Afghan Witness

امنیت دیجیتال برای زنان و دختران

افغان ویتنس

این راهنما برای توانمندسازی شما با دانش و ابزارهای مورد نیاز برای محافظت از شما در فضای دیجیتال ایجاد شده است. در حالیکه مخاطب اصلی این راهنما زنان و دختران افغانستان اند، اما محتویات آن برای همه قابل استفاده است.

در محیطی که آزادی محدود است، رسانه‌های اجتماعی و دیگر اشکال وسایل ارتباط دیجیتالی بعنوان وسایل مهم مشارکت استفاده می‌شوند. با این حال، امنیت و حریم خصوصی دیجیتال اغلب در معرض خطر اند و افراد را می توان بر اساس فعالیت های آنلاین، ارتباطات یا سایر داده های دیجیتالی آنها شناسایی کرد.

چه به دنبال آموزش باشید، چه به دنبال ارتباط با دیگران یا صرفاً در حال گشت و گذار در اینترنت هستید، درک چگونگی ایمن سازی فعالیت های آنلاین خود بسیار مهم است. با پیروی از روش‌های ذکر شده در اینجا، می‌توانید حریم خصوصی خود را تقویت کنید، از اطلاعات شخصی خود محافظت کنید و با اطمینان خاطر در دنیای دیجیتال علیرغم شرایط چالش برانگیزی که با آن روبرو هستید، شرکت کنید.

قدرت شما در نقطه ضعف‌های تان نهفته است.

فهرست مطالب

۱. شناسایی خطرات امنیتی

منشاء تهدید

برای محافظت از خود باید خطراتی که با آن روبرو هستید را درک کنید. در اینجا چند نمونه از اینکه تهدیدات ممکن است از کجا آمده باشند آورده شده است:

به این فکر کنید که یک تهدید ممکن است از کجا باشد:

- یکی از اعضای خانواده که حساب‌های رسانه‌های اجتماعی شما را تعقیب می کند.
- خواستگاری ناخواسته که عاشقانه شما را تعقیب می کند.
- مقامات شما را متوقف می کنند و تلفن شما را چک می کنند.
- یک فرد تأثیرگذار که به شما علاقه مند است.
- افراد ناشناس به دلیل پست‌های آنلاین شما را هدف قرار می دهند.

هر یک از این موقعیت ها **خطرات امنیتی متفاوتی** را به همراه دارد. اقدامات لازم برای محافظت از خود در برابر چک تصادفی تلفن با اقدامات لازم برای پنهان شدن از کاربران عصبانی اینترنت یا مقامات قدرتمندی که سعی در شناسایی شما دارند متفاوت است.

ریسک یا خطر بستگی به این دارد که 'عامل تهدید' (فردی که شما را تهدید می‌کند) چقدر درباره شما می‌داند، منابع، نفوذ و مهارت‌های فنی او چقدر قوی است. صرف نظر از اینکه تهدید از کجا می آید، همیشه بهترین کار این است که **حداکثر اقدامات احتیاطی** را انجام دهید.

محیط

خطرات امنیتی که با آن روبرو هستید به **محل زندگی** شما بستگی دارد.
در ایالات متحده یا اروپا، قوانین از داده‌های شخصی شما محافظت می کنند. به طور کلی، محتوای دستگاه‌های شما یا سابقه فعالیت آنلاین شما به راحتی قابل دسترسی نیست مگر اینکه دادگاه شما را بعنوان یک مجرم یا تهدید جدی امنیتی تلقی کند.
در این مکان‌ها، خطرات اصلی شما عبارتند از: اطلاعاتی که در پلتفرم‌های آنلاین به اشتراک می‌گذارید، دستگاه‌های شما از راه دور هک می‌شوند یا شخصی در محیط نزدیک شما به دستگاه شما دسترسی دارد.

در شرایطی مانند **افغانستان**، وضعیت متفاوت است.

بدون حمایت‌های قانونی، نه تنها پست‌های رسانه‌های اجتماعی، بلکه ترافیک اینترنتی و **هرگونه اطلاعات** موجود در دستگاه‌های شما می‌تواند خطرات امنیتی باشد.

حاکمان افغانستان مقدار زیادی **داده‌های بیومتریک** در مورد افرادی که با دولت سابق و دولت ایالات متحده کار کرده اند و همچنین داده‌های بسیاری در مورد جمعیت کشور دارند که از آنها برای شناسایی فعالان محلی، روزنامه نگاران و دیگران استفاده می کنند.

در اینجا، تهدیدها ممکن است از جانب یک فرد حسود با مهارت های فنی محدود یا از طرف یک آژانس امنیتی با اطلاعات و تخصص گسترده باشد. **توانایی های تکنولوژیکی کسی که به دنبال آسیب رساندن یا ردیابی آنلاین شماست را دست کم نگیرید.**

راهکارهای مختلف

سناریوهای مختلف تهدید ممکن است به راهکارها و سطوح حفاظتی متفاوتی نیاز داشته باشند.

در اینجا دو مثال برای نشان دادن این موضوع وجود دارد:

مهارت های بالا - بدون دسترسی فیزیکی

اگر 'عامل تهدید' شما مهارت‌های فنی بالایی دارد اما دسترسی فیزیکی مستقیم به دستگاه شما ندارد، بسیار مهم است تا:

- از **اپلیکیشن‌های متمرکز بر حریم خصوصی** برای ارتباط استفاده کنید
- از ابزارهایی مانند VPN یا مرورگر Tor برای **پنهان کردن ترافیک اینترنت** خود استفاده کنید
- از دستگاه‌های خود در برابر **هک محافظت** کنید
- تنظیمات حریم خصوصی خود را در **رسانه های اجتماعی** به **حداکثر** برسانید

مهارت های کم - دسترسی فیزیکی

اگر عامل تهدید شما مهارت‌های فنی پایینی دارد اما ممکن است مستقیماً به دستگاه شما دسترسی فیزیکی داشته باشد، باید اطلاعات حساس را به روشی پنهان کنید که به راحتی قابل تشخیص نباشد. این می تواند شامل موارد زیر باشد:

- استفاده از برنامه‌های غیرمعمول، **زبان رمزگذاری‌شده** یا **پرکردن دستگاه تان** با **داده‌های بی‌ضرر** مانند گروه‌های چت متعدد یا تصاویر مربوط به بچه گربه‌ها.
- همچنین می‌توانید داده‌های حساس را در یک درایو خارجی یا سرویس ابری پنهان کنید تا پیدا کردن هر چیزی که می‌تواند برای آسیب رساندن به شما استفاده کند را برای آنها سخت‌تر کنید.

به حداکثر رساندن حریم خصوصی و امنیت شما بسیار مهم است، به خصوص اگر مطمئن نیستید که تهدید از کجا می آید.

با این حال، اگر شخصی به دستگاه شما دسترسی پیدا کرد، مهم است که با داشتن **اپلیکیشن‌های متمرکز بر حریم خصوصی** یا یک **دستگاه کاملاً تمیز** بدون هیچ اطلاعاتی، **از ایجاد سوء ظن جلوگیری** کنید.

قضاوت شخصی در مورد اینکه **تعادل مناسب** در قضیه شخص خود تان چگونه به نظر می رسد در اینجا مهم است.

مهندسی اجتماعی

مهندسی اجتماعی چیست؟

مهندسی اجتماعی تاکتیکی است که توسط مهاجمان برای فریب دادن شما برای ارائه اطلاعات شخصی استفاده می شود. این مهاجمان ممکن است وانمود کنند فردی هستند که به آن اعتماد دارید، مانند یک دوست، یکی از اعضای خانواده یا حتی شرکتی که شما می شناسید.

تاکتیک های رایج مهندسی اجتماعی

جعل هویت: ممکن است شخصی وانمود کند که دوست یا خویشاوندی است که به کمک نیاز دارد. آنها می توانند از شما بخواهند که پول بفرستید یا اطلاعات شخصی را به اشتراک بگذارید. اگر کسی که می‌شناسید مثل همیشه با شما ارتباط برقرار نمی‌کند، مراقب باشید.

فوریت: مهاجمان ممکن است وضعیت اضطراری ایجاد کنند و ادعا کنند که اگر سریع اقدام نکنید اتفاق بدی رخ خواهد داد. به عنوان مثال، ممکن است بگویند "حساب شما قفل خواهد شد مگر اینکه بلافاصله رمز عبور خود را ارائه دهید!"

فیشینگ چیست؟

فیشینگ نوعی مهندسی اجتماعی است که در آن مهاجمان پیام‌های جعلی ارسال می کنند تا شما را فریب دهند تا اطلاعات حساس را فاش کنید.

این پیام‌ها می‌توانند از طریق ایمیل، پیامک، رسانه‌های اجتماعی یا تماس ارسال شوند.

نشانه‌های رایج فیشینگ

لینک‌های مشکوک: مراقب لینک‌های موجود در پیام هایی باشید که از شما می‌خواهند وارد شوید یا اطلاعات شخصی ارائه دهید. این لینک‌ها ممکن است به وب سایت‌های جعلی منجر شود که واقعی به نظر می رسند اما برای سرقت اطلاعات شما طراحی شده اند.

درخواست‌های غیرمعمول: مراقب پیام‌هایی باشید که اطلاعات شخصی، رمز عبور یا اطلاعات مالی را می‌خواهند. شرکت ها و سازمان های قانونی معمولاً از این طریق اطلاعات حساس را درخواست نمی کنند.

زبان ضعیف: بسیاری از پیام های فیشینگ حاوی اشتباهات املایی و دستوری هستند یا از زبانی استفاده می کنند که عجیب به نظر می رسد.

چگونه از خود محافظت کنید

منبع را تایید کنید: اگر پیام مشکوکی دریافت کردید، مستقیماً با استفاده از یک روش شناخته شده و قابل اعتماد (مانند شماره تلفن یا آدرس ایمیلی که قبلاً دارید) با شخص یا سازمان تماس بگیرید.

روی لینک‌های مشکوک کلیک نکنید: نشانگر را روی پیوندها نگه دارید تا قبل از کلیک کردن ببینید به کجا منتهی می‌شوند. اگر لینک عجیب به نظر می‌رسد یا با وب سایت معمول فرستنده مطابقت ندارد، روی آن کلیک نکنید.

استفاده از نرم افزار امنیتی: نرم افزار امنیتی را در دستگاه‌های خود نصب و آپدیت کنید. این می تواند به شناسایی و مسدود کردن پیام ها و وب سایت های مخرب کمک کند.

اگر مشکوک هستید که در معرض حمله فیشینگ قرار گرفته‌اید، چه کاری باید انجام دهید

پاسخ ندهید: اگر پیام مشکوکی دریافت کردید، پاسخ ندهید و روی هیچ لینکی کلیک نکنید.

آن را گزارش دهید: پیام را به پلتفرمی که آن را دریافت کرده اید گزارش دهید. به عنوان مثال، اگر از طریق ایمیل آمده است، می‌توانید آن را به عنوان 'اسپم' یا 'فیشینگ' علامت گذاری کنید.

پسورد خود را تغییر دهید: اگر فکر می‌کنید که ممکن است در معرض حمله فیشینگ قرار گرفته‌اید، برای جلوگیری از دسترسی بیشتر به حساب‌های خود فوراً رمزهای عبور یا پسورد خود را تغییر دهید.

۲. امنیت اپلیکیشن‌ها و دستگاه‌ها

دستگاه های شما ممکن است ناامن باشند

دستگاه‌های شما، مانند تلفن یا لپ‌تاپ، موقعیت داده‌ها (دیتا) و رفتار شما را به‌طور پیش‌فرض **ردیابی** می‌کنند. افرادی که دستگاه شما را **هک** کرده اند یا **مقامات** در صورت داشتن تخصص لازم می توانند به موارد متذکره دسترسی داشته باشند. اگر شخصی به دستگاه شما دسترسی داشته باشد، می‌تواند به راحتی از طریق برنامه‌هایی مانند واتس‌اپ، **تمام اطلاعات و ارتباطات شما را جستجو کند**.

رمزگذاری دستگاه تلفن همراه

در صورت مفقود شدن یا دزدیده شدن دستگاه، اطمینان از اینکه تلفن شما **رمزگذاری** شده است، برای محافظت از اطلاعات تان بسیار مهم است. رمزگذاری داده‌های یا دیتای شما را به قالبی تبدیل می‌کند که فقط با 'کلید رمزگشایی' درست که معمولاً به **رمز عبور یا PIN** تلفن شما مرتبط است، قابل خواندن است. **اطمینان حاصل کنید که یک رمز عبور قوی** برای به حداکثر رساندن امنیت دارید. **آیفون ها به طور پیش فرض رمزگذاری** می شوند. در مدل های **اندروید ۱۰** و بالاتر، دستگاه نیز به **طور پیش فرض رمزگذاری** شده است. در مدل های قدیمی تر، رمزگذاری باید به صورت دستی فعال شود.

در مدل‌های قدیمی‌تر اندروید، می‌توانید با رفتن به **'Settings > Security > Encryption'** بررسی کنید که آیا گوشی شما رمزگذاری شده است یا خیر.

اگر دستگاه شما رمزگذاری نشده است، می توانید رمزگذاری را از همان برگه (تنظیمات > امنیت > رمزگذاری) فعال کنید.

با این حال، توجه داشته باشید که این پروسه یک تا دو ساعت طول می کشد و نیاز به چارج کامل باتری دستگاه دارد - اگر دستگاه شما به طور تصادفی قبل از تکمیل پروسه خاموش شود، تلفن شما دیگر کار نخواهد کرد: باید دستگاه را مجددا تنظیم یا ریسیت (Reset) کنید و خطر از دست دادن اطلاعات خود را به جان بخرید.

از اپلیکیشن‌های امن پیام رسانی استفاده کنید

تماس از طریق **شبکه تلفن عادی** یا ارسال **پیامک** بسیار **ناامن** است زیرا محتویات ارتباطات شما به راحتی قابل **رهگیری** است. استفاده از سیستم عامل های پیام رسانی امن مانند **واتساپ** یا **سیگنال** ایمن تر است.

سیگنال یکی از امن ترین برنامه های پیام رسانی است. رمزگذاری سرتاسر ارائه می دهد، به این معنی که فقط شما و شخصی که با او در ارتباط هستید می توانید پیام ها را بخوانید. سیگنال همچنین منبع باز است، به این معنی که کد آن به صورت عمومی در دسترس کارشناسان است تا نحوه عملکرد آن را بررسی کنند و از شفافیت و اعتماد اطمینان حاصل کنند.

واتساپ همچنین رمزگذاری سرتاسری برای پیام‌ها، تماس‌ها، عکس‌ها و ویدیوها ارائه می‌دهد. کاربر پسند است و به طور گسترده مورد استفاده قرار می گیرد و آن را به انتخابی مناسب برای برقراری ارتباط امن تبدیل می کند.

برای افزایش امنیت، ویژگی‌های اضافی مانند **تایید هویت دو مرحله‌ای، پیام‌های ناپدید شونده و قفل اپلیکیشن‌ها** را فعال کنید ـ همانطور که در صفحات بعدی نشان داده می‌شود. در مورد اشتراک گذاری شماره خود به صورت عمومی محتاط باشید و **به طور منظم تنظیمات حریم خصوصی خود را بررسی کنید** تا کنترل کنید چه کسی می تواند اطلاعات شما را ببیند.

ایمن سازی کمپیوتر شما

ایمن سازی کمپیوتر شما برای محافظت از اطلاعات شخصی و حفظ حریم خصوصی تان، به ویژه در موقعیت‌های حساس بسیار مهم است. **نرم افزار آنتی ویروس معتبر** را نصب کنید و **فایروال** خود را **فعال** کنید تا از بدافزارها و دسترسی‌های غیرمجاز محافظت کند. به طور منظم سیستم عامل و برنامه های خود را برای رفع آسیب پذیری های امنیتی **آپدیت** کنید.

محافظت در برابر بدافزارها (MALWARE)

انتی ویروس

برای اکثر اهداف، اگر از کمپیوتر ویندوزی استفاده می کنید، نرم افزار Windows Defender به اندازه کافی امن است - تا زمانی که آن را به آپدیت و فعال نگه دارید. اگر برخی از ویژگی های اضافی می خواهید، یک گزینه خوب Bitdefender است که دارای گزینه های رایگان و پولی است.

برای کمپیوتر مک (Mac)، انتی ویروس پیش فرض نیز به طور کلی به اندازه کافی امن است. اما اگر به دنبال امنیت بیشتر هستید، Malwarebytes یک اسکنر ویروس و انتی ویروس رایگان ارائه می دهد.

از بیش از یک انتی ویروس استفاده نکنید - آنها ممکن است یکدیگر را از عملکرد درست مسدود کنند.

فایروال (Firewall)

فایروال‌ها جزء ضروری امنیت کمپیوتر شما اند و به عنوان **مانعی** بین دستگاه شما و تهدیدات احتمالی اینترنت عمل می کنند. فایروال ترافیک ورودی و خروجی شبکه را بر اساس قوانین امنیتی از پیش تعیین شده نظارت و **کنترل** می کند. این به عنوان یک فیلتر عمل می کند و اجازه می دهد تا ترافیک ایمن از آن عبور کند و در عین حال **ترافیک مضر یا مشکوک را مسدود می کند**.

ویندوز و کمپیوتر مک (Mac) هر دو دارای **فایروال داخلی** اند که با نظارت و فیلتر کردن ترافیک، سطح اولیه‌ای از محافظت را فراهم می‌کند. مدیریت آن از طریق **تنظیمات امنیت ویندوز**، یا در **تنظیمات امنیت و حریم خصوصی** برای کمپیوتر مک آسان است.

در ویندوز ۱۰ یا ۱۱، روی دکمه 'Start' کلیک کنید، و مراحل زیر را تعقیب کنید:

'Settings > Update & Security > Windows Security > 'Firewall & Network protection

در اینجا، وضعیت فایروال ویندوز خود را خواهید دید. مطمئن شوید که روی **'روشن' یا (ON) تنظیم** شده است.

اگر می‌خواهید امنیت و کنترل بیشتری فراتر از فایروال داخلی پیدا کنید، می‌توانید Tinywall را برای ویندوز (رایگان) و Little Snitch را برای کمپیوتر مک (پولی) انتخاب کنید.

به روز رسانی‌ها یا آپدیت‌ها

به روز نگه داشتن نرم افزار یکی از مهم ترین مراحل در حفظ امنیت دیجیتال است. آپدیت‌های منظم به محافظت از دستگاه‌های شما در برابر جدیدترین تهدیدها کمک می‌کند و اطمینان حاصل می‌کند که سیستم‌های شما به خوبی کار می‌کنند.

آسیب‌پذیری‌های جدید دائماً در نرم‌افزار کشف می‌شوند و هکرها به سرعت راه‌هایی را برای بهره‌برداری از آنها ایجاد می‌کنند. به‌روزرسانی‌های نرم‌افزار اغلب شامل اصلاحاتی برای این آسیب‌پذیری‌های تازه کشف‌شده اند. **با آپدیت کردن منظم نرم‌افزار خود، شکاف‌های امنیتی را که ممکن است یک هکر از آن سوء استفاده کند، می‌بندید.**

نکات عمومی

- بلوتوث را غیرفعال کنید.
- تاریخچه جستجو را حذف کنید یا از حالت مرور خصوصی استفاده کنید.
- اطلاعات حساس را روی گوشی خود ذخیره نکنید.
- از ارسال اطلاعات حساس در پیام ها خودداری کنید.
- پیام ها/عکس ها/فیلم های حساس را حذف کنید.
- هرگز گوشی خود را بدون مراقبت رها نکنید.
- از طریق تلفن شخص دیگری وارد حساب های خود نشوید.

از حمل این وسایل اجتناب کنید

اگر بازرسی فزیکی را پیش‌بینی می‌کنید!

این دستگاه‌ها می‌توانند خطر امنیتی ایجاد کنند، زیرا می‌توانند برای به دست آوردن یا ثبت اطلاعات شخصی شما استفاده شوند.

- گوشی های هوشمند
- ساعت های هوشمند
- لپ تاپ و تبلت
- سیستم های جی پی اس

سایر اقدامات مفید ایمنی

با رمز یا کد صحبت کنید

از عبارات یا علامات ساده برای انتقال پیام‌های مهم بدون اینکه جلب توجه کند، استفاده کنید.

به عنوان مثال، عبارت 'آب و هوا چگونه است؟' می‌تواند به عنوان رمز یا کد 'آیا شما امن هستید؟' استفاده شود.

چت‌های حساس را حذف کنید

برای محافظت از حریم خصوصی خود و در صورت نیاز، مکالمات مخاطره آمیز یا مخاطره آمیز را به طور منظم حذف کنید.

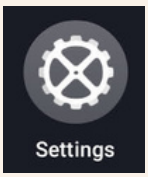
این نکات ممکن است کمی مرموز به نظر برسند، اما می توانند در موقعیت‌های دشوار نجات دهنده واقعی باشند. یک قدم جلوتر باشید و خود را ایمن نگه دارید!

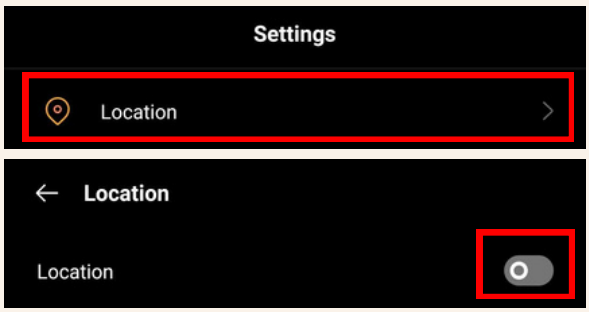
مراحل تنظیم امنیت دستگاه تلفن همراه

امنیت تلفن اندروید

وای فای، موقعیت مکانی GPS و انترنت تلفن همراه را غیر فعال کنید.

‘Settings’ → ‘Location.’



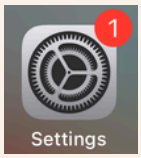


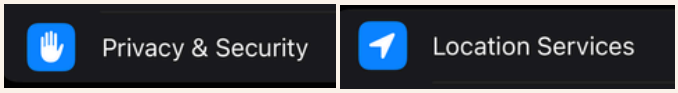
با کشیدن دکمه به سمت چپ، لوکیشن را خاموش کنید.

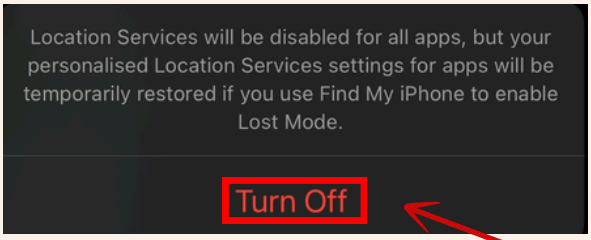
امنیت تلفن آیفون

وای فای و موقعیت مکانی GPS را غیر فعال کنید.

‘Settings’ → ‘Privacy & Security’ → ‘Location Services’





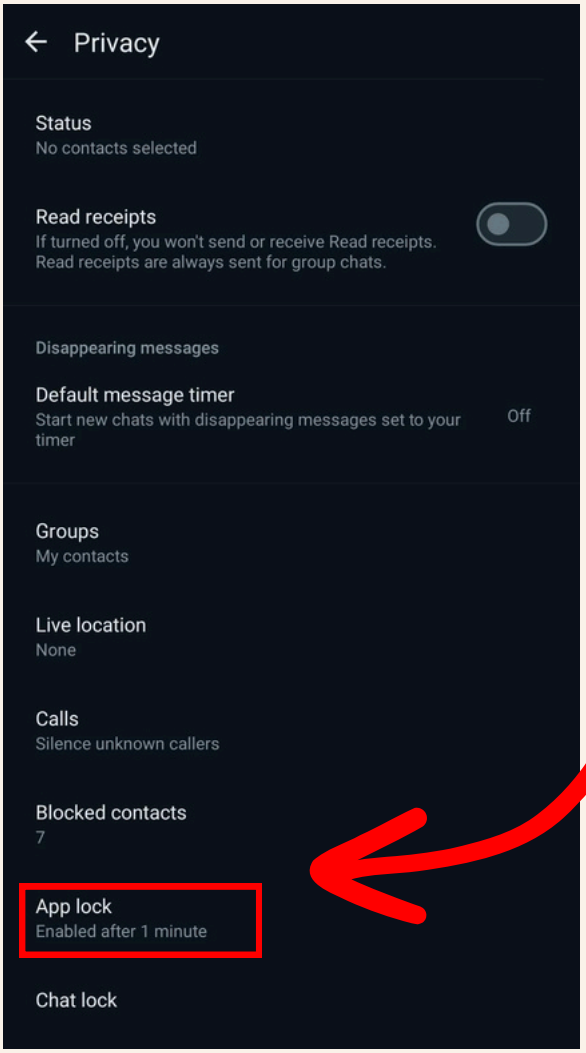


روی سلایدر بزنید تا لوکیشن خاموش شود.

تمام ‘Location Services’ را با استفاده از سلاید اصلی یا سلایدرهای جداگانه برای هر برنامه خاموش کنید.

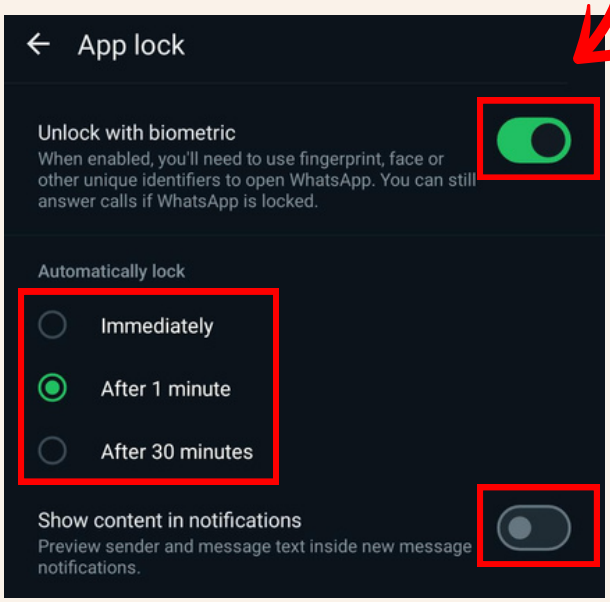
مراحل تنظیم حریم خصوصی در واتساپ

قفل کردن واتساپ



'تنظیمات' واتساپ را باز کنید:
'Settings' ← 'Privacy' ← 'App lock.'

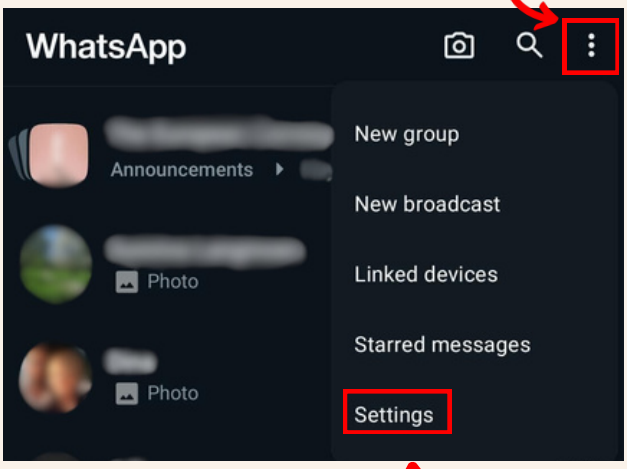
گزینه 'Unlock with biometric' را روشن کنید ← برای تایید، سنسور اثر انگشت را لمس کنید یا صورت خود را اسکن کنید.

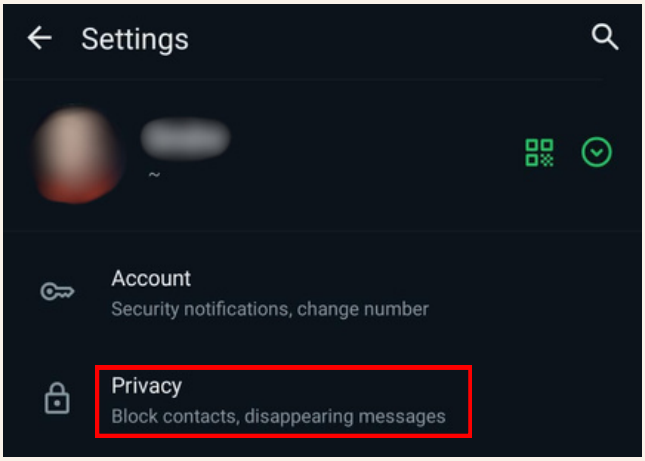


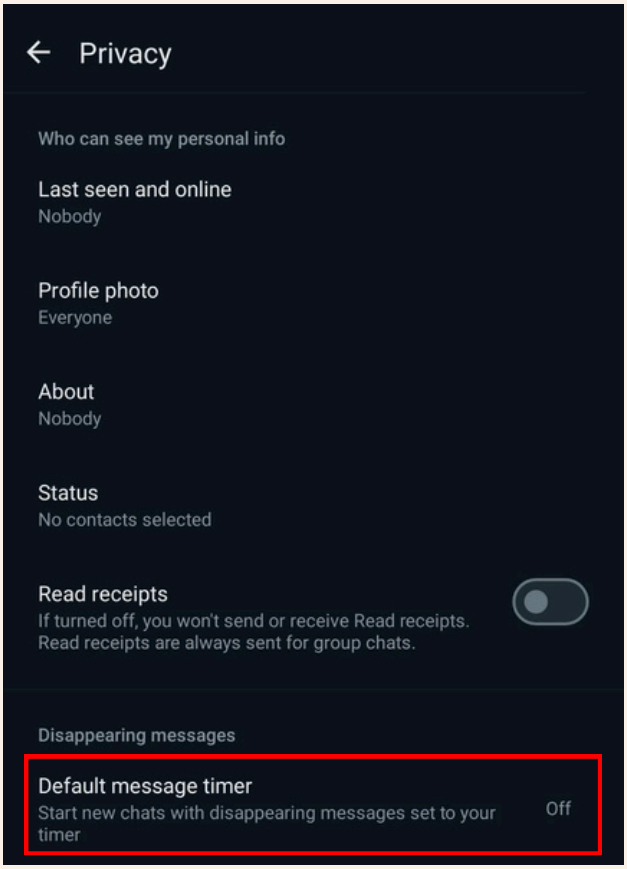
مدت زمانی را که پس از آن اپلیکیشن شما قفل می‌شود، تنظیم کنید، 'نمایش محتوا در اعلان‌ها' یا (show content in notifications) را غیرفعال کنید.

روشن یا خاموش کردن پیام‌های ناپدید شونده

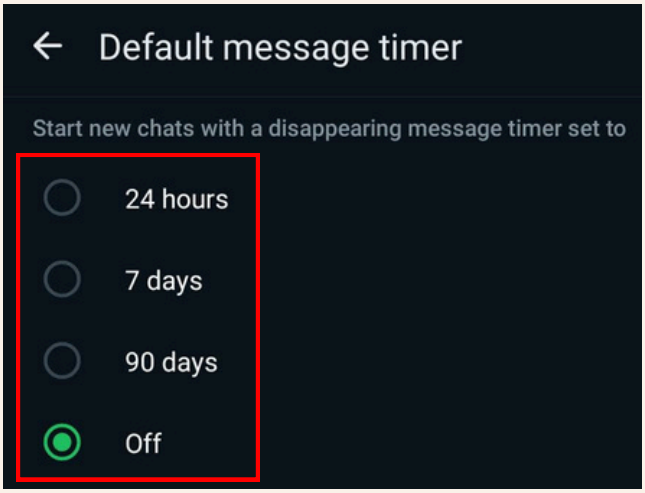
سه نقطه را انتخاب کنید ← ’تنظیمات‘ ← ’حریم خصوصی‘







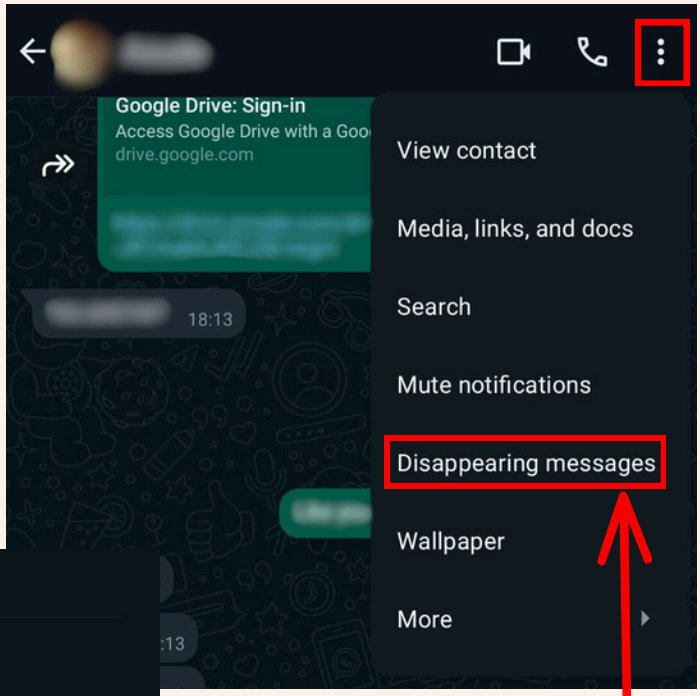
روی ’Default message timer‘ کلیک کنید.



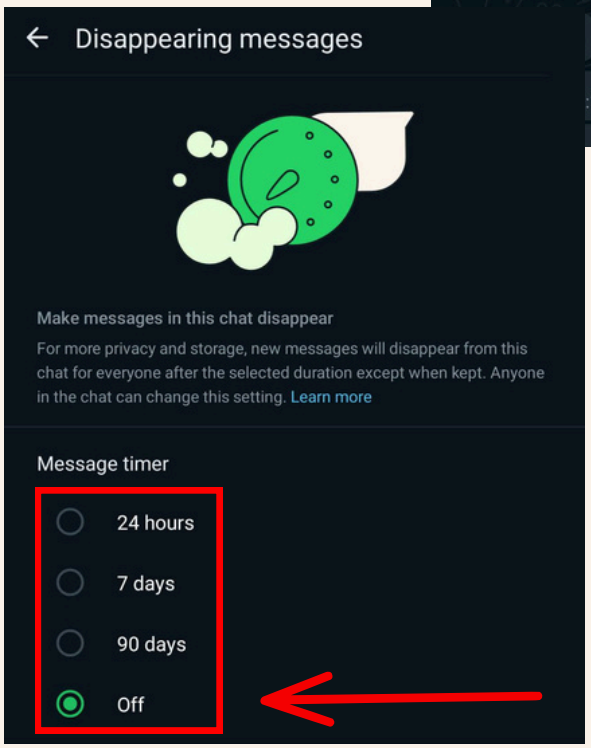
۲۴ ساعت، ۷ روز، ۹۰ روز یا ’Off‘ را انتخاب کنید.

روشن کردن پیام‌های مدت‌دار در گفتگوی خصوصی

گفتگویی را باز کنید و روی نام مخاطب کلیک کنید (یا سه نقطه را انتخاب کنید).



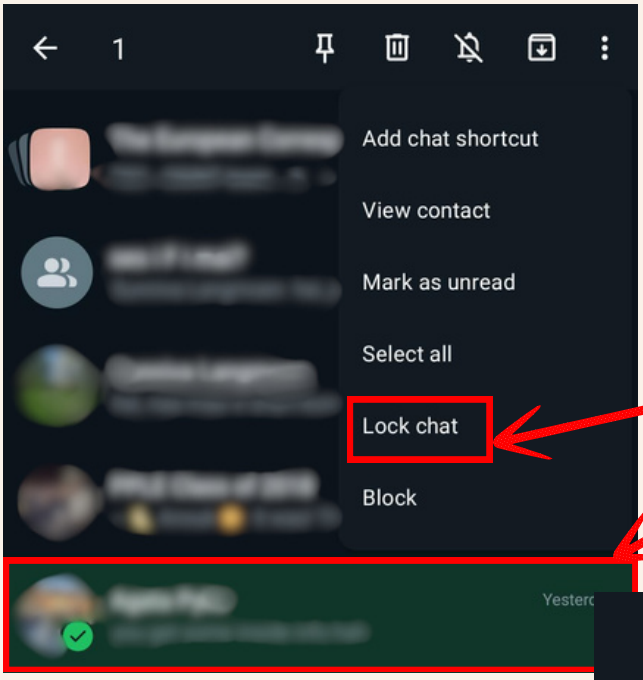
روی پیام‌های ناپدید شونده (Disappearing messages) کلیک کنید.



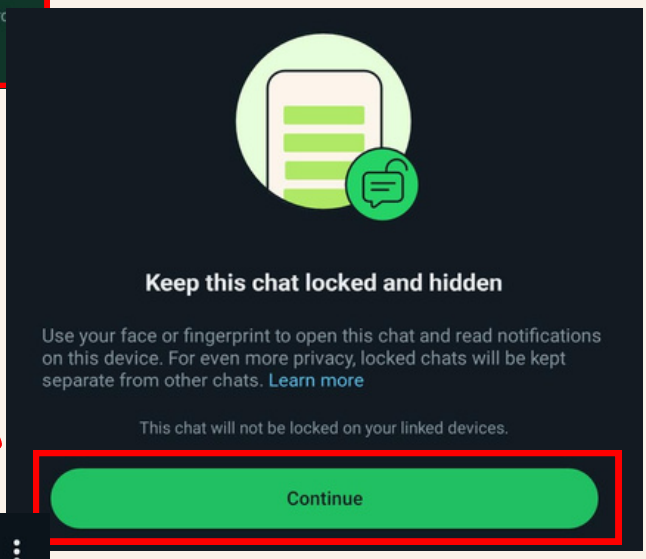
۲۴ ساعت، ۷ روز، ۹۰ روز یا 'Off' را انتخاب کنید.

نحوه قفل کردن چت

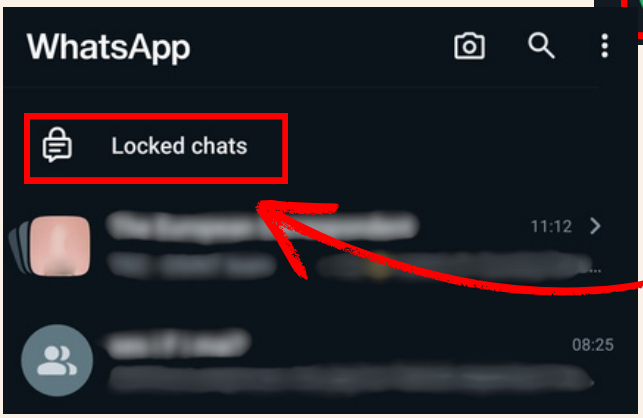
روی چتی که می‌خواهید قفل شود، به مدت چند ثانیه فشار دهید ← 'Lock Chat' را انتخاب کنید.



← روی گزینه 'Continue' فشار دهید.
← صورت یا اثر انگشت خود را برای قفل کردن تایید کنید.



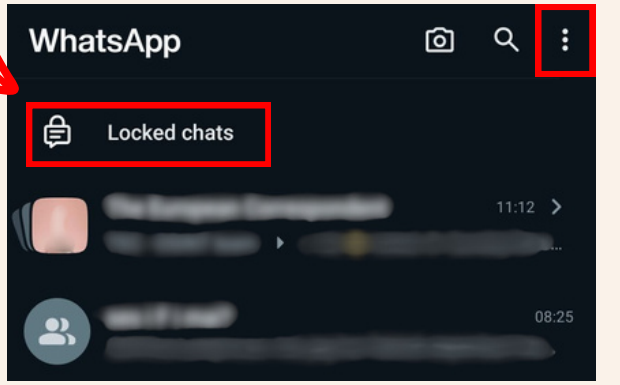
گفتگوی شما اکنون به فولدر 'چت های قفل شده' منتقل شده است!



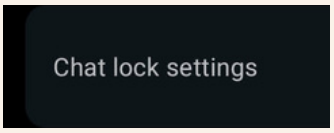
چت‌های خود را (با کد مخفی) قفل کنید

پس از فعال کردن قفل چت، می توانید چت‌های خود را با یک کد مخفی متفاوت از رمز عبور تلفن خود قفل کنید.

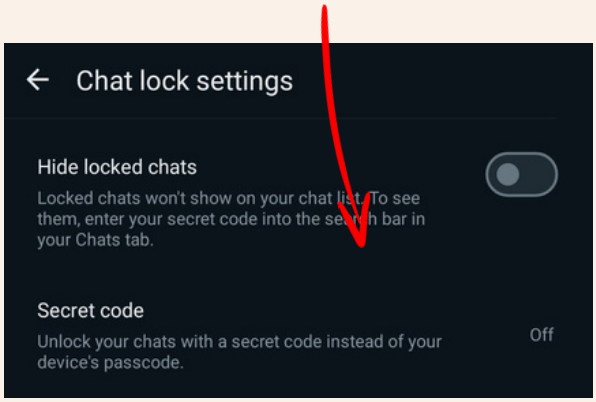
فولدر چت‌های قفل شده را باز کنید ← روی سه نقطه در قسمت بالای سمت راست صفحه کلیک کنید.



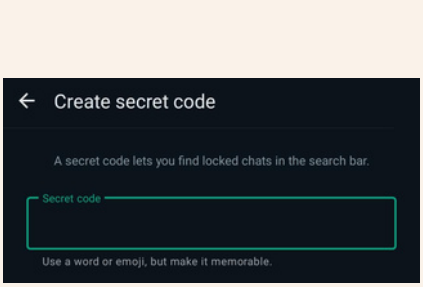
← ’تنضیمات قفل کردن چت‘ یا (Chat lock settings) را انتخاب کنید.



← روی ’کد مخفی‘ یا (Secret Code) کلیک کنید.



← کد مخفی ایجاد کنید و تایید کنید.

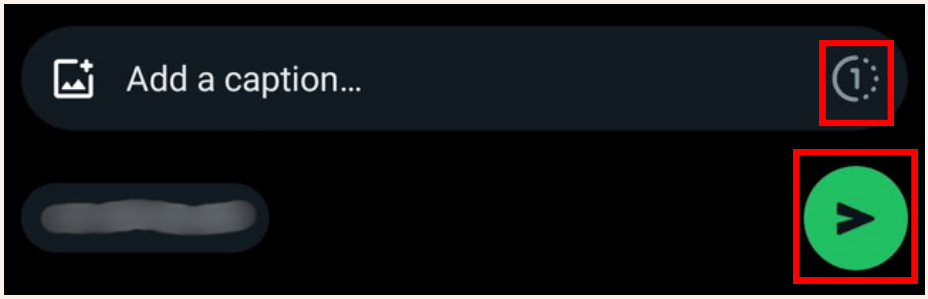


تصاویر/فیلم‌های قابل مشاهده یک بار را در واتساپ ارسال کنید

چت خصوصی یا گروهی را باز کنید.

تصویر یا ویدیویی را برای ارسال انتخاب کنید یا با کامره بگیرید.

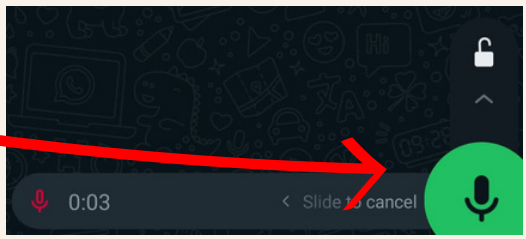
روی علامت ① در گوشه سمت راست پایین صفحه کلیک کنید و بعد علامت ➤ را فشار دهید.



پیام های صوتی قابل پخش یک بار را در واتساپ ارسال کنید

چت خصوصی یا گروهی را باز کنید.

میکروفون گوشه سمت راست پایین را نگه دارید و انگشت خود را به سمت بالا بکشید.

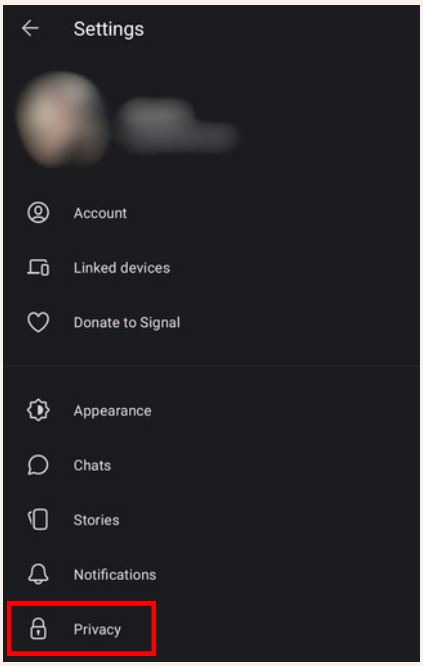


پس از ضبط کردن صدا علامت ⏸ را فشار دهید ← علامت ① را انتخاب کنید ← بعد دکمه ➤ را فشار دهید.

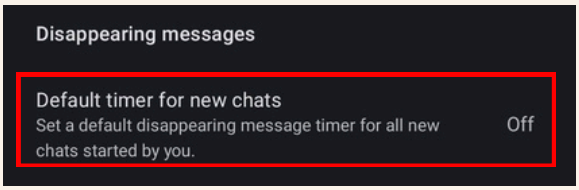
مراحل تنظیم حریم خصوصی در سیگنال

روشن یا خاموش کردن پیام‌های ناپدید شونده

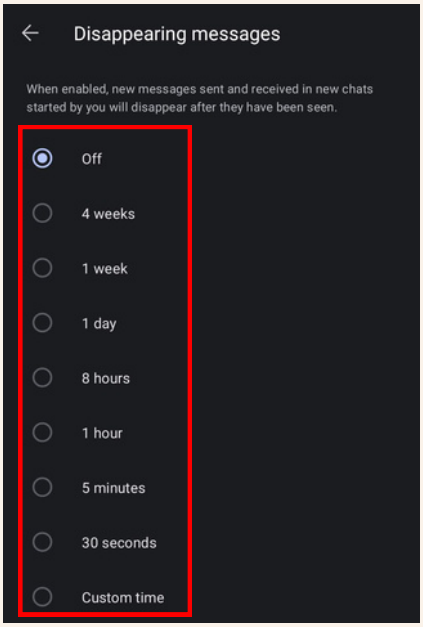
‘روی عکس پروفایل تان کلیک کنید ← ’حریم خصوصی



به ’پیام‌های ناپدید شونده‘ بروید و روی
’Default timer for new chats‘ کلیک کنید.

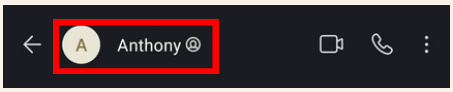


زمان مورد نظر خود را برای ناپدید شدن پیام ها انتخاب کنید.

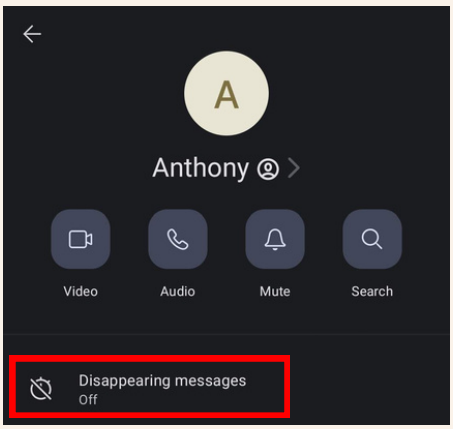


روشن کردن پیام‌های مدت‌دار در گفتگوی خصوصی

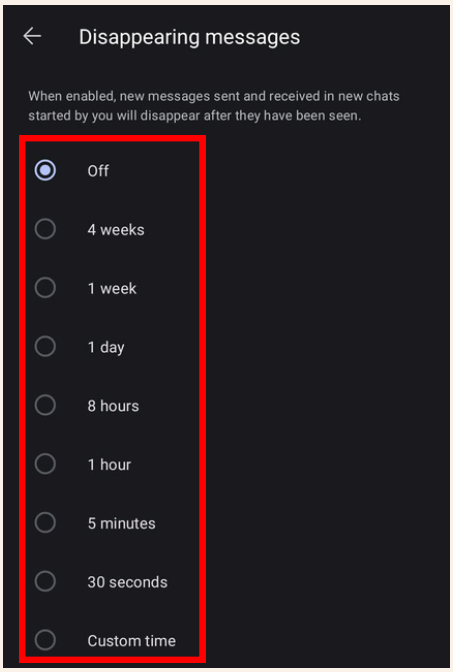
یک چت را باز کنید و روی نام مخاطب کلیک کنید.



روی پیام‌های ناپدید شونده (Disappearing messages) کلیک کنید.

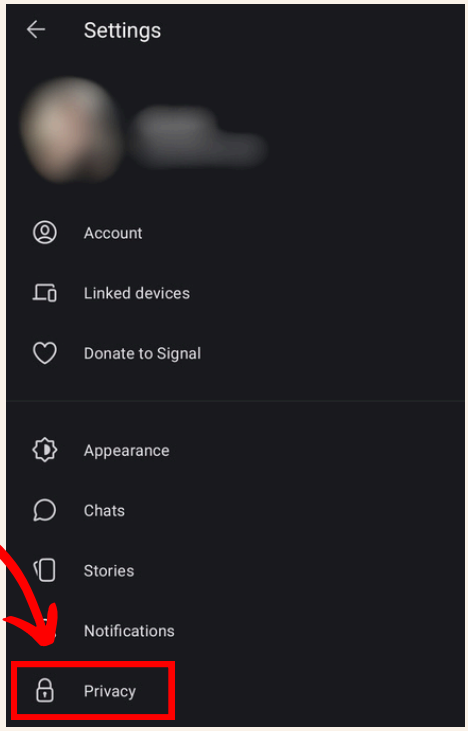


زمان مورد نظر خود را برای ناپدید شدن پیام ها انتخاب کنید.

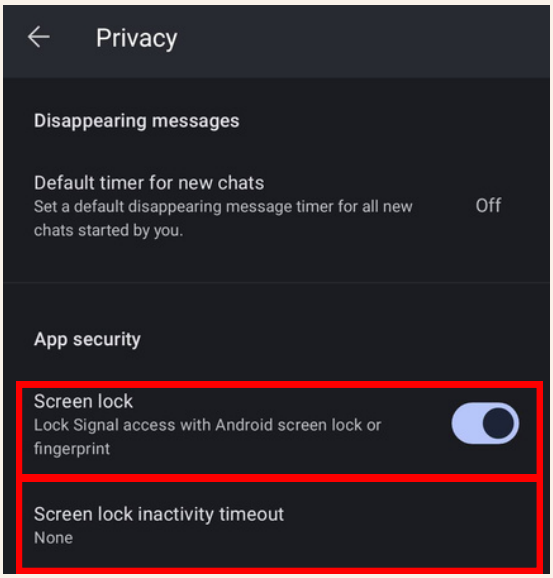


قفل کردن سیگنال

روی عکس پروفایل تان کلیک کنید
← ’حریم خصوصی‘



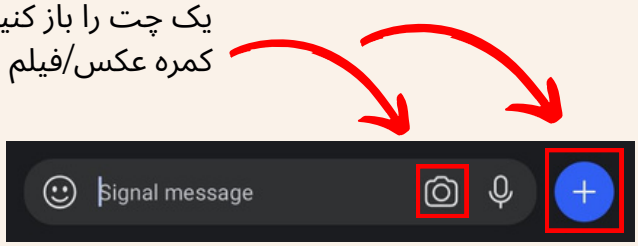
در بخش ’امنیت اپلیکیشن‘ یا
’App Security‘ دکمه ’قفل صفحه‘ یا
’Screen Lock‘ را تغییر دهید.



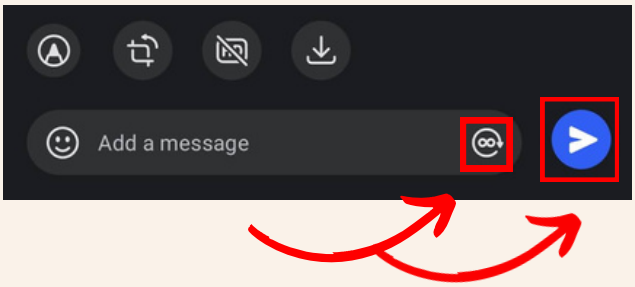
برای انتخاب مدت زمانی که پس از آن
برنامه سیگنال شما قفل می شود،
’Screen lock inactivity
timeout‘ را فشار دهید.

ارسال تصاویر/فیلم‌های ناپدید شونده در سیگنال

یک چت را باز کنید و یک عکس/فیلم را انتخاب کنید، یا با کمره عکس/فیلم بگیرید.

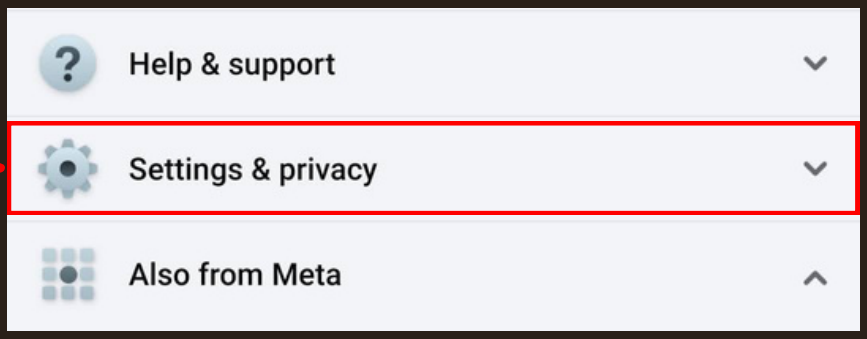


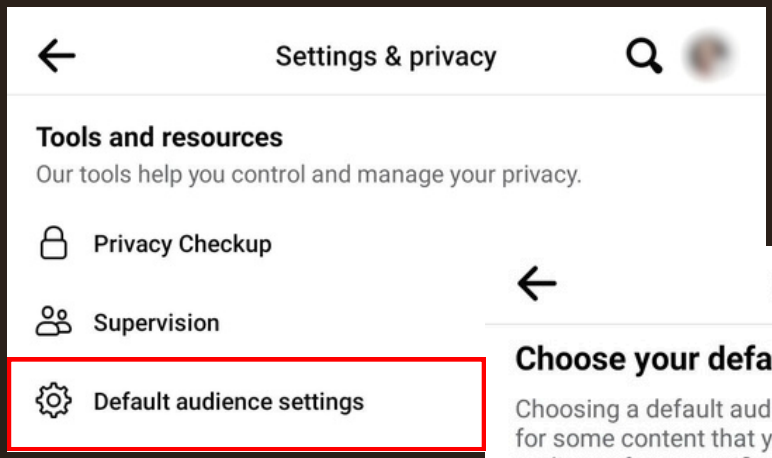
روی علامت در گوشه سمت راست پایین صفحه کلیک کنید و بعد علامت را انتخاب کنید.



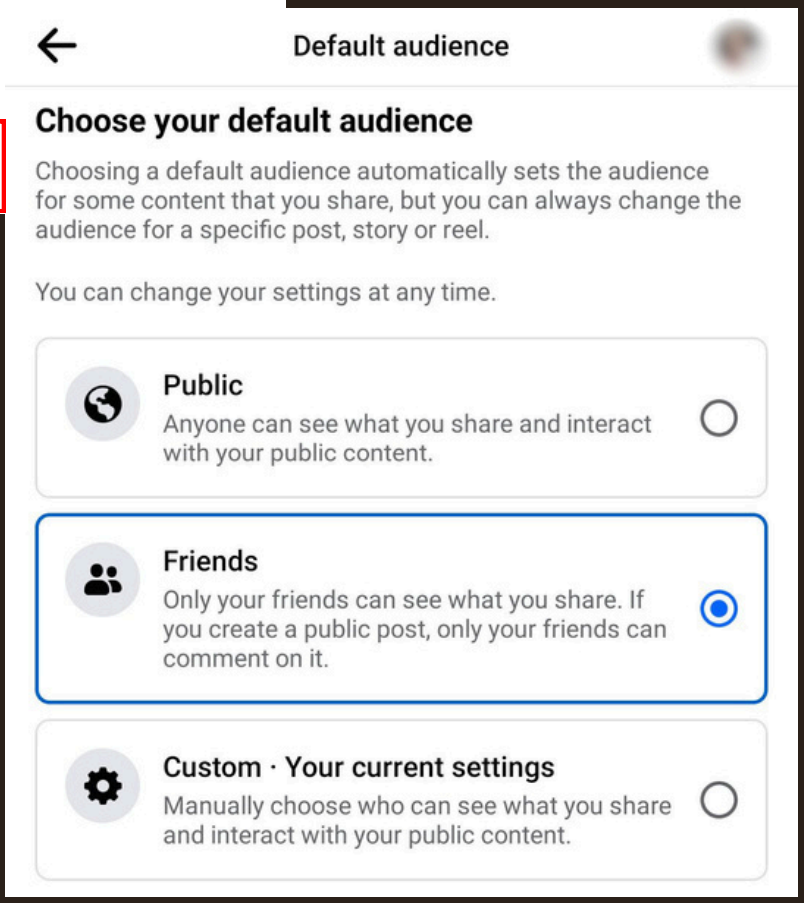
۳. امنیت حساب‌های کاربری رسانه‌های اجتماعی

مراحل تنظیم حریم خصوصی در فیسبوک

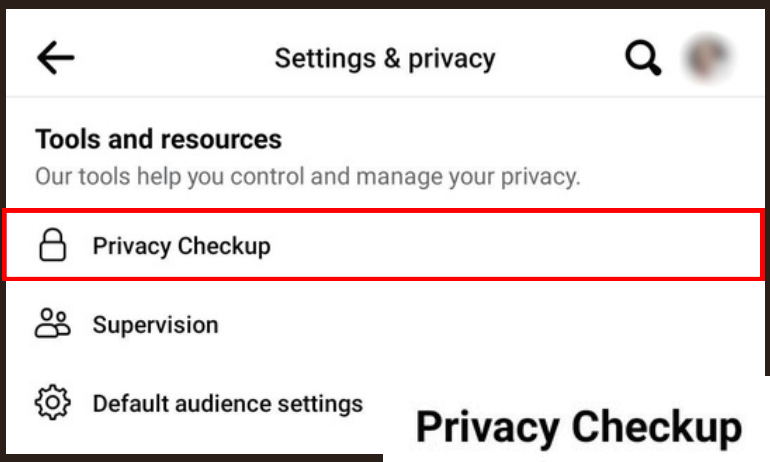


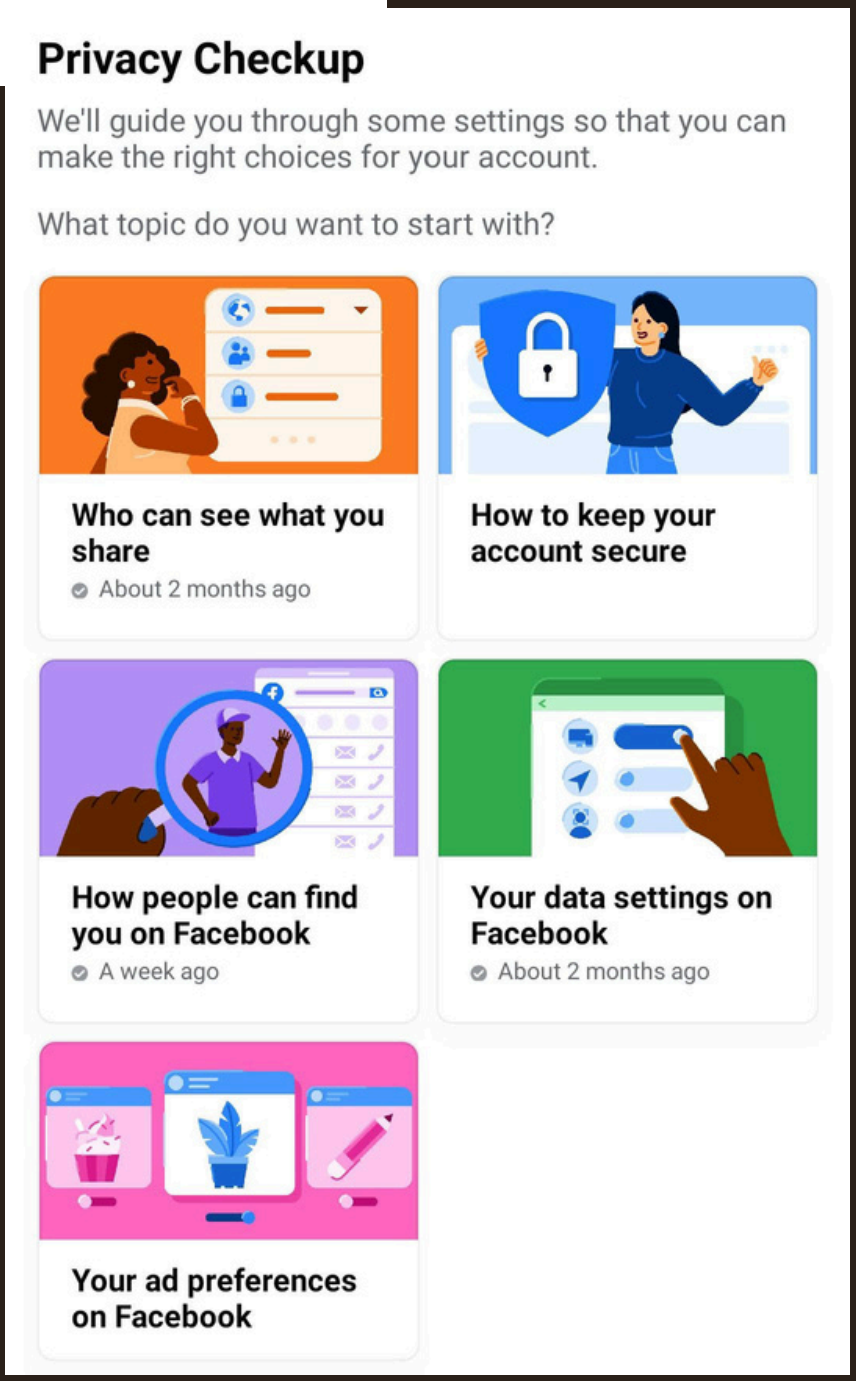


صفحه ‘Default audience settings’ به شما امکان می‌دهد تصمیم بگیرید چه کسی می‌تواند پست‌ها و موارد دیگر را ببیند.

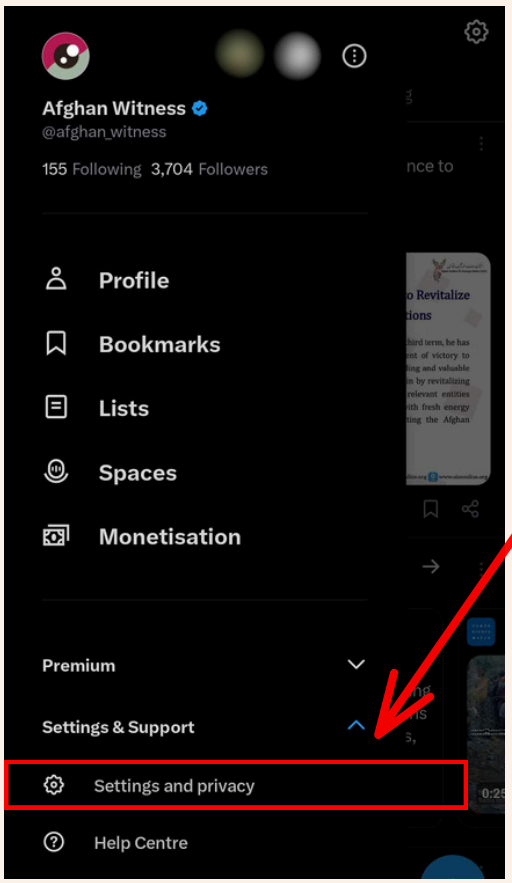


صفحه ‘Privacy Checkup’ تنظیمات دقیق‌تری را در اختیار شما قرار می‌دهد و به شما امکان می‌دهد تنظیمات حریم خصوصی را به حداکثر برسانید.

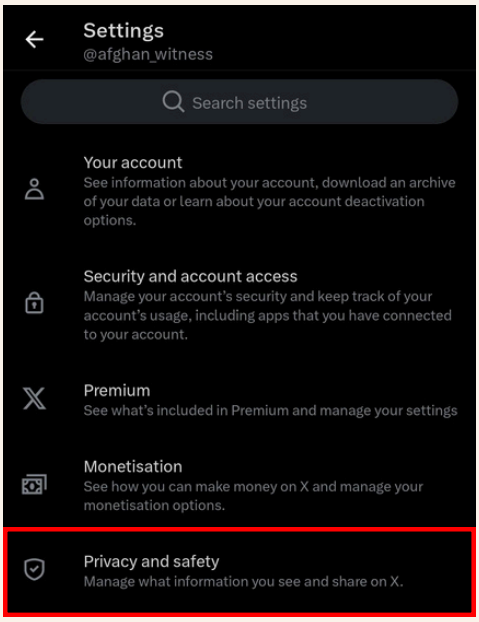




مراحل تنظیم حریم خصوصی در ایکس/توییتر

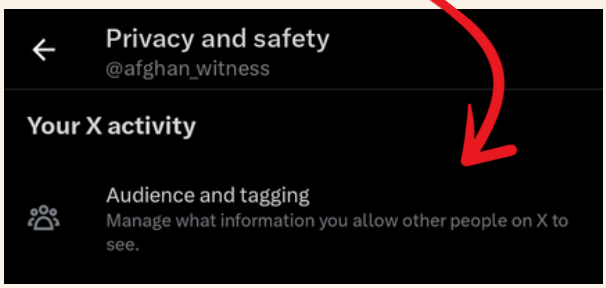


عکس پروفایل خود را فشار دهید، روی ‘Settings & Support’ و در ادامه روی ‘Settings and privacy’ کلیک کنید.

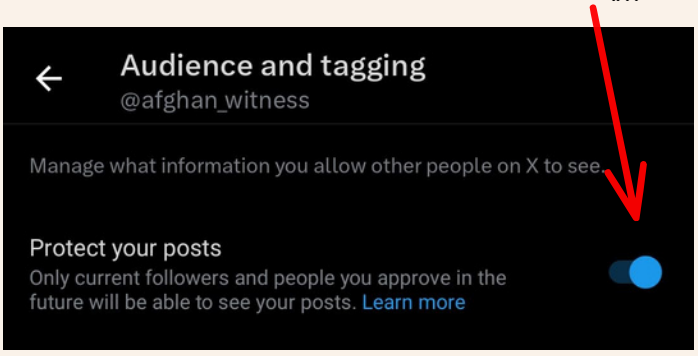


حالا روی ‘Privacy and safety’ کلیک کنید.

حالا ‘Audience and tagging’ را فشار دهید.



گزینه ‘Protect your posts’ را روشن کنید تا فقط دنبال کنندگان شما بتوانند پست های شما را ببینند.

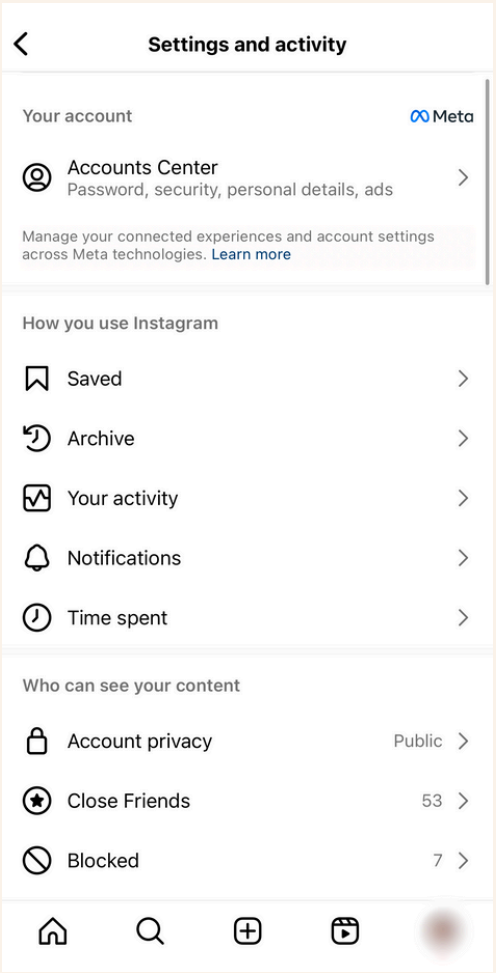


مراحل تنظیم حریم خصوصی در انستاگرام

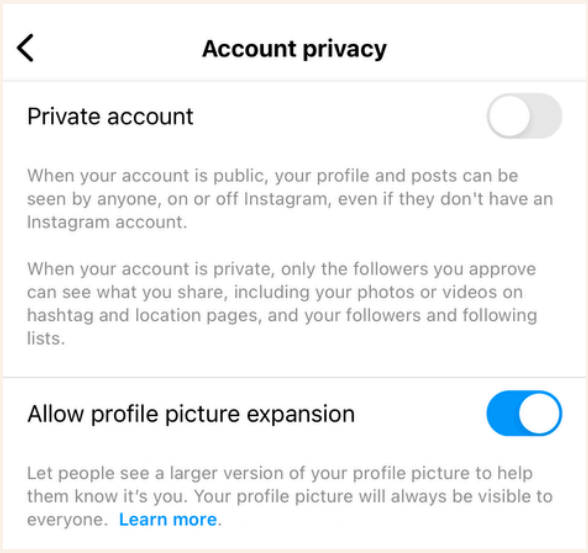
عکس پروفایل خود در پایین سمت راست صفحه را فشار دهید.

اکنون سه خط در بالای گوشه راست را فشار بدهید.

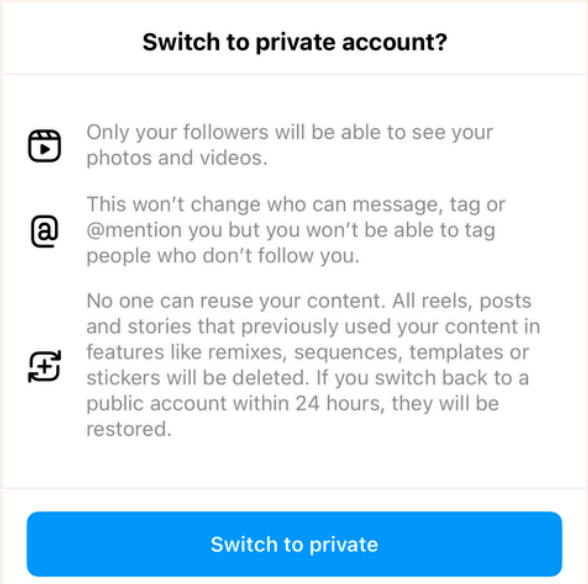
گزینه ‘Account privacy’ را که در زیر گزینه ‘Who can see your content’ قرار دارد را فشار بدهید.



برای خصوصی کردن حساب خود، سلاید ‘Private account’ را به سمت راست بکشید.



روی ‘Switch to private’ کلیک و تایید کنید.



۴. جستجو و گشت و گذار در اینترنت/وب

درک خطرات

هنگامی که در وب می گردید، خود را در معرض خطرات مختلفی قرار می دهید.

ممکن است توسط مقامات یا حتی اعضای خانواده مورد **ردیابی** و **نظارت** قرار بگیرید که می توانند به کل ترافیک اینترنت شما دسترسی داشته باشند.

ممکن است در معرض خطر **حملات بدافزار** (malware attacks) قرار بگیرید، جایی که دستگاه‌های شما توسط نرم‌افزاری آلوده می‌شوند که دیتای شما را می‌دزدد و فعالیت‌های شما را مشاهده می‌کند.

شما ممکن است هدف یک **حمله فیشینگ** قرار بگیرید. زمانی که یک مهاجم سعی می‌کند با استفاده از پیام‌ها، ایمیل‌ها یا وب‌سایت‌های جعلی که به این باور که مجاز هستند، شما را فریب دهد و اطلاعاتی مانند نام کاربری، رمز عبور یا جزئیات مالی را از شما بگیرد.

همچنین ممکن است قربانی فاش سازی یا **نشت اطلاعات** شوید. یعنی زمانی که سرویس‌های قابل اعتماد هک می‌شوند و داده‌های آن‌ها به سرقت می‌رود - داده‌هایی که ممکن است حاوی اطلاعات شخصی شما باشد.

با رعایت برخی اقدامات احتیاطی، می توانید **آسیب پذیری** خود را در برابر این حملات به **حداقل** برسانید.

شبکه‌های خصوصی مجازی (VPN) و مرور در حالت ناشناس

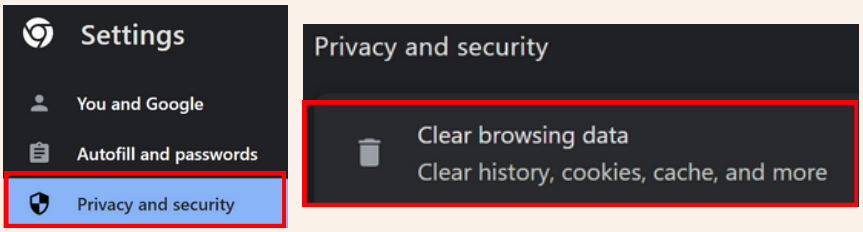
شبکه‌های خصوصی مجازی (VPN) آدرس IP شما را مخفی می‌کنند و اتصال شما به انترنت را رمزگذاری می‌کنند، و نظارت بر شما را برای هر کسی که فعالیت اینترنتی از دستگاه یا خانه شما را مشاهده می‌کند بسیار دشوار می‌کند. بهتر است تا یک سرویس VPN معتبر را انتخاب کنید. در حالی که اکثر خدمات VPN هزینه ماهانه دارند، Proton VPN یک گزینه رایگان عالی را در اختیار شما قرار داده است.

برای محافظت بیشتر، **مرورگر Tor** را انتخاب کنید. این مرورگر یا براوزر از یک شبکه رمزگذاری شده غیرمتمرکز ویژه استفاده می کند که تحت کنترل هیچ دولتی نیست و رایگان است. این مرورگر بیشترین ناشناس بودن را به صورت آنلاین به شما می دهد. با این حال، باید از ورود به حساب های شخصی خود با استفاده از Tor اجتناب کنید.

سابقه جستجوی خود را حذف کنید

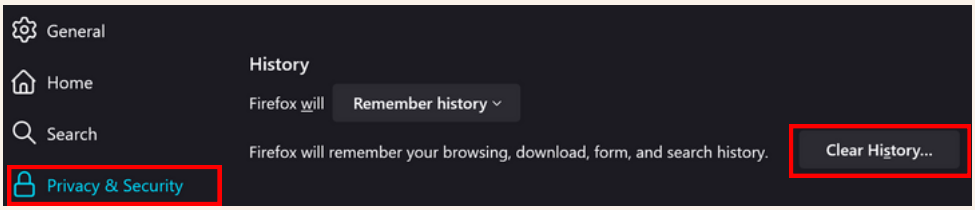
Chrome

‘Settings’ → ‘Privacy and security’ → ‘Clear browsing data’



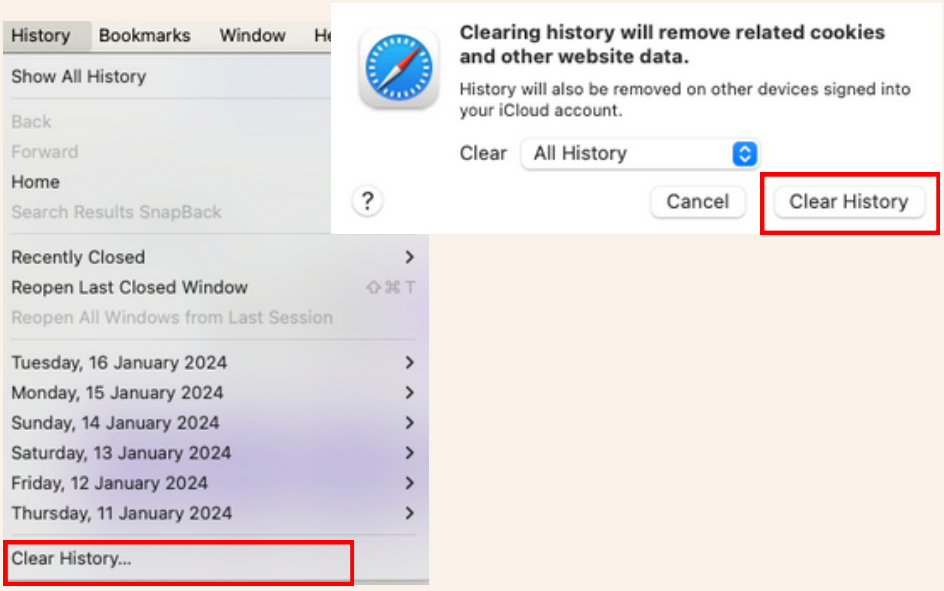
Firefox

‘Settings’ → ‘Privacy & Security’ → ‘History’



Safari

‘Settings’ → ‘Safari’ → ‘Clear History and Website Data’



از حالت جستجوی خصوصی استفاده کنید

برای استفاده از جستجوی خصوصی از میانبرهای (Shortcuts) زیر استفاده کنید:

Chrome — Ctrl + Shift + N

Firefox — Ctrl + Shift + P

Safari — Command + Shift + N

حالت جستجوی خصوصی یک ویژگی در مرورگرهای وب است که **از ذخیره سابقه، کوکی‌ها و سایر اطلاعات داخلی از جریان جستجوی شما جلوگیری می‌کند** و به محافظت از حریم خصوصی شما به صورت آنلاین کمک می کند.

با این حال، **هیچ کاری** علیه کسی که فعالیت‌های آنلاین شما را **از بیرون** مشاهده کند، و کسی که به شبکه یا نتورک شما دسترسی دارد، انجام نمی‌دهد - بنابراین باید اقدامات احتیاطی دیگری را روی دست بگیرید.

از شبکهٔ خصوصی مجازی (VPN) استفاده کنید

یک VPN یا یک شبکه خصوصی مجازی، راهی برای **پنهان کردن IP** شما و **رمزگذاری** تمام ترافیک اینترنت شما است تا کسی نتواند آنچه را که به صورت آنلاین مشاهده می‌کنید، پیدا کند.

خدمات VPN زیر پیشنهاد می‌شوند:

- Proton VPN (رایگان)
- Tunnelbear (۲ گیگ رایگان)
- Surfshark ($۲.۴۹ در ماه)
- NordVPN ($۳.۹۹ در ماه)
- Private Internet Access ($۳.۳۳ در ماه)

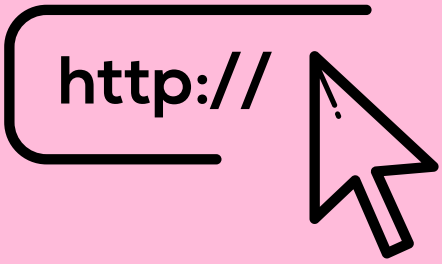
از نرم افزار پاک کننده کمپیوتر (PC Cleaning) استفاده کنید

پاک کننده های رایگان زیر پیشنهاد می‌شوند:

CCleaner

BleachBit

نرم‌افزارهای پاک کننده کمپیوتر مانند **CCleaner** و **BleachBit** با حذف خودکار سابقه جستجو هنگام استفاده از آن، به پاک کردن کمپیوتر، بهینه‌سازی عملکرد و حفظ حریم خصوصی کمک می‌کنند.



مرورگرها و موتورهای جستجوی جایگزین

برای حفظ حریم خصوصی بهتر، از **کروم** (Chrome)، **سافاری** (Safari) یا **ایج** (Edge) استفاده نکنید و از موتور جستجوی **گوگل** اجتناب کنید.

فایرفاکس (Firefox) گزینه خوبی است، مشروط بر اینکه آن را به درستی پیکربندی (Configure) کنید و چند برنامه افزودنی مرورگر (Browser extension) برای محافظت از حریم خصوصی خود نصب کنید.

مرورگرها و موتورهایی که توصیه می‌شوند

Brave ← مرورگری که تبلیغات و ردیاب‌ها را مسدود می‌کند

Tor ← ناشناس کردن مرورگر با استفاده از شبکه رمزگذاری شده

DuckDuckGo ← موتور جستجوی خصوصی

Startpage ← موتور جستجوی خصوصی

برنامه‌های افزودنی مرورگر (Browser Extensions)

برنامه‌های افزودنی مرورگر که به عنوان **add-ons** یا **plugins** نیز شناخته می‌شوند، برنامه‌هایی هستند که مرورگر وب را بهبود می‌بخشند.

آنها می توانند با **بلاک کردن اشخاص سوم** از **ردیابی فعالیت آنلاین شما** به محافظت از حریم خصوصی شما کمک کنند. با این حال، محتاط باشید زیرا برخی از برنامه‌های افزودنی می توانند مضر باشند.

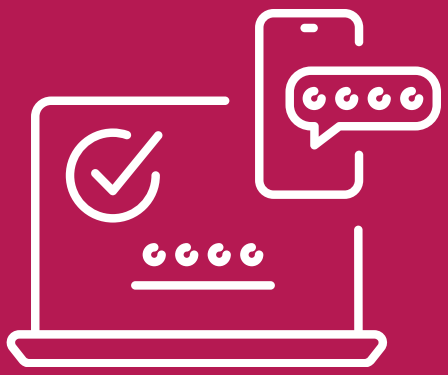
توصیه می کنیم **uBlock Origin** را نصب کنید، که نه تنها تبلیغات را مسدود می کند و جلسه مرور شما را بهبود می بخشد، بلکه از حریم خصوصی شما محافظت می‌کند و ردیابی تان را دشوارتر می کند.

۵. امنیت رمز عبور یا پسورد

امنیت رمز عبور **برای حفظ امنیت شخصی و حریم خصوصی ضروری است**.

متأسفانه، بسیاری از مردم از رمزهای عبور ضعیف مانند '123456'، 'password' یا نام‌ها و تاریخ تولد استفاده می‌کنند که به راحتی می‌توان حدس زد و به خطر افتاد. برخی از افراد همچنان رمزهای عبور خود را در یادداشت‌های خود یا در فایلی در دستگاه خود ذخیره می کنند که به راحتی برای هر کسی که آن را پیدا می‌کند قابل دسترسی است. دیگران از رمز عبور یکسان در تمام حساب های خود استفاده می کنند.

پیاده کردن امنیت رمز عبور قوی به محافظت از اطلاعات حساس کمک می‌کند و تضمین می کند که ارتباطات شخصی، مکان ها و فعالیت ها خصوصی باقی بمانند. استفاده از مدیر رمز عبور یا پسورد منیجر بهترین راه برای به حداکثر رساندن امنیت شما است: به طور خودکار رمزهای عبور امن را برای همه حساب های شما ایجاد می کند، در حالی که برای دسترسی به همه آنها فقط باید یک رمز عبور را به خاطر بسپارید.



شیوه‌های خوب:

✅ از حداقل **۱۵ کاراکتر** استفاده کنید.

✅ به جای رمز عبور به یک **عبارت** عبور فکر کنید:

یک **جمله** یا **مجموعه‌ای از کلمات تصادفی** یک رمز عبور تقریباً غیرقابل شکست را ایجاد می‌کند، در حالی که به راحتی می‌توان آن را بخاطر سپرد.

چیزی مانند '**smallfrogsittinginatree**' یا کاملاً تصادفی مانند **'frozenspouseimperfectjuice'** را امتحان کنید.

✅ ترکیب حروف بزرگ و کوچک، اعداد و سمبول‌ها می تواند امنیت را بهبود بخشد – اما اگر رمز عبور شما به اندازه کافی طولانی و تصادفی باشد، نیاز نیست این قاعده را دنبال کنید.

✅ **قدرت رمز عبور** خود را با ابزاری مانند www.passwordmonster.com تست کنید.

✅ رمز عبور را هر ۳ تا ۹ ماه یا در صورت نیاز **تغییر** دهید.

✅ از **رمزهای عبور مختلف** برای حساب های مختلف استفاده کنید.

✅ از **برنامه مدیریت رمز عبور** استفاده کنید.

✅ **تایید هویت دو مرحله‌ای (2FA)** را در حساب‌های خود فعال کنید. برنامه های موبایل مانند Google Authenticator نیز عالی کار می کنند!

شیوه‌های بد:

🚫 هرگز از **رمزهای عبور تکراری** استفاده نکنید.

🚫 **اجازه ندهید** مرورگر شما **رمزهای عبور** را **ذخیره** کند.

🚫 هیچ گونه **اطلاعات شخصی** را در رمزهای عبور خود استفاده نکنید (مانند تولد، نام کودک یا حیوان خانگی و غیره).

🚫 لیست رمزهای عبور خود را در کمپیوتر خود به صورت **متن ساده** ذخیره نکنید.

🚫 لیست رمزهای عبور خود را **روی کاغذ** ذخیره نکنید.

برنامه‌های مدیریت رمز عبور (Password Managers)

برنامه‌های **مدیریت رمز عبور** پسوردهای قوی و منحصر به فرد را تولید و ذخیره می کنند و امنیت دیجیتال را آسان تر می کنند. آنها رمزهای عبور را در یک 'طاق' امن نگه می دارند و از آنها با یک رمز عبور اصلی محافظت می کنند. مزایای آن شامل تولید رمز عبور، ذخیره‌سازی و تکمیل خودکار در دستگاه‌ها می‌شود.

البته مشکل آنها این است که یک نکته ضعف و شکست هستند. اگر شخصی به مدیر رمز عبور شما دسترسی پیدا کند، به تمام اطلاعات ورود به سیستم شما در تمام حساب‌های شما دسترسی خواهد داشت.

بسیار مهم است که یک پسورد اصلی قوی برای مدیریت رمز عبور خود انتخاب کنید و مطمئن شوید که دستگاه شما در برابر بدافزار محافظت می شود. در صورت امکان تایید هویت دو مرحله‌ای را فعال کنید.

KeePass یک مدیر رمز عبور رایگان، منبع باز و با استفاده آسان است که برای عملکرد به هیچ سرویس وب وابسته نیست.

پس از ایجاد دیتابیس پسورد و رمز عبور اصلی یا ماستر پسورد خود، می توانید فایل دیتابیس خود را در کمپیوتر یا تلفن خود نگه دارید، یا می توانید آن را در یک پلت فرم کلود (Cloud) مانند Google Drive قرار دهید، بنابراین می توانید در هر زمان و هر مکان به آن دسترسی داشته باشید. این انتخاب عملی‌تر است که به شما کنترل بیشتر و همچنان مسئولیت بیشتری برای آپدیت کردن برنامه و ایمن نگه داشتن فایل دیتابیس می‌دهد.

همچنان دارای برنامه هایی برای اندروید و iOS است.

BitWarden دارای گزینه های پولی و رایگان است. این یک گزینه کاربر پسندتر از KeePass است و رمزهای عبور شما بلافاصله در فضای کلود (Cloud) بکاپ (Backup) می‌شوند، بدون اینکه نیازی به مدیریت دیتابیس مانند KeePass داشته باشید. همچنان به طور خودکار آپدیت می‌شود. این یک انتخاب راحت تر از KeePass است.

همچنان دارای گزینه هایی برای اندروید و iOS است.

۶. امنیت فزیکی

حفاظت از دستگاه‌های شخصی

دستگاه‌ها را مخفی نگه دارید: همیشه تلفن، لپ‌تاپ یا تبلت خود را در زمانی که از آن استفاده نمی‌کنید، به‌ویژه در مکان‌های عمومی دور از دید قرار دهید. این امر خطر سرقت یا مصادره را کاهش می دهد.

فعال کردن رمزگذاری دستگاه: از ویژگی‌های رمزگذاری دستگاه برای محافظت از دیتای خود استفاده کنید. این تضمین می‌کند که اگر دستگاه شما مفقود یا دزدیده شود، بدون رمز عبور صحیح نمی‌توان به دیتا یا داده‌ها دسترسی داشت. این ویژگی در مدل‌های بالا به طور پیش فرض فعال است.

از دست دادن دستگاه

اگر دستگاه شما مفقود یا دزدیده شد، می توانید با استفاده از Find My Device (همچنان در iPhone) محتوای آن را از راه دور پاک کنید.

به منظور جلوگیری از از دست دادن دیتای خود در صورت مفقود شدن دستگاه، مطمئن شوید که به طور مرتب از دیتای مهم در یک سرویس کلود (Cloud) امن یا یک درایو خارجی رمزگذاری شده نسخه بکاپ تهیه کنید.

شیوه های امن آنلاین

از اشتراک گذاری موقعیت خود در زمان واقعی در رسانه‌های اجتماعی خودداری کنید. مراقب شریک ساختن جزئیاتی باشید که می‌تواند مکان شما را نشان دهد و مطمئن شوید که تنظیمات حریم خصوصی حساب خود را به حداکثر رسانده اید.

تشخیص نظارت فیزیکی

مراقب افراد ناآشنایی باشید که به نظر می‌رسد شما را دنبال می‌کنند یا تماشا می‌کنند. روال یا روتین خود را تغییر دهید تا از قابل پیش بینی بودن قدم بعدی تان جلوگیری کنید.

اگر مشکوک هستید که دنبال می‌شوید:

- مستقیماً به خانه **نروید**، تماس چشمی مستقیم با فرد برقرار نکنید، یا مستقیماً طرف مقصد خود فرار نکنید.
- **مشاهده کنید:** در نزدیک یک مغازه بایستید و برای مشاهده با احتیاط به اطراف تان نظر بیاندازید و برای مشاهده فردی که شما را تعقیب می کند زیر چشمی نگاه کنید. ظاهر و رفتار این فرد را به حافظه بسپارید.
- **در خیابان‌های عمومی بمانید:** به راه رفتن در خیابان‌های عمومی ادامه دهید، تا جایی که ممکن است به سمت شلوغی حرکت کنید و برای تغییر مسیر، به پیچ بعدی که در دسترس است بروید. مراحل را تکرار کنید تا زمانی که تعقیب کننده خود را گم کنید.
- **نشانه‌ها را بشناسید:** به خاطر داشته باشید که وقوع یکباره یک رویداد طبیعی است، دو بار ممکن است تصادفی باشد، اما سه بار یا بیشتر نشان دهنده یک تهدید بالقوه است.

روال‌های اضطراری

ایجاد روال‌های اضطراری می تواند امنیت شما را به میزان قابل توجهی افزایش دهد و آرامش خاطر را برای شما و افراد مورد اعتماد تان فراهم کند.

در اینجا چند روش موثر وجود دارد که می توانید آنها را اجرا کنید:

<u>افراد قابل اعتماد خود را از برنامه های تان مطلع سازید</u>

برنامه سفر خود را به اشتراک بگذارید:

- قبل از حرکت: همیشه یک شخص مورد اعتماد را در مورد برنامه های سفر خود از جمله مقصد، مسیر و زمان مورد انتظار رسیدن خود مطلع کنید.
- برنامه‌های روزانه: برنامه روزانه خود را به اشتراک بگذارید، به خصوص هنگام شرکت در جلسات یا بازدید از مکان‌های ناآشنا.

تماس‌های منظم:

- تماس‌های زمان‌بندی‌شده: در زمان‌های مشخصی برای تماس با شخص مورد اعتماد خود توافق کنید. این می تواند از طریق یک تماس تلفنی سریع، پیام متنی یا به روز رسانی رسانه‌های اجتماعی باشد.
- کلمات رمزی: از کلمات یا عبارات رمز از پیش تعیین شده استفاده کنید تا بدون ایجاد سوء ظن، ایمنی خود را تأیید کنید یا ناراحتی خود را نشان دهید. به عنوان مثال، عبارتی مانند 'من با خاله سارا هستم' می تواند نشان دهد که همه چیز خوب است، در حالی که 'من می روم به دیدن پسر کاکایم' ممکن است نشان دهد که شما در مشکل هستید.

<u>سیگنال های اضطراری و پروتکل های هشدار</u>

برقرار نکردن تماس:

- اقدام فوری: اگر یک تماس برنامه ریزی شده را از دست دادید، شخص مورد تماس شما باید سعی کند از طریق تمام راه‌های موجود (تماس های تلفنی، پیام ها و غیره) با شما تماس بگیرد.
- فعال‌سازی هشدار: اگر نتوانند در یک بازه زمانی از پیش تعیین‌شده با شما تماس بگیرند، باید به مقامات مربوطه مورد اعتماد یا سایر افراد تماس اضطراری تعیین‌شده هشدار دهند. از قبل روی این روند توافق کنید.

سیگنال های ناراحتی:

- هشدارهای بی صدا: اگر به کمک نیاز دارید اما نمی توانید آزادانه صحبت کنید از سیگنال های ظریف استفاده کنید. این می تواند ارسال یک ایموجی مورد توافق یا یک پیام رمز باشد.
- برای کمک تماس بگیرید: اگر در خطر هستید، با مخاطب مورد اعتماد خود تماس بگیرید و اجازه دهید تلفن همچنان وصل بماند، حتی اگر نمی توانید صحبت کنید. این به مخاطب شما امکان آن را می‌دهد آنچه را که اتفاق می افتد بشنود و اقدامات لازم را انجام دهد.

هنگام مسافرت یا عبور از مرزها

درک خطرات

هنگام سفر، به ویژه هنگام عبور از مرزها، ماموران امنیتی اغلب آزادانه دستگاه‌های الکترونیکی شما را جستجو می‌کنند که می‌تواند دیتای حساس شما را در معرض دید قرار دهد. آنها ممکن است دستگاه‌های شما را مصادره کنند و دیتای موجود در آن ممکن است کاپی و بررسی شوند. آنها ممکن است به عکس‌ها، مخاطبین و ارتباطات شخصی شما دسترسی داشته باشند، که ممکن است نه تنها شما، بلکه دیگران را نیز در معرض خطر قرار دهد.

با انجام اقدامات احتیاطی، ممکن است خود را در برابر چنین عملی ایمن کنید.

آمادگی قبل از سفر

یک دستگاه 'پاک' با خود داشته باشید: همه فایل‌های غیر ضروری را حذف کنید، در حالت ایده‌آل با استفاده از یک ابزار حذف امن این کار را انجام دهید. **اطمینان حاصل کنید که داده‌ها و فایل ها در فولدر جنک (Junk) شما باقی نمی‌مانند.**

از حساب‌های شخصی خارج شوید، اطلاعات ذخیره شده ورود یا لاگن به حساب تان را حذف کنید، تمام دیتای ذخیره شده خود را پاک کنید و هر برنامه حساس را حذف کنید.

از اطلاعات خود در یک مکان امن، یا در یک سرویس کلود (Cloud) یا به درایو یا دستگاه دیگری که به دستگاه شما متصل نیست بکاپ تهیه کنید. این به شما کمک می کند تا زمانی که در امنیت هستید، دیتای خود را بازیابی کنید، یا در صورت مفقود شدن یا مصادره دستگاه، به شما امکان می‌دهد که اطلاعات خود را دوباره بدست آورید.

حساب‌های ایمیل و رسانه‌های اجتماعی موقت را برای استفاده در سفر ایجاد کنید، و با پنهان کردن حساب‌های شخصی خود، سوء ظن را کاهش دهید.

در صورت امکان با تلفن یا لپ تاپ موقتی که فقط اطلاعات ضروری و مطمئن را به آن منتقل کرده اید، سفر کنید.

مراقب باشید که دستگاه شما آنقدر تمیز نباشد که مشکوک باشد - تلاش کنید که تلفن تان عادی به نظر برسد و حاوی تعدادی عکس، پیام و اپلیکشن‌ها باشد.

پس از مسافرت یا عبور از مرز

دستگاه‌های خود را برای نشانه‌های دستکاری، مانند برنامه‌های ناآشنا یا تنظیمات تغییر یافته، بازرسی کنید. **اگر مشکوک که دستگاه تان دستکاری شده، دستگاه را از یک نسخه بکاپ پاک و بازیابی (Restore) کنید.**

پسوردهای حساب‌هایی را که در طول سفر به آنها دسترسی پیدا کرده‌اید، تغییر دهید. این کار امکان به خطر افتادن رمزهای عبور شما را کاهش می دهد.

هنگامی که در مکان امن هستید و به اینترنت دسترسی دارید، می‌توانید داده های خود را از نسخه های بکاپ یا پشتیبان خود بازیابی کنید.

منابع اضافی

به زبان‌های فارسی/دری، پشتو و انگلیسی

لینک‌ها

Access Now — Guide to Safer Travel (انگلیسی)

Chayn — Advanced DIY Privacy for Every Woman (انگلیسی)

Chayn — DIY Online Safety (فارسی)

CiviCert — The Digital First Aid Kit (فارسی)

EFF — Surveillance Self-Defense guide (انگلیسی)

EFF — Street-Level Surveillance project (انگلیسی)

Freedom of the Press Foundation — Secure communication (انگلیسی)

Human Rights First — Steps to Protect Your Online Identity from the Taliban: Digital History and Evading Biometrics Abuses (فارسی و پشتو)

Privacy Guides — Knowledge Base (انگلیسی)

Tactical Tech — Resources (انگلیسی)

The New Oil — The Beginner's Guide to Data Privacy & Cybersecurity (انگلیسی)

تعریف اصطلاحات

رمزگذاری: تبدیل اطلاعات به یک کد مخفی به طوری که فقط افراد دارای کلید بتوانند آن را بخوانند و از دیگران در امان باشند.
رمزگذاری End-to-End: راهی برای ارسال پیام‌ها به طوری که فقط فرستنده و گیرنده بتوانند آنها را بخوانند و مطمئن شوند که هیچ کس دیگری نمی تواند اطلاعات را ببیند.

منبع باز: نرم افزاری که هر کسی می تواند آن را ببیند، استفاده کند، تغییر دهد و به اشتراک بگذارد. اغلب توسط برنامه نویسان ایجاد می شود.

فایروال: یک ابزار امنیتی است که از ورود ترافیک مضر اینترنت به کمپیوتر یا شبکه شما جلوگیری می‌کند و مانند یک مانع برای محافظت از داده های شما عمل می کند.

انتی ویروس: برنامه ایست که نرم افزارهای مضر (ویروس ها) را که می‌توانند به کمپیوتر شما آسیب بزنند یا اطلاعات شما را بدزدند، پیدا، حذف و از آن محافظت می‌کند.

بدافزار (Malware): هر نرم افزاری که برای آسیب رساندن به کمپیوتر یا سرقت اطلاعات شما از جمله ویروس‌ها، spyware و ransomware طراحی شده است.

حمله فیشینگ: نوع خاصی از کلاهبرداری که در آن پیام‌های جعلی سعی می‌کنند شما را فریب دهند تا اطلاعات شخصی‌تان را فاش کنید، اغلب با تظاهر به اینکه از یک شرکت یا شخص مورد اعتماد است.

مهندسی اجتماعی: فریب دادن مردم با استفاده از ترفندهای روانشناختی یا با تظاهر به قابل اعتماد بودن، تا افراد اطلاعات محرمانه را در اختیار شان قرار دهند.

VPN (شبکه خصوصی مجازی): سرویسی که یک اتصال امن و خصوصی از طریق اینترنت ایجاد می کند، فعالیت‌های آنلاین شما را مخفی می‌کند و از دیتای شما در برابر جاسوسی محافظت می کند.

تایید هویت دو مرحله‌ای (2FA): یک لایه امنیتی اضافی برای ورود به حساب‌ها، که نه تنها به رمز عبور بلکه به چیز دیگری مانند کد ارسال شده به تلفن تان نیاز دارد.

رمز عبور یا پسورد: مجموعه‌ای از اعداد یا حروفی که برای باز کردن قفل تلفن، کمپیوتر یا اپلیکیشن‌های خود استفاده می‌کنید و به حفظ امنیت اطلاعاتتان کمک می‌کنند.

برنامه مدیریت پسورد (Password Manager): نرم افزاری که رمزهای عبور شما را به صورت ایمن ایجاد، ذخیره و مدیریت می کند، بنابراین شما باید فقط یک رمز عبور اصلی را به خاطر بسپارید.

تعریف اصطلاحات

کوکی‌های ردیابی: فایل‌های کوچکی که وب‌سایت‌ها در کمپیوتر تان ذخیره می‌کنند تا عملکرد و اولویت‌های شما را به خاطر بسپارند و اغلب برای ردیابی عادت‌های جستجو و مرور تان برای تبلیغات استفاده می‌شوند.

حالت جستجوی خصوصی: ویژگی در مرورگرهای وب (Web browsers) که کوکی‌ها یا سوابق جستجوی شما را ذخیره نمی کند و به خصوصی نگه داشتن گشت و گذار تان در اینترنت کمک می کند.

اطلاعات بیومتریک: داده‌های مبتنی بر ویژگی‌های فیزیکی مانند اثر انگشت، تشخیص چهره یا اسکن عنبیه چشم که برای شناسایی و تأیید افراد استفاده می‌شود.

Adblocker: ابزار یا افزونه مرورگر (Browser Extension) است که از نمایش تبلیغات در وب سایت‌هایی که بازدید می‌کنید جلوگیری می‌کند و تجربه مرور شما را تمیزتر و سریع تر می کند.

نرم افزار پاک کننده کمپیوتر: برنامه‌هایی مانند CCleaner و BleachBit که کمپیوتر شما را تمیز می‌کنند، عملکرد را بهبود می‌بخشند و با حذف تاریخچه و فایل‌های غیر ضروری، حریم خصوصی را حفظ می‌کنند.

مرورگر Tor: یک مرورگر وب ویژه است که فعالیت آنلاین شما را از طریق اتصال به چندین سرور (Server) پنهان می کند و ردیابی کارهایی که آنلاین انجام می‌دهید را برای هر کسی دشوار می‌کند.

موقعیت مکانی GPS: سیستمی که از ماهواره‌ها برای یافتن و نشان دادن موقعیت دقیق شما بر روی نقشه استفاده می‌کند که برای جهت یابی و خدمات مبتنی بر مکان مفید است.

بلوتوث: فناوری ای که به دستگاه هایی مانند تلفن، هدفون و کمپیوتر اجازه می‌دهد تا اطلاعات را به صورت بی سیم در فواصل کوتاه به هم متصل کرده و به اشتراک بگذارند.

برنامه‌های پیام رسان امن: برنامه‌هایی مانند سیگنال یا واتساپ که از رمزگذاری قوی برای محافظت از پیام‌های شما استفاده می‌کنند تا فقط شما و شخصی که با او صحبت می‌کنید بتوانید آنها را بخوانید.

نشت اطلاعات: زمانی که اطلاعات خصوصی به طور تصادفی یا عمدی افشا می‌شود، در دسترس افرادی قرار می‌گیرد که نباید به آن دسترسی داشته باشند.

برنامه‌های افزودنی مرورگر (Browser Extension): برنامه‌های نرم‌افزار کوچکی که می‌توانید به مرورگر یا براوزر وب خود اضافه کنید تا به آن ویژگی‌های بیشتری بدهید، مانند مسدود کردن تبلیغات یا ترجمه زبان‌ها.

#WOMENSAFEONLINE

afghanwitness.org

@afghan_witness

@AfghanWitnessOfficial

@afghan_witness