگرام خود را روی خصوصی تنظیم کنید



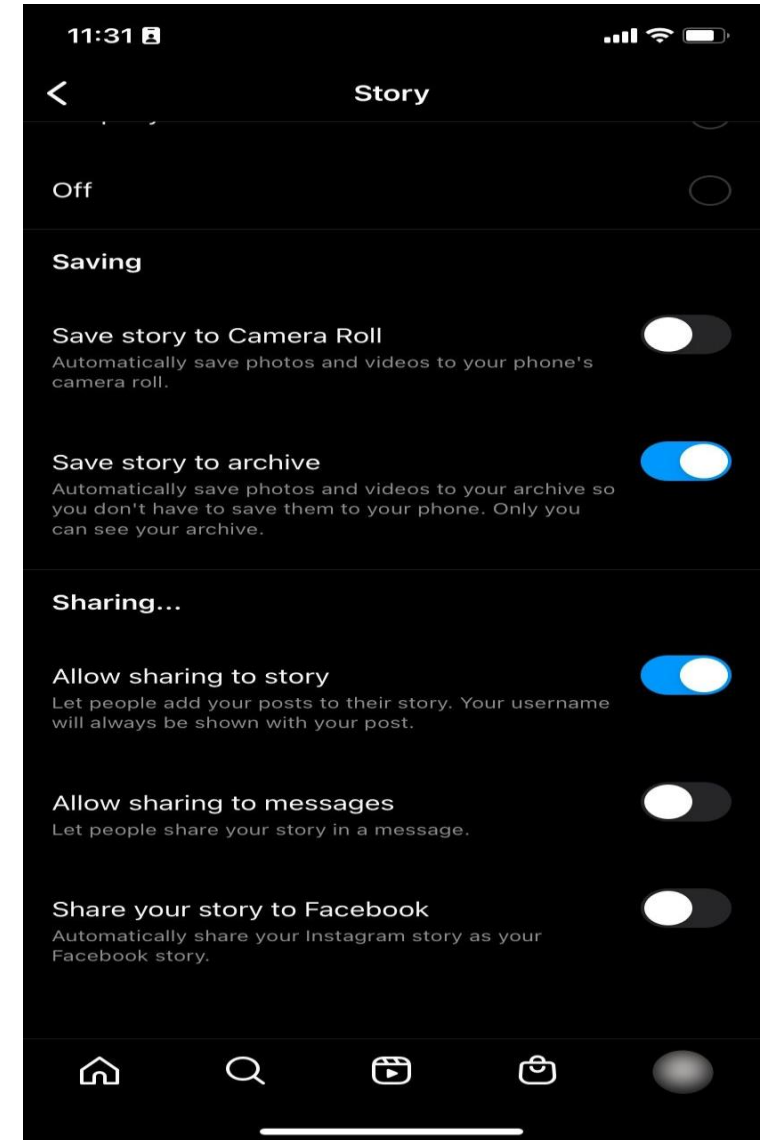
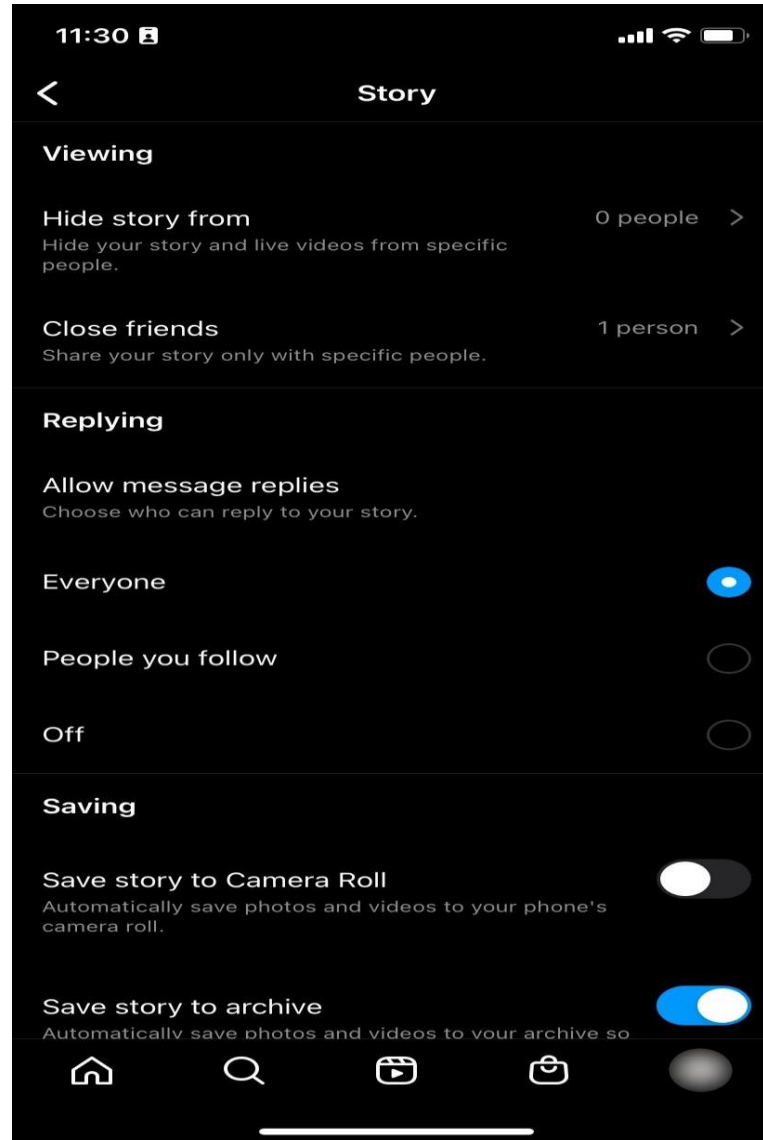
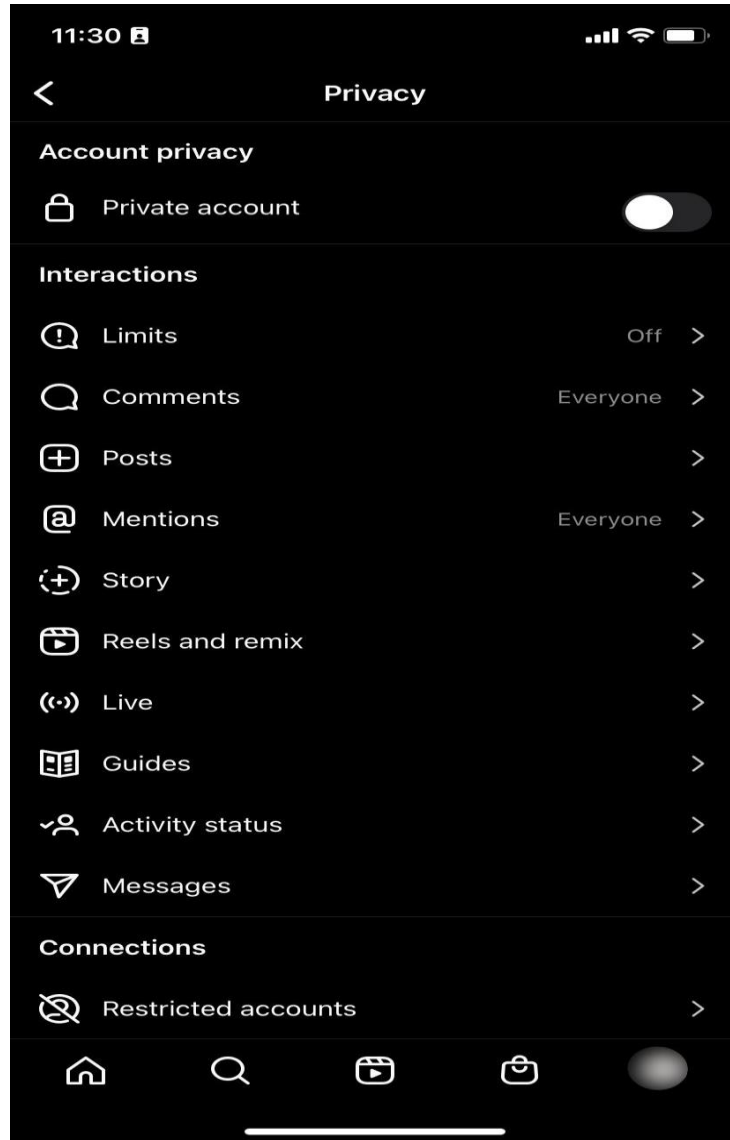
3. Pick and Choose Your Close Friends

دوستان نزدیک خود را انتخاب کنید



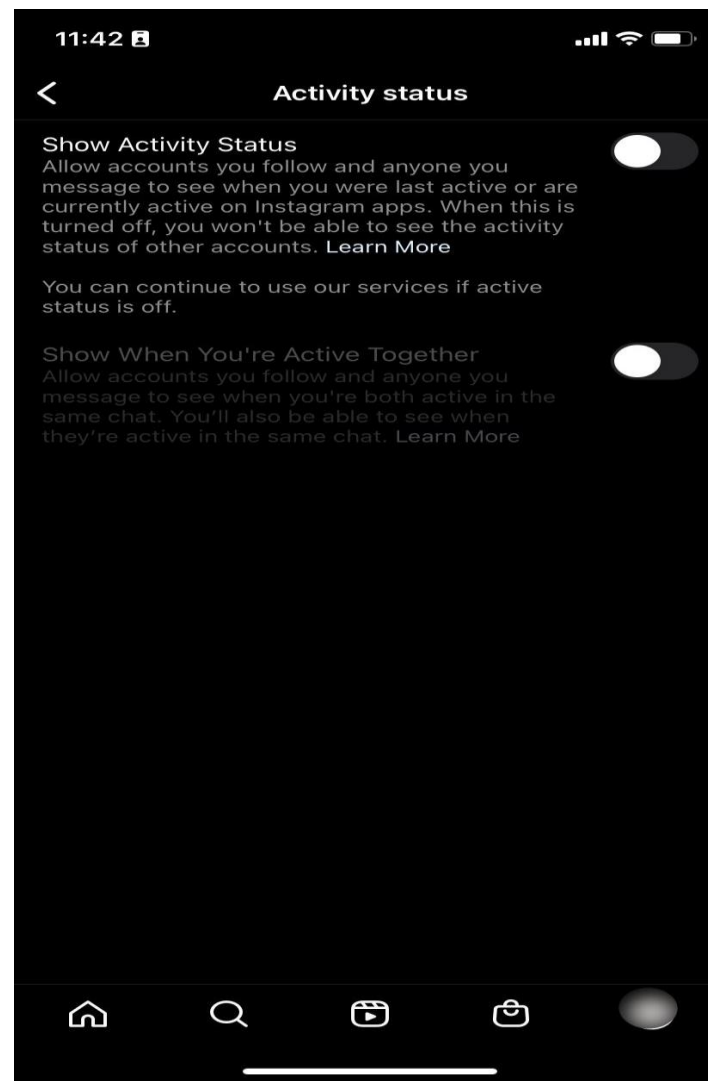
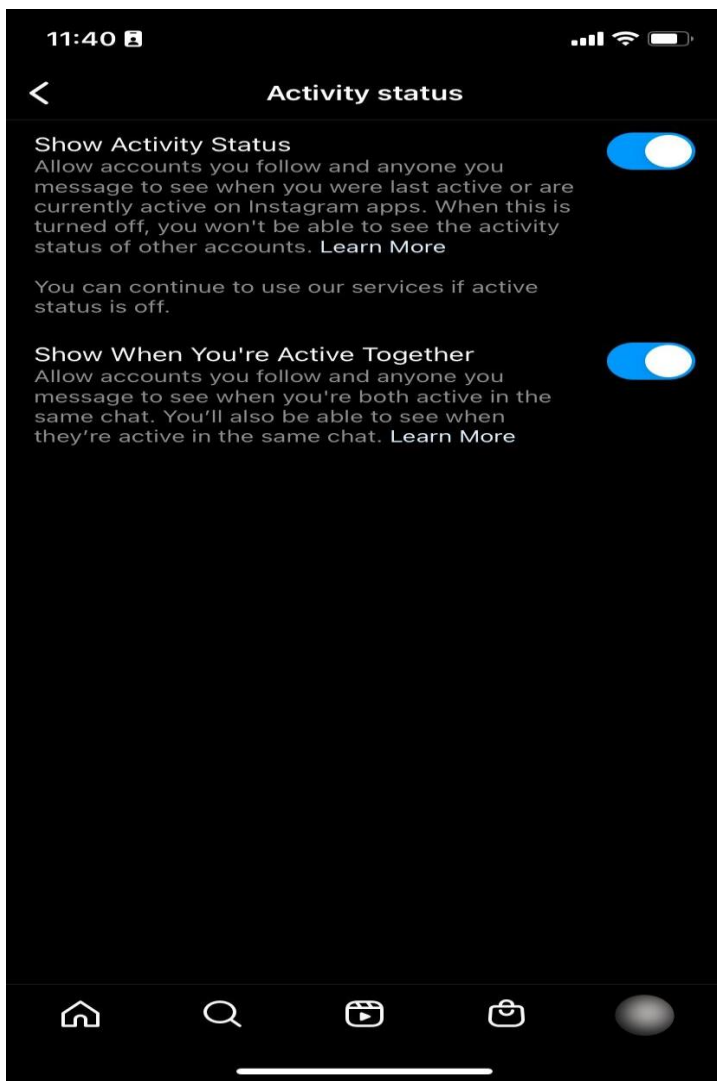
4. Take Control of Your Stories

داستان های خود را کنترل کنید



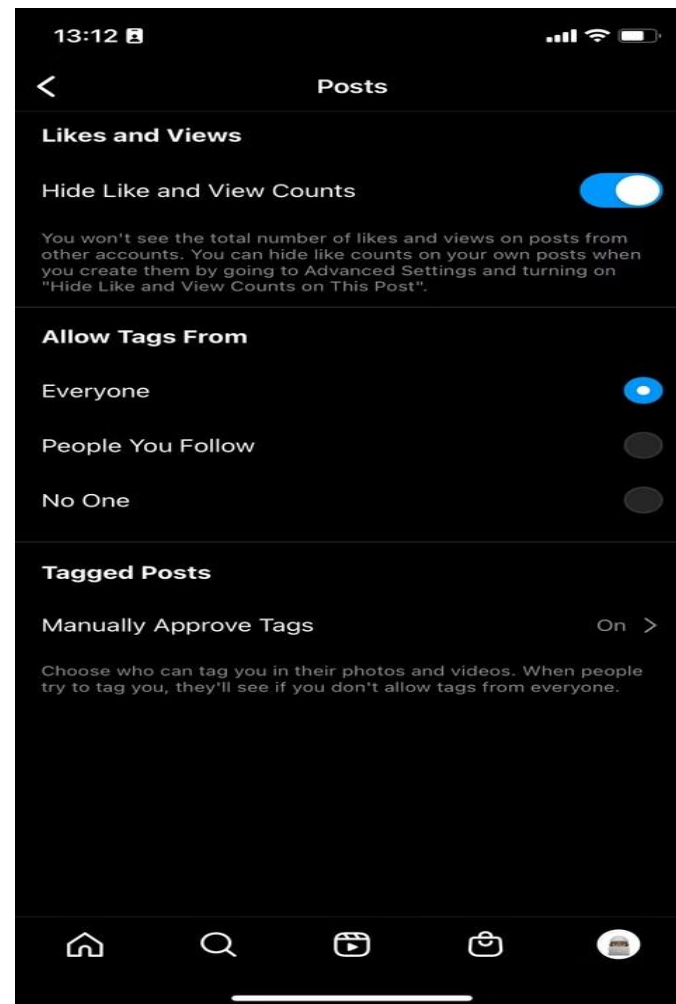
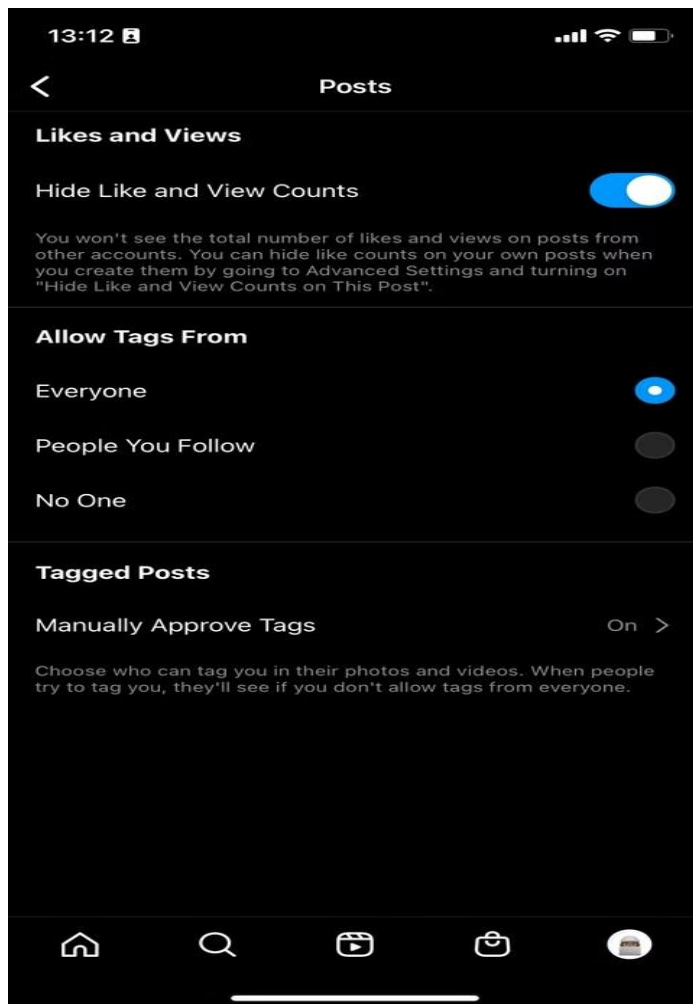
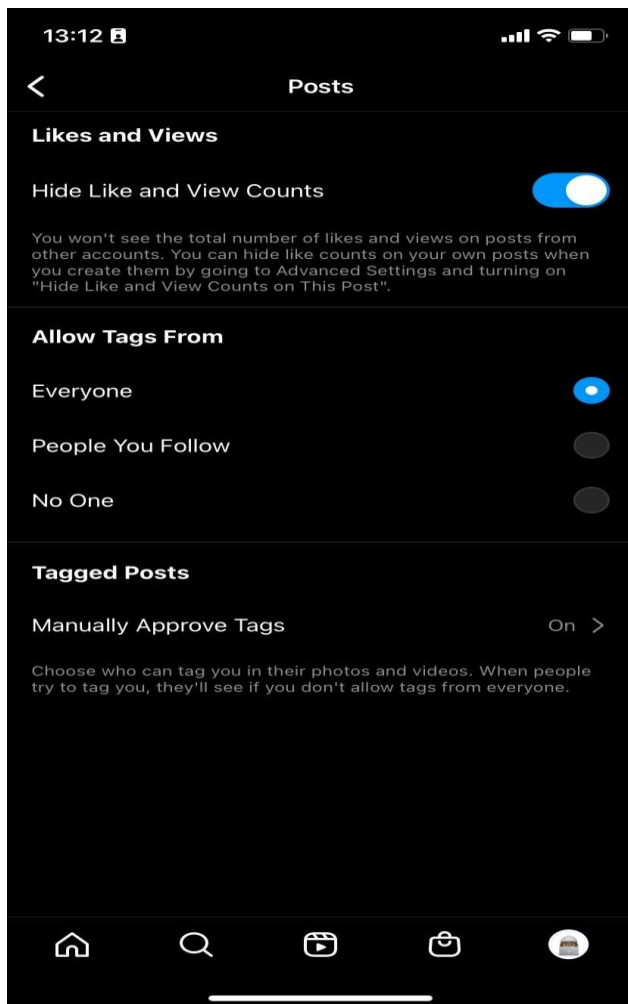
5. Disable Your Activity Status

وضعیت فعالیت خود را غیرفعال کنید



6. Stop Automatic Posting

توقف ارسال خودکار



Hide Your Whereabouts

مکان خود را پنهان کنید

iOS devices, open **Settings**, scroll down to the app section, and select Instagram. Tap Location and select **Never** under **Allow Location Access**.

On Android, open your **Settings** app, then tap Privacy > Permission manager. Select **Location** to see the apps that have access. If Instagram is available, select it and choose **Don't allow** on the next page. Steps will vary across devices, but you can [manage your Android permissions using third-party apps](#) that standardize the whole process.

How to Make WhatsApp More Secure and Private



1. Enable Disappearing Messages for Sensitive Conversations

To activate Disappearing messages in a given chat, tap the contact's name at the top and select **Disappearing messages**. Next, choose a period after which a message will be deleted.

2. Turn On Security Code Change Notifications

To turn on security code change notifications, go to **WhatsApp > Settings > Account > Security > Show security notifications** and flip the toggle to green.

On Android, tap **Settings > Account > Security Notifications** and toggle on **Show Security Notifications on This Phone**.

3. Enable Two-Step Verification

To enable two-step verification on WhatsApp just go to **Settings > Account > Two-step verification > Enable**.

4. Lock WhatsApp With Fingerprint or Face Verification

On Android, you can lock your WhatsApp app by hitting the **three-dot menu** in the top right, selecting **Settings > Privacy > Fingerprint lock**, then toggling **Unlock with fingerprint**. You'll then be asked to add a fingerprint, and then you can select the standby time before WhatsApp is automatically locked.

On iOS, go to **Settings > Privacy > Screen Lock** and toggle on **Require Touch ID** or **Require Face ID**. Finally, select the time standby time before WhatsApp automatically locks.

5. Encrypt Cloud Backups

On Android, tap the three-dot menu in the top right and select **Settings > Chats > Chat backup > End-to-end encrypted backup > Turn on**. You can do the same on iPhone by going to **Settings > Chats > Chat Backup > End-to-end encrypted backup > Turn on**.

6. Beware of Common Scams

7. Get the Official WhatsApp Desktop Apps

To use WhatsApp on your computer, you need to link your phone with WhatsApp Web or the WhatsApp desktop apps. To be on the safe side, get the official desktop app.

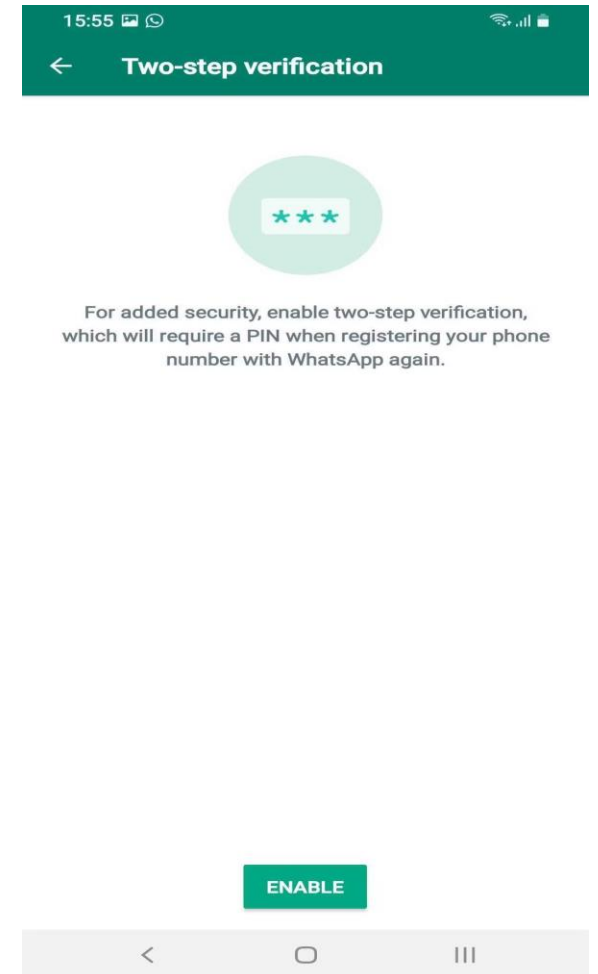
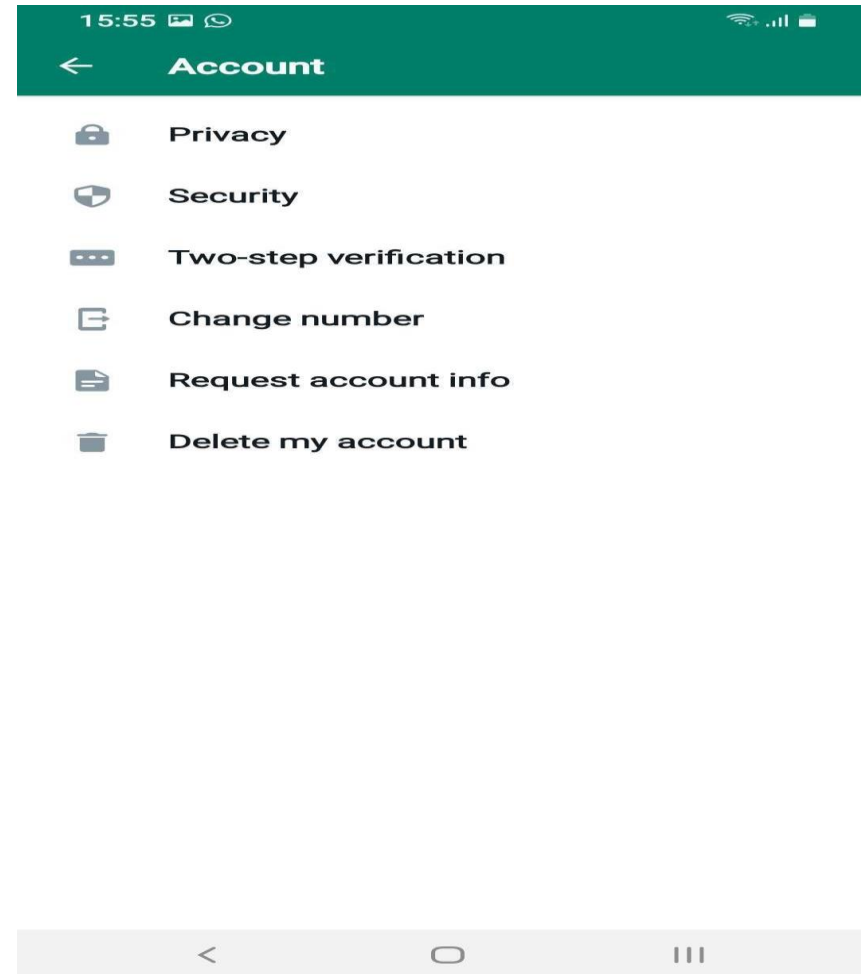
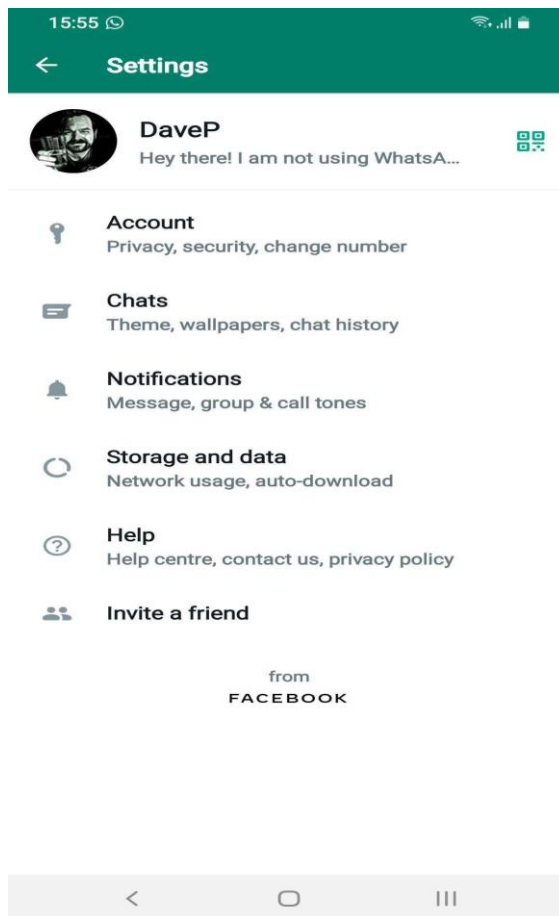
8. Adjust Your WhatsApp Privacy Settings

WhatsApp isn't the most private messenger out there, but it gives users at least some control. Go to **Settings > Account > Privacy** to see everything at your disposal.

How to Enable Two-Step Verification on WhatsApp



To enable two-step verification on WhatsApp just go to **Settings > Account > Two-step verification > Enable**. You'll then be asked to create a six-digit PIN which you'll be required to input every time you need to verify your phone number. You will also be prompted to enter your PIN periodically to help you remember it.



Have fun and be safe

خوش بگذره و ایمن باش

تلگرام راهی عالی برای محافظت از پیام‌های شماست، اما مراحل وجود دارد که می‌توانید خارج از برنامه برای بهبود حریم خصوصی و امنیت خود انجام دهید. مهمترین مرحله استفاده از یک برنامه ۲ FA مانند Google یا Authy است. استفاده از یکی از این برنامه‌ها در کنار استفاده صحیح از ویژگی‌های داخلی تلگرام، دسترسی شخصی به حساب شما را بدون اجازه شما عملاً غیرممکن می‌کند.



Top 10 tips for using Telegram safely and securely

Use secret chats to encrypt your messages

از چت های مخفی برای رمزگذاری پیام های خود استفاده کنید

To start a secret chat, follow these steps:

- Open Telegram.
- Tap the **pencil** icon in the lower-right corner.
- Tap **New Secret Chat**.
- Select a contact to start a secret chat

Enable two-step verification to prevent unauthorized access

برای جلوگیری از دسترسی غیرمجاز، تأیید دو مرحله‌ای را فعال کنید

- Open Telegram.
- Tap the **menu** button in the upper-left corner of your screen.
- Tap **Settings**.
- Tap **Privacy and Security**.
- Tap **Two-Step Verification**.
- Enter a password.

Disable active sessions on other devices

جلسات فعال را در دستگاه های دیگر غیرفعال کنید

- Open Telegram.
- Tap the **menu** button in the upper-left corner of your screen.
- Tap **Settings**.
- Tap **Privacy and Security**.
- Tap **Active Sessions**.
- Tap **Terminate all other sessions**.

Send self-destructing media

ارسال رسانه های خود ویرانگر

- Open Telegram
- Select a chat.
- Tap the **Attach** icon in the lower-right corner of your screen.
- Choose an existing image or take a new one.
- Tap the **stopwatch** button next to the **Send** button.
- Select how long you wish your media to last.
- Tap the **Send** button.

Delete messages for ultimate privacy

برای حفظ حریم خصوصی، پیام ها را حذف کنید

- Open Telegram.
- Open a chat.
- Long press any chat message.
- Tap the **Delete** button in the upper-right corner of your screen.
- Select the **Also delete for** checkbox to delete it for the other person.
- Tap **Delete**.

Lock the Telegram app with a password

برنامه تلگرام را با رمز عبور قفل کنید

- Open Telegram.
- Tap the **menu** button in the upper-left corner of your screen.
- Tap **Settings**.
- Tap **Privacy and Security**.
- Tap **Passcode Lock**.
- Tap **Enable passcode**.
- Choose a passcode, and then tap **Confirm**.

Hide your IP address with a proxy server

خود را با یک سرور پروکسی مخفی کنید IP آدرس

Here's how to set up a Telegram proxy server:

- Open Telegram.
- Tap the **menu** button in the upper-left corner of your screen.
- Tap **Settings**.
- Tap **Data and Storage**.
- Scroll down and tap **Proxy settings**.
- Tap **Add Proxy**

Double-check your group permissions

مجوزهای گروه خود را دوباره بررسی کنید

- Open Telegram.
- Tap the **menu** button in the upper-left corner of your screen.
- Tap **Settings**.
- Tap **Privacy and Security**.
- Tap **Groups**.
- Change **Everybody** to **My Contacts**.

How to clear payments and shipping information

نحوه پاک کردن اطلاعات پرداخت و حمل و نقل

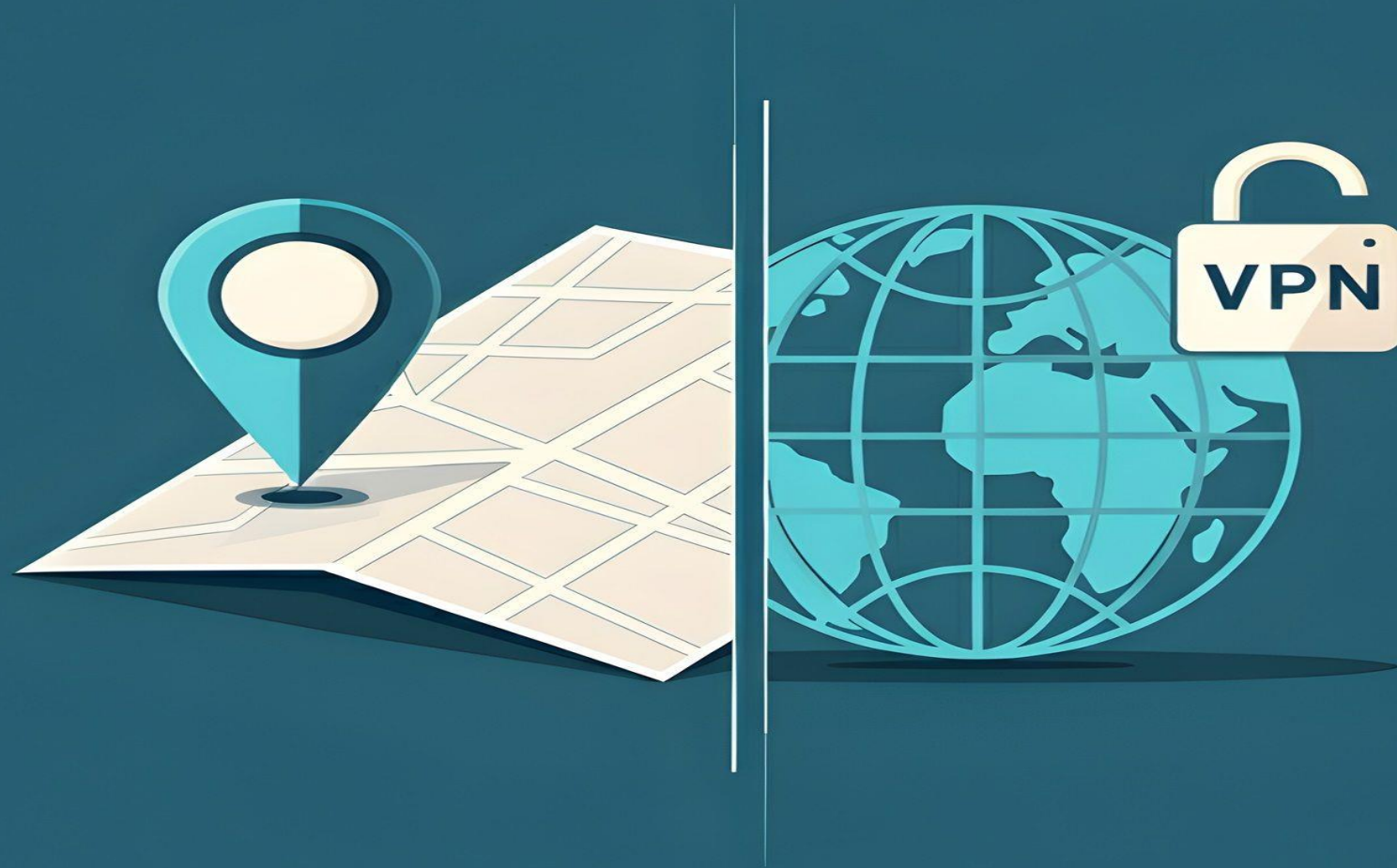
- Open Telegram.
- Tap the **menu** button in the upper-left corner of the app.
- Tap **Settings**.
- Tap **Privacy and Security**.
- Tap **Clear Payment and Shipping Info**.
- Select the **Shipping info** and **Payment info** checkboxes.
- Confirm your changes by tapping **Clear**.

Automatically delete your account after losing access

پس از از دست دادن دسترسی، به طور خودکار حساب خود را حذف کنید

- Open Telegram.
- Tap the **menu** button in the upper-left corner of your screen.
- Tap **Settings**.
- Tap **Privacy and Security**.
- Tap **If away for** under the **Delete my Account** heading.
- Choose a period of time.

Location Spoofing vs. VPN: What's the Difference?



• **جعل موقعیت مکانی و VPN** اغلب هنگام بحث در مورد حریم خصوصی و امنیت آنلاین به جای یکدیگر استفاده می شوند، اما آنها یکسان نیستند. هر دو می توانند مکان دیجیتال شما را تغییر دهند و به شما کمک کنند از حریم خصوصی خود محافظت کنید، اما این کار را به روش های مختلف و به دلایل مختلف انجام می دهند.



What Is Location Spoofing?

جعل موقعیت مکانی تقریباً همان چیزی است که به نظر می رسد - برنامه ها، وب سایت ها یا سرویس ها را فریب می دهد تا فکر کنند شما جای دیگری هستید. اغلب از آن برای جعل مختصات GPS یا آدرس IP شما استفاده می شود و به نظر می رسد که در شهر، کشور یا حتی قاره دیگری هستید.

می تواند به عنوان جایگزین VPN برای مواردی مانند دسترسی به برنامه ها یا ویژگی های موجود فقط در مناطق خاص یا بازی با برنامه های مبتنی بر مکان مانند Pokémon Go عمل کند. با جعل موقعیت مکانی خود، می توانید قفل سرویس ها یا محتوایی را که در غیر این صورت در مکان واقعی شما در دسترس نیستند، را باز کنید.

شایان ذکر است که اگرچه جعل موقعیت مکانی سرگرم کننده است و تنظیم آن نسبتاً آسان است، اما هیچ گونه حفاظت واقعی از حریم خصوصی ارائه نمی دهد. شما فقط مکان خود را تغییر می دهید، نه داده های خود را رمزگذاری می کنید یا فعالیت آنلاین خود را پنهان می کنید.

VPN چیست





ابزاری است که برای حفظ حریم خصوصی، امنیت، و بله، تغییر مکان آنلاین شما طراحی شده است. اما برخلاف جعل موقعیت مکانی اولیه، VPN بسیار عمیق تر است. تمام ترافیک اینترنت شما را رمزگذاری می کند و آن را از طریق یک سرور در مکان دیگری هدایت می کند. این دو کار اصلی را انجام می دهد: آدرس IP شما را پنهان می کند و از داده های شما در برابر رهگیری توسط هکرها، ارائه دهندگان خدمات اینترنت (ISP) یا هرکس دیگری که سعی در جاسوسی از شما دارد محافظت می کند.

Key Differences Between Location Spoofing and VPN

Feature	Location Spoofing	VPN
Primary Function	Fakes your location for apps and websites	Encrypts your data and changes your IP address
Privacy	Limited—does not encrypt data or provide real privacy	High—encrypts data, hides browsing activity from ISPs
Security	None—vulnerable to tracking and data leaks	High—protects against hacking, especially on public Wi-Fi
Common Use Cases	Accessing region-locked apps, games, or content; GPS tricks	Accessing geo-blocked content, securing online transactions
How It Works	Modifies GPS or IP address, typically without encryption	Routes internet traffic through an encrypted tunnel
Effect on Internet Speed	Minimal impact, unless using proxies	Can slow down speeds due to encryption and server routing
Access to Streaming Services	May not work, as many streaming services block fake IPs or GPS locations	More reliable, as VPNs can bypass geo-restrictions on streaming
Setup	Simple—usually just an app or browser extension	Requires subscribing to a VPN service and installing software
Legal Considerations	Generally legal, but some apps may ban users for spoofing	Legal in most countries, but may be restricted in some places

تفاوت های کلیدی بین جعل موقعیت مکانی و VPN

ویژگی	جعل مکان	VPN
عملکرد اولیه	موقعیت مکانی شما را برای برنامه ها و وب سایت ها جعلی می کند	شما را IP داده های شما را رمزگذاری می کند و آدرس تغییر می دهد
حریم خصوصی	محدود - داده ها را رمزگذاری نمی کند یا حریم خصوصی واقعی را ارائه نمی دهد	داده ها را رمزگذاری می کند، فعالیت مرور را از High-ISP ها پنهان می کند
امنیت	هیچکدام - در برابر ردیابی و نشست داده ها آسیب پذیر است	در برابر هک کردن محافظت می کند، به خصوص High-Wi-Fi در عمومی
موارد استفاده رایج	دسترسی به برنامه ها، بازی ها یا محتوای قفل شده در منطقه؛ ترفندهای جی پی اس	دسترسی به محتوای جغرافیایی مسدود شده، ایمن سازی تراکنش های آنلاین
چگونه کار می کند	را معمولاً بدون رمزگذاری تغییر می دهد IP یا GPS آدرس	ترافیک اینترنت را از طریق یک تونل رمزگذاری شده مسیریابی می کند
تاثیر بر سرعت اینترنت	تاثیر حداقلی، مگر اینکه از پروکسی استفاده کنید	می تواند سرعت را به دلیل رمزگذاری و مسیریابی سرور کاهش دهد
دسترسی به خدمات جریانی	ممکن است کار نکند، زیرا بسیاری از سرویس های استریم آی پی های را مسدود می کنند GPS جعلی یا مکان های	ها می توانند محدودیت های VPN قابل اطمینان تر، زیرا جغرافیایی در جریان را دور بزنند
راه اندازی	ساده—معمولاً فقط یک برنامه یا افزونه مرورگر	و نصب نرم افزار دارد VPN نیاز به اشتراک در سرویس
ملاحظات حقوقی	به طور کلی قانونی است، اما برخی از برنامه ها ممکن است کاربران را به دلیل جعل ممنوع کنند	در اکثر کشورها قانونی است، اما ممکن است در برخی مکان ها محدود شود

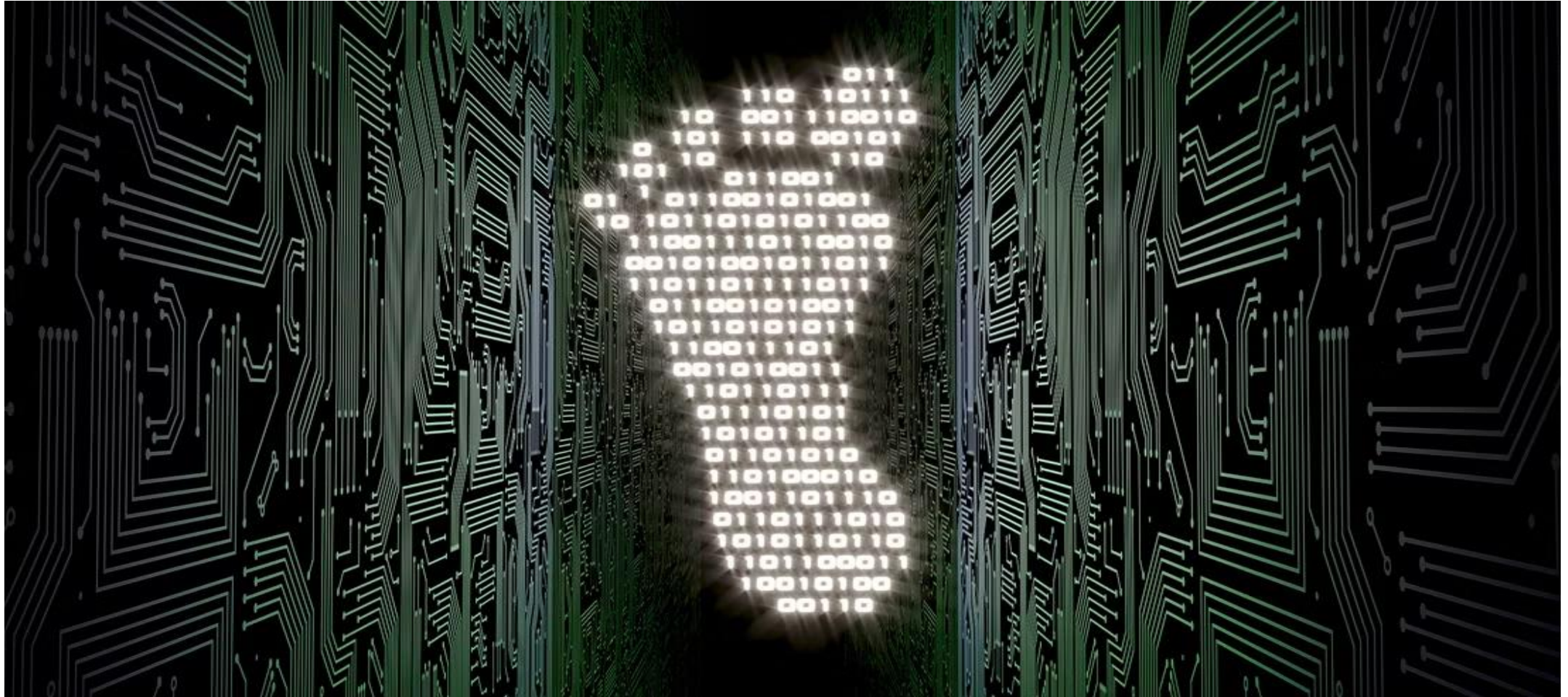
Which One Should You Use?



انتخاب بین جعل موقعیت مکانی و VPN به نیاز شما بستگی دارد. اگر فقط به دنبال فریب دادن برنامه‌ها یا وبسایت‌ها هستید تا فکر کنند در مکان دیگری هستید - شاید برای دسترسی به یک بازی یا سرویسی که در منطقه شما در دسترس نیست - جعل مکان سریع و آسان است.

با این حال، اگر اولویت شما حفظ حریم خصوصی و امنیت آنلاین است، به خصوص هنگام استفاده از Wi-Fi عمومی یا برخورد با اطلاعات حساس، VPN گزینه بهتری است. VPN ها فقط مکان شما را تغییر نمی دهند. آنها همچنین داده های شما را رمزگذاری می کنند و ردیابی فعالیت های آنلاین شما را برای هکرها، تبلیغ کنندگان یا حتی ارائه دهنده اینترنت شما بسیار سخت تر می کنند

What Is a Digital Footprint? Here's What to Know About Your Online Trail



How Can Your Digital Footprint Be Used?

چگونه می توان از ردپای دیجیتالی شما استفاده کرد؟

- **1. Personalized Marketing and Ad Targeting** بازاریابی شخصی و هدف گذاری تبلیغات
 - **2. Account Takeover and Fraud Prevention** تصاحب حساب و جلوگیری از کلاهبرداری
 - **3. Credit Scoring and Financial Services** امتیازدهی اعتباری و خدمات مالی
 - **4. Employment and Recruitment** استخدام و استخدام
 - **5. Law Enforcement and Security** اجرای قانون و امنیت
- مجری قانون می تواند از ردپای دیجیتالی مانند تاریخچه مرور، پست های رسانه های اجتماعی، ایمیل ها، متن ها و داده های موقعیت مکانی تلفن برای حل پرونده ها و ردیابی فعالیت های مجرمانه استفاده کند. تمام آن جزئیاتی که بدون فکر کردن به اشتراک می گذاریم، می توانند به عنوان مدرکی برای یا علیه ما در صورت درگیر شدن در یک موضوع قانونی، به پایان برسند.
- **6. Social and Political Influence** نفوذ اجتماعی توییت زدن و سیاسی

social networks

Types of Active Digital Footprints

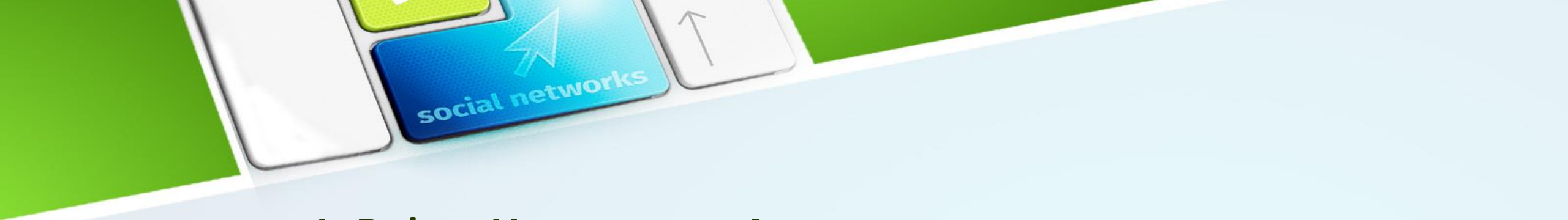


- 
- **Social media footprints**
 - **Email footprints**
 - **Blog posts and comments**
 - **Download footprints**
 - **Photo and video footprints**
 - **Web search footprints**
 - **Online purchases**

A close-up photograph of a laptop keyboard. A prominent blue key features a white mouse cursor icon and the text 'social networks'. To its right is a white key with a grey upward-pointing arrow. The background is a soft-focus light blue.

10 Easy Ways to Reduce Your Online Footprint With a Few Clicks



- 
- **1. Delete Unnecessary Accounts**
 - **2. Don't Provide Your Personal Email Address**
 - **3. Use Fake Information (if Legal)**
 - **4. Check Your Privacy Settings**
 - **5. Don't Login With Facebook**
 - **6. Think Before You Post**
 - **7. Protect Against Data Dumps**
 - **8. Use Incognito Windows**
 - **9. Use a Privacy Extension**
 - **10. Use a VPN**



Social Engineering: 10 Ways To Protect Your Business



- 
1. Cyber Security Policies
 2. Mobile Device Management
 3. Multi-Factor Authentication
 4. Regular Backups
 5. Password Management
 6. Security Awareness Training For Employees
 7. Encrypting Emails and Data
 8. Keep Software/OS Up to Date
 9. Define Roles and Verify Identities
 10. Utilise Next-Gen Firewall and Anti-Virus



EXIF



social networks

Online Photos and Personal Privacy: 4 Things to Check Before You Upload





3 Ways to Remove Metadata From Photos

- **1. Remove EXIF Data With Windows File Explorer**
 - Open File Explorer (**Windows key + E** shortcut).
 - Navigate to your image.
 - Right-click on your image and select **Properties**.
 - Click the **Details** tab
- **2. Remove EXIF Data Using GIMP**
 - GIMP is a free and open-source software that can easily strip EXIF data from an image. It may even be easier than the Windows 10 method above!
- **3. Remove EXIF Data Using a Mobile App**
 - Download: [Photo Metadata Remover for Android](#) (Free)
 - Download: [Metapho for iOS](#) (Free, in-app purchase for metadata removal)



11 Tips For Safely Using Anonymous Accounts On Social Networks

- **1) Create A Dedicated Email Address** یک آدرس ایمیل اختصاصی ایجاد کنید
- **2) Pick A Unique Username** یک نام کاربری منحصر به فرد را انتخاب کنید
- **3) Avoid Using The Same Photos Across Personal And Anonymous Accounts**
- **4) Clear Your Browsing History (Or Use Incognito Mode)**
- **5) Pay Anonymously** web money , cash , digital



11 Tips For Safely Using Anonymous Accounts On Social Networks

- **6) Keep Personal Secrets To Yourself**
اسرار شخصی را برای خود نگه دارید
- **7) Always Use Strong Passwords**
- **8) Keep Meetings Separate From Your Everyday Life**
جلسات را از زندگی روزمره خود جدا نگه دارید
- **9) Keep Your Anonymous And Real Life Completely Separated**
از اعتماد بیش از حد خودداری کنید



ZERO TRUST NETWORK

یک مدل امنیتی و کنترل شبکه است که در سازمانهای فناوری محور استفاده می شود، در این مدل امنیتی به صورت پیش فرض به هیچ ماشین، سرویس و یا شخصی اعتماد نمیشود و در تمام مراحل و از هر جایی (داخل شبکه ، **Dmz**، بیرون شبکه سازمانی) کاربران و دستگاهها باید احراز هویت و تایید شوند و دسترسی آنها به صورت حداقل سطح دسترسی به منبع خاص مورد نیاز تعریف میشود.

با احراز هویت مداوم و محدود کردن سطوح دسترسی به فقط منابع کاملاً ضروری فرصت های بسیار کمتر و محدود تری به هکرها و بد افزارها برای دستیابی به اطلاعات حیاتی داده میشود.

شبکه ای که با این مدل طراحی اجرا و مدیریت میشود اصطلاحاً شبکه بدون اعتماد، شبکه با اعتماد صفر گفته میشود.

© 2013 by the author



**TOMORROW
YOU WILL WISH
YOU HAD
STARTED TODAY**





What Is Endpoint Security and Why Is It Important?

