امنیت دیجیتال و حریم خصوصی

برای فعالان و مدافعان حقوق بشر فعال در افغانستان
سپتامبر 2022

موسسه توسعه و دموکراسی افغانستان
(ADDO)

فهرست مطالب

موسسه دموکراسی و توسعه افغانستان (ADDO)

موسسه دموکراسی و توسعه افغانستان (ADDO)[1] یک موسسه غیر دولتی است که در سال 2014 در وزارت اقتصاد جمهوری اسلامی افغانستان ثبت شد. این موسسه در ولایات مرکزی، جنوبی، شمالی افغانستان و همچنان کابل از سال ۲۰۱۴ بدین سو فعال بوده است. هدف از تاسیس ADDO ایجاد جامعه ای است که در آن حاکمیت قانون، دموکراسی و احترام به حقوق بشر سنگ بنای حکومت و جامعه باشد و مردم به ثبات اجتماعی، آزادی و و خودکفایی اقتصادی دست یابند. هدف این موسسه، پیشبرد اصول دموکراتیک و حقوق بشر از طریق تقویت ظرفیت های شهروندان افغان، مشارکت آنها در برنامه های دادخواهی و تحقیق، و ارایه یک تصویر مطلوب تر از افغانستان برای جهانیان است. ADDO در شهر ها و روستا های افغانستان، با متنفذان و سیاست گذاران افغان، نهادهای جامعه مدنی، گروه های حامی حقوق زنان و موسسات جوانان برای تقویت دموکراسی از طریق آموزش، تحقیق، نظارت بر قوانین، دادخواهی ، ظرفیت سازی، و حفظ حقوق و آزادی های بشری فعالیت مینماید.

در باره این رهنمود

این رهنمود با استفاده از جدیدترین اطلاعات در مورد امنیت دیجیتال تهیه شده است. این یک رهنمود کاربری مفید برای تمام فعالان افغان و مدافعان حقوق بشر است که در افغانستان و خارج از مرزهای این کشور فعالیت می کنند. از آنجایی که نیاز به یک رهنمود مختصر بود، ما تلاش کرده‌ایم تا از درج جزئیات غیر ضروری که سبب گیج شدن خوانندگان شود اجتناب کنیم. ولی در عوض، وبسایت ها و پیوندهای (websites and links) مرتبط را برای هر موضوع خلاصه شده در پایین، ارائه کرده ایم. در این رهنمود وبسایت های مفید زیادی وجود دارند که می‌توانند اطلاعات بیشتری در مورد هر یک از موضوعاتی مورد بحث، ارائه دهند. برای اطلاعات دقیق تر و مفیدتر، خوانندگان می توانند به هر یک از این وبسایت ها سر بزنند.

این رهنمود با پشتیبانی سخاوتمندانه مالی موسسه ACCESSNOW[2] تهیه شده و در اختیار شما قرار گرفته است. ADDO از موسسه بین المللی ACCESSNOW جهت پشتیبانی مالی و ایجاد فرصت برای تهیه این رهنمود قدردانی می نماید. مسئولیت مطالب و نظرات بیان شده در این رهنمود بر عهده ACCESSNOW نیست و لزوماً منعکس کننده نظرات آن نمیباشد. ADDO از هرگونه نظر در مورد محتوای این رهنمود (از جمله اصلاح هر گونه اشتباه) استقبال می کند.

[1] http://addo.org.af
[2] https://www.accessnow.org

فهرست مخفف ها

- AES - Advanced Encryption Standard
- BYOD – Bring Your Own Device
- GMIC - Government Media and Information Center – Afghanistan
- HTTPS - Hypertext Transfer Protocol Secure
- IDS - Intrusion Detection System
- IoT - The Internet of Things
- ISP - Internet Service Provider
- NSA - National Security Agency
- OS - Operation System
- PC - Personal Computer
- RFID - Radio Frequency Identification
- SSL - Secure Sockets Layer
- SMS - Short Message Service
- UDHR - Universal Declaration of Human Rights
- VPN - Virtual Private Network

امنیت دیجیتال و حریم خصوصی

بدون شک ما از کامپیوتر، تلفن های هوشمند و اینترنت برای جستجو، ذخیره و تبادل اطلاعات استفاده می کنیم. بنابراین، امنیت در دنیای دیجیتال به امنیت اطلاعات ما مربوط می شود. ما باید از اطلاعات خود در جایی که ممکن به سرقت برود، محدود شود، و یا به خطر افتاده و آسیب ببیند محافظت کنیم. در یک سیستم مطلوب، همه افراد از فرصت برای دسترسی به اطلاعات و انتشار آن برخوردارند. ولی، برخی از دولت‌ها جریان اطلاعات را کنترل می‌کنند و در عین حال می‌خواهند، محدودیت‌هایی برای دسترسی به اطلاعات اعمال کنند. مشکل دیگر این است که کاربران اینترنت افراد مخربی را تجربه می‌کنند که ویروس‌هایی را برای کامپیوترها و تلفن‌های هوشمند ایجاد نموده و سیستم امنیتی آن‌ها را هک می‌کنند تا به کاربران آسیب های مالی و انترنتی وارد کنند و اطلاعات با ارزش آنها را به سرقت ببرند.

اکنون سردرگمی عجیبی در دنیای دیجیتال ما حاکم است. ما امیدوارانه میگوییم که هیچ چیز قطعی نیست ولی، هر چیز ممکن اتفاق بیفتد. ما یک ایمیل ارسال مینماییم، برای شخصی پیام می فرستیم، اسناد و مدارک مهمی را از طریق ابزارهای ارتباطات رسانه های اجتماعی به یکدیگر ارسال می کنیم و یا هم یک سند مهمی را می نویسیم، اما هرگز خطرات ناامنی دیجیتالی را در نظر نمی گیریم. بدون شک، ما نمی‌توانیم کاربران مطمئنی در دنیای دیجیتال باشیم. ما باید از توانایی ها و ضعف های خود از بزرگراه های اطلاعاتی و فناوری که در عصر جدید ظهور می کند کاملاً آگاهی داشته باشیم. ما باید آگاه باشیم و مهارت هایی برای بقای برنامه ها و انجام کار روزانه خود در اینترنت با خیال راحت داشته باشیم.

برخی از کشورها قوانین سختگیرانه ای را تصویب می کنند و فناوری های جدیدی را جهت کسب قدرت نظارت بیشتر معرفی می نمایند. به عنوان مثال، پروژه ECHELON[3] یک سیستم نظارت جهانی را معرفی می کند که می تواند ارتباطات ما را روی تلفن، اینترنت و ماهواره ها ضبط و پردازش نماید. با این حال، حق و امکان دسترسی به اطلاعات از نقطه اتصال اینترنتی محدود شده است. بسیاری از دولت هایی که حاضر نبودند به شهروندان خود حق بدهند، از آن استفاده کرده و حق دسترسی آزاد به اینترنت را محدود نمودند. سیستم های فیلترینگ خاص بر مبنای مقتضای هر دولت جهت محدود کردن و مسدود کردن اطلاعات اینترنتی که نامناسب پنداشته شود و یا برخلاف قوانین در این کشور ها باشد، ایجاد شده‌اند.

محدودیت ها و نظارت جهانی بر اینترنت در حال افزایش است. از آنجایی که آزادی عمومی آنلاین کاهش یافته است، دولت‌ها در سرتاسر جهان تلاش‌های نظارتی و محدودیت های اینترنتی خود را افزایش می‌دهند. از جون 2014 بدینسو در بیش از نیمی از 65 کشوری که در یک بررسی دخیل بودند، آزادی آنلاین کاهش یافته است. فرانسه که در پی حملات شارلی ابدو قانونی وضع کرد، شاهد یکی از بدترین محدودیت ها بود. از ایران، سوریه و چین به عنوان کشورهایی با شدیدترین محدودیت ها برای آزادی آنلاین نامبرده شده است. در مجموع، 14 کشور قوانینی برای افزایش نظارت دولت بر انترنت تصویب کرده اند. شرکت‌های خصوصی در 42 کشور از 65 کشور مجبور به حذف یا محدود کردن اطلاعات اینترنتی شده اند، زیرا اظهارات انتقادی در مورد مقامات دولتی بیشتر منجر به سانسور شده است. علاوه بر این، بسیاری از دولت‌ها نگرش‌های سختگیرانه‌تری را علیه فناوری‌های ناشناس و رمزگذاری (encryption) آنلاین اتخاذ کرده اند[4].

چین "Great Firewall" را معرفی کرد که تمام ارتباطات بین المللی را در این کشور (بعد از بازرسی) جهت میدهد. " Great Firewall" از طریق "Proxy Servers" در ورودی های موثق (official gateways) عمل میکنند. وزارت امنیت عامه این کشور توانسته است تک تک کاربران انترنت و محتویات کاربری آنها را شناسایی نماید، حق دسترسی به اطلاعات دیجیتالی را مشخص و در نهایت بر ترافیک داخل و خارج از کشور در این ورودی های موثق نظارت داشته باشد[5]. اکنون، " Great

[3] پنج چشم، که همچنان به نام استرالیا، کانادا، نیوزلند، بریتانیا و ایالات متحده نیز شناخته می‌شوند، پنج کشور امضاکننده توافقنامه امنیتی UKUSA هستند و برنامه نظارت بر دنیای دیجیتال را مدیریت می کنند.

[4] https://www.reuters.com/article/cybersecurity-report-idINKCN0SM1NJ20151028

[5] https://www.techtarget.com/whatis/definition/Great-Firewall-of-China

Firewall" در چین در حال تغییر یک نسل به صورت کامل است[6]. به دنبال آن، چین «Golden Shield » را معرفی کرد. این یک بدیل بلند پروازانه برای سیستم قبلی بود. «Golden Shield » متکی به اینترنت ملی است و از اینترنت جهانی جدا شده است. پروژه «Golden Shield » باید یک بانک اطلاعاتی از هر کاربر اینترنتی ذخیره نموده و از آن برای کمک به حفظ امنیت ملی استفاده نماید. در اصل، این یک ترفند برای جاسوسی گسترده در چین بود. چین توانایی استخبارات نظارتی در این شبکه ایجاد کرده است که به آن اجازه می دهد ببیند، بشنود و حتی فکر کند[7]. اکنون فیلتر محتوای مطالب از سطح شهروندان به میلیون‌ها دستگاه اطلاعاتی و ارتباطی در مکان‌های عمومی و خانه‌های شهروندان منتقل شده است. در نهایت « Golden Shield» با یک فناوری فوق العاده پیچیده مجهز است.

این محدودیت ها ظرفیت ما را برای استفاده از اینترنت و سفر به فراسوی مرزها برای دستیابی به دانش و ارتباطات محدود می کند. علاوه بر این، آنها تعدادی از مقررات اعلامیه جهانی حقوق بشر (UDHR) را که حق همه افراد را برای حفظ حریم خصوصی و آزادی بیان تضمین می کند، نقض می کنند.

تکنیک‌های نظارت و بررسی از کنترل افسران اطلاعاتی به سیستم‌های سخت‌افزاری و نرم‌افزاری که توسط شرکت‌های خصوصی و نهادهای دولتی اداره می‌شوند، منتقل شده است.

پیش از این، فردی که تهدیدی برای امنیت ملی محسوب می شد، مورد بررسی و تجسس قرار میگرفت. به دلیل مکانیسم های نظارت و فیلتری که دولت ها در اینترنت ایجاد کرده اند، اکنون همه ما از دید دولت مشکوک هستیم. این فناوری همیشه بین کاربران تمایز قائل نمی‌شود، زیرا کاربران نه بلکه عبارات خاصی را در ایمیل، پیام‌ها و جستجوگر های وب ما تماشا می‌کند و هنگامی که آنها را شناسایی می‌کند، به تیم‌های نظارتی هشدار می‌دهد و یا فورا ارتباطات اینترنتی ما را غیرفعال می‌نماید.

یکی از آخرین خطوط دفاعی برای حفظ حریم خصوصی آنلاین، رمزگذاری (encryption) است. این به ما امکان می دهد ارتباطات خود را رمزگذاری کنیم تا فقط گیرنده مورد نظر بتواند آنها را بخواند. حتی معماری اینترنت شامل لایه ای از رمزگذاری برای پشتیبانی از معاملات مالی ایمن است که به آن لایه سوکت های امن (SSL) می گویند[8] . این فناوری زمانی که برای ایمن سازی اطلاعات غیرمالی مورد استفاده قرار گرفت، در بسیاری از کشورها با انتقاد شدید مواجه شد. دولت ایالات متحده امریکا در ابتدا می خواست تمام رمزگذاری SSL را که پیچیدگی آنها بیشتر از توانایی رمزگشایی آنها بود غیرقانونی کند[9]. حالا، همه ایمیل های رمزگذاری شده احتمالاً برای بررسی بیشتر توسط یک سیستم نظارتی جهانی مانند ECHELON (یا هر سیستم دیگری) جمع آوری می شوند، فقط به این دلیل که در وهله اول رمزگذاری شده اند. بنابراین، هر تلاشی برای حفظ حریم خصوصی به عنوان تمایل به پنهان کردن چیزی تعبیر خواهد شد که دولت ها را ممکن نگران سازد.

فعالان و مدافعان حقوق بشر در کشورهای خودشان با تهدیدات خاصی روبرو هستند. فعالان حقوق بشر اغلب مورد نظارت و محدودیت بیشتری قرار می گیرند. توانایی آنها برای استفاده از حق آزادی بیان به طور منظم محدود می شود.

آنها اغلب برای ادامه کار خود با مجازات های شدید روبرو می شوند. برای آنها، عصر دیجیتال هم یک فرصت و هم یک چالش بوده است. از یک طرف، آنها با همکاران جهانی خود در ارتباط هستند و سرعت ارتباطات و گزارش های نقض حقوق بشر می تواند به سرعت انتشار پیدا کند. از اینترنت برای بسیج مردم استفاده می شود و بسیاری از ابتکارات اجتماعی به ویژه در جریان COVID-19 به صورت آنلاین تغییر کرده اند. علاوه بر این، خلاع و فقدان دیجیتالی و دسترسی به اینترنت بسیاری از فعالان و

[6] https://www.politico.com/news/magazine/2020/09/01/china-great-firewall-generation-405385
[7] https://basecreative.co.uk/
[8] https://www.ssl.com/faqs/faq-what-is-ssl/
[9] https://www.ssl.com/blogs/june-2020-security-roundup/

مدافعان کشورهای کمتر توسعه یافته را از مشارکت در گفت و گوهای جهانی و اطلاع رسانی باز داشته است. ناامنی دستگاه های تلفن هوشمند آنها هر روز افزایش می یابد.

ایمیل ها به دست دریافت کننده گان مورد نظر خود نمی رسند، صفحات رسانه های اجتماعی هک می شوند، اتصالات اینترنتی قطع و صل می شوند، ابزارهای ارتباطی رسانه های اجتماعی به شدت نظارت می شوند، مکالمات تلفنی شنیده می شوند، کامپیوترها توقیف می شوند و ویروس ها سال ها کار و دستاورد های ما را خراب می کنند. این مسائل معمولی و شناخته شده است. علاقه فزاینده مقامات به انتشار آنلاین یکی دیگر از اتفاقات مکرر است. وقتی محتوای «ناخواسته» از سوی یک فعال و یک مدافع حقوق بشر به نشر میرسد، مقامات به سرعت تلافی می کنند. آنها به طور فعال از طریق سایت های خبری آنلاین، صفحات رسانه های اجتماعی و وبلاگ ها جستجو گر موضوعات را دنبال می کنند.

طبقه بندی دیجیتال[10]، سرکوب تسهیل شده دیجیتالی، نقض حق دسترسی به انترنت به نام امنیت، آسیب پذیری سایبری سیستمی و ناامنی دیجیتال تنها معدود چالش هایی است که برای فعالان و مدافعان حقوق بشر در سراسر جهان وجود دارد.

فعالان و مدافعان حقوق بشر با آشنایی با کامپیوتر، تلفن های هوشمند و فعالیتهای اینترنتی، بهتر می توانند از کار خود محافظت کنند. بنابراین، آنها در دفاع از حقوق خود و پیشبرد حقوق دیگرانی که می خواهند به آنها کمک کنند، موفق تر خواهند بود.

نظارت دولت

دولت‌ها برای ردیابی فعالیت‌های آنلاین شهروندان خود روی تجهیزات پیشرفته سرمایه‌گذاری بیشتری می‌کنند. استفاده روزافزون دولت ها از نظارت بر رسانه‌های اجتماعی که سبب بازداشت کاربران به دلیل فعالیت قانونی آنلاین آنها از رسانه‌های اجتماعی شده، تهدید برای کاهش فضای فعالیت مدنی در پلتفرم‌های دیجیتال را نشان میدهد. بسیاری از دولت ها رفتار آنلاین شهروندان خود را توسط سرویس های اطلاعاتی نظارت می کنند. ارائه‌دهنده خدمات اینترنت شما (ISP) از همه کارهایی که به صورت آنلاین انجام می‌دهید محرمانه است ولی مقامات می‌توانند آنها را مجبور کنند تا اطلاعات شما رابه اختیار آنها بگذارند[11].

نظارت بر رسانه های اجتماعی چالش دیگری برای فعالان و مدافعان حقوق بشر است که مستلزم جمع‌آوری و مدیریت اطلاعات خصوصی بوده که از طریق ابزارهای ارتباطی آنلاین جمع‌آوری میشوند. این اطلاعات خصوصی اغلب از طریق استفاده از نرم‌افزار خودکار که امکان جمع‌آوری، مدیریت و تجزیه و تحلیل فوری حجم قابل‌توجهی از فرادیتا و محتوا را فراهم می‌کند، صورت میگیرد. نظارت بر رسانه‌های اجتماعی را نمی‌توان به‌عنوان مداخله بی اهمیت رد کرد، زیرا این نامطلوبتر از «spyware» ابزار جاسوسی انترنتی اند، که با تمرکز بر دستگاه‌های افراد خاص، مکالمات را رهگیری می‌کنند. این پلتفرم های دیجیتال توسط میلیاردها نفر در سراسر جهان برای ارتباط با دوستان و خانواده، تعامل با عزیزان و بیان عقاید سیاسی، اجتماعی و مذهبی مورد استفاده قرار میگیرند. اطلاعاتی که درباره کاربران این پلتفرم ها جمع‌آوری، ایجاد و استنباط می‌شود، حتی زمانی که به ندرت از آنها استفاده میکنند، برای تبلیغ‌کنندگان و همچنین به‌طور فزاینده‌ای برای مجریان قانون و مقامات اطلاعاتی ارزش زیادی دارند. دولت‌ها متخصصانی را برای نظارت بر گفتگوهای رسانه‌های اجتماعی برای مدت طولانی به کار گرفته‌اند، از جمله با راه‌اندازی حساب‌های جعلی برای برقراری ارتباط با کاربران واقعی و دسترسی به آنها. مقامات ایرانی درباره ارتش 42000 نفری خود که متشکل از داوطلبان که مراقب گفتگوهای آنلاین هستند، پرده برداشته اند. در سایت پولیس سایبری (FATA) هر شهروندی می تواند برای انجام این وظیفه سهیم شود. به همین ترتیب، چین صدها نفر را استخدام کرده است تا

[10] digital divide

[11] https://freedomhouse.org/report/freedom-on-the-net/2019/the-crisis-of-social-media/social-media-surveillance

از طریق اینترنت به این موضوع بپردازند و به مقامات در مورد هر گونه حساب یا محتوای مشکوک گزارش دهند. جاسوسان چینی فعالانه با شرکت های بزرگ همکاری می کنند تا مردم را به صورت آنلاین تحت نظر داشته باشند. حساب کاربری، ارتباطات و فایل های به اشتراک گذاشته شده توسط 364 میلیون کاربر رسانه های اجتماعی در چین در یک پایگاه دیتا های ناامن پیدا شد که توسط محققان امنیتی برای ردیابی این کاربران جهت معرفی آنها به مجریان قانون استفاده می‌شد. دولت چین از طریق مقررات مبهم شبکه های انترنتی به اطلاعات کاربران و ابردیتا های آنها دسترسی دارد که شناسایی و مجازات افرادی را که محتوای حساس منتشر می کنند را برای این مقامات آسان تر می کند[12].

افغانستان امروز، بسیار متفاوت تر از کشوری است که در سال 2001 اینترنت در آن غیرقانونی بود. دکل های تلفن هوشمند در سراسر کشور توسط دولت قبل ساخته شد، که ایالات متحده از آن حمایت میکرد. به نقل از شرکت تحقیقات بازار Statista، تعداد کاربران تلفن هوشمند از تنها یک میلیون در سال 2005 به بیش از 22 میلیون نفر در سال 2019 افزایش یافت. طبق گفته کارشناسان، 70 درصد از مردم به موبایل و تلفن هوشمند دسترسی دارند.

طالبان که قبلاً با غیرقانونی کردن اینترنت بر افغانستان حکومت می‌کردند، از رسانه‌های اجتماعی به عنوان سلاح قوی برای سرکوب مخالفان و انتشار دیدگاه‌های خود استفاده میکنند. حالا، آنها از هزاران حساب توییتر، برخی رسمی و برخی ناشناس دیدگاه های شان را منتشر مینمایند. آن‌ها نشان می‌دهند که جنگجویان شان در طول سال‌های جنگ، مهارت‌های تکنولوژیکی را به دست آورده‌اند و نگاهی اجمالی به چگونگی استفاده از این منابع برای کنترل افغانستان از خود نشان می‌دهند. برای حفظ امنیت شان، شهروندان، کاربران شبکه‌های اجتماعی تصاویر و پست‌های خود را حذف کرده اند و حتی حساب‌های خود را با پخش وحشت توسط طالبان بسته نموده اند. فیسبوک و توییتر هر دو متعهد شده اند که برای محافظت از حساب های کاربری اقدام کنند. حساب های رسانه های اجتماعی شرکت کنندگان در کمپین های ضد طالبان حذف شده است. بدون کمک های خارجی، طالبان امروز به سختی می توانند پیام های که از خارج وارد افغانستان میشود را محدود کنند، همانطور که چین و روسیه انجام می دهند[13].

بسیاری از افغان‌ها، به‌ویژه آن‌هایی موقعیت اجتماعی شان آنها را هدف طالبان قرار میدهد، با شروع بازجویی افراد، و بررسی تیلفونهای همراه شان و جستجوی خانه به خانه برای یافتن هرگونه سلاح، شروع به حذف یا ویرایش حساب‌های رسانه‌های اجتماعی و حضور آنلاین خود کردند. آنها این کار را به این دلیل انجام می دهند که می دانند طالبان روش نظارت خاص خود شان برای کانترول رسانه های اجتماعی پیروی می کنند تا قدرت شان را تقویت نمایند. در حالی که طالبان به استفاده از رسانه‌های اجتماعی برای کنترل و نظارت گفتگوها مشهور است، دولت قبلی تحت حمایت ایالات متحده با استراتژی‌های مشابهی دست به کار شده بود و هرازگاهی دستور تعطیلی برنامه‌های پیام‌رسانی مانند واتس‌اپ و تلگرام در کشور را می‌داد[14].

اکنون به عنوان یک فعال و مدافع حقوق بشر، اگر به طور مکرر از رسانه های اجتماعی استفاده می کنید، در کنفرانس ها صحبت می نمایید یا در مورد تعامل خود با نهاد های جامعه مدنی به صراحت حرف میزنید، ممکن است هدف نظارت دولت قرار بگیرید. این امر به ویژه در صورتی اتفاق می افتد که علناً خواستار اصلاحات شده، از حقوق بشر حمایت کرده باشید، یا از فساد اداری موجود و یا هم از نقض حقوق بشر پرده برداری نمایید. البته، نظارت هدفمند مستلزم این نیست که شما مرتکب جرم شده باشید. دولت‌ها از انواع ابزارهای پیچیده سایبری برای تجسس از افراد فعال از جمله روزنامه‌نگاران، محصلان و حتی خود مقامات دولتی استفاده می‌کنند. این عمل در همه جا اتفاق می افتد. مقامات برای دسترسی به دستگاه ها از طریق تکنیک های نظارت، بازیابی مخاطبین، یافتن رمز عبور، ردیابی پیام ها و تماس های تلفنی و مداخله در فعالیت فعالان شناخته شده دخیل بوده اند. دولت‌ها از دیتای جمع‌آوری‌شده از طریق روش‌های نظارتی برای بد جلوه دادن فعالان، به تصویر کشیدن آنها به عنوان مجرم و جعل اتهامات برای زندانی کردن آنها سوء استفاده کرده‌اند.

[12] https://freedomhouse.org/report/freedom-on-the-net/2019/the-crisis-of-social-media/social-media-surveillance
[13] https://www.nytimes.com/2021/08/20/technology/afghanistan-taliban-social-media.html
[14] https://www.mei.edu/publications/how-digital-rights-are-key-protecting-afghans-under-taliban

محافظت از اتصال اینترنت شما

از آنجایی که ارائه‌دهنده خدمات اینترنتی (ISP) شما ترافیک اینترنت شما را مدیریت می‌کند، می‌تواند تمام کارهایی را که به صورت آنلاین انجام می‌دهید پیگیری کند. ISP شما ممکن است بتواند فایل‌ها، ایمیل‌ها، رمزهای عبور، خریدهای آنلاین و حتی سوالاتی که از بلندگوی هوشمند خود می‌پرسید را مشاهده کند. بدتر از آن این است که ISP شما ممکن است اطلاعات کافی در مورد شما جمع آوری کند تا فعالیت های متعدد شما را شناسایی نموده، شاید به مجریان قانون در جمع آوری شواهد علیه شما کمک کند. ISP ها ادعا می کنند که اطلاعات شما را با کسی به اشتراک نمی گذارند. با این حال، ممکن است از آنها خواسته شود که اطلاعات شما را به مقامات دولتی و مجریان قانون تحویل دهند. به عنوان مثال، ISP ها در استرالیا موظف اند به پولیس فدرال اجازه دسترسی به دیتا های وبگردی کاربران را بدهند. برخی از این اطلاعات تا دو سال نگهداری می شوند.

برای اتصال امن، از یک شبکه خصوصی مجازی (VPN) استفاده کنید. در اینجا برخی از VPN ها دارای سابقه ضد سانسور هستند:

- TunnelBear: https://www.tunnelbear.com/download
- VPNGate: https://www.vpngate.net
- ProtonVPN: https://protonvpn.com
- Mullvad: https://mullvad.net/en/download/
- Bitmask: https://bitmask.net

در حال حاظر، بهترین گزینه برای شما این است که برای یک VPN قابل اعتماد جهت مبارزه با نفوذپذیری VPN های ISP بودیجه هزینه کنید و برای دسترسی به این VPN حق اشتراک بپردازید. سپس، وقتی آنلاین می‌شوید VPN یک اتصال خصوصی و امن به شما می‌دهد و به ناشناس کردن رفتار آنلاین شما کمک می‌کند. چندین لایه امنیتی توسط VPN ها استفاده می شود و راه اندازی آنها نسبتاً ساده است:

از رمزگذاری استفاده کنید

(Strong 256-AES) استاندارد رمزگذاری پیشرفته برای محافظت از اتصال شما با VPN های ممتاز استفاده می شود. این کار افراد فضول را از نظارت بر یا از تجسس در رفتار آنلاین شما باز می دارد. در نتیجه وبسایت هایی که بازدید می‌کنید و سرویس‌هایی که استفاده می‌کنید برای ISP یا سایر طرف‌های خارجی قابل مشاهده نخواهند بود[15].

یک VPN با شرایط بدون NO-LOGS انتخاب کنید

VPN را انتخاب کنید که به شدت به قانون عدم ورود به سیستم پایبند باشد تا نتواند هیچ یک از دیتا های کاربر شما را در سرورهای خود به شمول جریان مرور و جزئیات شخصی شما حفظ کند. اگر مامورین اطلاعات درباره شما چیزی بخواهند، VPN چیزی برای تحویل دادن به آنها نخواهد داشت[16].

[15] https://www.techtarget.com/searchsecurity/definition/Advanced-Encryption-Standard
[16] Please see: 3. protecting your internet connection

IP آدرس خود را پنهان کنید

هزاران سرور در سراسر جهان در VPN های بزرگتر قرار دارند. آدرس IP واقعی شما هنگام اتصال به IP VPN پنهان می شود. انجام این کار باعث می شود کسی نتواند فعالیت های آنلاین شما را به شما پیوند دهد[17].

ریسک VPN رایگان را نپذیرید

چندین VPN رایگان وجود دارد که ادعا می کنند از حریم خصوصی آنلاین و اطلاعات مهم شما محافظت می کنند. بسیاری از آنها دارای معایب و خطرات قابل توجهی هستند، مانند:

- محدودیت در میزان دیتا های قابل استفاده و تعداد دستگاه هایی که بتوانید از ردیاب های شخص ثالث در برنامه آنها محافظت کنید.
- گزینه های حداقل سرور.
- تاخیر اتصال به اینترنت هنگام استفاده ازVPN .
- موجودیت نرم افزارهای تبلیغاتی مزاحم و بدافزارهای مخفی.
- نمایش در تبلیغات پاپ آپ که ادعا می کنند دیتا های شما با اشخاص ثالث به اشتراک گذاشته شده است.

دور زدن سانسور آنلاین

اگر در کشوری با محدودیت‌های آنلاین شدید زندگی می‌کنید، احتمالاً نمی‌توانید به وبسایت‌های خبری، برنامه‌ها یا رسانه‌های اجتماعی خاصی دسترسی داشته باشید. با این حال، می‌توانید در کشورهایی که وبسایت‌ها و برنامه‌های خاصی با استفاده از VPN قابل اعتماد مسدود نشده‌اند، به سرورهای VPN متصل شوید. شما می توانید به محتوای محدود جغرافیایی و منابع خنثی کننده دسترسی داشته باشید و حتی با تغییر مکان دیجیتال خود، فعالیت خود را به صورت آنلاین با آنها هماهنگ کنید. بنابراین، عاقلانه است که تحقیق کنید کدام VPN در منطقه شما مؤثرتر است زیرا هر VPN نمی تواند به همه محتوای مسدود شده دسترسی داشته باشد.

امنیت را افزایش دهید

VPNهای Premium را می توان در محبوب ترین سیستم های عامل دسکتاپ و موبایل استفاده کرد. حتی تلویزیون های هوشمند، روترها[18] و چند ابزار مرتبط دیگر نیز می توانند از آنها استفاده کنند.

[17] https://www.expressvpn.com/go/what-is-my-ip/hide-my-ip-1?category=DSA&subcategory=All&lang=en&gclid=Cj0KCQjw08aYBhDlARIsAA_gb0fTCTXscDgpdFV8XemQ8uB2NtWkbDmoNe4WDZ5CzEs9EekoMhkdolYaAsN3EALw_wcB

[18] Routers

دسترسی به اینترنت به صورت ناشناس با استفاده از شبکه TOR

یک رویکرد فوق العاده برای فعالان جهت دسترسی امن و ناشناس به اینترنت، از طریق Tor (The Onion Router) [19] است. تمام فعالیت‌ها و دیتاهای اینترنتی شما در حین اتصال به شبکه Tor چندین بار رمزگذاری می‌شوند و شناسایی شما از هر یک از آن‌ها غیرممکن می‌شود.

برای به حداکثر رساندن حریم خصوصی و حفاظت از آن، توصیه می کنیم VPN را با Tor ترکیب کنید. قبل از اتصال بهTor ، باید به یک VPN از طریق TOR متصل شوید. با انجام این کار، گره Tor نمی تواند آدرس IP شما را ببیند و شما از تمام حفاظت های حریم خصوصی ارائه شده توسط شبکه Tor بهره مند خواهید شد. استفاده از VPN از طریق Tor دارای مزایای دیگری نیز است.

شبکه اینترنت خانگی شما به دلیل ترافیک رمزگذاری شده VPN شما نمی تواند تشخیص دهد که از Tor استفاده می کنید. در مکان‌هایی که Tor محدود است، یک VPN می‌تواند به شما امکان دسترسی به شبکه را بدهد. هنگام استفاده از شبکه Tor ممکن نیست توسط VPN خود ردیابی شوید. VPN شما یک درجه امنیتی اضافی بین شما و هر اشکالی که ممکن است در مرورگر Tor وجود داشته باشد اضافه کند.

از وای WiFI عمومی به صورت امن استفاده کنید

ترافیکی که از طریق یک شبکه WiFi باز عبور می کند، معمولاً امن نیست، و آن را به یک هدف آشکار برای جاسوسان آنلاین تبدیل می کند. این امر استفاده از وای فای عمومی را مخاطره آمیز می سازد. اگر مجبور هستید در یک شبکه اینترنتی عمومی یا همان WiFi عمومی در فعالیت‌های مرتبط حقوق بشری شرکت کنید، بسیار مهم است که اقدامات احتیاطی ذیل را انجام دهید.

- دیتا های خود را با استفاده از VPN رمزگذاری کنید تا فعالیت اینترنت شما غیرقابل نفوذ باشد و ردیابی آن غیرممکن شود.
- فقط از وب سایت های دارای امنیت HTTPS دیدن کنید.
- اگر از کامپیوتر عمومی استفاده می کنید، مطمئن شوید که از همه حساب های کاربری خود خارج شده باشید.
- فایروال خود را برای دفاع بیشتر از ویروس روشن نگه دارید.
- از یک روتر قابل حمل شخصی برای مدیریت اتصال شبکه خود استفاده کنید.
- هرگز به شبکه های غیر قابل اعتماد نپیوندید.
- بدون محافظت از رمز عبور به شبکه نپیوندید.
- اتصال Wi-Fi خودکار را برای دستگاه های خود فعال نکنید.
- در صورت عدم استفاده، هرگز Bluetooth یا WiFi خود را متصل نگه ندارید.
- با استفاده از Wi-Fi عمومی، اطلاعات یا اسناد خصوصی را ارسال یا آپلود نکنید.

[19] https://www.vpn-mentors.com/best-vpn-for-tor/?keyword=tor%20network&geo=9000786&device=&cq_src=google_ads&cq_cmp=10810894927&cq_term=tor%20network&cq_plac=&cq_net=g&cq_plt=gp&gclid=Cj0KCQjw08aYBhDlARIsAA_gb0dJGmeR8Q3oUBfjrPFFXETlP7Y_LVDmhi7yzJanyxrLAK7gKNviMjAaAkI6EALw_wcB

محافظت از کامپیوتر شما

اطلاعات خصوصی هنگفت و ارزشمند در کامپیوتر شما وجود دارد. احتمالاً شما هر روز از انواع کامپیوترها از جمله لپ‌تاپ، تبلت، تلفن هوشمند، دسکتاپ خانه و دسکتاپ اداره استفاده می‌کنید. اطلاعات بانکی، ایمیل‌ها، فایل‌ها، تصاویر، ویدیوها و سایر ارتباطات دیجیتال شما در این دستگاه‌ها ذخیره می‌شوند. اولین قدم برای محافظت از همه دستگاه‌ها و دیتاهای آنلاین، امنیت کامپیوتر شخصی شما است.

اکثر فعالان کامپیوترهای دارند که سیستم عامل آنها مایکروسافت ویندوز است. پرکاربردترین نسخه ها ویندوز 11[20]، 10[21] و 7[22] هستند. کامپیوتر شما باید یک سیستم عامل امن داشته باشد تا از حملات آنلاین محافظت شود. در جستجوی کامپیوترهای شخصی آسیب‌پذیر که فاقد ارتقاء امنیتی خاص هستند، هزاران هکر به طور مداوم آدرس‌های IP را بررسی می‌کنند. به‌روزرسانی‌های امنیتی هفتگی باید روی همه نسخه‌های ویندوز نصب شوند، حتی اگر رایانه کاملاً نو باشد. اگر اجازه دهید، اکثر نسخه های ویندوز، این به روزرسانی ها را به صورت خودکار انجام می دهند.

فعالان برای بررسی ایمیل‌های خود، اجرای کمپین‌ها، پیوستن به جنبش‌های خارج از محدوده جغرافیایی شان، پیوستن به جلسات آنلاین، مطالعه آنلاین، شرکت در رسانه‌های اجتماعی، و انجام سایر فعالیتهای حیاتی – علیرغم وجود نظارت مقامات دولتی و هکرهای اینترنتی، به اینترنت متکی هستند. با این حال، حتی در سازمان‌های بزرگ با نهادهای امنیتی پیشرفته، ما اغلب در مورد نفوذ کامپیوتری قابل توجهی مواجه هستیم. از دستورالعمل های استاندارد زیر برای محافظت از کامپیوتر ها و اطلاعات حساس موجود در آنها استفاده کنید:

فایروال را فعال کنید

قبل از دسترسی به اینترنت فایروال را فعال کنید. فایروال به عنوان دیواری بین شبکه شما و دنیای بیرون عمل می کند و امنیت اولیه را فراهم می نماید. گاهی اوقات فایروال یک سرور مستقل است، گاهی اوقات یک روتر است و گاهی اوقات یک نرم افزار کامپیوتری است. فایروال، به هر شکل که باشد، ترافیک شبکه ورودی و خروجی از سیستم را کنترل می کند. در متابعت با فایروال، یک سرور پروکسی اغلب برای پوشاندن آدرس IP شبکه داخلی از نمایش یک آدرس IP واحد برای افراد خارجی استفاده می نماید. محیط توسط فایروال ها و سرورهای پراکسی محافظت می شود که ترافیک را تجزیه و تحلیل می کنند و مانع رفتن آن به جایی می شوند که توسط administrator ممنوع شده است. یک سیستم تشخیص نفوذ (IDS) اغلب برای تکمیل این دو اقدام امنیتی استفاده می شود. یک IDS صرفاً ترافیک را ردیابی می کند و هر گونه فعالیت غیرمعمولی را که نشان دهنده تلاش برای نقض باشد پیگیری می کند.

انتی وایروس نصب کنید

[20] https://www.microsoft.com/en-ca/software-download/windows11
[21] https://www.microsoft.com/en-ca/windows/get-windows-10
[22] https://www.microsoft.com/en-ca/software-download/

برنامه های انتی وایروس متعددی برای کامپیوتر های شخصی مبتنی بر ویندوز در دسترس قرار دارند. کامپیوتر شما از نرم افزارهای مخرب و کدهای غیرمجاز توسط برنامه های آنتی ویروس مانند Avast ، Bitdefender، Panda Free Antivirus و Malwarebytes محافظت می شود. بدافزارها و ویروس های کامپیوتری فراگیر هستند. ویروس‌ها ممکن است دلیل اصلی کندی کامپیوتر شما یا پاک کردن فایل‌های مهم باشند، و ممکن است کمتر خود شان را نشان بدهند. نرم افزار آنتی ویروس هر فعالیتی را کنترل می کند و به طور مداوم در جریان است. هر باری که شما به فایلی در اینترنت دسترسی پیدا می کنید، انتی وایروس ها به فعالیت شان میپردازند و اعمال می شوند. همه فایل های جدید توسط این نرم افزار ها اسکن می شوند و هر فایلی را که مشکوک بدانند فورا قرنطینه می کنند. معمولاً پس از آن از شما خواسته می شود تا اقدام کنید. هنگام نصب و فعال سازی برنامه انتی ویروس خود، دو گام بسیار مهم وجود دارد که باید در نظر گرفته شود. اولین گام این است که تأیید کنید که به روز رسانی انتی ویروس شما اعمال می شود. تنها به این اطمینان نداشته باشید که یک محصول انتی ویروس روی کامپویتر شما نصب شده است، باید به صورت دایمی به روز رسانی شود. دومین گام مهم این است که اگر بیش از یک برنامه انتی ویروس نصب کرده باشید، آنها برای کنترل کامپیوتر شما با یکدیگر رقابت خواهند کرد و کامپیوتر شما از فعالیت باز بماند. بنابر این از یک انتی ویروس همیش استفاد کنید. می توانید 10 انتی ویروس برتر سال 2022 را در اینجا پیدا کنید:

https://www.antivirussoftwareguide.com/best-windows-antivirus

نرم افزار ضد تجسس را نصب کنید

نرم افزار تجسسی نوعی نرم افزار خاص است که به طور مخفیانه دیتای افراد یا موسسات را دریافته و جمع آوری می کند. برخی از نرم افزارهای تجسسی هر کلیک را به منظور دسترسی به رمزهای عبور و سایر دیتا های مالی حساس ثبت می کنند. تمام فعالیت های کامپیوتری ممکن توسط برنامه های تجسسی نظارت شوند و اشخاص ثالث می توانند به روش های مختلف به این دیتا دسترسی داشته باشند. معمولی ترین تکنیک از تروژنها استفاده می کنند. علاوه بر این، اگر به سادگی در حال مرور یک وبسایت خاص هستید، ممکن است بدافزار در پس زمینه شروع به دانلود کند.

همانطور که برنامه‌های تجسسی معدودی طراحی شده اند، خوشبختانه، برنامه‌های نرم‌افزاری متعددی هم وجود دارند که برای یافتن و از بین بردن نرم‌افزارهای تجسسی در نظر گرفته شده‌اند. اگرچه نرم افزار ضد تجسس فقط در مقابل این تهدید ساخته شده است، اما اغلب در بسته‌های انتی ویروس شرکت‌هایی مانند Webroot ، McAfeeو Norton گنجانیده شده اند. امنیت آنی توسط محصولات ضد تجسس ارائه می شود که تمام دیتای دریافتی را بررسی کرده و تهدیدات را متوقف می نمایند. علاوه بر این، این برنامه ها از لحاظ مالی قابل استطاعت هستند. بهترین اقدامی که می توانید برای جلوگیری از آلوده شدن نرم افزارهای تجسسی به کامپیوتر خود انجام دهید این است که هرگز چیزی را از اینترنت دانلود نکنید که از یک وبسایت بسیار معتبر و قابل اعتماد نباشد. اکثر برنامه های انتی ویروس فعلی یا به صورت استاندارد با افزار آنتی جاسوسی عرضه می شوند یا آن را به عنوان یک افزونه اختیاری ارائه می دهند. می توانید 10 انتی وایروس برتر را از جمله افزار ضد تجسس برای سال 2022 را در اینجا پیدا کنید:

https://www.antivirussoftwareguide.com/best-windows-antivirus

از رمز عبور پیچیده استفاده کنید

استفاده مؤثر از کامپیوتر مستلزم استفاده از یک رمز عبور قوی میباشد. یک رمز عبور قوی مهمترین بخش هر سیستم در امنیت دیجیتال است. رایج ترین روشی که هکرها و مهاجمان سیستم های اطلاعاتی شما را هدف قرار می دهند، از طریق

شکستن رمز عبور است. برای حل این معضله میتوانید از برنامه های مدیریت رمز عبور مانند Dashlane[23] ، Sticky Password[24]، LastPass[25] یا Password Boss[26] استفاده کنید. در کامپیوتر تان رمز عبور قوی داشته باشید، اما برای حفظ امنیت اطلاعات خود به رمز عبور ویندوز وابسته نباشید. آنها به سرعت نابود می شوند. به جای استفاده از یک رمز عبور کوتاه و واضح، ترجیحاً رمز عبور خود را یادداشت کرده و در یک جای امن ذخیره کنید. هر بار از یک رمز عبور متفاوت استفاده کنید و خود تان را مطمین سازید که رمز عبوری تان هیچ ارتباطی به علایق شخصی و زندگی خصوصی تان ندارد یعنی از واژه ها و اعداد که بیانگر اسامی اعضای فامیل و یا تاریخ تولد است صرف نظر کنید. هرگز رمز عبور خود را برای کسی فاش نکنید. هر سه تا شش ماه یکبار رمز عبور خود را تغییر دهید. به خاطر داشته باشید که انواع ابزارهای آنلاین رایگان وجود دارد که شما را در ایجاد یک رمز عبور قوی برای ویندوز، شبکه بی سیم و حتی کامپیوتر تان کمک میکنند.

سیستم عامل، اپلیکیشن ها و مرورگر خود را به روز کنید

ارتقاء (upgrade) سیستم عامل و نرم افزار انتی وایروس شما چندان دشوار نیست. این ویژگی(feature) قبلاً به طور پیش فرض در محصولات فعلی فعال شده و وجود دارد. با این حال، ممکن است برخی از برنامه های نرم افزاری که روی کامپیوتر خود قرار داده اید، به روز رسانی امنیتی دریافت نکنند. مرورگرهای وب (Web browsers)، جاوا [27] (Java)، Adobe Reader[28] و بسیاری از برنامه های دیگر در این ردیف قرار می گیرند. به روز رسانی این برنامه ها ضروری است. شاید قبلاً متوجه شده باشید که Adobe Reader هر بار که یک فایل PDF را باز می کنید از شما می خواهد که برنامه را به روز کنید. برخی به روز رسانی ها نواقصی را برطرف می کنند که امکان حمله نرم افزارهای مخرب به این برنامه ها را فراهم می کند.

هر بار به‌روزرسانی جدید سیستم عامل کامپیوتر و محصولات دیگری را که در اختیار دارید اجرا کنید. اکثریت به‌روزرسانی‌ها دارای وصله‌های (pacthes) امنیتی هستند که هکرها را از دسترسی به دیتای شما باز می‌دارد. اپلیکیشن ها تفاوتی ندارند. مرورگرهای وب امروزی به ویژه از نظر حریم خصوصی و امنیت هوشمندتر شده اند. علاوه بر انجام تمام به روز رسانی های جدید، به یاد داشته باشید که تنظیمات امنیتی مرورگر خود را بررسی کنید. به عنوان مثال، می توانید حریم خصوصی آنلاین خود را با استفاده از مرورگر خود افزایش دهید تا وبسایت ها از ردیابی حرکات شما جلوگیری کنند. از طرف دیگر، از یکی از مرورگرهای وب امن استفاده کنید.

اسپم[29] ها را نادیده بگیرید

اکثر خوانندگان احتمالاً نام اسپم را شنیده اند. اسپم یک ایمیل ناخواسته و نامطلوب است که بین چندین دریافت کننده ایمیل توزیع می شود. اگرچه اغلب برای اهداف بازاریابی مورد استفاده قرار می گیرند، اما همچنین می تواند برای اهداف نامناسبتر نیز از آنها سوء استفاده شود. به عنوان مثال، اسپم یک روش معمولی برای انتشار ویروس یا (worm) است. مخربان از آنها به منظور سرقت هویت دریافت کننده ایمیل استفاده می نمایند. اسپم همچنین برای ارسال ایمیل هایی استفاده می شود که افراد دریافت کننده ایمیل را وسوسه می کند تا از وب سایت های فیشینگ (phishing) بازدید کنند. در اصل، اسپم در بهترین حالت یک مزاحم و در بدترین حالت یک روش دریافت بدافزارها (در کامپیوتر دریافت کننده ایمیل) از جمله نرم‌افزارهای تجسسی، وایروس‌ها، کرم‌ها و حملات فیشینگ است. بنابراین، هنگام باز کردن پیوست‌ها یا کلیک کردن روی پیوندها در ایمیل‌های

[23] https://www.dashlane.com
[24] https://www.stickypassword.com
[25] https://www.lastpass.com/features/password-generator
[26] https://www.passwordboss.com
[27] https://www.java.com/en/
[28] https://www.adobe.com
[29] https://www.malwarebytes.com/spam

شخصی که نمی‌شناسید، هوشیار باشید. فیلترهای جعبه ورودی ایمیل شما اسپم در خود جا داده و شما را کمک میشوند تا از خطر کلیک کردن به صورت ناخودآگاه مصون باشید. با این حال، ایمیل‌های فیشینگ پیچیده‌تر که جعل هویت دوستان، همکاران و موسسات قابل اعتماد شما (مانند بانک) هستند، محبوبیت زیادی پیدا کرده‌اند، بنابراین در مورد هر چیزی که مشکوک به نظر می‌رسد هوشیار باشید.

از کامپیوتر خود پشتوانه (backup) داشته باشید

در صورتی که هکرها موفق به نفوذ به سیستم کامپیوتر شما شده و اطلاعات دیتای شما از بین برود، داشتن یک نسخه پشتیبان یا همان بکاپ ضروری است. همیشه مطمئن شوید که در صورت از دست دادن اطلاعات و دیتای تان بعد از یک حادثه، می توانید آنها را با بیشترین سرعت ممکن بازیابی کنید. این عملیه را میتوانید با برنامه های بک اپ گیری با Windows File History[30] و macOS Time Machine[31] شروع کنید. این ابزارهای کمکی همچنین می توانند با ظرفیت کافی روی یک هارد دیسک بک اپ بیرونی (external hard disk) به طور موثر استفاده شوند.

در بین افراد، این فرضیه که "هیچ اتفاق نمی افتد" اغلب بر لزوم دید تهیه نسخه بک اپ از محتویات کامپیوتر اولویت دارد. برای جلوگیری از فراموشی، از دست دادن یا آسیب رسیدن به اطلاعات و دیتا، هم روی خود و هم بر فناوری باید حساب کنیم و از آنها باید استفاده کرد.

به نوعیت، حجم و تعداد دفعات بک اپ گیری اطلاعات و دیتای خود تمرکز داشته، می‌توانید یک کپی از تمام دیتا و اسناد خود را در iCloud[32] و Dropbox[33] داشته باشید، اما ممکن است بخواهید از یک USB همراه برای داشتن کاپی دیتای تان استفاده نمایید. یک کامپیوتر سرور در موسسه ای که آنجا کار میکنید علاوه بر اسنادی که کاربران در آن نگهداری می کنند، به بک اپ گیری منظم از نرم افزار هاَ اطلاعات و دیتای شما کمک میکند.

کامپیوتر خود را بعد از استفاده خاموش کنید

بسیاری از موسسات به‌ویژه نهادهایی که سرورهای وب دارند از «all systems go » ، استفاده مینمایند. با این حال، اگر از یک نهاد پیچیده مبتنی بر اینترنت استفاده نمی کنید، کامپیوتر خود را در شب یا برای مدت طولانی در حالی که از آن استفاده نمی کنید خاموش کنید. خاموش کردن کامپیوتر شما، هر گونه ارتباطی را که ممکن است هکر با شبکه شما ایجاد کرده باشد، از بین ببرد و از بروز هرگونه آسیب احتمالی جلوگیری کند، زیرا روشن ماندن رایانه شما آن را آشکارتر و هدفی برای هکرها قرار دهد.

شبکه خود را امنیت ببخشید

اکثر روترها با بالاترین سطوح امنیتی فعال حمل نمی شوند. هنگام پیکربندی[34] شبکه خود، به روتر دسترسی پیدا کنید و با استفاده از راه اندازی رمزگذاری شده و ایمن، رمز عبور را وارد کنید. این مانع از دسترسی هکرها به شبکه شما و تغییر تنظیمات آن می شود.

[30] https://support.microsoft.com/en-us/windows/file-history-in-windows-5de0e203-ebae-05ab-db85-d5aa0a199255
[31] https://support.apple.com/en-ca/guide/mac-help/mh35860/mac
[32] https://www.dropbox.com
[33] https://support.apple.com/en-ca/guide/mac-help/mh35860/mac
[34] configuring

از احراز هویت دو مرحله‌ای (TWO-FACTOR AUTHENTICATION) استفاده نمایید

خط دفاعی اصلی شما در برابر هکرهای کامپیوتری رمز عبور است، اما افزودن یک لایه دیگر امنیت را افزایش می دهد. بسیاری از وب‌سایت‌ها به شما اجازه می‌دهند تا احراز هویت دو مرحله‌ای را فعال کنید، که با نیاز به ارائه کد عددی علاوه بر رمز عبور هنگام ورود، امنیت را افزایش می‌دهد. این کد به تلفن یا آدرس ایمیل شما ارسال می شود و شما بعد از ورد آن میتوانید به حساب تان دسترسی داشته باشید.

از رمزگذاری (Encryption) میتوانید استفاده کنید

رمزگذاری می تواند مانع دسترسی هکرها به دیتای شما شود، حتی اگر آنها بتوانند به شبکه و فایل های شما دسترسی پیدا کنند. می توانید هر درایو فلش USB را که حاوی اطلاعات حساس است رمزگذاری کنید، هارد ویندوز یا macOS خود را با[35] (BitLocker) ویندوز یا [36] (FileVault) Mac رمزگذاری کنید و از VPN برای ایمن سازی ترافیک وب استفاده نمایید. فقط از وب سایت های امن خرید کنید. همچنان شما می‌توانید با«HTTPS» فرق بین وب ها را تشخیص دهید.

محافظت از تلفن های هوشمند

استفاده از دستگاه های تلفن هوشمند به عوض کامپیوتر روزانه افزایش می یابد. تهدیدات دیجتالی در مقابل امنیت دستگاه های تلفن هوشمند در حال افزایش است. در بیش از 1 میلیون دستگاه کاربر، Kaspersky حدود 3.5 میلیون قطعه بدافزار[37] را در سال 2014 کشف کرد. الگوریتم‌های تشخیص آزمایشگاهی Kaspersky روزانه 360000 فایل مخرب را تا پایان سال 2017 پردازش می‌کردند. علاوه بر این، 78 درصد از این فایل‌ها برنامه‌های بدافزار بودند. نرخ شناسایی روزانه بیش از 280000 فایل بدافزار، که بسیاری از آنها برای دستگاه های تلفن هوشمند هدف قرار می گیرند. در اینجا برخی از تهدیدات دستگاه تلفن هوشمند و پیش بینی ها برای آینده ارایه می شود[38].

Wi-Fi نا امن

وقتی هات اسپات های Wi-Fi رایگان در دسترس هستند، هیچ کس نمی خواهد از Cellular Data تلفن هوشمند خود استفاده کند، اما شبکه های Wi-Fi رایگان اغلب ناامن هستند[39]. سه سیاستمدار بریتانیایی که به شرکت در یک آزمایش امنیتی رایگان Wi-Fi رضایت دادند، به آسانی توسط متخصصان سایبری در معرض خطر قرار گرفتند. چت های VoIP، معاملات PayPal و حساب های رسانه های اجتماعی آنها همگی در معرض خطر و هک قرار گرفتند. برای استفاده از Wi-Fi رایگان در دستگاه تلفن هوشمند خود دقت کنید و به صورت امن از آن استفاده نمایید. علاوه بر این، هرگز از آن برای دسترسی به خدمات خصوصی یا محرمانه مانند جزئیات بانکی یا کارت اعتباری استفاده نکنید[40].

[35] https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview
[36] https://support.apple.com/en-ca/HT204837
[37] malware
[38] https://www.kaspersky.com
[39] https://whatismyipaddress.com/unsecured-network-2
[40] https://securityaffairs.co/wordpress/38510/cyber-crime/3-uk-politicians-hacked-wifi.html

شبکه های جعلی (Spoofing Networks)

در فضای عمومی پرترافیک اینترنت مانند کافی شاپ ها و فرودگاه ها، هکرها اسپات های جعلی دسترسی به انترنت را ایجاد می کنند - اتصالاتی که به نظر می رسد شبکه های Wi-Fi هستند اما دام هستند. برای تشویق مردم به اتصال اینترنت، مجرمان سایبری به این اسپات های دسترسی به انترنت نام‌های آشنا مانند «Free Airport Wi-F » یا «Coffeehouse » می‌دهند. حتی مهاجمان اینترنتی برای دسترسی به این خدمات رایگان اینترنتی کاربران را ملزم میدانند تا ثبت نام نموده و ایمل، شماره تماس و اسم کامل خود را در سیستم وارد نمایند. هکرها می توانند به ایمیل کاربران دسترسی یابند، و از معاملات الکترونیک و سایر اطلاعات آنها سوء استفاده نمایند زیرا بسیاری از کاربران از ترکیب ایمیل و رمز عبور یکسان برای چندین حساب استفاده می کنند. در هنگام اتصال به Wi-Fi رایگان، علاوه بر این که محتاط باشید ، هرگز اطلاعات شخصی خود را اوارد نکنید. و همیشه هر زمان که از شما خواسته شد یک رمز عبور خاص ایجاد کنید، خواه برای Wi-Fi یا هر برنامه دیگری باشد نباید از رمز عبوری یکسان در همه حسابها استفاده نمایید[41]. برای اطلاعات بیشتر در این مورد، لطفا مراجعه کنید به:

https://www.techtarget.com/searchsecurity/definition/IP-spoofing

حملات فیشینگ (Phishing)

دستگاه های تلفن هوشمند هدف اکثریت حملات فیشینگ قرار میگیرند چون این دستگاه ها دائما روشن هستند. از آنجایی که کاربران اغلب ایمیل خود را به محض دریافت چک می کنند، با خواندن و باز کردن ایمیل ها، این دستگاها بیشتر در معرض دید هکر ها قرار می گیرند. همچنان به دلیل اندازه کوچک صفحه نمایش، برنامه های ایمیل در این دستگاه ها اطلاعات کمتری را نشان می دهند و این سبب میشود که کاربران را آسیب پذیرتر کند مگر اینکه نوار اطلاعات[42] را گسترش دهید. یک ایمیل ممکن است فقط نام فرستنده را پس از باز شدن نشان دهد. با این حال، هرگز روی پیوندهای[43] ایمیل‌هایی که نمی‌شناسید کلیک نکنید. اگر موضوع عاجل نیست، بگذارید هر وقت دسترسی به کامپیوتر تان داشتید به آن ایمل پاسخ دهید. در اینجا اطلاعات بیشتری در مورد حملات فیشینگ و نحوه جلوگیری از آنها وجود دارد:

https://www.tripwire.com/state-of-security/security-awareness/6-common-phishing-attacks-and-how-to-protect-against-them/

نرم افزارهای تجسسی (Spyware)

اگرچه بسیاری از کاربران دستگاه تلفن هوشمند نگران ارسال بدافزار[44] مرتبط به هکرها هستند، ولی نرم افزارهای تجسسی تهدید جدی تری به حاسب میایند. کاربران این دستگاه ها باید اغلب نگران نرم افزارهای تجسسی باشند که توسط شرکا، همکاران یا کارفرمایان که می خواهند بر حرکات و رفتار آنها نظارت داشته باشند کارگذاری میشود نه بدافزار های مهاجم ناشناس. بسیاری از این برنامه ها که اغلب به آنها استالکر[45] نیز می گویند، برای نصب روی دستگاه تلفن هوشمند بدون اطلاع یا رضایت کاربران نصب میشوند. این نوع برنامه ها به دلیل نحوه ورود آن ها به دستگاه شما و هدفی که دنبال میکنند، متفاوتتر از سایر بدافزارها

[41] https://www.techtarget.com/searchsecurity/definition/IP-spoofing
[42] Header
[43] Links
[44] Malware
[45] Stalkers

هستند. بنابراین از یک مجموعه کامل آنتی ویروس جهت شناسایی این نرم افزار های تجسسی باید استفاده صورت گیرد. برای اطلاعات بیشتر لطفا مراجعه کنید به:

https://www.malwarebytes.com/spyware

رمز نگاری شکسته (BROKEN CRYPTOGRAPHY)

هنگامی که انکشاف دهندگان اپلیکیشن ها از تکنیک های رمزگذاری ناکارآمد استفاده می کنند یا از رمزگذاری قوی به صورت نا مناسب و اشتباه استفاده می کنند، ممکن رمزنگاری شکسته شود. برای تسریع روند توسعه اپلیکیشن ها در سناریوی اول، انکشاف دهندگان ممکن است علیرغم نقص های امنیتی تأیید شده خود، از تکنیک های رمزگذاری شناخته شده استفاده کنند. به همین دلیل، هر مهاجم می تواند از معایب آن برای شکستن رمز عبور و دسترسی به آن استفاده کند. در مورد دوم، انکشاف دهندگان از الگوریتم های بسیار امن استفاده می کنند اما دروازه های پشتی[46] اضافی را در دسترس قرار می دهند که کارایی آنها را کاهش می دهد. به عنوان مثال، هکرها ممکن است نتوانند رمزهای عبور را حدس بزنند، اما اگر انکشاف دهندگان اشکالاتی را در کد معرفی کنند که این اشکالات ممکن به مهاجمان اجازه دهد ویژگی‌های سطح بالای اپلیکیشن را تغییر دهند - مانند ارسال یا دریافت پیام - ممکن است حتی برای ایجاد مشکل به رمز عبور نیاز نداشته باشند. قبل از انتشار اپلیکیشن ها، مسئولیت اجرای معیار های رمزگذاری بر عهده شرکت ها و انکشاف دهندگان این اپلیکیشن ها است. برای اطلاعات بیشتر لطفا مراجعه کنید به:

https://knowledge-base.secureflag.com/vulnerabilities/broken_cryptography/broken_cryptography_category.html

مدیریت فعالیت نادرست

بسیاری از اپلیکیشن ها از «Token» استفاده می‌کنند که به کاربران امکان این را می‌دهد تا فعالیت های شان را، بدون نیاز به احراز مجدد هویت جهت پشتیبانی از دسترسی آسان به معاملات مالی، انجام دهند. توکن‌ها توسط اپلیکیشن ها برای شناسایی و اعتبارسنجی دستگاه‌ها ایجاد می‌شوند، درست مانند یک رمز عبور. برای هر بار ورد، اپلیکیشن های ایمن توکن های جدیدی ایجاد می کنند که باید خصوصی نگه داشته شوند. ادعای هم صورت میگیرد که مدیریت نامناسب ورود به اپلیکیشن زمانی اتفاق می‌افتد که این اپولیکیشن ها به طور ناخواسته توکن‌های ورودی را به اشتراک بگذارند، مثلاً توکنها را با افراد مخرب که می‌توانند به عنوان کاربران واقعی با آنها ظاهر شوند شریک سازد. این اغلب در نتیجه ورودی اتفاق می افتد که پس از خروج کاربر، اپلیکیشن یا وبسایت هنوز فعال باشد. به عنوان مثال، اگر شما ازکامپیوتر خود وارد یک سایت اینترنت محل کار شوید و فراموش کرده باشید که پس از اتمام کار از سیستم خارج شوید، یک مخرب سایبری ممکن دسترسی نامحدودی به وبسایت و سایر شبکه کاری شما پیدا کند[47].

در آینده چه تهدیداتی در مقابل امنیت تلفن های هوشمند وجود خواهد داشت؟

با وجود تبدیل شدن تلفن های هوشمند به یک هدف مهم برای هکرها، امنیت آنها مانند امنیت شبکه های اینترنتی و کامپوتر شخصی اولویت ندارد. بر اساس تحلیل دانشگاه هاروارد، حتی در داخل اکوسیستم تلفن های هوشمند، توجه کمتری به امنیت آنها در مقایسه با انکشاف اپلیکیشن ها صورت گرفته است. با افزایش وابستگی به دستگاه های تلفن هوشمند، ارزش دیتا نیز

[46] back doors

[47] https://owasp.org/www-project-mobile-top-10/2014-risks/m9-improper-session-handling

افزایش می یابد که به هکرها انگیزه بیشتری می دهد. علاوه بر خطرات متذکره امنیتی تلفن هوشمند که ما در مورد آن صحبت کردیم، مراقب تهدیدهای بیشتری هم باشید که موارد ذیل اند[48]:

SMiShing:[49] مجرمان سایبری ازSMiShing ، تکنیکی شبیه به کلاهبرداری فیشینگ، استفاده می کنند تا کاربران را به دانلود بدافزار ها، کلیک بر روی لینک های مضر یا افشای اطلاعات شخصی وادار نمایند. به عوض ایمیل، یک حمله SMiShing از طریق متنهای ارسالی راه اندازی می شود.

BYOD:[50] دسترسی سطح بالای کارمندان شرکت های خصوصی به دستگاه های تلفن هوشمند شخصی سبب میشود که آنها، اساساً جای کامپیوتر ها را در انجام معاملات بگیرند. ولی این دستگاه ها امنیت یکپارچه و قوی را که کامپیوتر های شرکت دارد، ندارند که ممکن هدف حملات متعددی قرار گیرند.

اینترنت اشیا[51](IoT) : از آنجایی که انواع دستگاه‌های هوشمند به سرعت در حال گسترش هستند، از تراشه‌های RFID گرفته تا ترموستات‌ها و حتی لوازم خانگی، ما نمی‌توانیم هر لحظه کاربران یا برنامه‌های انتی‌وایروس را زیر نظر داشته باشیم. بنابر این باید گفت که دستگاه های IoT هدف مطلوبی برای هکرهایی هستند که از آنها به عنوان مسیر ورود به شبکه های بزرگتر استفاده می کنند[52].

محافظت از رمز عبور (Password)[53]

رمز عبور شما رایج ترین روشی است که یک هکر کامپیوتر از آن برای آسیب رساندن به دیتای شما استفاده می کند. شرکت‌های آنلاین اغلب از ما می‌خواهند که اطلاعات ورود خود را به‌روزرسانی کرده و رمزعبوری را انتخاب کنیم که از معیارهای امنیتی شدید برخوردار باشد. هنگامی که رمز عبور شما بسیار کوتاه و فاقد یک کاراکتر خاص، یک عدد و یک حرف بزرگ است، ممکن است زیاد شکننده باشد. اگرچه رعایت معیار های امنیتی ناخوشایند است، اما برای محافظت از دیتای شما حتمی و حیاتی است. قبل از ارائه پاسخ ساده به این نیازها، باید اهمیت رمز عبور امن را درک کرد. هنگام ایجاد یک رمز عبور موارد ذیل را در نظر بگیرید:

- برای حفظ امنیت اطلاعات و دیتای خود به رمز عبور ویندوز وابسته نباشید .آنها به سرعت شکننده اند.
- رمز عبوری را استفاده کنید که حداقل هشت کاراکتر باشد.
- یک جمله مختصر نیز می تواند به عنوان رمز عبور شما استفاده شود.
- به عوض استفاده از رمز عبور کوتاه و واضح، ترجیحاً از رمز عبور پیچیده استفاده نموده و آنرا یادداشت کرده و به صورت امن ذخیره کنید.
- رمز عبور خود را از نمادها، حروف بزرگ، حروف کوچک و ارقام و اعداد تشکیل دهید.
- هر بار از یک رمز عبور متفاوت استفاده کنید.

[48] https://www.securitymagazine.com
[49] https://www.kaspersky.com/resource-center/threats/what-is-smishing-and-how-to-defend-against-it
[50] https://www.freshbooks.com/hub/other/what-is-byod?ref=&campaignid=16988866217&adgroupid=&targetid=&crid=&dv=c&geo=9000786&ntwk=x&source=GOOGLE&gclid=Cj0KCQjw08aYBhDlARIsAA_gb0csfHZJ8sfHlpNIE7kwIyt5Th03upAvoO25MO8M-xwJTmXzipAZfSUaAnnPEALw_wcB
[51] https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT
[52] https://www.kaspersky.com
[53] https://www.ibm.com/docs/en/zos/2.4.0?topic=security-what-is-password-protection

- از رمز عبوری استفاده کنید که ارتباط نزدیکی با علایق شخصی، نام، تخلص یا زندگی شما نداشته باشد.
- هرگز رمز عبور خود را با کسی فاش نکنید.
- هر سه یا شش ماه یکبار رمزهای عبور خود را تغییر دهید.
- به خاطر داشته باشید که انواع ابزارهای آنلاین رایگان برای تشکیل رمز عبور ویندوز، رمزگذاری شبکه و تقریباً هر نوع رمز عبور کامپیوتری دیگر که ممکن است داشته باشید، در دسترس هستند.

حملات بر رمز عبور[54]

بسیاری از ما از معیارهای امنیتی ارائه شده توسط برنامه های نرم افزاری معروف استفاده می کنیم. شما میتوانید از رمز عبور برای امنیت فایل یا نرم‌افزار های تان که از شرکت‌هایی مانند Microsoft، Quicken، Adobe و دیگران دریافت کرده اید استفاده کنید. برنامه‌های مایکروسافت آفیس (Microsoft Office) مانند مایکروسافت ورد (Microsoft Word) نمونه‌ای از این فایل ها و نرمافزار ها هستند. این واژه پرداز (word processor) یک ویژگی امنیتی را ارائه می دهد که به شما امکان این را فراهم مینماید از هر سند با یک رمز عبور محافظت کنید. از هر کسی که بخواهد سند را باز کند، رمز عبور درخواست می شود و تا زمانی که رمز عبور وارد نشود، هیچ محتوایی در سند قابل دید نمی باشد. با این اقدام امنیتی، که صرفاً یک لایه است، فقط افراد عادی دور نگه داشته می شوند ولی هکر ها ممکن بتوانند فایل شما را باز کنند.

استفاده مؤثر از کامپیوتر مستلزم استفاده از رمز عبور قوی است. خواه یک ایمیل باشد، ورود به یک شبکه و یا هم بانکداری آنلاین، آنها با احراز هویت، برای دسترسی به خدمات ضروری، به عنوان یک مانع امنیتی عمل می کنند. شما حق دارید از رمزهای عبور مختلف برای حساب های متفاوت استفاده کنید ولی با انجام این کار شما وارد چالش های جدیدی میشوید. به همین دلیل، از نظر فنی، اطلاعاتی که رمز عبور شما از آن محافظت می‌کند باید آنقدر به شما مهم باشد که اینگار از یک سیف پول یا گاوصندوق محافظت میکنید. یک رمز عبور قوی مهمترین جزء هر سیستم برای تامین امنیت دیجیتال شما میباشد. طبق تاریخچه هک شدن سیستم ها، متداول ترین روشی که هکرها و مهاجمان سیستم های اطلاعاتی و دیتای شما را هدف قرار می دهند، شکستن رمز عبور است.

نمایه سازی (profiling)

نمایه سازی مستلزم حدس و پیش بینی در مورد فردی است که رمز عبور را با جمع آوری حقایق و علایق شخصی خود تهیه میکند. رمز عبور ما معمولاً چیزی است که به خاطر سپردن آن برای ما ساده باشد، مانند سال تولد، نام یک شخص خاص، شهری که در آن زندگی میکنیم، تیم فوتبال مورد علاقه ما و غیره. این ها و سایر حقایق وعلایق مشابه توسط نمایه سازان در نظر گرفته می شوند. از آنجایی که ممکن رمزهای عبور زیادی داشته باشید، می توان گفت که به خاطر سپردن همه آنها کار دشوار است بنا بر این شما از کلمات آشنا و مرتبط به علایق شخصی و زندگی روزمره تان استفاده میکنید تا به یاد داشتن آنها برای تان آسان باشد. با این حال، نمایه سازی محبوب ترین رویکرد برای نفوذ به سیستم کامپیوتر شما برای هکرها است چون میتوانند به سادگی رمزو عبور شما را حدس زده باز کنند.

مهندسی اجتماعی

[54] https://securityboulevard.com/2022/05/what-is-a-password-attack-in-cyber-security/

از طریق سناریوها و سوالات مبتکرانه، بسیاری افراد فریب هکر ها را خورده و رمز عبور خود را فاش کرده اند. این نوع ترفند ممکن به شکل یک تماس تلفنی از طرف ISP شما باشد، که ادعا می کند در حال ارتقای سرور است و به رمز عبور شما نیاز دارد تا مطمئن شود هیچ ایمیلی را در این فرآیند از دست نمی دهید. یا ممکن هکر وانمود کند که یکی از همکاران بخش دیگری از شرکت شما است و رمز عبور ایمیل شما را به این دلیل که مالک در حال حاضر بیمار است و او نیاز به ارسال سریع اسناد و مدارکی دارد، بخواهد. این عمل را مهندسی اجتماعی می نامند. به وسیله این ترفند تلاش هکرها برای نفوذ به سیستم کامپیوتر هنوز هم امکان پذیر است[55].

حملات لغتنامه ای

حمله توسط لغتنامه مستلزم وارد کردن هر کلمه در لغتنامه، که ممکن به عنوان رمز عبور از آن در سیستم استفاده شود صورت میگیرد تا به کامپیوتر و اطلاعات شما دسترسی یابند. حمله توسط لغتنانه همچنین می تواند برای رمزگشایی ارتباطات محرم و یا سند رمزگذاری شده نیز استفاده شود. در این ترفند، فهرستی از رمزهای عبور احتمالی مورد استفاده قرار میگیرند. مجموعه‌ای از لغتنامه های رایگان به صورت آنلاین وجود دارند و این ترفند را برای هکر ها ساده تر میسازند که آنرا به عنوان حمله توسط لغتنامه میشناسند[56].

حملات BRUTE FORCE[57]

در بیشتر موارد حملات بریوت فورس در کمتر از پنج ثانیه به پایان می رسد. این ترفند متکی به یک لیست از پیش بارگذاری شده[58] از رمزهای عبور احتمالی نیست. در عوض، هر رمز عبور احتمالی را امتحان می‌کند، از جمله رمزهایی که دارای حروف، اعداد و کاراکترهای خاص هستند. اگرچه ممکن به دلیل قدرت پردازش قوی که در حال حاضر در هر کامپیوتر موجود است دست نیافتنی به نظر برسد، ولی نباید آنرا نادیده گرفت. در این ترفند ممکن اپلیکیشن هکر از رمز عبور چهار تا ده کاراکتر استفاده کند چون اکثر رمزهای عبور کمتر از چهار کاراکتر ندارند.

ایجاد یک رمز عبور قوی

اکنون می دانیم که رمزهای عبور مانند "apple"، "Michael"و حتی "banana4" ناامن هستند. به همین دلیل خدمات آنلاین به تکیه گاه امنتری نیاز دارد. اکثریت وبسایت ها به رمز عبوری نیاز دارند که حداقل هشت کاراکتر داشته باشد و این کارکتر ها شامل یک عدد و یک علامت خاص باشد. عده ای هم ممکن بر حروف بزرگ پافشاری کنند. ایجاد رمز عبوری که به خاطر داشتن آن ساده باشد و با این معیارها مطابقت داشته باشد، می تواند برای هکر ها چالش برانگیز باشد. من توصیه می کنم شما از یک رمز عبور با ساختاری پیچیده استفاده کنید. به طور مثال، رمز عبور یکی از حساب‌های بانکی آنلاین خود را به‌روزرسانی میکنید و باید از معیارهای امنیتی رمز عبوراستفاده نمایید. اگر «apple» را در رمز عبور تان استفاده کرده اید، به عوض آن از یک ساختار پیچیده تری مثل «OraNge23$%18No» استفاده کنید. راه های زیادی برای ایجاد رمز عبور قوی وجود دارد که هم حدس زدن آن ها سخت و هم به خاطر سپردن آن ها ساده باشد. (password managers) ها بهترین گزینه ها برای ایجاد یک رمز عوبر قوی هستند. جهت معلومات بیشتر به بخش 4.3 این رهنمود مراجعه نمایید. برای تهیه یک رمز عبور

[55] https://www.kaspersky.com/resource-center/definitions/what-is-social-engineering
[56] https://www.hypr.com/security-encyclopedia/dictionary-attack
[57] https://www.kaspersky.com/resource-center/definitions/brute-force-attack
[58] Downloaded

پیچیده از وبسایت های مانند Dashlane[59] ، Sticky Password[60]، LastPass[61]، و یا Password Boss[62] استفاده کنید.

رمز عبور شما اولین و مهم ترین تضمین برای محافظت از دیتای شما است. و آن به عنوان قفل دروازه خانه شما عمل می کند. استفاده از یک رمز عبور ضعیف مثل این است که دروازه خانه شما تمام شب باز باشد. شاید کسی وارد نشود، و یا هم ممکن کسی همه چیز شما را کسی بدزدد. در مورد نحوه ساخت رمزهای عبور و مکان ذخیره آنها بسیار مراقب باشید.

ذخیره خودکار رمز عبور (auto save)

اکثر اپلیکیشن ها و سیستم های عامل کامپیوتر ها تلاش میکنند تا همه چیز را ساده بسازند. ارائه گزینه ذخیره خودکار رمز عبور یکی از روش هایی است که مرورگرهای وب و سایر اپلیکیشن ها آنرا به همین دلیل انجام می دهند. به عنوان مثال، اکثر مرورگرهای وب هنگام اتصال به وب سایت و ورود به یک حساب آنلاین، از شما می خواهند رمز عبور تان را ذخیره کنید. وقتی این گزینه را انتخاب و رمز عبور خود را وارد می کنید، به مرورگر اجازه داده اید که رمز عبور را در کامپیوتر شما ذخیره کند. ولی اپلیکیشن های متعددی برای بازیابی رمز های عبوری که در کامپیوتر ها ذخیره شده است تهیه شده اند تا این رمزها را دریابند و هکر ها وارد حساب شما شوند. برای حل این مشکل، یک راه حل آسان وجود دارد. هرگز اجازه ندهید نرم افزار کامپیوتر تان رمزهای عبور شما را ذخیره کند. اگر مرورگر وبسایت شما در حال حاضر هنگام بازدید از یک وبسایت، پس از اینکه اجازه ذخیره رمز عبور خود را به آن داده‌اید، شما را وارد سیستم کند، می‌توانید این را تغییر دهید. در اینجا توضیح خواهیم داد که چگونه رمزهای عبور خود را از اینترنت اکسپلورر، موزیلا فایرفاکس، گوگل کروم و سافاری پاک کنید، حتی اگر نتوانیم نحوه انجام این کار را برای هر برنامه مشخص کنیم، چهار مرورگر وب برتر برای ویندوز، مک و لینوکس را برای تان توضیح خواهیم داد[63] .

اینترنت اکسپلورر(IE) [64]

"Tools"را از "Menu Bar" انتخاب کنید و سپس روی "Internet Options" کلیک کنید. بعد یک پنجره جدید با تعدادی از گزینه ها ظاهر می شود. روی دکمه "Delete" در زیر "Browsing History"در "General Tab" کلیک کنید. در نتیجه "Temporary files" "History" "Cookies" "Saved Passwords" و تمام دیتای شما از فورم وب شما حذف می‌شوند.

موزیلا فایرفاکس (Mozila Firefox[65])

"Tools"را از "Menu Bar" انتخاب کنید و سپس روی "Internet Options" کلیک کنید. باید بخشی با عنوان "Passwords" را در زیر منوی "Security" مشاهده کنید. با کلیک بر روی "Saved Passwords" پنجره جدیدی باز می شود که همه رمزهای عبور ذخیره شده در آن کامپیوتر را نمایش می دهد. با کلیک کردن بر روی "Delete" می توانید رمزهای عبور ذخیره شده را حذف کنید. پس از اتمام، روی "Close" کلیک کنید و در بخش "Options" علامت " Remember Passwords for Sites" را برداشته و غیر فعال کنید.

[59] https://www.dashlane.com/
[60] https://www.stickypassword.com
[61] https://www.lastpass.com/features/password-generator
[62] https://www.passwordboss.com
[63] https://www.techadvisor.com/article/745824/is-it-safe-to-store-passwords-in-your-web-browser.html
[64] https://www.microsoft.com/en-ca/download/internet-explorer.aspx
[65] https://www.mozilla.org/

گوگل کروم (Google Chrome[66])

روی "Settings" در "Menu Bar" واقع در گوشه سمت راست بالای صفحه کلیک کنید. بعد صفحه جدیدی با تعدادی از گزینه ها ظاهر می شود. پس از اسکرول به سمت پایین، در پایین صفحه روی "Show Advanced Settings" کلیک کنید. در نتیجه گزینه های بیشتر، از جمله بخشی برای رمزهای عبور، باز می‌شوند. بعد "Manage Stored Passwords" را انتخاب کنید. سپس می توانید رمزهای عبور خود را از حافظه حذف کنید. همچنان برای محافظت از حملات انترنتی بالای رمزهای عبور تان در آینده، علامت "Offer to keep passwords I type on the web" را پس از انجام کار، غیر فعال سازید .

سافاری (SAFARI[67])

پس از کلیک بر روی "Safari" در "Menu Bar"، "Preferences"را انتخاب کنید. یک پنجره جدید حاوی گزینه های متعدد ظاهر می شود. با انتخاب گزینه "Passwords" می توانید تمام رمزهای عبور ذخیره شده خود را مشاهده کنید. دکمه " Delete All" را می توان در پایین این پنجره یافت. با کلیک بر روی آن، رمزهای عبور ذخیره شده حذف می شوند.

ورود به سیستم به شیوه خودکار (AUTO LOGIN)

سیستم های عامل "Operating Systems" همچنین امکان ذخیره رمز عبور و ورود خودکار را به شما می دهند. این هم فوق‌العاده مفید و هم بسیار خطرناک است. این روش مطلوب است در صورتیکه فقط یک کامپیوتر در سیستم بسته انترنتی موجود بوده و تنها مورد استفاده خود شما باشد. اما اگر افراد دیگری گاهی اوقات به کامپیوتر شما دسترسی داشته باشند، ممکن است خطرناک باشد. تمام اسناد و اطلاعات خصوصی شما در کامپیوتر شما ذخیره می شود. اگر کامپیوتر شما به طور خودکار همانطور که شما وارد حساب های تان به صورت خودکار میشوید، هیچ چیز مانع از سرقت اطلاعات شما نمی شود. با فعال کردن رمز عبور در حساب کاربری خود، می توانید این کار را چالش برانگیز کنید.

حفاظت از حریم خصوصی وبسایت

مرورگرها (BROWSERS[68])

اطلاعات اتصال به اینترنت و فعالیت آنلاین شما به طور مرتب توسط مرورگرهای وب جمع آوری و ذخیره می شود. معمولاً یک مرورگر وب استاندارد در حال جمع‌آوری و ذخیره اطلاعات مربوط به اتصال و فعالیت‌های آنلاین شما است. این مرورگرها دیتای زیر را به وبسایت هایی که بازدید می کنید ارسال می کند.

- آدرس IP شما.
- نوع دستگاه شما.
- نام مرورگر (browser) شما.

[66] https://www.google.com/chrome/
[67] https://www.apple.com/ca/safari/

- تنظیمات کوکی (Cookie) شما.
- افزونه های (add-ons) مرورگر شما.
- کلیک ها و حرکات ماوس (Mouse) شما.
- موقعیت بازدید و منطقه زمانی شما.
- وضوح (resolution) صفحه نمایش و میزان چارج باتری شما.

اکثر این دیتا ممکن است بی‌اهمیت به نظر برسند، اما وقتی جمع شوند و شما را در معرض شناسایی قرار دهند، وب‌سایت‌ها ممکن است از انگشت دیجیتالی (Digital Fingerprint) برای شناسایی و نظارت آنلاین شما استفاده کنند . حرکات انگشت شما روی کامپیوتر تان به وسیله این مرورگرها برای شخص ثالث قابل مشاهده خواهد بود، حتی اگر شما "Cookies" (فایل‌های محدودی که وبسایت‌ها در دستگاه شما ذخیره می‌کنند)، سابقه (History) خود را حذف کرده ، و (Private/Incognito Windows) پنجره ناشناس/خصوصی استفاده کنید. این ممکن است ارتباط روشنی بین شما و فعالیت های بشردوستانه شما ایجاد کند. ممکن است باور داشته باشید که تنها چیزی که برای جلوگیری از ردیابی لازم است یک تغییر ساده در تنظیمات حریم خصوصی مرورگرتان است. در واقع، این ممکن است منحصر به فرد بودن اثر انگشت مرورگر شما را افزایش دهد.

بهترین مرورگر برای حفظ حریم خصوصی[69]

مرورگر های متعددی وجود دارد که بهترین‌های آنها، هفت مورد زیر هستند، اما ایمن‌ترین آنها (Firefox) در مقایسه با Chrome، Edge، Safari، Opera، Brave و Internet Explorer است.

نحوه استفاده ایمن از مرورگر

ترفند (CLEAN & CLICK)

با یک کلیک، هر مرورگری را که در حال حاضر دارید خاموش کنید. این شامل دیتای فرم، کوکی‌ها، حافظه پنهان (Cache)، و رمز های عبور است که قبلاً ذخیره کرده‌اید، و همچنان مرورگر شما و سابقه دانلود می شود.

ترفند (PUBLICITY BADGER)

ردیاب ها را بلاک کنید و فوراً فعالیت مشکوک را در وبسایت هایی که بازدید می کنید شناسایی نمایید. هر چیزی که بر خلاف رضایت کاربر باشد بلاک شده است.

ترفند (VPN CYBERGHOST)

شما می توانید آدرس IP خود را با کمک یک سرویس VPN مخفی کنید. (VPN) گزارش فعالیت شما را ذخیره نمی کند و همچنین تمام ردیابی آنلاین را غیرفعال می سازد

[69] https://www.mozilla.org/en-CA/firefox/browsers/compare/

اگر نمی‌خواهید مرورگرهای وب را تغییر دهید، راه‌های دیگری برای کاهش ردیابی و و عدم ذخیره دیتای تان در فعالیت آنلاین شما وجود دارد، مانند: محدود کردن تعداد کوکی‌هایی که می‌پذیرید. مرورگر خود را به گونه‌ای تنظیم کنید که تبلیغات ردیابی و ردیاب‌های نامرئی را بلاک کند، و به طور معمول حافظه پنهان و کوکی‌های خود را پاک کنید تا خطر ردیابی شما کاهش یابد.

این روش ها مفید هستند، اما اثر انگشت مرورگر شما را به طور قابل توجهی تغییر نمی دهند. همانطور که قبلاً اشاره شد، تغییر چند تنظیمات ممکن است در واقع اثر انگشت دیجیتال مرورگر شما را برای وب‌سایت‌هایی که بازدید می‌کنید متمایزتر نشان دهد.
استفاده از شبکه TOR یک روش خوب برای کاهش احتمال اثرانگشت مرورگر شما است. مهم نیست از چه دستگاه یا سیستم عاملی استفاده می کنید، هر کاربر TOR باید دقیقاً همان اثر انگشت مرورگر را داشته باشد.

مرورگرهای ترجیحی و ایمن برای فعالان و مدافعان حقوق بشر

مرورگر (TOR)

با کمک مکانیسم های امنیتی از پیش تنظیم شده و (relay server)، Tor، مسلماً شناخته شده ترین مرورگر متمرکز بر حریم خصوصی، و محافظ از جاسوسی غیرمجاز درانترنت است.

مرورگر (EPIC[70])

وقتی از مرورگر EPIC استفاده میکنید، گزینه پیش فرض حریم خصوصی به صورت دیفالت روشن است. مرورگر هنگام استفاده از موتور جستجوی خصوصی (DuckDUckGo)، کوکی‌ها، ردیاب‌ها و تبلیغات را غیرفعال می‌کند. اطلاعات ورود، سابقه مرور و سایر اطلاعات شما نیز ذخیره نمی شود.

مرورگر (FIREFOX)

به دلیل محافظت از حریم خصوصی که از شما در برابر ردیابی، وایروس ها و cryptominers محافظت می کند، این مرورگر یکی از امن ترین مرورگرهای موجود است. علاوه بر این، برای کمک به کنترل تهدیدات، اغلب به صورت خودکار به روز می شود.

موتورهای جستجو

هر حرکت اینترنتی شما توسط گوگل و سایر موتورهای جستجو ردیابی می شود. آنها اغلب ممکن است داده های کاربر را به اشخاص ثالث منتقل کنند. اطلاعاتی که گوگل و سایر موتورهای جستجو در مورد شما دارند ممکن است شما را شگفت زده کند. آنها اطلاعات معدودی را برای ارائه تبلیغات هدفمند و سفارشی کردن مرور وب شما جمع آوری می کنند.

[70] https://www.epicbrowser.com

آنچه گوگل می داند[71]

در مورد خود شما

Google از نام، سن، جنسیت، دیتای تشخیص چهره و صدا، اطلاعات تناسب اندام، دیدگاه‌های جنسیتی، سیاسی و مذهبی شما آگاه است. چگونه می‌داند، از طریق فرآیند ثبت‌نام درGoogle ، جستجوی Google ، Google Fit و Google Assistant.

شما کجا و از کجا هستید

Google از مکان تولد و مکان فعلی شما و همچنین مکان های گذشته، حال و آینده شما آگاه است. نحوه حمل و نقل و جستجوهای مکان شما برای Google نیز شناخته شده است. چگونه می داند، از طریق Waze و Google Maps .

با کی ها ملاقات دارید

قرار های ملاقات شما برای گوگل شناخته شده است. دیتای حساس، از جمله مسیرهای راهپیمایی، برنامه‌ریزی بایکات یا اعتصاب، مکاتبات و دادخواست‌ها ممکن است در دسترس Google باشد. این اطلاعات را از طریق Google Drive ، Google Calendar، Google Hangoutsو Gmail میداند.

شما کی هستید

Google میداند شما از کجا، کی و چی طرز فکری دارید همچنان از کتاب‌ها، مقالات و فیلم‌ها، خوانده، دیده و خریداری و جستجو کرده‌اید، آگاه است. چگونه می‌داند، از طریقGoogle News ، YouTube، Google Search، و Google Shopping Ads، Google Books.

شما چی را جستجو میکنید

Googleاز تاریخچه وبسایت‌هایی که بازدید کرده‌اید، از جمله نام‌های کاربری و رمزهای عبور ذخیره‌شده، آگاه است.

نحوه استفاده از (Chrome[72])

باید توجه داشته باشید که اکثریت موتورهای جستجو توسط مجریان قانون یا مقامات دولتی مجبور شوند تاریخچه جستجو و مرور شما را به اختیار آنها بگذارند. در نظر بگیرید که اگر مرتباً دنبال اطلاعاتی درباره مخالفان و شخصیت‌های دولتی و همچنان حمایت مالی و حقوقی از سازمان‌های بین‌المللی هستید و از طریق انترنت جستجو میکنید، برای شما به‌عنوان یک فعال چه نتیجه‌ای خواهد داشت.

[71] https://www.businessinsider.com/what-does-google-know-about-me-search-history-delete-2019-10
[72] https://support.google.com/a/users/answer/9310344?hl=en

ما می دانیم که گوگل محبوب ترین موتور جستجو است. اما وقتی نوبت به ردیابی و جمع آوری دیتای کاربر می رسد، یکی از بدترین هاست. آسوشیتدپرس اخیراً دریافته است که حتی اگر گزینه "تاریخچه موقعیت مکانی" را غیرفعال کنید، گوگل به ردیابی مکان شما همچنان ادامه می دهد.

موتورهای جستجوگر ترجیحی برای حفظ حریم خصوصی

موتور جستجوگر (DUCKDUCKGO[73])

DUCKDUCKGO محرمانه و در ضمن ساده برای استفاده است. نه کوکی ها و نه دیتای کاربر توسط آن جمع آوری می شود. علاوه بر این، لاگ های IP سرورها را پاک می کند. می توانید به DUKDUCKGO در آدرس زیر دسترسی داشته باشید:

https://duckduckgo.com/?va=b&t=hc.

موتور جستجوگر (METAGER[74])

موتور جستجوی چندزبانه آلمانی تاکید زیادی بر حفاظت از حریم خصوصی کاربران دارد و همچنان پروفایل‌ها و دیتای مربوط به کاربران خود را جمع‌آوری نمی‌کند. از Tor برای دسترسی مستقیم به MetaGer استفاده کنید. شما می توانید به MetaGer در اینجا دسترسی پیدا کنید:

https://metager.org

موتور جستجوگر (STARTPAGE[75])

با استفاده از فناوری Google بدون ردیابی، (Startpage) یک تجربه گشت و گذار راحت اما خصوصی را به شما ارائه می دهد. هیچ گونه اطلاعات کاربری را ثبت نمی کند یا آن را به اشخاص خارجی فاش نمی سازد. شما می توانید به (Startpage) در اینجا دسترسی داشته باشید:

https://www.startpage.com

حفاظت از حریم خصوصی دیتا (Data)

فعالان و مدافعان حقوق بشری اغلب اطلاعات مهمی در اختیار دارند و بسیاری از آنها به موضوعات مهمی دسترسی دارند که به اهداف آنها کمک میکند. این دارایی های معنوی که در قالب دیتا نگهداری می شوند، در معرض حملات مخرب همه طرف ها هستند.

[73] https://duckduckgo.com/?va=b&t=hc
[74] https://metager.org
[75] https://www.startpage.com

یک بدیلی برای نگهداری امن این دیتا رمزگذاری روی درایوهای فلش (memory sticks) است، اما انجام این کار ممکن است اطلاعات شما را حتی بیشتر در معرض سرقت، گم شدن یا مشکلات تکنولوژیکی قرار دهد. ظرفیت ذخیره سازی دستگاه های فیزیکی نیز محدود است.

در نتیجه ذخیره سازی در (Cloud) بسیار اهمیت پیدا کرده است. دیتای موجود در این ذخیره گاه ها قابل اشتراک‌گذاری هم هستند، که برای فعالانی که نیاز به انتشار اطلاعات برای پیشبرد اهداف خود دارند، بسیار مهم است.

ذخیره در کلاود (Cloud)

ممکن است از اکثر ارائه دهندگان خدمات ذخیره سازی کلاود مهم خواسته شود که به مجریان قانون و کارمندان دولت حق دسترسی به دیتای شما را بدهند.

باید هوشیار بود که در فضای کلاود دیتای رمزگذاری شده شما متضمن امنیت خصوصی دیتای شما نیست. مجریان قانون و کارمندان دولت ممکن شرکت‌های ذخیره کلاود بزرگ را مجبور به همکاری کنند، و رمزگذاری به تنهایی از این امر محافظت نمی‌کند، زیرا برخی از سرویس‌ها برای تبادل دیتا و فایل‌ها با سازمان‌های جاسوسی دولتی مانند آژانس امنیت ملی (NSA) در ایالات متحده شناخته شده‌اند.

نحوه امینت ذخیره سازی در کلاود

با انتخاب یک ارائه‌دهنده خدمات فضای ذخیره‌سازی در کلاود که فایل‌های شما را قبل از آپلود به کلاود در دستگاه خود شما رمزگذاری می‌کند، می‌توانید از فضای ذخیره‌سازی کلاود خود محافظت کنید (این برخلاف کلاود هایی است که فایل‌هایی شما را در جریان انتقال به کلاود رمزگذاری می کنند). به خاطر داشته باشید که ارائه دهندگان این خدمات ممکن است به کلیدهای رمزگذاری شما دسترسی داشته باشند و بتوانند فایل های شما را رمزگشایی کنند یا در صورت لزوم آنها را در اختیار مقامات دولتی قرار دهند.

اکیداً توصیه می شود که قبل از ارسال دیتا به یک سرویس کلاود، آنها را خود شما رمزگذاری کنید. تا زمانی که خود شما رمز خود را با فایل های خود آپلود نکنید، تنها کسی خواهید بود که رمز دیتای خود را دارید.

برنامه های رمزگذاری متعدد رایگان و یا هم به شکل پیش پرداخت وجود دارد، اما مطمئن شوید که دستگاه‌های شما با ارائه‌دهنده ذخیره‌سازی کلاود شما سازگار باشند. مطمئن شوید که این برنامه که شما استفاده میکنید از رمزگذاری سرتاسر استفاده کند، تا تضمینی باشد که فایل‌های شما از لحظه خروج از گوشی هوشمندتان رمزگذاری شده و تا زمانی که دوباره بتوانید به آن‌ها دسترسی داشته باشید امن باشند.

اشتراک گذاری دیتا

برنامه Veracrypt[76] به کاربران اجازه می دهد تا فایل های رمزگذاری شده را در هارد دیسک ها و حافظه های آنلاین، Google Drive یا Dropbox ذخیره کنند، که برای دیگران مانند فایل های عادی یا فایل های مرتبط به کامپیوتر به نظر می رسند. این

[76] https://veracrypt.fr/

کار برای اطمینان از امنیت اسناد و فایل های شما هنگام ذخیره قبلا محاسبه شده و پیش از آپلود آنها برای اشتراک گذاری و ذخیره سازی آنلاین انجام می شود. برای جلوگیری از جلب توجه به این برنامه، پس از استفاده از Veracrypt برای رمزگذاری اسناد و فایل های تان، حتی از سطل زباله (recycle bin)، برنامه را حذف کنید. برای بدیل های امن (end-to-end encrypted)، گزینه های زیر را انتخاب کنید:

- https://cryptpad.fr/drive
- https://ufile.io
- https://send.tresorit.com
- https://send.tresorit.com

حفاظت از رسانه های اجتماعی و نحوه ارتباطات

نحوه استفاده از ارتباطات امن

فعالان و مدافعان حقوق بشر اغلب اطلاعات خصوصی را با دیگر فعالان، گروه ها، وکلا و روزنامه نگاران مبادله می کنند. بهترین رویکرد برای انجام یک چت واقعا خصوصی، باز دید از یکدگر است، اما این بدیهی است و همیشه ممکن نیست.

بهتر است هنگام مکالمه آنلاین از خدمات ارتباطی رمزگذاری شده مانند سیگنال (Signal)، وایر (Wire) و کی بیس (KeyBase) استفاده کنید. در این روش از رمزگذاری (end-to-end) برای محافظت از آنچه شما می گویید استفاده می شود.

لطفاً توجه داشته باشید که تلگرام اطلاعاتی را نقض کرده است و رمزگذاری (end-to-end) به‌طور پیش‌فرض (default) فعال نیست، به استثنای «چت‌های خصوصی» و تماس‌های صوتی و تصویری. در قسمت ارایه دهنده گان خدمات ایمیل باید گفت که آنها ممکن مجبور شوند اطلاعات شما را به مقامات دولتی ارائه دهند. حتی شما ممکن در معرض پالیسی های مبهم حریم خصوصی رسانه های اجتماعی قرار بگیرید.

ایمیل ها (Emails)

اکثریت شرکت های خدمات ایمیل امن هستند و مکانیسم های سختگیرانه ای برای محافظت در برابر نشت دیتای شما دارند. با این حال، باید در نظر داشت که آنها هم از روش های استفاده میکنند که بدون خطا نیستند. بعید است که اقدامات امنیتی شما را امن نگه دارد اگر این شرکت ها ایمیل شما را ملزم به ارائه به مقامات دولتی بدانند.

خصوصی نگهداشتن شناسه ایمیل (Email Identity)

شما باید اقدامات امنیتی بیشتری را برای حفظ حریم خصوصی خود انجام دهید تا احتمال اینکه تجسس ادارات دولتی در مکاتبات شما را کاهش دهد. عملی ترین رویکرد، استفاده از سرویس ایمیل خصوصی مانند (ProtonMail[77])، (Fastmail[78]) یا (Zoho Mail[79]) است. چون رمزگذاری ایمیل هم نیاز به زمان دارد و هم تلاش بیشتری می برد.

(Rise Up[80]) و (Aktivix[81]) سرویس‌های ایمیل امن هم وجود دارند که برای فعالان و مدافعان حقوق بشر ایجاد شده‌اند، رایگان هستند زیرا به حمایت کمک‌های مالی دونر ها اداره میشوند. با این حال، آنها ممکن است به اندازه ارائه دهندگان تجاری از ایمیل های ذخیره شده پشتیبانی نکنند، بنابراین ممکن مدیریت ایمیل های اضافی مانند آرشیف ایمیل های قدیمی نیاز به یک مرکز ذخیره سازی کلاود امن داشته باشد.

بهتر است حساب های ایمیل شخصی تان را و حساب های ایمیل خود را که برای فعالیت های بشردوستانه استفاده میکنید به طور جداگانه حفظ کنید. این مانع از اتصال حساب های شما که اطلاعات شخصی و قابل شناسایی شما را دارد به حساب هایی که برای برنامه ریزی فعالیت های بشردوستانه استفاده میکنید و با سایر فعالان در ارتباط هستید، می شود.

ایمنی ایمیل

فیشینگ (phishing) نوعی کلاهبرداری انترنتی است و زمانی تحقق میابد که کلاهبرداران آنلاین یا سایر افرادی که تجسس میکنند را وانمود کند که کسب‌وکارهای قابل اعتماد دارند و یا افرادی هستند که می‌شناسید و معمولاً از طریق ایمیل اتفاق می افتد. هدف آنها این است که کاربران را به افشا کردن اطلاعات خصوصی شان فریب میدهند. این افراد برای متقاعد کردن شما به دانلود نرم افزارهای مخرب یا کلیک بر روی پیوندهایی که به نظر قانونی می رسند تلاش میکنند و میخواهند شما را فریب دهند. هرگز روی پیوندها یا دانلودهایی که از طریق ایمیل توسط فرستنده ناشناس برای شما ارسال شده است، کلیک نکنید. با بررسی مجدد آدرس ایمیل، مطمئن شوید که مشروع است. روی پیوندهای موجود در ایمیلی که شما را از مشکل یک حساب کاربری خاص مطلع می کند، کلیک نکنید. ترجیحاً مستقیماً به وب سایت یا خدمات همان برنامه بروید و در آنجا برنامه و یا وبسایت را باز کنید. لطفاً توجه داشته باشید که هر یک از این تکنیک ها می تواند توسط این افراد برای بدست آوری دیتا و حسابهای فعالان و مدافعان حقوق بشر استفاده شود[82].

رسانه های اجتماعی

شرکت‌هایی که در عقب شناخته‌ترین اپلیکیشن‌ها و سایت‌های اجتماعی قرار دارند، به خصوص در مورد حفظ حریم خصوصی و امنیت حسابها، با وجود این که رسانه‌های اجتماعی برخی از مفیدترین ابزارها را برای فعالان و مدافعان حقوق بشر ارائه می‌دهند تا در برنامه های مشارکت جمعی، جنبش‌های هدفمند، رویدادها فعالانه و بدون مشکل سهیم شوند، مورد مناقشه قرار گرفته‌اند که از دیتای آنها در قسمت تبلیغات استفاده مینمایند. به عنوان مثال، معظله کمبریج آنالیتیکا در سال های اخیر نشان داد که چگونه فیسبوک اجازه جمع آوری اطلاعات شخصی میلیون ها کاربر را می دهد. چنین نقض حریم خصوصی نشان

[77] https://account.proton.me/login
[78] https://www.fastmail.com
[79] https://www.zoho.com/mail/
[80] https://account.riseup.net
[81] https://en.exp.activix.ca/users/sign_in
[82] https://www.tripwire.com/state-of-security/featured/essential-tips-for-keeping-your-email-safe/

می دهد که رسانه های اجتماعی چقدر اطلاعات درباره شما دارند. شاید فکر کنید اطلاعاتی که در این شبکه‌ها افشا می‌کنید آنقدر خصوصی نیستند.

جیوتگنگ (Geotagging) اغلب در رسانه های اجتماعی برای مشخص کردن مکان دقیق شما استفاده می شود. فیسبوک بیشتر از همه موقعیت مکانی شما را ردیابی می کند. همچنین خریدها، جستجوهای وب و مخاطبین شما را ثبت می کند. به همین دلیل این پلتفرم دائماً از شما درخواست دسترسی به مخاطبین، سابقه تماس و پیامک های شما را دارد.

اطلاعات مهم در مورد تشخیص چهره (Facial Recognition)

برچسب زدن روی چهره شما (tagging) به صورت فراگیر و ناخواسته توسط افراد دیگر خطر نظارت توسط مقامات دولتی بر شما را افزایش می دهد. نرم افزار تشخیص چهره در سیستم های اشتراک گذاری عکس رسانه های اجتماعی تعبیه شده است. پلتفرم ها در حال جمع آوری مجموعه های عظیم تصاویر چهره کاربر هستند. سایت های شبکه های اجتماعی معمولاً اطلاعات چهره افراد را در اختیار مقامات دولتی قرار می دهند. هنگامی که عکسی را آپلود می کنید، به مالکیت پلتفرم تبدیل می شود. وقتی یک بار وارد شدید، هیچ راهی برای انصراف از سیستم های تشخیص چهره فعلی وجود ندارد.

همانطور که بارها نشان داده اند، اطلاعات شخصی شما در فیسبوک یا سایر پلتفرم های رسانه اجتماعی امن نیست. هرچه اطلاعات شخصی بیشتری در رسانه های اجتماعی ارسال کنید، حریم خصوصی شما به همان پیمانه در خطر میباشد. برای فعالان و مبارزان معروف، انتخاب بین مشارکت و در معرض دید قرار داشتن یک شمشیر دو لبه است.

الزامیت تغییر دهی تنظیمات رسانه های اجتماعی

برای تضمین ناشناس ماندن، به عنوان یک فعال و مدافع حقوق بشر، همیشه باید تنظیمات حریم خصوصی خود را از پیش فرض های پلتفرم (platform default) تغییر دهید. شما می‌توانید کنترل کنید چه کسی می‌تواند نمایه، پست‌ها، موقعیت مکانی، عکس‌ها و جزئیات تماس شما را ببیند، همچنین اینکه آیا افراد می‌توانند شما را برچسب‌گذاری (tag) کنند یا در جستجوی نمایه پیدا کنند یا نه.

همچنین می توانید تنظیمات امنیتی را در حساب های رسانه های اجتماعی خود بهبود بخشید. می‌توانید احراز هویت دو مرحله‌ای را در اینجا تنظیم نمایید، نمایه‌های کاربر را ممنوع کنید، و (notification) حساب تان را فعال کنید قبل از آن که تلاش غیرمجاز برای دسترسی به حسابتان انجام شود.

راه اندازی یک حساب ایمن در رسانه های اجتماعی

اگر می خواهید یک حساب کاربری امن در شبکه های اجتماعی داشته باشید:

- هرگز از نام کامل یا واقعی خود استفاده نکنید.
- هنگام ثبت نام از یک آدرس ایمیل متفاوت از آدرس ایمیل اصلی/ واقعی خود استفاده کنید.
- فقط اطلاعات مورد نیاز را که با علامت (*) ارائه دهید.
- برا پروفایل خود عکسی را انتخاب کنید که از طریق متاتگ برای تشخیص صورت دقیق شما یا موقعیت مکانی شما استفاده نشود.
- احراز هویت دو مرحله (two-factor authentication) را تنظیم کنید و یک رمز عبور امن انتخاب کنید.

- پاسخ های ساختگی را برای بازیابی رمز عبور انتخاب کنید، سپس انتخاب های خود را در یک (password manager) ذخیره کنید.
- افزونه مرورگری (browser extension) را نصب کنید که کوکی ها و ردیاب های شخص ثالث را بتواند غیر فعال کند.

شاید لازم باشد شرایط (Terms and Conditions) حفظ حریم خصوصی را به دقت بخوانید تا تنظیمات رسانه های اجتماعی خود را به درستی درک کنید، که ممکن زمان بر و دشوار باشد.

لازم به ذکر است که در قسمت شرایط (Terms and Conditions) همان بخشی بسیار مهم است که نحوه استفاده از دیتای شما را در زمان ارائه به اشخاص ثالث و نحوه واکنش به درخواست مقامات دولتی را توضیح می دهد.

همچنین به خاطر داشته باشید که تنظیمات حریم خصوصی می تواند تغییر کند. به‌روزرسانی‌ها را بررسی کنید تا مشخص شود آیا اطلاعات خصوصی قبلی که شما مخالف هستید ممکن است اکنون به اشتراک گذاشته شود یا خیر، اما همچنان در زمان برروزرسانی به دنبال گزینه‌های جدیدی باشید که می‌تواند کنترل حریم خصوصی بیشتری به شما بدهد[83].

امنیت و ایمنی پلتفرم های رسانه های اجتماعی و ابزارهای ارتباطات

ما برخی از پلتفرم‌های رسانه‌های اجتماعی و ابزارهای ارتباطی را که به طور گسترده در افغانستان مورد استفاده قرار می‌گیرند، در این بخش شرح می‌دهیم. ما از پرداختن به جزئیات در مورد هر یک از این پلتفرم‌ها و ابزارهای پرکاربرد خودداری می‌کنیم. فیسبوک، توییتر، اینستاگرام، تیک تاک و یوتیوب محبوب ترین شبکه های اجتماعی در افغانستان هستند. جیمیل، یاهو، مسنجر، واتس‌اپ، وایبر، تلگرام، اسکایپ، زوم و سیگنال محبوب‌ترین ابزارهای ارتباطات رسانه‌های اجتماعی محسوب میشوند. باید خاطر نشان ساخت که تحت این عنوان از تکرار نکات مهم که قبلا تذکر رفته خودداری می کنیم. اگر می‌خواهید از پلتفرم‌های رسانه‌های اجتماعی و ابزارهای ارتباطات بیان شده در این فصل به شیوه‌ای ایمن استفاده کنید و حریم خصوصی خود را حفظ نمایید، لطفاً تمام فصل‌های این راهنما را بخوانید، زیرا بسیاری از نکات مهم را از فصل‌های دیگر بازگو نمی‌کنیم.

نکات مهم در ارتباط به پلتفرم های رسانه های اجتماعی

حین استفاده از رسانه های اجتماعی و ابزار های ارتباطات آنها باید یک سلسله تدابیر، ترفند ها و اقدامات را در نظر داشت تا از آنها به صورت امن استفاده کرد. تمام این موارد تحت هر کدام از این پلتفرم ها و ابزارهای ارتباطات به صورت جداگانه به معرفی گرفته شده است که قرار ذیل است.

فیسبوک (Facebook)

- احراز هویت دو مرحله ای (Two-factor authentication) به محافظت از حساب فیسبوک شما کمک می کند. این یک ویژگی امنیتی است که برای محافظت از حساب شما و ورود به سیستم طراحی شده است. نحوه فعال کردن:

https://www.facebook.com/help/148233965247823

[83] https://www.mcafee.com/blogs/privacy-identity-protection/how-to-protect-your-social-media-accounts/

- باید کنترل کنید که چه کسی می تواند شما را در فیسبوک پیدا کند. می توانید موتورهای جستجو و جستجوی فیسبوک را تحت کنترل داشته باشید. نحوه فعال سازی:

https://www.facebook.com/help/1718866941707011

- می توانید موقعیت مکانی خود را در فیسبوک خاموش کنید. نحوه فعال سازی:

https://www.facebook.com/help/275925085769221

- اگر به حریم خصوصی بیشتری در فیسبوک نیاز دارید، نمایه خود را قفل (lock) کنید. نحوه فعال سازی:

https://www.facebook.com/help/196419427651178

- از یک برنامه مدیریت رمز عبور[84] استفاده کرده و یک رمز عبور پیچیده انتخاب کنید. به صورت متواتر رمز عبور خود را تغییر دهید. هرگز از یک رمز عبور در چندین وب سایت استفاده نکنید. برای ایجاد رمزهای قوی دو دریافت برنامه مدیریت رمز عبور:

https:/www.dashlane.com
https://www.stickypassword.com
https://www.lastpass.com/features/password-generator
https://www.passwordboss.com

- در صورت استفاده از کامپیوتر که از خود شما نیست، ملاحظات ایمنی را در نظر گرفته و با امنیت وارد حساب فیسبوک خود شوید. برای استفاده خصوصی تر از اینترنت می توانید از یک شبکه خصوصی مجازی (VPN) استفاده کنید .ابتدا امنیت مرورگر را بررسی کنید .گزینه ذخیره رمز عبور را پس از اتمام کار و خروج از حساب کاربری انتخاب نکنید.

- مراقب حملات فیشینگ باشید .هرگز اجازه ندهید حساب های جعلی شما را فریب دهند تا اطلاعات ورود به حساب خود را ارائه دهید .آنها معمولاً پیام های ساختگی را ارسال می کنند و درخواست میدهند تا رمز عبور تان را تغییر دهید.

- اگر حساب کاربری شما به خطر افتاده است رمز عبور خود را تغییر دهید .اگر قادر به تغییر رمز عبور خود نیستید، به پیوند راهنما مراجعه کنید .اطلاعات بیشتر:

https://www.facebook.com/help/203305893040179

- جدول زمانی (timeline)، پست ها و برچسب های (tags) خود را کنترل کنید. چطور این کار را بکنیم:

https://www.facebook.com/help/203305893040179

[84] Password Manager

- لطفا گوشی خود را باز نگذارید و آن را به شخص دیگری ندهید. حساب های فیسبوک در اکثر گوشی ها به راحتی قابل دسترسی هستند. بنابراین، هر کسی که به تلفن همراه شما دسترسی داشته باشد می تواند به حساب شما دسترسی داشته باشد.
- از کلیک بر روی هر لینک مشکوک خودداری کنید. در عوض، تنها پس از تأیید صحت یک پیوند، روی آن کلیک کنید. اطلاعات بیشتر:

https://www.facebook.com/help/166863010078512

توییتر (Twitter)

- احراز هویت دو مرحله ای (Two-factor authentication) به محافظت از حساب توییتر شما کمک می کند. این یک لایه امنیتی اضافی برای حساب توییتر شما است. نحوه فعال سازی:

https://help.twitter.com/en/managing-your-account/two-factor-authentication

لطفاً تا زمانی که احراز هویت دو مرحله‌ای فعال است، گوشی خود را باز نگذارید و آن را به شخص دیگری ندهید.

- از یک برنامه مدیریت رمز عبور استفاده کنید. یک رمز عبور پیچیده ایجاد کنید و آن را به طور مکرر تغییر دهید. هرگز از رمز عبور قدیمی و رمز عبور یکسان برای چندین حساب استفاده نکنید. برنامه های مدیریت رمزهای عبور:
-

https:/www.dashlane.com
https://www.stickypassword.com
https://www.lastpass.com/features/password-generator
https://www.passwordboss.com

- توییت های خود را، چه عمومی و چه خصوصی، مدیریت کنید. شما می توانید حریم خصوصی توییت های خود را کنترل کنید:

https://help.twitter.com/en/safety-and-security/how-to-make-twitter-private-and-public
https://help.twitter.com/en/safety-and-security/public-and-protected-tweets

- مکان توییت خود را کنترل کنید و مکان کشور حساب خود را پنهان کنید.

https://help.twitter.com/en/using-twitter/tweet-location
https://help.twitter.com/en/managing-your-account/how-to-change-country-settings

- اگر از کامپیوتری استفاده می کنید که از شما نیست، با درنظرداشت ملاحظات ایمنی وارد حساب توییتر خود شوید. برای استفاده خصوصی تر از اینترنت می توانید از یک شبکه خصوصی (VPN) استفاده کنید. ابتدا امنیت مرورگر را بررسی کنید. گزینه ذخیره رمز عبور را انتخاب نکنید. پس از اتمام کار تان، از حساب کاربری خارج شوید.

- اگر حساب شما به خطر افتاده است، اما هنوز می توانید وارد شوید، می توانید حساب خود را ایمن کنید و رفتارهای اجتناب پذیر را متوقف کنید. اگر قادر به ورود به حساب کاربری خود نیستید، به (help with a potentially hacked account) بروید و روی آن کلیک کنید. چطور این کار را بکنیم:

https://help.twitter.com/en/safety-and-security/twitter-account-compromised

- به طور پیش فرض[85]، کاربران می توانند از آدرس ایمیل و شماره تلفن شما برای پیدا کردن شما در توییتر استفاده کنند. علاوه بر این، موتورهای جستجو می توانند توییتر شما را نیز کشف کنند. می‌توانید قابلیت کشف خود را از طریق ایمیل، تلفن و موتورهای جستجو کنترل کنید. نحوه فعال سازی:

https://help.twitter.com/en/safety-and-security/email-and-phone-discoverability-settings
https://help.twitter.com/en/safety-and-security/remove-twitter-profile-from-google-search

- با فعال کردن و غیرفعال کردن (برچسب‌گذاری «Tagging»، قابلیت کشف «Discoverability»، ردیابی آگهی و دیتا «Ads and Data Tracking »، فیلتر کیفیت «the Quality Filter »، پنهان کردن محتوای حساس « Hide Sensitive Content »، مسدود کردن و بی‌صدا کردن حساب‌ها «Block and Mute Accounts »، بی‌صدا کردن کلمات «Mute Words »، بستن DM و گزارش حساب‌ها« Shut Down your DMs and Reporting Accounts ») می‌توانید توییت‌های خود را کنترل کنید و با خیال راحت از توییتر استفاده کنید. نحوه فعال و غیرفعال کردن:

https://help.twitter.com/en/safety-and-security/control-your-twitter-experience

انستاگرام (INSTAGRAM)

- احراز هویت دو مرحله ای (Two-factor authentication) به محافظت از حساب اینستاگرام و رمز عبور شما کمک می کند. این یک ویژگی امنیتی است که برای امنیت حساب شما ضروری پنداشته میشود. نحوه فعال سازی:

https://help.instagram.com/566810106808145

- از یک برنامه مدیریت رمز عبور استفاده کنید. یک رمز عبور پیچیده ایجاد کنید و آن را به صورت تصادفی تغییر دهید. هرگز از رمز عبور قدیمی و رمز عبور یکسان برای چندین حساب استفاده نکنید. برنامه های مدیریت رمزهای مفید:

https:/www.dashlane.com
https://www.stickypassword.com
https://www.lastpass.com/features/password-generator
https://www.passwordboss.com

[85] Default

- در انستا گرام، شما کنترل اینکه چه کسی شما را دنبال کند، چه کسی عکس های شما را می بیند و چه کسی می تواند روی آنها نظر دهد در دست شماست. علاوه بر این، می توانید کنترل کنید که چه کسی به حساب اینستاگرام شما دسترسی دارد. نحوه فعال و غیرفعال کردن:

https://help.instagram.com/116024195217477

- تنظیمات و اطلاعات حریم خصوصی خود را کنترل کنید. چگونگی تنظیم:

https://help.instagram.com/196883487377501
https://help.instagram.com/377830165708421/?helpref=hc_fnav

- اگر حساب شما به خطر افتاده است یا فکر می‌کنید حسابتان هک شده یا به خطر افتاده است، می‌توانید مراحل متعددی را با استفاده از وب‌سایت یا برنامه برای ایمن کردن حساب خود انجام دهید. چطور این کار را بکنیم:

https://help.instagram.com/149494825257596

- می توانید کاربران را در اینستاگرام بلاک کنید. راه های زیادی برای بلاک کردن افراد در اینستاگرام وجود دارد:

https://help.instagram.com/426700567389543/?helpref=hc_fnav

- می‌توانید با استفاده از ویژگی‌های گزارش داخلی اینستاگرام، هرزنامه‌ها[86]، پست‌های ناخوشایند، نظرات یا افرادی را که شرایط اجتمای اینستاگرام را نقض می‌کنند گزارش دهید. چطور این کار را بکنیم:

https://help.instagram.com/165828726894770/?helpref=hc_fnav

تیک تاک (TikTok)

- قبل از استفاده ازTikTok ، باید رهنمود چهارگانه ایمنی آنرا (safety guides) که شامل رهنمود آگهی‌ها و دیتا (Ads and Your Data)، رهنمود رفاه (Well-being Guide) ، راهنمای کاربر جدید (New User Guide)، و رهنمود متولیان و والدین (Guardian’s Guide) را مطالعه کنید. شما می توانید راهنماها را از اینجا دریابید:

https://www.tiktok.com/safety/en/

- احراز هویت دو مرحله‌ای، که TikTok آنرا به صورت پیش فرض فعال می‌کند، هر بار که وارد سیستم می‌شوید، تأیید بیشتری ایمنی را ضروری می‌سازد. این کار حساب و رمز عبور شما را ایمن نگه می‌دارد. در اینجا نحوه فعال کردن احراز هویت دو مرحله ای بیان شده است:

https://www.tiktok.com/safety/youth-portal/keep-your-account-secure?lang=en

[86] spams

- برای ایجاد رمز عبور از برنامه مدیریت رمز عبور استفاده کنید. یک رمز عبور پیچیده ایجاد کنید و معمولاً آن را تغییر دهید:

https://support.tiktok.com/en/log-in-troubleshoot/log-in/reset-password

هرگز از رمز عبور قدیمی و رمز عبور یکسان برای چندین حساب استفاده نکنید. برنامه های مدیریت رمز عبور که می توانند به شما کمک کنند:

https:/www.dashlane.com
https://www.stickypassword.com
https://www.lastpass.com/features/password-generator
https://www.passwordboss.com

- می‌توانید یک حساب خصوصی داشته باشید، اما فقط افرادی که به آنها اجازه می‌دهید می‌توانند شما را دنبال کنند و ویدیوها، ویدیوهای زنده، بیو، لایک‌ها و همچنین لیست فالوورها و فالوورهای شما را مشاهده کنند. اگر یک حساب خصوصی داشته باشید، سایر کاربران نمی توانند ویدیوهای شما را دوئت (duet) کنند، بپیچند یا دانلود کنند. در اینجا نحوه خصوصی یا عمومی کردن حساب بیان شده است:

https://support.tiktok.com/en/account-and-privacy/account-privacy-settings/making-your-account-public-or-private

- می‌توانید افرادی را که می خواهند شما را در TikTok و موتورهای جستجو دنبال کنند محدود کنید. اگر می‌خواهید افرادی که می‌توانند به حساب TikTok شما دسترسی داشته باشند محدود کنید، به گزینه تنظیمات در گوشه سمت راست بالای نمایه خود بروید:

https://support.tiktok.com/en/account-and-privacy/account-privacy-settings/suggested-accounts

- برای حفظ حریم خصوصی بیشتر، باید موقعیت مکانی خود را در TikTok خاموش کنید. در اینجا نحوه غیرفعال کردن خدمات مکان در TikTok آمده است:

https://support.tiktok.com/en

- از کلاهبرداری های فیشینگ با خبر باشید. مهاجمان اغلب از پیام‌های جعلی استفاده می‌کنند که به عنوان فیشینگ نیز شناخته می‌شوند تا قربانیان را متقاعد کنند که اطلاعات حساسی از جمله رمز عبور، شماره کارت اعتباری، و سایر اطلاعات شخصی را فاش کنند. ایمیل، اس ام اس (پیام متنی)، ارتباطات درون برنامه ای و برنامه های پیام رسانی همگی می توانند برای ارسال پیام های جعلی یا فیشینگ استفاده شوند. در اینجا می توانید نحوه جلوگیری از فیشینگ را بیابید:

https://support.tiktok.com/en/safety-hc/account-and-user-safety/avoid-fraudulent-message-attacks-on-tiktok

یوتیوب (YouTube)

- از احراز هویت دو مرحله ای یا تأیید دو مرحله ای برای افزایش ایمنی و امنیت حساب های Google خود از جمله حساب YouTube استفاده کنید. با این کار می توانید در صورت به خطر افتادن رمز عبور، امنیت حساب خود را تقویت بخشید. پس از فعال سازی، می توانید با استفاده از تلفن یا رمز عبور خود به حساب خود دسترسی پیدا کنید. در اینجا نحوه انجام آن آمده است:

https://support.google.com/accounts/answer/185839?hl=en&co=GENIE.Platform%3Ddesktop

- با کلیک روی تنظیمات Safety Mode درYouTube ، حالت ایمنی YouTube را روشن نگه دارید. این عملکرد می تواند به فیلتر کردن محتوای اعتراض آمیز و ناخواسته بزرگسالان کمک کند. در اینجا نحوه انجام آن آمده است:

https://support.google.com/youtube/answer/174084?hl=en&co=GENIE.Platform%3Ddesktop

- از یک برنامه مدیریت رمز عبور استفاده نموده و یک رمز عبور پیچیده ایجاد کنید. به صورت تصادفی رمز عبور خود را تغییر دهید. هرگز از یک رمز عبور در بسیاری از وب سایت ها استفاده نکنید. برنامه های مدیریت رمز عبور که می توانند به شما در داشتن رمز عبور قوی کمک کنند:

https:/www.dashlane.com
https://www.stickypassword.com
https://www.lastpass.com/features/password-generator
https://www.passwordboss.com

- در صورت استفاده از کامپیوتری که مال شما نیست، با نظرداشت مراحل ایمنی وارد حساب YouTube خود شوید. برای استفاده خصوصی تر از اینترنت می توانید از یک شبکه خصوصی مجازی (VPN) استفاده کنید. ابتدا امنیت مرورگر را بررسی کنید. گزینه ذخیره رمز عبور را انتخاب نکنید. پس از اتمام کار، از حساب کاربری خارج شوید.

- یک حساب YouTube در معرض خطر را می توان برگرداند. این پلتفورم متعلق به گوگل است. اگر تصور می کنید حساب YouTube شما هک، تصرف یا به نوعی در معرض خطر قرار گرفته باشد، می توانید دستورالعمل هایی را برای بازیابی آن دنبال کنید. در اینجا نحوه بازیابی آن آمده است:

https://support.google.com/youtube/answer/76187?hl=en

- طوریکه تذکر رفت یوتیوب متعلق به گوگل است. می توانید با تقویت امنیت و ایمنی حساب Gmail خود که به YouTube پیوند داده اید، ایمنی آنرا بهبود بخشید:

https://support.google.com/youtube/answer/76187?hl=en#zippy=%2Crequired—step-verification-for-creators-in-the-youtube-partner-program

- حساب خود را از ارتباطات و دادن اطلاعات به افراد ناشناس ایمن کنید که به این فیشینگ میگویند و آن زمانی اتفاق می افتد که یک هکر به عنوان یک فرد قابل اعتماد برای سرقت اطلاعات شخصی ظاهر می شود و میخواهد دیتای شما را بدزدد. دیتای شخصی ممکن است شامل موارد زیر باشد:

- اطلاعات مالی
- اطلاعات شخصی (نمبر کارت هویت، پاسپورت، و غیره)
- اعداد روی کارت های اعتباری
- هکرها ممکن است از ایمیل‌ها، متن‌ها یا وبسایت‌هایی استفاده کنند تا خود را به عنوان یک موسسه با اعتبار، خویشاوند یا همکار شما نشان دهند.

- توجه داشته باشید که رمز عبور تان، آدرس ایمیل یا هر اطلاعات حساب دیگری هرگز توسط YouTube درخواست نخواهد شد. اگر کسی با شما تماس می گیرد که از YouTube است، اعتماد نکنید:

https://support.google.com/youtube/answer/9701986?hl=en&ref_topic=7071231

- اگر احساس ناامنی و فقدان ایمنی می‌کنید، کانال YouTube خود را پنهان یا حذف کنید، می‌توانید کانال خود را به طور کامل حذف کنید یا به طور موقت برخی از مطالب را در آن پنهان کنید. توجه داشته باشید که اگر یک کانال YouTube را پنهان یا غیرفعال کنید، پست‌ها، نظرات و پاسخ‌های شما برای همیشه حذف می‌شوند:

https://support.google.com/youtube/answer/55759?hl=en&ref_topic=7071231

- در نهایت، همانطور که گفته شد، ایمن نگه داشتن حساب YouTube شما خطر هک شدن، تصرف یا به خطر افتادن آن یا کانال شما را کاهش می دهد. به یاد داشته باشید که چگونه از حساب خود محافظت کنید اگر فکر می کنید در معرض خطر قرار گرفته است، نکات ذیل را در نظر بگیرید:

- یک رمز عبور پیچیده ایجاد کنید و آن را به خاطر بسپارید.
- از رمز عبور خود در برابر هکرها محافظت کنید.
- از رمز عبور قدیمی استفاده نکنید
- از رمز عبور یکسان برای حساب های متعدد استفاده نکنید.
- هرگز جزئیات ورود خود را فاش نکنید.
- بررسی های امنیتی معمولی را انجام دهید.
- گزینه هایی را برای بازیابی حساب به روز کنید یا اضافه کنید.
- هویت دو مرحله ای را روشن کنید.
- کاربران مشکوک را از حساب خود حذف کنید و وب سایت ها و برنامه های غیر ضروری متصل را حذف کنید.
- نرم افزار خود را به روز کنید و از حساب کاربری تان پشتیبان[87] داشته باشید.
- از درخواست های مشکوک دوری کنید.
- از وب سایت های مشکوک دوری کنید.
- هر نوع فیشینگ و یا اسپم را گزارش کنید.

[87] backup

نکات مهم ابزارهای ارتباطات رسانه های اجتماعی

جیمیل (Gmail)

- از استفاده از نام کامل تان در حساب خود اجتناب کنید. شما باید نام اصلی و نام خانوادگی خود را در حساب تان خصوصی نگه دارید. حساب تان را با نام جعلی یا لقب تان بسازید:

https://support.google.com/accounts/answer/6304920?hl=en&co=GENIE.Platform%3DDesktop

- از یک برنامه مدیریت رمز عبور استفاده و یک رمز عبور پیچیده ایجاد کنید. به صورت متواتر رمز عبور خود را تغییر دهید. هرگز از یک رمز عبور در سایر حساب ها استفاده نکنید. برنامه های مدیریت رمز عبور که می تواند به شما در داشتن رمز عبور قوی کمک کند:

https:/www.dashlane.com
https://www.stickypassword.com
https://www.lastpass.com/features/password-generator
https://www.passwordboss.com

- مدیریت حریم خصوصی آنلاین شما در تمام سرویس های Google اولویت شماست. شما میتوانید برخی از اطلاعات حساب Google تان را عمومی یا خصوصی کنید. سپس می‌توانید تصمیم بگیرید که چه کسی می‌تواند به اطلاعاتی مانند تاریخ تولد یا شماره تلفن شما در همه سرویس‌های Google دسترسی داشته باشد.

https://support.google.com/accounts/answer/6304920?hl=en&co=GENIE.Platform%3DDesktop

- احراز هویت دو مرحله ای عامل کلیدی در ایمن سازی حساب های Gmail و یا Google شما است. برای ایمن کردن حساب های گوگل خود از احراز هویت دو مرحله ای استفاده کنید. با این کار، برای جلوگیری از ورود هکرها به حساب خود یک لایه حفاظتی دیگر اضافه کرده اید. وقتی وارد سیستم می‌شوید، احراز هویت دو مرحله ای به اطمینان از حفظ حریم خصوصی، امنیت و ایمنی اطلاعات شخصی شما کمک می‌کند:

https://support.google.com/accounts/answer/185839?hl=en&co=GENIE.Platform%3DAndroid

- در صورت استفاده از کامپیوتری که از شما نیست، با در نظرداشت مراحل ایمنی وارد حساب Gmail خود شوید. برای استفاده خصوصی تر از اینترنت می توانید از یک شبکه خصوصی مجازی (VPN) استفاده کنید. ابتدا امنیت مرورگر را بررسی کنید. ابروها به صورت خصوصی گزینه ذخیره رمز عبور را انتخاب نکنید. پس از اتمام کار، از حساب کاربری خارج شوید. برای اطلاعات بیشتر:

https://support.google.com/accounts/answer/2917834?hl=en&co=GENIE.Platform%3DDesktop

- یک حساب کاربری Gmail در معرض خطر را می توان نجات داد. اگر ممکن است Gmail شما هک شده باشد، تصرف شده باشد، یا به نحوی در معرض خطر قرار گرفته باشد، برای بازیابی آن، می توانید دستورالعمل هایی را دنبال کنید. برای نحوه بازیابی آن به اینجا مراجعه کنید:

https://support.google.com/accounts/answer/6294825?hl=en

- حساب Gmail خود را در برابر فیشینگ ایمن کنید. فیشینگ استفاده از ایمیل‌های جعلی، پیام‌ها، تبلیغات یا وبسایت‌هایی است که از وبسایت‌های قانونی که شما اغلب بازدید می‌کنید، برای سرقت اطلاعات شخصی یا دسترسی به حساب‌های آنلاین تقلید می‌کنند. آنها معمولا:

  - در مورد جزئیات مالی یا شخصی شما میپرسند.
  - از شما میخواهند نرم افزار را دانلود کنید یا روی یک لینک کلیک کنید.
  - خود را به عنوان یک شرکت معتبر، مانند بانک، پلتفرم رسانه اجتماعی که شما استفاده می کنید یا سایت کار شما معرفی کند.
  - وانمود میکنند که فردی هستند که می شناسید، مانند یکی از اقوام، آشنایان یا همکاران.
  - دقیقاً پیامی برای شما میفرستند که شما از یک منبع با اعتماد دریافت می کنید.

- از این نکات برای دوری از درخواست ها و پیام های گمراه کننده استفاده کنید:

  - به هشدارهای گوگل توجه کنید.
  - هرگز اطلاعات شخصی را در صورت درخواست ارائه ندهید.
  - هرگز پس از کلیک روی پیوند پیام، رمز عبور خود را وارد نکنید.
  - مراقب ارتباطاتی باشید که خیلی فوری و عالی به نظر میرسند.
  - قبل از اینکه کلیک کنید، توقف کنید و فکر کنید.
  - برای شناسایی ایمیل های فیشینگ، از Gmail استفاده کنید.
  - از قابلیت مرورگر ایمن Chrome استفاده کنید.
  - هرگونه رمز عبور ذخیره شده مشکوک را بررسی کنید.
  - با تنظیم احراز هویت دو مرحله ای از رمز عبور حساب Google خود محافظت کنید.
  - در صورت دریافت ایمیل فیشینگ، گزارشی به Google ارسال کنید.

https://support.google.com/mail/answer/8253?hl=en

- امنیت حساب خود را تقویت کنید. گوگل به ایمنی آنلاین متعهد است. توصیه می شود که به‌منظور محافظت از حساب Google خود، اقدامات ذکر شده زیر را به‌طور منظم انجام دهید.

  - بررسی امنیتی انجام دهید.
  - نرم افزار خود را به روز رسانی کنید.
  - از رمزهای عبور ایمن، پیچیده و منحصر به فرد استفاده کنید.
  - هر گونه برنامه افزودنی و برنامه های غیر ضروری مرورگر را حذف کنید.
  - روی پیام‌ها و محتواهای مشکوک کلیک نکنید.

https://support.google.com/accounts/answer/46526?hl=en&ref_topic=7189123

لطفا توجه داشته باشید که Google و Yahoo ایمنی ترین خدمات ایمیل را ارائه نمی دهند. هیچ یک از آنها پیام های شما را به صورت سرتاسر رمزگذاری[88] نمی کنند .

یاهو (Yahoo)

- از استفاده نام کامل خود در Yahoo خود داری کنید. شما باید نام و نام خانوادگی خود را خصوصی نگه دارید. نام جعلی یا لقب باید ارائه شود. در Yahoo Mail ، نام ارسال خود را با استفاده از مراحل زیر تغییر دهید:

- وارد Yahoo Mail شوید.
- روی تنظیمات (Setting)کلیک کنید.
- روی (Mailbox) کلیک کنید .
- حسابی را انتخاب کنید که نیاز به ویرایش دارد.
- برای تغییر یا حذف نام ارسالی خود، روی لینک "Your Name" کلیک کنید.
- سپس روی (save) کلیک کنید.

https://help.yahoo.com/kb/SLN28072.html

- **اولین خط دفاع شما در برابر هکرها و کلاهبرداران یک رمز عبور قوی است. در اینجا چند نکته مفید برای ایجاد رمز عبور قوی وجود دارد که دیتای شما را ایمن نگه می دارد. برای ایجاد رمز عبور قوی:**

- **از کلمات منحصر به فرد استفاده کنید.**
- **دارای ۱۲ حرف و کاراکتر یا بیشتر باشد.**
- **رمز عبور تان را با استفاده از اطلاعات شخصی تان نسازید.**
- **از حروف، اعداد و کاراکتر های تکراری جلوگیری کنید.**
- **برای هر حساب کاربری از یک رمز عبور متفاوت استفاده کنید.**
- **از عبارات در ایجاد رمز عبور تان استفاده کنید.**
- **از یک رمز عبور استفاده کنید که قبلا استفاده نکرده باشید.**
- **از نرم افزار آنتی ویروس برای کامپیوتر خود استفاده کنید.**
- **رمز عبور خود را با تغییر مرتب آن حفظ کنید.**
- **برای ورود به سایت Yahoo.com مراجعه کنید.**
- **مراقب باشید - وقتی از شما خواسته میشود که رمز عبور خود را تغییر دهید.**
- **به جای کلیک کردن روی پیوند در ایمیل، URL را در نوار آدرس مرورگر[89] خود تایپ کنید.**
- **از کلید حساب[90] استفاده کنید - اگر نگران دزدیده شدن رمز عبور خود هستید.**

https://in.help.yahoo.com/kb/SLN3012.html

- همچنین می توانید با استفاده از لینک های زیر از برنامه های مدیریت رمز عبور استفاده کنید.

[88] End-to-end encryption
[89] browser menu bar
[90] account key

https:/www.dashlane.com
https://www.stickypassword.com
https://www.lastpass.com/features/password-generator
https://www.passwordboss.com

- Yahoo ادعا میکند که به حریم خصوصی شما احترام میگذارد. از طریق داشبورد حریم خصوصی می توانید از نحوه استفاده از اطلاعات خود را با محصولات Yahoo مشاهده و مدیریت کنید:

https://in.help.yahoo.com/kb/viewing-managing-account-data-sln28671.html

- احراز هویت دو مرحله‌ای را فعال کنید تا هنگام تلاش برای ورود به سیستم از یک دستگاه یا مرورگر جدید، کدی علاوه بر رمز عبور شما درخواست شود. برای استفاده از تأیید صحت دو مرحله‌ای، اگر در حال حاضر برای ورود به سیستم از آن استفاده می‌کنید، باید کلید حساب Yahoo را غیرفعال کنید:

https://help.yahoo.com/kb/SLN5013.html

- در صورت استفاده از کامپیوتری که مال شما نیست، با در نظرداشت مراحل ایمنی وارد حساب خود شوید. برای استفاده خصوصی تر از اینترنت می توانید از یک شبکه خصوصی مجازی (VPN) استفاده کنید. ابتدا امنیت مرورگر را بررسی کنید. گزینه ذخیره رمز عبور را انتخاب نکنید. پس از اتمام کار، از حساب کاربری خارج شوید. برای اطلاعات بیشتر:
https://ph.help.yahoo.com/kb/sln5283.html?redirect=true

- اگر فرض می کنید حساب شما به خطر افتاده است، مراحل زیر را برای ایمن سازی آن دنبال کنید:

  - بلافاصله رمز عبور خود را تغییر دهید.
  - رمزهای عبور اپلیکیشن را که تأیید نمی کنید حذف کنید.
  - بررسی کنید که آیا گزینه های بازیابی شما به روز هستند یا خیر.
  - در صورت تغییر تنظیمات ایمیل تان، آنها را به شکلی که خود تان میخواهید برگردانید.
  - مطمئن شوید که نرم افزار انتی وایروس را در کامپیوتر شخصی خود نصب و به روز کرده اید.
  - از کلید حساب یا تأیید دو مرحله ای استفاده کنید تا مطمئن شوید حساب شما دارای یک لایه امنیتی اضافی است.

https://help.yahoo.com/kb/SLN2090.html

لطفا توجه داشته باشید که گوگل و یاهو امن ترین خدمات ایمیل را ارائه نمی دهند. هیچ یک از آنها پیام های شما را به صورت سرتاسر رمزگذاری نمی کنند.

مسنجر (Messenger)

- از رمزگذاری سرتاسر در پیام رسان خود استفاده کنید. در یک مکالمه، رمزگذاری سرتاسر امنیت و حفاظت بیشتری را اضافه می‌کند تا فقط شما و شخص دیگر بتوانید پیام‌ها و تماس‌هایی را که تبادله می‌کنید ببینید، بشنوید یا بخوانید. مسنجر دیگر از حالت Vanish پشتیبانی نمی کند. در یک چت رمزگذاری سرتاسر، کاربران همچنان می توانند پیام های ناپدید شده را ارسال کنند:

https://www.facebook.com/help/messenger-app/1084673321594605

- در مسنجر، می‌توانید با تصمیم‌گیری در مورد اینکه چه کسی می‌تواند وضعیت فعال شما را ببیند، انتخاب مخاطب برای استوری‌ها، استفاده از مکالمات مخفی و موارد دیگر، حریم خصوصی خود را مدیریت کنید. در اینجا نحوه مدیریت حریم خصوصی در مسنجر بیان شده است:

https://www.facebook.com/help/messenger-app/408883583307426?helpref=faq_content

- می توانید کنترل کنید چه کسانی به لیست چت شما دسترسی دارند. اگر شخصی در فیسبوک برای شما پیامی ارسال کند، اما شما با آنها مرتبط نباشید، درخواست پیام دریافت خواهید کرد. به یاد داشته باشید که پاسخ به درخواست پیام، ارتباطی بین شما و فرستنده برقرار می کند و هر محتوایی را که برای شما ارسال کرده قابل مشاهده میباشد. اینجا،
- نحوه محدود کردن افرادی که در مسنجر می توانند با شما چت جدیدی را شروع کنند بیاموزید:

https://www.facebook.com/help/936247526442073?helpref=related&source_cms_id=907368596013605
https://www.facebook.com/help/messenger-app/2258699540867663?helpref=faq_content

- اگر افرادی هستند که نمی خواهید از آنها بشنوید، آنها را بلاک کنید، مخفی کنید یا بی صدا کنید. می توانید اعلان های پیام رسان را برای همه مکالمات کنترل کنید. نحوه نادیده گرفتن و بلاک کردن افراد در مسنجر را در اینجا بیاموزید:

https://www.facebook.com/help/messenger-app/204908296312159?helpref=faq_content
https://www.facebook.com/help/messenger-app/1245152242249842?helpref=faq_content
https://www.facebook.com/help/messenger-app/330627630326605?helpref=faq_content

- اگر متوجه کلاهبرداران شدید، از پاسخ دادن خودداری کنید و کلاهبردار را به مسنجر گزارش دهید:

https://www.facebook.com/help/messenger-app/833709093422928?helpref=faq_content

- در تلفن هوشمند خود، می توانید برنامه را لاک کنید. می‌توانید ویژگی لاک برنامه مسنجر را برای دستگاه Android یا iOS خود فعال کنید تا امنیت و حریم خصوصی بیشتری برای حساب مسنجر شما فراهم شود:

https://www.facebook.com/help/messenger-app/2585155295072006?locale=en_US&helpref=faq_content

- برای امنیت و ایمنی بیشتر مسنجر لطفا به آدرس زیر مراجعه کنید:

https://www.facebook.com/help/messenger-app/1064701417063145/?helpref=hc_fnav

توجه: شما می توانید با استفاده از حساب فیسبوک خود به مسنجر دسترسی پیدا کنید زیرا مسنجر به فیسبوک پیوند داده شده است. هم مسنجر و هم فیسبوک متعلق به Meta هستند. لطفاً برای اطلاعات بیشتر در مورد امنیت و ایمنی مسنجر خود به جزئیات ایمنی فیسبوک مراجعه کنید.

واتس‌اپ (WahtsApp)

- هرگز کد تأیید واتس اپ خود را برای کسی فاش نکنید. کد تأیید پیام صادر شده به شماره تلفن شما جهت کنترل حساب شما در صورت تلاش افراد برای انجام این کار ضروری است. بدون این کد، هر کسی که بخواهد شماره تلفن شما را کسب کند، نمی تواند این کار را انجام دهد و از شماره شما در واتس اپ استفاده کند. این بدان معناست که حساب WhatsApp شما هنوز تحت کنترل شما است:

https://faq.whatsapp.com/619670298808780/?locale=en_US

- تأیید دو مرحله ای را فعال کنید و آدرس ایمیل خود را وارد کنید تا در صورت گم شدن پیام، یادآوری دریافت کنید:

https://faq.whatsapp.com/585667085685460/?locale=en_US

- می توانید یک کد دستگاه تنظیم کنید. برای استفاده همزمان از واتس اپ روی حداکثر چهار دستگاه متصل، لازم نیست تلفن خود را متصل نگه دارید. در واتس اپ، هر بار یک گوشی را می توان متصل کرد:

https://faq.whatsapp.com/381777293328336/?locale=en_US

- واتس‌اپ رمزگذاری سرتاسری را برای همه پیام‌هایی که ارسال و دریافت می‌کنید ارائه می‌کند تا اطمینان حاصل شود که فقط شما و شخصی که با او صحبت می‌کنید می‌توانید پیام‌های شخصی‌تان را بخوانید یا گوش دهید. در اینجا نحوه فعال سازی آمده است:
https://faq.whatsapp.com/629089898272226/?locale=en_US

- اگر شما فریب خورده اید و کد WhatsApp خود را فاش کرده اید و دسترسی به آن را از دست داده اید، مراحل ذکر شده در زیر می تواند به شما کمک کند تا دوباره به حساب WhatsApp خود دسترسی پیدا کنید:

https://faq.whatsapp.com/690494414810591/?locale=en_US

- در صورت نیاز می توانید چت ها را در WhatsApp مخفی کنید. با استفاده از ویژگی چت بایگانی، می توانید گفتگوهای خود را با مخفی کردن یک چت فردی یا گروهی خاص از لیست چت های خود بهتر سازماندهی کنید:

https://faq.whatsapp.com/154568698849853/?helpref=search&query=hide%20chats&search_session_id=a71f37c78ad24eb384f8975249d20c9f&sr=8

- اگر شماره شما در یک چت گروپ توسط کسی که شماره شما را دارد اضافه شود، تمام اشخاصی که در گروپ عضو هستند، چه شماره شما را داشته باشند و یا نداشته باشند، شماره شما، اسم شما و عکس پروفایل شما را میبینند.

- برای جزئیات بیشتر در مورد ایمنی و امنیت چت های خود در واتس اپ، لطفاً به آدرس زیر مراجعه کنید:

https://faq.whatsapp.com

وایبر (Viber)

- وایبر به طور پیش فرض دارای رمزگذاری سرتاسراست. دستگاه شما پیام هایی را به عنوان یک کد رمزگذاری شده به دستگاه گیرنده ارسال می کند که فقط آن دستگاه می تواند با استفاده از یک کلید رمزگذاری رمزگشایی کند تا به صورت متن ساده نشان داده شود. کلیدهای رمزگذاری فقط در دستگاه های کاربر و هیچ جای دیگر وجود ندارد. بنابراین، هیچ کس نمی تواند پیام های شما را ببیند، حتی خود وایبر:
https://www.viber.com/en/security/

- وایبر دارای ویژگی پیام‌های ناپدید شده است. برای هر پیام در چت خود یک تایمر خود-تخریبی تنظیم کنید تا اطمینان حاصل کنید که پیام شما پس از خوانده شدن توسط همه طرف های دخیل، به طور خودکار از چت وایبر پاک شود. همچنان، در حالی که مکالمه روشن است، اقدامات مربوط به اسکرین شات ها گزارش می شود:

https://www.viber.com/en/security/

- ویرایش و حذف همه پیام ها امکان پذیر است. ارسال پیامی که دارای اشتباه تایپی است ممکن است خسته کننده باشد، اما نگران نباشید - فقط روی پیام کلیک کنید تا به سرعت آن را برطرف نمایید. اگر می خواهید، حتی میتوانید پیامی را که دیده شده باشد، در مکالمه ارسال شده پاک کنید. آنچه شما افشا می کنید به شما بستگی دارد:

https://www.viber.com/en/security/

- در وایبر، می توانید از چت های مخفی با شماره استفاده کنید. هنگامی که با افراد جدیدی در یک گروه آشنا می‌شوید، فوراً چت امن‌تری را شروع کنید یا آن‌ها را در Viber با جستجوی نام، بدون نیاز به فاش کردن یا مبادله شماره تلفن خود یا آنها پیدا کنید:
https://www.viber.com/en/security/

- می توانید از مخفی کردن چت ها در وایبر به طور موثرتری استفاده کنید. اگر شما نمی خواهید کسی حین چک نمودن گوشی تان چت شما را بخواند و یا هم بشنود، چت ها را می توان از لیست چت شما پنهان کرد و در هر زمان با استفاده از یک پین[91] به آنها دسترسی داشت. فقط شما یک پین تنظیم میکنید:

[91] Pin

https://www.viber.com/en/security/

- اگر متوجه یک «spammer» شدید، این امکان را دارید که هرکسی را که فکر می کنید، بلاک کرده و گزارش دهید. بررسی خودکار «spam» را فعال کنید تا وایبر بتواند پیام‌های دریافتی با محتوای مخرب از مخاطبینی را که در لیست مخاطبین شما نیستند، بررسی کند:

https://help.viber.com/en/article/protect-yourself-and-your-privacy-on-viber

- اگر می خواهید تمام داده های ذخیره شده در دستگاه شخص دیگری حذف شود، حساب Viber خود را غیرفعال کنید. فوراً تمام مکالماتی را که با هرکسی از دستگاه خود و آن‌ها انجام داده‌اید، حذف خواهد شد.

https://help.viber.com/en/article/deactivate-or-uninstall-viber-on-your-phone

تلگرام (Telegram)

- می توانید شماره تلفن خود را در تلگرام مخفی کنید. می توانید بدون فاش کردن شماره تلفن خود در تلگرام به صورت گروهی و در چت های خصوصی پیام ارسال کنید. به طور پیش فرض، فقط مخاطبینی که به عنوان مخاطب به دفترچه آدرس خود اضافه کرده اید می توانند شماره تلفن شما را ببینند. با این حال، می توانید آن را پنهان کنید:

https://telegram.org/faq

- در تلگرام می توانید یک چت مخفی داشته باشید. کاربری که می خواهید با پروفایل او تماس بگیرید باید باز شود. روی «...» و سپس «شروع چت مخفی» کلیک کنید. به خاطر داشته باشید که چت های خصوصی تلگرام مختص همان دستگاه است. در یکی از دستگاه‌هایتان، اگر شما و یکی از دوستانتان مکالمه خصوصی را شروع کنید، فقط آن دستگاه به آن دسترسی خواهد داشت:
https://telegram.org/faq#q-how-are-secret-chats-different

- می توانید از رمزگذاری سرتاسردر تلگرام لذت ببرید. دستگاه‌های شرکت‌کننده از تبادل کلید Diffie-Hellman برای تبادل کلیدهای رمزگذاری هنگام ایجاد یک چت مخفی استفاده می‌کنند. پس از ایجاد اتصال امن سرتاسر، تلگرام یک تصویر گرافیکی ایجاد می کند که نشان دهنده کلید رمزگذاری برای چت شما است. وقتی این تصویر را با دوست خود مقایسه می کنید، اگر این دو عکس یکسان هستند، مطمئن باشید که مکالمه مخفی ایمن است و حمله شخص ثالث[92] نمی تواند موفق شود:

https://telegram.org/faq#q-how-do-i-start-a-secret-chat

- تلگرام احراز هویت دو مرحله ای دارد و می توانید آن را روشن کنید. اگرچه استفاده از کد SMS برای ورود به سیستم یک استاندارد صنعت پیام‌رسانی است، اما اگر می‌خواهید محافظت بیشتری داشته باشید یا دلایلی برای مشکوک بودن به شرکت مخابراتی تلفن همراه یا دولت خود دارید، می‌توانید چت‌های کلاود خود را با یک رمز عبور اضافی ایمن کنید.

[92] Middle Man Attack

https://telegram.org/faq#q-how-does-2-step-verification-work

- بزرگترین مشکل تلگرام این است که همه می توانند شما را در تلگرام پیدا کنند و پروفایل و تصاویر شما را مشاهده کنند. همه افرادی که عضو گروه هستند می توانند نام شما را در لیست اعضا ببینند.بدتر اینکه، شما می توانید از هر کسی پیام دریافت کنید.

https://telegram.org/faq#q-do-you-have-a-privacy-policy

اسکایپ (Skype)

- از یک برنامه مدیریت رمز عبور استفاده کنید و یک رمز عبور پیچیده ایجاد کنید. به صورت تصادفی رمز عبور خود را تغییر دهید. هرگز از رمز عبور قدیمی استفاده نکنید. برنامه های مدیریت رمز عبور که می توانند به شما در داشتن رمز عبور قوی کمک کنند:

https:/www.dashlane.com
https://www.stickypassword.com
https://www.lastpass.com/features/password-generator
https://www.passwordboss.com

- می توانید از رمزگذاری سرتاسردر اسکایپ استفاده کنید. صدا، ویدئو، انتقال فایل و پیام های فوری بین کاربران اسکایپ به اسکایپ همگی رمزگذاری شده اند. این شما را از گوش دادن توسط افراد دیگر محافظت می کند. باید خاطر نشان ساخت که بخشی از تماس شما که از طریق PSTN ، شبکه تلفن معمولی هنگام تماس با تلفن های همراه و تلفن ثابت از Skype عبور می کند، رمزگذاری نشده است:

https://support.skype.com/en/faq/FA31/does-skype-use-encryption

- اسکایپ مربوط به مایکروسافت است. ویژگی امنیتی احراز هویت دو مرحله‌ای مایکروسافت با سخت‌تر کردن دسترسی کاربران غیرمجاز به حساب شما و برای ایمن نگه داشتن Skype شما کمک میکند. در اینجا نحوه فعال کردن آن آمده است:

https://answers.microsoft.com/en-us/skype/forum/all/skype-login-two-factor-authentication/303d1b3b-8827-49b4-bdaa-ea7f823d971c

- اگر حساب شما به خطر افتاده و یا هک شده است، لطفاً به نحوه بازیابی یک حساب مایکروسافت هک شده یا در معرض خطر مراجعه کنید:

https://support.microsoft.com/en-us/account-billing/how-to-recover-a-hacked-or-compromised-microsoft-account-24ca907d-bcdf-a44b-4656-47f0cd89c245

- اگر از شماره تلفنی برای ثبت نام یا ورود به اسکایپ استفاده می کنید یا اگر شماره تلفنی در نمایه خود دارید، افراد می توانند با استفاده از شماره تلفن شما را جستجو کنند تا با شما ارتباط برقرار کنند. اگر تصمیم گرفتید شماره تلفن خود را غیرقابل جستجو کنید، هر لحظه می توانید این کار را انجام دهید:

https://support.skype.com/en/faq/FA34934/can-people-find-me-with-my-phone-number-in-skype

- شما کنترل دارید که چه کسی می تواند به جزئیات نمایه اسکایپ و وضعیت حضور شما دسترسی داشته باشد. برخی از اطلاعات عمومی هستند، اما اگر نمی خواهید در نمایه شما نمایش داده شود، می توانید آن را خالی بگذارید. آدرس ایمیل شما در اسکایپ نمایش داده نمی شود. وقتی به نمایه شما نگاه می کند، هیچ کس نمی تواند آن را ببیند. آدرس ایمیل شما را به جز دوستانی که قبلا آن را دریافت کرده اند نمی توانند برای احراز آن دست یابند:

https://support.skype.com/en/faq/FA34745/who-can-see-my-skype-profile-and-presence-status

- اگر از کامپیوتر کسی دیگر استفاده می کنید که مال شما نیست، با در نظر گفتن تدابیر ایمنی وارد حساب Skype خود شوید. برای استفاده خصوصی تر از اینترنت می توانید از یک شبکه خصوصی مجازی (VPN) استفاده کنید. ابتدا امنیت مرورگر را بررسی کنید. گزینه ذخیره رمز عبور را انتخاب نکنید. پس از اتمام کار، از حساب کاربری خارج شوید.

سیگنال (Signal)

- سیگنال به طور پیش فرض دارای رمزگذاری سرتاسراست. سیگنال به گونه ای ساخته شده است که هرگز داده های خصوصی را جمع آوری یا ذخیره نمی کند. تماس ها و ارتباطات سیگنال همیشه رمزگذاری شده، خصوصی و ایمن هستند، بنابراین نه سیگنال و نه شخص ثالث دیگری میتواند به آنها دسترسی داشته باشن:

https://support.signal.org/hc/en-us/articles/360007318911-How-do-I-know-my-communication-is-private-

- برای پاک نگهداشتن جریان چت خویش، از گزینه پیام های ناپدید شده استفاده کنید. پس از اتمام شمارش معکوس، پیام از دستگاه شما حذف خواهد شد. از این گذشته، شخصی که پیام ناپدید شدنی را دریافت می کند، اگر واقعاً می خواهد یک رکورد از آن داشته باشد، باید با دستگاه دیگری از آن عکس بگیرد در غیر آن بعد از مدت معین ناپدید میشود. در اینجا نحوه انجام آن آمده است:

https://support.signal.org/hc/en-us/articles/360007320771-Set-and-manage-disappearing-messages

- ویرایش و حذف همه پیام ها در سیگنال امکان پذیر است. اگر همچنان می‌خواهید پیامی را که برای همه افراد در مکالمه ارسال شده است پاک کنید، حتی اگر دیده شود می‌توانید این کار را انجام دهید. در اینجا نحوه انجام آن آمده است:

https://support.signal.org/hc/en-us/articles/360007320491-Delete-messages-alerts-or-chats

- صفحه قفل را روی سیگنال تنظیم کنید. آنرا میتوانید با «pin» ، و یا هم با، «TouchID» یا «FaceID» باز کرد. در اینجا نحوه فعال کردن آن آمده است:

https://support.signal.org/hc/en-us/articles/360007059572-Screen-Lock

- «pin» سیگنال کدی است که از ویژگی هایی مانند شناسه هایی که بر اساس شماره تلفن نیستند پشتیبانی می کند. این بدان معنی است که اگر دستگاه تان را گم کنید یا تعویض کنید، «pin» شما می تواند به شما در بازیابی نمایه، تنظیمات، مخاطبین و کاربران مسدود شده کمک کند. یک قفل ثبت نام اختیاری که از پین استفاده می‌کند می‌تواند مانع از ثبت شماره شما توسط شخص دیگری از طرف شما شود. برای اطلاعات بیشتر و تغییر «pin» به آدرس زیر مراجعه کنید:

https://support.signal.org/hc/en-us/articles/360007059792-Signal-PIN

- سیگنال صفحه کلید موجود یا ویرایشگر روش ورودی (IME) را در دستگاه تلفن همراه شما اجرا می کند. می‌توانید صفحه‌کلید ناشناس را فعال کنید تا نرم‌افزار صفحه‌کلید مجازی‌تان را از نظارت بر الگوهای تایپ شما و استفاده از آن اطلاعات برای سفارشی کردن سرویس‌های خود، در صورتی که نگران آن هستید، باز دارد. در اینجا نحوه فعال کردن آن آمده است:

https://support.signal.org/hc/en-us/articles/360055276112-Incognito-Keyboard

- با استفاده از سیگنال می توانید چهره ها را روی عکس ها محو کنید. برای محافظت از حریم خصوصی شما، تمام پردازش ها به صورت محلی، در دستگاه شما انجام می شود. برای رسیدن به آن، «Blur faces» را روشن کنید و چهره‌ها به‌طور خودکار شناسایی و پنهان می‌شوند.

قوانین دولتی در مورد آزادی بیان که بر حقوق دیجیتالی تأثیر می گذارد

در 19 سپتامبر 2021، طالبان یک قانون یازده ماده ای را برای رسانه های خبری و روزنامه نگاران وضع کردند. نه مورد از این مقررات بر نحوه فعالیت رسانه ها و فعالان تأثیر دارد. طبق این قوانین، انتشار یا ارسال هر یک از موارد زیر خلاف قانون است:

- آن موضوعاتی که با اسلام در تضاد باشد نشر نشود.
- در فعالیت‌های رسانه به شخصیت های ملی توهین نشود.
- به حریم ملی و شخصی توهین نشود.
- رسانه ها و خبرنگاران در محتویات خبری تحریف نکنند.
- ژورنالیست‌ها در نوشتار خود اصول ژورنالیستی را مد نظر داشته باشند.
- رسانه‌ها در نشرات خود توازن را مدنظر داشته باشند.
- موضوعاتی که صحت آن معلوم نیست و از سوی مسئولان تایید نشده، در نشر آن احتیاط شود.
- موضوعاتی که بروی افکار عمومی تاثیر منفی دارد و یا روحیه مردم را خراب می کند، در نشر آن احتیاط شود.
- رسانه‌ها در نشر اخبار بی‌طرفی خود را حفظ و هر آنچه را واقعیت است منتشر کنند.
- مرکز رسانه‌های حکومت تلاش می‌کند تا با رسانه‌ها و خبرنگاران همکار باشد و در تهیه گزارش‌ها تسهیلاتی را فراهم کند و رسانه‌ها بعد از این در هماهنگی با این اداره گزارش‌های تفصیلی شان را تهیه خواهند کرد.
- در دفتر رسانه‌های حکومت برای سهولت رسانه‌ها و خبرنگاران، یک فرم مشخص آماده شده تا با همکاری آن گزارش‌ها تهیه شود.

آنها یک چارچوب نظارتی بر اساس ایده ها و میکانیسم هایی ایجاد کردند که با روزنامه نگاری به عنوان یک مسلک حرفوی سازش ندارد. سه ماده اول که روزنامه نگاران را از پخش یا انتشار مطالبی که «مخالف با اسلام»، «توهین به شخصیت های ملی» یا «نقض حریم خصوصی است» منع می کند. موارد مهمی که در قانون قبلی رسانه های افغانستان شامل است در این قانون یازده ماده ای وجود ندارد، که مهمترین آنها رعایت اسناد و قوانین بین المللی مثل میثاق بین المللی حقوق مدنی و سیاسی و اعلامیه جهانی حقوق بشر بود.

فقدان این الزام در قانون جدید، فضا را برای سانسور و سرکوب روزنامه نگاران باز می‌گذارد، زیرا مشخص نیست که چه کسی و بر مبنای چی تصمیم می‌گیرد که مطالب نشر شده نقض حریم خصوصی است یا خیر، توهین به شخصیت های ملی است یا خیر و یا در مخالفت با اسلام است و یا خیر.

سه مورد از این قانون، روزنامه نگاران را به پیروی از آنچه به عنوان استانداردهای اخلاق در نظر گرفته می شود، ملزم میداند. آنها باید «از ارزش‌های روزنامه‌نگاری پیروی کنند»، «تلاش برای تغییر محتوای خبری نداشته باشند» و «اطمینان حاصل کنند که گزارش‌هایشان متعادل است». با این حال، این احکام ممکن است به دلیل عدم موجودیت قوانین بین‌المللی، مورد سوء استفاده یا تفسیر خودسرانه قرار گیرند .

مواد هفت و هشت این قانون، محدودیت های را بالای رسانه ها بازمیگرداند که در بیست سال گذشته در افغانستان وجود نداشت. طبق این قوانین، "مسائلی که در زمان انتشار توسط مقامات تایید نشده اند باید با احتیاط برخورد شود" و "مسائلی که می تواند تأثیر بدی بر اذهان عامه داشته باشد یا روحیه آنها را تحت تأثیر قرار دهد باید هنگام پخش با دقت رسیدگی شود".

دو ماده آخر (ده و یازده) نشان می دهد که "مرکز رسانه های حکومت GMIC چارچوب خاصی را برای گزارشدهی رسانه ها در این اداره طراحی میکند که کار را به رسانه ها دشوار تر میسازد" و اینکه در آینده، رسانه ها باید "گزارش های تفصیلی را با هماهنگی این نهاد تهیه کنند." این موضوع در هماهنگی با GMIC خطر بازگشت به کنترل اخبار یا سانسور قبلی را افزایش می دهد. و هنوز مبهم است که این "گزارش های مفصل" چیست.

ماده نهم که رسانه‌ها را موظف می‌کند «به مفهوم بی‌طرفی در آنچه منتشر می‌کنند پایبند باشند» و «فقط حقیقت را گزارش کنند» می‌تواند به طرق مختلف تفسیر شود و روزنامه‌نگاران را در معرض تلافی‌های خودسرانه قرار دهد.

منابع

کتابها

- Chuck Easttom, 2019, Computer Security Fundamentals, Third Edition,
- Michael Bazzell, 2018, Personal Digital Security, New Version
- Carla Mooney, 2015, Online Privacy An Social Media
- Melody Karle, 2020, A Social Media Survival Guide
- S.M. Iacus G. Porro, 2021, Subjective Well-Being and Social Media
- Kevin Mitnick and Robert Vamosi, 2017, The Art of Invisibility
- Christopher J. Hadnagy, 2018, Social Engineering: The Science of Human Hacking

وبسایت ها

- https://www.accessnow.org
- https://rsf.org/en/
- https://www.mei.edu/
- https://www.techtarget.com
- https://www.politico.com
- https://basecreative.co.uk
- https://www.ssl.com
- https://www.ssl.com
- https://freedomhouse.org/
- https://www.cyberghostvpn.com/
- https://www.kaspersky.com/
- https://www.tunnelbear.com/download
- https://www.vpngate.net
- https://protonvpn.com
- https://mullvad.net/en/download/
- https://bitmask.net
- https://cryptpad.fr/drive
- https://ufile.io
- https://send.tresorit.com
- https://send.tresorit.com
- https://veracrypt.fr/en/Home.html
- https://www.dropbox.com
- https://www.techtarget.com
- https://www.expressvpn.com
- https://www.vpn-mentors.com

- https://www.cloudflare.com
- https://www.microsoft.com
- https://www.antivirussoftwareguide.com
- https:/www.dashlane.com/
  https://www.stickypassword.com
- https://www.lastpass.com/features/password-generator
- https://www.passwordboss.com
- https://whatismyipaddress.com
- https://www.tripwire.com
- https://www.malwarebytes.com
- https://knowledge-base.secureflag.com
- https://owasp.org
- https://www.ibm.com
- https://securityboulevard.com
- https://www.techadvisor.com
- https://www.hypr.com
- https://www.businessinsider.com
- https://duckduckgo.com
- https://metager.org
- https://www.startpage.com
- https://account.proton.me/login
- https://www.fastmail.com
- https://www.zoho.com/mail
- https://account.riseup.net
- https://en.exp.activix.ca/users/sign_in
- https://www.facebook.com
- https://help.twitter.com
- https://help.instagram.com
- https://www.tiktok.com/safety
- https://support.google.com
- https://help.yahoo.com
- https://faq.whatsapp.com
- https://www.viber.com
- https://telegram.org/faq
- https://support.skype.com
- https://support.signal.org