human rights first

American ideals. Universal values.

ین راهنما برخی از بهترین شیوه ها برای امنیت دیجیتال را پوشش می دهد ، به ویژه برای جلوگیری از نظارت بر ارتباطات و مکان شما. به یاد داشته باشید ، هیچ امنیت کاملی وجود ندارد - کسی که تقریباً زمان و پول نامحدودی دارد به احتمال زیاد می تواند بر پروتکل های امنیتی شما غلبه کند. اما هرچه کار آنها را سخت تر کنید ، احتمال تلاش آنها کمتر می شود و منابع کمتری برای هدف قرار دادن دیگران خواهند داشت. شما می توانید اقدامات لازم را انجام دهید تا از یک هدف آسان جلوگیری کنید.

همه چیز با روشهای جدید برای هدف قرار دادن اطلاعات افراد و روشهای جدید برای محافظت در برابر این تهدیدها دائماً تغییر می کند. مهم است که از آخرین شیوه های امنیتی به روز باشید تا سیستم های شما در برابر حملات جدید محافظت شوند.

مهمترین نکاتی که باید به خاطر بسپارید:

همیشه نرم افزار خود را به روز نگه دارید. به روز رسانی برنامه ها نقاط ضعف امنیت فناوری را برطرف می کند.

برای دسترسی به حساب های خود احراز هویت دو عاملی را روشن کرده و استفاده کنید.

مرحله 1: با Clean Slate شروع کنید

1a یک شخصیت جدید ایجاد کنید - انواع ابزارهای متن باز برای ایجاد یک شخصیت تصادفی برای شما وجود دارد. See: https://backgroundchecks.org/justdeleteme/fake-identity-generator/ or https://www.fakenamegenerator.com/ or https://randomuser.me/ مشاهده کنید:

1b توجه: ممکن است یک ) https://thispersondoesnotexist.com/ یک عکس نمایه را از اینجا بارگیری کنید: (دشمن باتجربه به دنبال تصاویر مصنوعی مانند این باشد)

1c شخصیت تازه ایجاد شده خود را با حساب های دیجیتالی جدید مرتبط کنید: برداشتن پول نقد ، کارت نقدی یکبار مصرف ، خرید تلفن مشعل ، کیف پول رمزنگاری شده با ایمیل رایتر که برای ایجاد آن به یک تلفن مشعل نیاز دارید. (این ممکن است با توجه به شرایط فعلی بانکداری غیر ممکن باشد ، مانند همیشه ، قبل از اقدام آنچه ممکن است درک کنید)

برای راهنما مراجعه کنید: https://theintercept.com/2020/06/15/protest-tech-safety-burner-phone/

برای راهنما مراجعه کنید: https://www.dailydot.com/debug/how-to-create-digital-identity/

مرحله 2: مکان خود را پنهان کنید

(مکان (فعلی و قبلی

تنظیمات پیش فرض تلفن

Android: https://support.google.com/accounts/answer/3467281?hl=en

Apple: https://support.apple.com/en-us/HT207092

https://lifehacker.com/psa-your-phone-logs-everywhere-you-go-heres-how-to-t-1486085759

کیسه / قفس فارادی دستگاهی است که از سیگنال هایی که از تلفن شما می آید و می تواند مکان شما را ردیابی کند جلوگیری می کند. توصیه می کنیم تلفن و لپ تاپ خود را در کیف فارادی در مواقعی که از آن استفاده نمی کنید ، نگهداری کنید. بسته .کردن تلفن و لپ تاپ ها با قلع/آلومینیوم می تواند کمک کند

برخی از گزینه های احتمالی عبارتند از:

https://www.amazon.com/Mission-Darkness-Non-Window-Faraday-Laptops/dp/B01A7NDHZO/

https://www.amazon.com/Mission-Darkness-Non-Window-Faraday-Phones/dp/B01A7MACL2/

.استفاده کنید Mic Lock گوش دادن غیر مجاز را می توان با نرم افزار فعال کرد. برای جلوگیری از آن از ابزاری مانند

https://www.amazon.com/Mic-Lock-Microphone-Blocker-Pack-Surveillance/dp/B01LPQJGA2/

مرحله 3: امنیت داده ها و ارتباطات خود را حفظ کنید

داده های محلی - ایمیل ، مخاطبین ، عکس ها ، فیلم ها و غیره

.رمزگذاری داده ها برای جلوگیری از مشاهده دیگران

روشن کردن رمزگذاری برای تلفن های همراه

iPhone - https://www.zdnet.com/article/how-to-turn-on-iphone-ipad-encryption-in-one-minute/

Android - https://www.androidcentral.com/how-enable-encryption-android

روشن کردن رمزگذاری برای لپ تاپ ها

MacOS - https://support.apple.com/en-us/HT204837

Windows - https://support.microsoft.com/en-us/help/4028713/windows-10-turn-on-device-encryption

اثر انگشت) را خاموش کرده و گذرواژه ها و رمزهای عبور را روشن کنید ، FaceID) ورود بیومتریک

این از ورود اجباری فیزیکی بیومتریک برای بازکردن دستگاه شما جلوگیری می کند

هنگام مرور آنلاین ایمن باشید

مرورگر TOR: https://www.torproject.org/

برای مرور وب استفاده می کند ، تا TOR از پروتکل ، USB سیستم عامل به منظور خالی شدن درایو :Tails سیستم عامل حدودی پیچیده برای اجرا اما امن ترین

https://tails.boum.org/about/index.en.html

گزینه های مختلف شبکه خصوصی مجازی به صورت رایگان در دسترس هستند که ردیابی فعالیت آنلاین شما را - VPN برای شما دشوار می کند.

در حال حاضر دسترسی TunnelBear همه گزینه های خوبی هستند - TunnelBear ، ExpressVPN ، NordVPN رایگان تا 10 گیگابایت اول منتقل شده در افغانستان را ارائه می دهد

یک سیستم خوب دیگر با گزینه های رایگان است ProtonVPN

https://protonvpn.com/blog/open-source/ همچنین اخیراً سیستم های خود را با منبع باز باز کرده اند:

خود را تنظیم کنید ، نیاز به سطح بالاتری از پیچیدگی فنی دارد ، اما امنیت برخلاف شخص ثالث به کاربر - OpenVPN https://openvpn.net/ بستگی دارد:

خط پایانی: یکی را بیابید که کار می کند و توسط سازمان های شخص ثالث رتبه خوبی دارد

دسترسی به اینترنت - چه زمانی به وای فای و بلوتوث اعتماد دارید؟

استفاده نکنید یا آن را روشن نکنید مگر اینکه مطمئن شوید که شبکه ای که به آن ملحق می شوید امن است Wi -Fi از

برای محافظت از لپ تاپ و تلفن خود از یک کیف فارادی در حین حمل و نقل استفاده کنید یا دستگاه های خود را در فویل قلع/آلومینیوم بپیچید.

چت و پیامگذاری رمزگذاری شده (E2EE)

در دسترس هستند: سیگنال ، تلگرام ، واتساپ قوی ترین هستند E2EE بسیاری از گزینه های

آیا تلگرام امن است؟ به طور پیش فرض - مطمئن شوید که عملکرد چت امن روشن است

استفاده می کنید ، در Whatsapp سیگنال به دلیل سیاست های حفظ حریم خصوصی از واتساپ ایمن تر است. اگر از صورت امکان آخرین نسخه را بارگیری کرده و یکی را فعال کنید

ایمیل رمزگذاری شده - ایمیل های رمزگذاری شده رایگان ، از جمله

https://protonmail.com/ (خط موضوع را رمزگذاری نمی کند) Protonmail

https://tutanota.com/ (رمزگذاری موضوع) Tutanota

/ استفاده کنید https://www.sendsafely.com/ Sendsafely برای رمزگذاری پیوست ها از

نسبتاً امن است Gmail

مرحله 4: از خود در برابر بدافزارها محافظت کنید (برای اطلاعات بیشتر به مراجعه کنید) https://securityinabox.org/en/guide/malware

، در Whatsapp ایمن تر است. در صورت استفاده از WhatsAppسیگنال به دلیل سیاست های حفظ حریم خصوصی از صورت امکان آخرین نسخه را بارگیری کرده و پیامهای ناپدید شده را به مدت یک هفته فعال کنید

ایمیل رمزگذاری شده - ایمیل های رمزگذاری شده رایگان ، از جمله

Protonmail (خط موضوع را رمزگذاری نمی کند) https://protonmail.com/

Tutanota (رمزگذاری موضوع) https://tutanota.com/

/ استفاده کنیدSendsafely https://www.sendsafely.comبرای رمزگذاری پیوست ها از

نسبتاً امن استGmail

مرحله 4: از خود در برابر بدافزارها محافظت کنید (برای اطلاعات بیشتر به مراجعه کنید)https://securityinabox.org/fa/guide/malware

سیار

فیشینگ از طریق پیام کوتاه

روی پیوندهای فرستنده هایی که نمی شناسید یا نمی شناسید کلیک نکنید

لپ تاپ

فیشینگ از طریق ایمیل

روی پیوندهای فرستنده هایی که نمی شناسید یا نمی شناسید کلیک نکنید

راه حل های بدون آنتی ویروس (توجه داشته باشید: برخی از بازیگران پیچیده ممکن است بتوانند از آنتی ویروس فرار کنند)

سوفوس در خانه

Sophos at home https://home.sophos.com/en-us.aspx
Bitdefender https://www.bitdefender.com/
Adaware https://www.adaware.com/
AVG https://www.avg.com/en-us/homepage#mac

مرحله 5: از انتقال فایل ناشناس استفاده کنید

الف - این فهرست خدمات ذخیره سازی فایل آنلاین را که نیازی به ثبت نام و مراجعه ندارند ، بررسی کنید

با رمزگذاری تا 30 روز.

خواندن پیشنهادی دیگر:

https://securityinabox.org/en/

https://www.securityplanner.org/#/