بسته کمک‌های اولیه دیجیتال

(نسخه بتا)

کار مشترک:

EFF, GLOBAL VOICES, HIVOS & THE **DIGITAL DEFENDERS PARTNERSHIP, FRONT LINE DEFENDERS, INTERNEWS, FREEDOM HOUSE, ACCESS, QURIUM, CIRCL, IWPR, OPEN TECHNOLOGY FUND** و برخی متخصصان امنیت

The table of contents is empty because you aren't using the paragraph styles set to appear in it.

مقدمه

هدف بسته کمک‌های اولیه دیجیتال این است که کسانی را که با تهدیدات بسیار شایع دیجیتالی روبه‌رو می‌شوند ، حمایت کند. این بسته، به مدافعان حقوق بشر، وبلاگ‌نویسان، کنش‌گران و روزنامه‌نگاران مورد تهدید، ابزاری برای تشخیص مشکلات احتمالی پیش آمده ارائه می دهد و همچنین دستور العمل هایی برای کمک به افراد در معرض خطر فراهم می کند.

قسمت اول این بسته آموزشی با ارائه ی راههای امن ارتباطی آغاز می شود که چگونه شما و یا شخصی که در معرض خطر دیجیتال است بتواند توسط راهی امن تقاضای کمک کند. قسمت های بعدی شامل بخش‌هایی چون دزدیده شدن حساب کاربری، مصادره دستگاه، آلودگی بدافزاری و حمله‌های گسترده عدم سرویس‌دهی DDoS است. هر بخش با پرسش‌هایی در مورد شما، دستگاه و شرایط شما آغاز می‌شود. این پرسش‌ها شما را راهنمایی می کنند برای اینکه بتوانید مشکل را درست ارزیابی کنید و یا فردی که می خواهد کمک کند رابهتر از شرایط پیش آمده مطلع کنید . در بخش بعدی قدم های اولیه برای فهم و حل بالقوه مشکل توضیح داده می شود.این گام‌ها به شما و یا فرد راهنما برای تشخیص زمان مناسب کمک‌گیری از یک متخصص کمک می‌کنند.

بسته کمک‌های اولیه دیجیتال قرار نیست به عنوان یک راه حل نهایی برای همه‌ی مشکلات اورژانسی شما عمل کند. تلاش این بسته، دادن ابزارهایی برای یک ارزیابی اولیه از اتفاقات است و همچنین از طریق این بسته تعیین کنید که آیا خودتان می‌توانید برای کاهش مشکل کاری بکنید یا نه. اگر هرلحظه در مورد به کارگیری هرکدام از راه حل‌های ارائه شده دچار عدم اطمینان شدید، سریعاً از متخصصان کمک بگیرید.

این بسته هنگامی ایجاد شد که تعدادی از سازمان‌های فعال در عرصه مسائل اورژانسی دیجیتال مشاهده کردند که کسانی که مورد تهدید دیجیتالی قرار می‌گیرند غالباً نمی‌دانند چه کنند یا چه زمانی تقاضای کمک کنند. این بسته الهام گرفته از این باور بود که همه دارای توانائی به کارگیری اقدامات پیشگیرانه هستند. هم‌چنین، همه می‌توانند به همکاران خود در هنگام خطر کمک کنند. این بسته به خود شخص این امکان را می دهد که مشکل پیش آمده را تشخیص دهد و خصوصا کمک مفیدی است برای خبرنگاران، وبلاگ‌نویسان، کنش‌گران و مدافعان حقوق بشر که سریع متوجه مشکلات امنیتی بوجود آمده برای دستگاه خود شودند و به راحتی تشخیص دهند چه زمانی نیاز دارند از متخصص تقاضای کمک کنند و همچنین در بهبود امنیت دیجیتالی فردی آن‌ها یاری می‌رساند. علاوه بر این، بسته ی آموزشی موجود به عنوان یک چک‌لیست راهنما برای افرادی که مورد مراجعه افراد مورد خطر هستند عمل می‌کند.

این بسته حاصل تلاش مشترک EFF، Global Voices، The Digital Defenders Partnership & Hivos، Frontline Defenders، Internews، Freedom House، Access، Qurium، CIRCL، IWPR، Open Technology Fund و متخصصان امنیت فردی که درزمینه‌ٔ امنیت دیجیتال و پاسخگویی سریع فعالیت می‌کنند است. این بسته دائماً موردبررسی و اصلاح قرار می‌گیرد، برای دادن پیشنهاد برای اضافه کردن موردی، یا دادن نظرات و سؤال در مورد هر بخش لطفاً به GitHub مراجعه کنید.

بخش‌ها

ارتباط امن

در این بخش راه‌هایی برای برقراری ارتباط امن در هنگام برخورد با تهدید دیجیتالی و چگونگی تقاضای کمک، آورده شده است. به عنوان یک اصل کلی، مهم است بدانید که بیش‌تر ابزار ارتباطی «عادی» در برار خطر شنود امن نیستند. ارتباطات تلفن ثابت و همراه رمزگذاری نشده‌اند و می‌توانند توسط دولت‌ها، مراجع قانونی و دیگر مراجعی که دارای لوازم فنی مورد نیاز هستند مورد شنود قرار بگیرند. فرستادن پیغام‌های رمزگذاری نشده مانند فرستادن یک کارت‌پستال است؛ هر کس به آن دست‌رسی داشته باشد می‌تواند آن را بخواند. فرستادن پیغام‌های رمزگذاری شده مثل قرار دادن کارت‌پستال در یک گاوصندوق و فرستادن آن گاوصندوق در حالی است که تنها شما و فردی که به او اعتماد دارید رمز آن را دارد و می‌تواند آن را باز کند و پیغام را بخواند.

ارتباط امن همیشه سازش و معامله‌ای بین امنیت و سهولت است. انتخاب مناسب‌ترین نوع ارتباط امن به شرایط خاص شما، نوع تهدیدی که با آن روبه‌رو هستید و فعالیت‌های خاص شما بستگی دارد. بسته کمک‌های اولیه مشخصاً برای فردی که مورد تهدید شدید دیجیتالی قرار دارند تهیه‌شده بنابراین، در این بخش فرض بر این است که شما جزء این دسته‌اید.

در آخر، در هنگام ایجاد ارتباط، سطوح متفاوتی از امنیت وجود دارد. نوع و نحوه‌ی ابزار رمزگذاری، سطح امنیت ارتباط شما را کاهش یا افزایش می‌دهد. یک ابزار ارتباطی که دارای سیستم رمزگذاری نقطه به نقطه (end to end) است (مانند رایانامه (ایمیل)های رمزگذاری شده با PGP و یا گفت‌وگو با OTR و Textsecure روی تلفن همراه) از یک ابزار دارای رمزگذاری لایه‌ی انتقال (مانند جی میل، فیس‌بوک و توییتر) بهتر است و این سیستم به نوبه‌ی خود از ارتباط رمزگذاری نشده (مانند کارت‌پستال، تلفن و یا پیام کوتاه) بهتر است. با توجه به منابع و مهارت‌های خود، امن‌ترین انتخاب موجود را کنید. با امن‌ترین فرم ارتباط شروع کنید. فردی که از او تقاضای کمک می‌کنید ممکن است بتواند در صورت لزوم به شما برای ایجاد یک خط ارتباطی امن‌تر کمک کند. در بسیاری از موارد، بهتر است که با ابزاری غیر امن تقاضای کمک کنید تا این که اصلاً تقاضای کمک نکنید.

از کجا شروع کنیم؟ اگر فکر می‌کنید امنیت رایانه شما توسط بدافزارها مورد خطر قرارگرفته و نمی‌توانید به آن اعتماد کنید لطفاً مستقیماً به بخش استفاده‌ی امن‌تر از رایانه مراجعه کنید. اگر فکر می‌کنید که ارتباط شما مورد هدف است و یا به رایانه‌ی امن‌تری دست‌رسی دارید به بخش استفاده‌ی امن‌تر از رایانه و بخش ارتباط امن‌تر روی تلفن‌های هوشمند مراجعه کنید. گام‌های زیر برای ایجاد ارتباط امن شما را راهنمایی می‌کند.

جستجو و تأمین کمک از راه دور

هنگام کمک گرفتن از یک شخص سوم لطفاً موارد زیر را در نظر بگیرید:

۱. اگر فکر می‌کنید که در دستگاه یا حساب کاربری‌تان اشکالی وجود دارد، نگران هستید و نمی‌دانید باید چه‌کار کنید، از یک متخصص فنی آموزش‌دیده یا یک ارگان ملی/بین‌المللی مورد اعتمادتان کمک بگیرید. راهنمایی‌های قرار داده‌شده در بخش منابع نیز کمک‌کننده خواهند بود. در صورت امکان، به افراد ناشناس آنلاین اعتماد نکنید. بعضی از سازمان‌هایی که می‌توانید به آن‌ها اعتماد کنید شامل موارد زیر می‌شوند:

EFF

- URL: https://www.eff.org/
- email: info@eff.org

Front Line Defenders

- URL: http://www.frontlinedefenders.org/
- email: info@frontlinedefenders.org

CPJ

- URL: https://www.cpj.org/

- email: info@cpj.org

RSF
- URL: http://en.rsf.org/
- email: internet@rsf.org

Access
- URL: https://www.accessnow.org/
- email: help@accessnow.org
- PGP key fingerprint: 6CE6 221C 98EC F399 A04C 41B8 C46B ED33 32E8 A2BC

Digital Defenders Partnership
- URL: http://digitaldefenders.org/
- ddp@hivos.org

Freedom House
- URL: http://freedomhouse.org/

Internews
- URL: https://www.internews.org/

IWPR
- URL: https://www.cyber-arabs.com/

Open Technology Fund
- URL: https://www.opentechfund.org
- email: info@opentechfund.org
- PGP key fingerprint: 67AC DDCF B909 4685 36DD BC03 F766 3861 965A 90D2

Iran Security Team
- URL: https://www.iransec.org
- email: support@iransec.org

۲. در هنگام درخواست کمک، در نظر داشته باشید که دستگاه مورد استفاده‌ی شما نیز ممکن است موردحمله و تهدید قرار گرفته باشد. برای ایجاد یک خط ارتباطی امن با کسی که می‌تواند به شما کمک کند، ممکن است لازم باشد که از وسیله‌ی جایگزین مورد اعتماد استفاده کنید.

استفاده امن‌تر از رایانه: در هنگام عدم اطمینان به دستگاه خود چه باید کرد؟

اگر امکانش را دارید، به یک دستگاه کاملاً جدا مراجعه کنید، دستگاهی که هیچ دلیلی برای شک امنیتی به آن ندارید. به دستگاه دوستان و خانواده فکر کنید. کافی‌نت‌ها می‌توانند یک گزینه باشند، اما در بسیاری از کشورها کافی‌نت‌ها تحت تدابیر شدید امنیتی و شنود توسط دولت‌های محلی و مراجع قانونی هستند.

اگر به یک دستگاه امن دسترسی ندارید ممکن است بتوانید یک نسخه از سیستمعامل رایگان Tails را دریافت و نصب کنید. Tails یک «دیسک زنده»ی USB است که سیستمعاملی سفارشی است. Tails بسیار امن طراحی

شده و هیچ اطلاعاتی از رایانه‌ای که روی آن اجرا میشود را تغییر نمیدهد. این برنامه امکانات زیادی برای محافظت شما در برابر رایانه‌های تحت خطردارد .

با پیروی از دستورالعمل‌های آمده در تارنمای Tails، آن را با دقت انتخاب، بازبینی و نصب کنید. شما به یک DVD خالی و یا یک فلش مموری یا کارت حافظه‌ی جانبی که ۲ گیگابایت یا بیش‌تر حجم داشته باشد احتیاج خواهید داشت. بعضی از مراحل، مخصوصاً مرحله‌ی بررسی دریافت، دشوار خواهند بود. این گام‌ها برای اطمینان حاصل کردن از این که آن چه دریافت کرده‌اید، دقیقا همانی است که قصدش را داشته‌اید، ضروری هستند. شما می‌خواهید مطمئن باشید که به سیستمی با امنیت بیش‌تر، و نه کم‌تر، منتقل می‌شوید.

ارتباطات امن‌تر: وقتی نمی‌توانید به کانال‌های ارتباطی خود اعتماد کنید چه باید بکنید؟

اگر فکر می‌کنید ارتباطات شما مورد تهدید قرارگرفته‌اند باید استفاده از خدمات ارتباطی یا حساب کاربری مورد خطر و تهدید را سریعاً قطع کنید. یک حساب کاربری جدید بازکنید و به خاطر داشته باشید که از نام کاربری، رمز عبور و یا حساب رایانامه (ایمیل) قبلی برای جستجوی کمک استفاده نکنید.

نکته: اگر نمی‌توانید یک رایانامه (ایمیل) رمزگذاری شده با PGP در Thunderbird و یا OTR در Pidgin و Adium راه بیندازید، از افزونه‌ی Mailvelope برای رایانامه (ایمیل) و Cryptocat برای گفت‌وگو در فایرفاکس و کروم استفاده کنید. این دو افزونه راه‌های ساده و امن برای ایجاد ارتباطات امن‌تر در موارد اورژانسی هستند.

پیشنهادهای مهمی که در ادامه می‌آیند شما را در ایجاد کانال‌های جدید ارتباط امن یاری می‌رسانند:

- پس از آن که به دستگاه جدید نقل مکان کردید، یک حساب کاربری جدید با یک رمز عبور امن و جدید بسازید. به هیچ‌عنوان از حساب‌ها و رمزهای عبوری که قبلاً استفاده می‌کردید استفاده نکنید. در این پیوند راهنمایی‌های ساختن رمز عبور قوی را می‌یابید.
- غیر از مواردی که تهدید شامل شنود و نظارت توسط دولت‌هایی با امکانات بسیار بالا شود (مانند آمریکا، بریتانیا و چین و یا دولت‌های فهرست شده در گزارش شفافیت گوگل) استفاده از محصولات گوگل درجه‌ای از محافظت را برای شما فراهم می‌آورند. ابزار گوگل (مخصوصاً استفاده از ابزار گوگل روی گوگل کروم) به طرز قابل توجهی امنیت شما را بالا می‌برند و دسترسی شما را به رایانامه (ایمیل)، گفت‌وگو، ویدیو و ویدیو کنفرانس امن‌تر می سازد. این امنیت فقط درون گوگل عمل می‌کند، یعنی جی‌میل به جی‌میل و جی‌تاک به جی‌تاک. اگر کسی اطلاعات را به خارج از گوگل فوروارد کند و یا از آدرس‌های رایانامه (ایمیل) دیگری به یک گفتگو در جی‌تاک اضافه شود، سطح امنیت پائین می‌آید.
- یک جایگزین برای گوگل رایزآپ است. رایزآپ را یک گروه داوطلب برای ایجاد جایگزین‌های دموکراتیک راه انداخته است و امکان ارتباط امن و کنترل آن توسط کاربر را میدهد. آن‌ها خدماتی مثل جی‌میل و جی‌گفت‌وگو ارائه می‌دهند اما باید در نظر داشت که رایزآپ ابزارها و امکانات گوگل را در اختیار ندارد. با این وجود، بستگی به شرایط شما، رایزآپ می‌تواند گزینه‌ی مناسب‌تری نسبت به بقیه‌ی گزینه‌ها باشد.
- برای امنیت نقطه به نقطه (end-to-end)، ابزارهای بسیاری با رمزگذاری قوی موجود هستند. چند پیشنهاد:
  - Pidgin (برای ویندوز و لینوکس) و Adium (برای Mac) با رمزگذاری نقطه به نقطه (end-to-end) با استفاده از OTR، به شما این امکان را می‌دهد که گفت‌وگویی امن داشته باشید. این پیوند یک راهنماست برای نصب و راه‌اندازی Pidgin و افزونه‌ی OTR برای آن.
  - Jitsi برای گفت‌وگوی متنی، تصویری و صوتی رمزگذاری شده و قابل‌استفاده است. از این راهنما برای نصب و راه‌اندازی آن استفاده کنید.
  - در این تارنما می‌توانید برای یک تماس صوتی/تصویری امن و رایگان یک حساب کاربری ایجاد کنید.
  - PGP به شما امکان رمزگذاری رایانامه (ایمیل) هایتان را می‌دهد. این راهنما برای استفاده از PGP در کنار تاندربرد روی رایانه است.
  - بسته‌ی مرورگر تور امنیت و حریم خصوصی شما را در هنگام بازدید تارنماها افزایش می‌دهد. این کار با پخش ارتباطات شما از طریق یک شبکه گسترده از سرورها و اشخاص داوطلب در سراسر جهان رخ می‌دهد.
  - همه‌ی ابزارهای امن بالا به علاوه‌ی ده‌ها نرم‌افزار دیگر از پیش روی Tails نصب شده‌اند. تنها کافی است Tails را دریافت و اجرا کنید.

ارتباط امن‌تر روی گوشی‌های هوشمند
اگر گوشی هوشمند دارید، ابزارهای زیر می‌توانند از امنیت شما محافظت کنند. در نظر بگیرید که تلفن شما به طورکلی به هویت شما وصل است (از طریق قبوض، خدمات کاربری و یا ثبت سیم‌کارت) و می‌تواند محل شما را فاش کند. این ابزارها در برابر این موارد شما را محافظت نمی‌کنند، این ابزارها تنها محتوای ارتباطات شما را رمزگذاری می‌کنند.

گوشی‌های هوشمند مبتنی بر اندروید

- RedPhone برای پیغام‌های صوتی و TextSecure برای پیام متنی کارآمد هستند. معادل این نرم‌افزار در گوشی‌های هوشمند مبتنی بر iOS (مثل آیفون) با نام Signal ارائه شده است.
- ChatSecure از پروژه‌ی گاردین قابلیت ارتباط‌گیری با نرم‌افزارهایی مانند Jitsi و Pidgin را دارد (با استفاده از سرویس پیام‌رسان گوگل و یا Jabber/XMPP)، امکان رمزگذاری نقطه به نقطه (end-to-end) و فرستادن فایل‌های صوتی و توصیری را اضافه می‌کند.
- با csipsimple می‌توانید تماس‌های امن برقرار کنید (مانند سرویس Ostel)
- Orbot از پروژه گاردین و پروژه تور یک برنامه است که به کاربران گوشی‌های هوشمند امکان وصل شدن به شبکه‌ی تور، فرستادن و دریافت پیام فوری و رایانامه (ایمیل)، بدون نظارت یا مسدود شدن توسط خدمات‌دهندگان شبکه‌ی تلفن همراه را فراهم می‌سازد. Orbot ویژگی‌ها و عمل‌کرد تور را به سیستم‌عامل گوشی هوشمند مبتنی بر اندروید می‌آورد.
- این برنامه‌ها در Google Play store و F-Droid موجود هستند و با پیوندهای داده‌شده قابل دریافت می‌باشند.

گوشی‌های هوشمند مبتنی بر iOS (مانند آیفون)
انتخاب‌های iOS محدود هستند، اما برنامه‌ی Signal توسط تیم توسعه‌دهنده‌ی TextSecure/RedPhone در اندروید طراحی شده و همان قابلیت‌ها را داراست. برنامه ChatSecure روی آیفون با همکاری برنامه ChatSecure در اندروید طراحی‌شده و ویژگی‌های مشابهی دارد. Onion Browser امکانات مشابه تور و اربوت را برای iOS فراهم می‌آورد.

اعتماد سازی
چنان چه از راه دور به کسی کمک می‌کنید یا از شخص سومی کمک می‌گیرید، اعتمادسازی بسیار حیاتی و در عین حال پیچیده است. همیشه باید فرض کنید که یک دشمن به حساب کاربری و هم‌چنین به اطلاعات اصلی شما در هنگام کمک خواستن دست‌رسی دارد. این دشمن مشخصاً قصد ایجاد اختلال در کانال ارتباطی امن شما دارد و عمداً به شما راهنمایی غلط می‌دهد. ابزارهای امنیت راه های به شما ارائه می دهند که از هویت شخصی که از او کمک می‌گیرید ، مطمئن شوید. در هنگام گرفتن کمک، راهنمایی‌ها را با مفاهیم ارائه‌شده در برنامه های مورد قبولی چون امنیت در جعبه و منابعی چون EFFو How Encryption Worksمقایسه کنید.

اطلاعات بیش‌تر در مورد جنبه های فنی گوناگون اعتماد، در بخش اعتمادسازی موجود است.

منابع مفید

امنیت در جعبه؛ انتخاب و نگه‌داری رمز عبورهای امن

راهنماهای گسترده EFF؛ چگونگی ساختن رمز عبور

دزدی حساب کاربری

آیا برای دسترسی به رایانامه (ایمیل)، شبکه اجتماعی یا دیگر حساب‌های کاربری در شبکه‌های اجتماعی دچار مشکل شده‌اید؟ آیا یک حساب کاربری فعالیت‌هایی را نشان می‌دهد که شما انجام نداده‌اید؟ برای رفع این مشکل کارهای زیادی می‌توانید انجام دهید.

کار را با پاسخ دادن به این سؤالات ساده آغاز کنید.

- با کدام تارنماها دچار مشکل شده‌اید؟
- آیا تنها شما از این حساب استفاده می‌کنید؟ گاهی اوقات چندین فرد به صفحات یک گروه فیس‌بوکی، وبلاگ‌های وردپرس و یا حساب رایانامه (ایمیل) دسترسی دارند. اگر افراد متعددی به این حساب کاربری دسترسی دارند، اول با آن‌ها موضوع را در میان بگذارید.
- نام کاربری و آدرس اینترنتی (URL) این حساب چیست؟
- آیا نمی‌توانید به حساب کاربری خود وارد شوید؟
- آیا می‌بینید که کس دیگری در حال استفاده از حساب کاربری شماست؟
- آیا اخطاری دریافت کردید و یا دوستان و افراد در ارتباط با شما پیام‌های عجیب از جانب شما دریافت کرده‌اند؟
- چه نشانه‌ها و مدارک دیگری از وجود مشکل مشاهده کرده ید؟

اولین گام‌ها برای کاهش مشکل

اگر هنوز به حساب خود دسترسی دارید

از رایانه‌ی دیگری استفاده کنید؛ رایانه‌ی که ازنظر شما امن است و در معرض خطر نیست. وارد حساب خود شده و رمز عبور خود را تغییر دهید. سپس گام‌های زیر را بردارید:

- گام اول: پیش از دریافتن کامل و همه جانبه‌ی دلیل مشکل، از این حساب کاربری برای اطلاعات و پیام‌های حساس استفاده نکنید.
- گام دوم: در صورت امکان، تاریخچه‌ی اتصال و فعالیت‌های حساب کاربری را مرور کنید (این امکان در فیس‌بوک و جیمیل و دیگر تارنماها وجود دارد). بررسی کنید که آیا حساب شما در زمان‌هایی که شما آنلاین نبودید استفاده شده است و یا آیا حساب شما از یک مکان یا IP ناآشنا مورداستفاده قرارگرفته است.
- گام سوم: به تنظیمات حساب نگاهی بیندازید. آیا تغییر کرده‌اند؟ در مورد رایانامه (ایمیل)، به فورواردهای خودکار (Automatic Forwarding)، تغییرات احتمالی در تلفن یا آدرس رایانامه (ایمیل) پشتیبان، همگام‌سازی (Synchronizing) با دستگاه‌های مختلف شامل تلفن همرا و رایانه و تبلت توجه کنید.
- گام چهارم: رمز عبور همه‌ی حساب‌هایی که به این حساب وصل بوده‌اند را تغییر دهید. برای نمونه، اگر رایانامه (ایمیل)، آدرس پشتیبان رایانامه‌ی دیگری است، رمز عبور آن را هم تغییر دهید.
- گام پنجم: هنوز کار تمام نشده است! گام‌های مهم بعدی را هم دنبال کنید.

اگر دیگر به حساب خود دسترسی ندارید

روش‌های بازگردانی حساب کاربری ارائه‌دهندگان مختلف را دنبال کنید. در نظر داشته باشید که خدمات مختلف، راه‌های متفاوتی برای بازسازی رمز عبور حساب کاربری شما را دارند. بعضی از آن‌ها به شما یک پیوند برای تغییر رمز عبورتان می‌فرستند، درحالی‌که بقیه رمز عبور شما را بر اساس آخرین رمز عبورتان بازسازی می‌کنند. در این مورد، بسیار مهم است که رمز عبورتان را به محض دسترسی به حساب خود تغییر دهید. اگر این گام‌ها عمل نمی‌کنند و حساب شما هم‌چنان مورد سوءاستفاده قرار می‌گیرد. در این صورت بهتر است که با یکی از سازمان‌های فهرست شده برای پشتیبانی در بستن حساب کاربری‌تان تماس بگیرید.

هنوز کار تمام نشده! گام‌های مهم بعدی را دنبال کنید:

اگر مشکوکید که فرد دیگری به حساب کاربری شما دست‌رسی دارد، کارهای زیر را انجام دهید:

- گام اول: به این سؤالات جواب دهید: چه کسی ممکن است به حساب شما دست‌رسی داشته باشد (دوستان، همکاران، همسر، فرزندان)؟ چه دستگاه‌هایی (رایانه، تلفن همراه، تبلت)؟ آیا خودتان قبلاً به این حساب واردشده‌اید؟ در چه مکان‌هایی (خانه، اداره، کافی‌نت، اینترنت عمومی)؟
- گام دوم: از همین رمز عبور برای حساب‌های دیگر هم استفاده می‌کنید؟ در این صورت، همین بررسی‌ها را برای آن حساب‌ها هم انجام دهید. برای هر حساب رمز عبورهای جدا و منحصربه فرد ایجاد کنید.
- گام سوم: فکر کنید که از این حساب خود برای چه‌کارهایی استفاده کرده و می‌کنید. آیا این حساب حاوی اطلاعات حساس است؟ این اطلاعات حساس می‌تواند شامل لیست افراد در ارتباط با شما، اطلاعات راجع به مکان شما و یا محتوای پیغام‌های شما باشند. اگر فکر می‌کنید که این اطلاعات می‌تواند شما و افراد در ارتباط با شما را درخطر قرار دهد به آن‌ها خبر دهید.
- گام چهارم: بررسی تاریخچه اتصال و فعالیت‌های حساب را حداقل هفته‌ای یک‌بار برای مدت یک ماه، تکرار کنید تا مطمئن شوید که حساب شما فعالیت‌های عجیب نشان نمی‌دهد. اگر فعالیت‌های عجیب ادامه داشتند به بخش بدافزارها مراجعه کنید.

در برابر حمله‌کنندگان، اقدامات احتیاطی اضافی در پیش گیرید.

اگر خدماتی که از آن استفاده می‌کنید دارای تصدیق دو مرحله‌ای (2nd Step Verification) است، آن را فعال کنید. این فرایندی است که از شما می‌خواهد هویت خود را به هنگام وارد شدن، در یک دستگاه دیگر نیز تائید کنید (معمولاً در یک تلفن همراه). گوگل، فیسبوک، توئیتر، وردپرس و بسیاری دیگر از تارنماها دارای این امکان هستند.

توجه کنید که فعال کردن سیستم تایید دومرحله‌ای در گوگل، شما را مجبور می‌کند که از رمز عبورهای پیش-برنامه‌ای سفارشی، برای برنامه‌هایی مانند thunderbird، Jitsi، Pidgin و برنامه‌های که از طریق رابط شبکه وصل نمی‌شود استفاده کنید. این امکان می‌تواند در تنظیمات حساب روی شبکه تنظیم شوند.

تحقیق کنید

خوب است بفهمید که چرا حساب شما مورد سواستفاده واقع شده است. فکر می‌کند چه کسی ممکن است بخواهد شما یا سازمانتان را مورد هدف قرار دهد؟ آیا این تهدید به شغل و کار شما مرتبط است؟ در بخش منابع مفید پیوندهایی برای راهنماهایی وجود دارند که به شما پیشنهادهایی و حقه‌هایی برای جلوگیری از موقعیت‌های اورژانسی دیجیتالی و فعال بودن در امنیت دیجیتالی ارائه می‌دهد.

پیوندها و منابع مفید

امنیت در جعبه

الگوهای تهدید و دفاع شخصی در برابر نظارت

ضبط شدن دستگاه

آیا دستگاه خود را گم‌کرده‌اید؟ آیا این دستگاه توسط شخص سومی دزدیده یا ضبط‌شده است؟ در این صورت بسیار مهم است که تصویر روشنی از اتفاق داشته باشید؛ چه اطلاعات و حساب‌هایی ممکن است مورد خطر قرارگرفته باشند و چه گام‌هایی برای جلوگیری از فاش شدن این اطلاعات و سوءاستفاده از اطلاعات و افراد در ارتباط با شما و حساب‌های شما باید برداشته شود.

کار را با پاسخ دادن به این سؤالات ساده شروع کنید:

چه اتفاقی افتاده است؟

- چه نوع دستگاهی گم‌شده است؟ رایانه، تلفن همراه، تبلت و یا یک هارد اکسترنال؟
- کی و کجا دستگاه خود را گم‌کرده‌اید؟
- چگونه دستگاه را از دست دادید؟ آیا توسط فردی یا یک اورگان دولتی ضبط‌شده و یا آن را گم کردید؟
- آیا هنوز آن را پیدا نکرده‌اید؟

دستگاه شما دارای چه ابزارهای امنیتی‌ای بود؟

- آیا دستگاه توسط رمز عبور یا یک تدبیر امنیتی دیگر محافظت می‌شده؟
- سیستم‌عامل دستگاه چه بود؟ آیا این سیستم‌عامل یک نسخه قانونی بود یا یک نسخه غیرقانونی؟ آیا به دستگاهتان واردشده بودید؟
- آیا امکان رمزگذاری کل دستگاه (Full Disk Encryption) فعال‌شده بود؟
- در هنگام از دست دادن دستگاه شما در چه وضعیتی بود؟ آیا واردمحیط سیستم‌عامل شده بود؟ آیا دستگاه روشن ولی به وسیله رمز عبور قفل بود؟ آیا در حالت خواب (Hibernate) بود؟ کاملاً خاموش بود؟
- آیا کنترلی از راه دور (Remote Control) به دستگاه خود دارید؟

درون دستگاه چه داشتید؟

- فهرستی از اطلاعات حساس مختلفی که در دستگاه شما بود تهیه کنید. برای نمونه رایانامه (ایمیل)، تاریخچه‌ی گفت‌وگو، شبکه‌های اجتماعی، تماس‌ها (رایانامه، اسکایپ، گفت‌وگو و غیره)، فایل‌ها، اطلاعات مکان، کارت اعتباری و هر آن چه که مهم است.
- سیستم‌عانل دستگاه چه بود؟ ویندوز، لینوکس، مک، اندروید، iOS یا غیره؟
- آیا برای رایانامه (ایمیل) و گفت‌وگو از ابزارهای رمزگذاری استفاده می‌کردید (مانند PGP و OTR)؟
- این دستگاه به چه حساب کاربری دست‌رسی دارد؟ این شامل رایانامه (ایمیل)، شبکه‌های اجتماعی، گفت‌وگو، پیغام فوری و حساب‌های بانکی که دستگاه ممکن است به آن دست‌رسی داشته باشد، مرورگرهایی که رمز عبور حساب‌ها را ذخیره کرده‌اند، کوکی‌هایی که تاریخچه‌ی مرورگری روی اینترنت را نشان می‌دهند، رمزهای احراز هویت شامل اثر انگشت روی آیفون ۵ و حساب‌هایی که از دستگاه برای احراز هویت ثانویه استفاده می‌کنند.
- آیا دستگاه شما رمز عبور ذخیره‌شده دارد و یا به صورت خودکار وارد می‌شود؟ این برای برنامه‌هایی مانند رایانامه (ایمیل) و اسکایپ و دیگر برنامه‌های گفت‌وگو متداول است، یا اگر رمز عبور خود را در مرورگر به جای مدیریت پسوردهایی مانند KeePass ذخیره کرده باشید.

گام‌های اول برای کاهش مشکل:

اگر دستگاه شما هنوز پیدا نشده

اگر دستگاه گم‌شده یا توسط فرد سومی ضبط‌شده و هنوز آن را پس نگرفته‌اید، گام‌های اول به شرح زیر است:

- گام اول: وقتی‌که دستگاه شما به حساب‌های کاربری دست‌رسی دارد (رایانامه، شبکه‌های اجتماعی و یا حساب در شبکه‌های اجتماعی) این دستگاه را از همه حساب‌هایتان قطع کنید. برای این کار، به صورت آنلاین به حساب‌هایتان بروید و حق دست‌رسی‌های حساب‌ها را تغییر دهید.
- گام دوم: رمز عبور همه‌ی حساب‌هایی که این دستگاه به آن‌ها دست‌رسی دارد را تغییر دهید.
- گام سوم: احراز هویت دو مرحله‌ای را برای همه‌ی حساب‌هایی که این دستگاه به آن‌ها دست‌رسی دارد فعال کنید. لطفاً توجه کنید که احراز هویت دو مرحله‌ای توسط همه‌یی حساب‌ها پشتیبانی نمی‌شود. (به نکته‌های مربوط به حساب دو مرحله‌ای در بخش دزدی حساب کاربری نگاه کنید).
- گام چهارم: اگر ابزاری دارید که روی دستگاه ازدست‌رفته‌ی شما نصب‌شده است که به شما امکان پاک کردن اطلاعات و تاریخچه‌ی دستگاه را می‌دهد از آن استفاده کنید.

اگر دستگاه خود را پس گرفتید

اگر دستگاه شما گم‌شده بود، توسط فرد سومی از شما گرفته‌شده بود و یا در هنگام گذشتن از مرز از شما تحویل گرفته‌شده ولی دوباره برگردانده شده، مواظب باشید زیرا شما نمی‌دانید چه کسی به دستگاه شما دست‌رسی داشته است. بسته به سطح خطری که با آن مواجه هستید، ممکن است بخواهید دستگاه خود را مورد تهدید در نظر بگیرید. سؤال‌های زیر را از خود بپرسید و میزان خطر را ارزیابی کنید:

- چه مدت دستگاه دور از دید شما بود؟
- چه کسی احتمالاً به آن دست‌رسی داشته است؟
- چرا ممکن است کسی خواسته باشد به آن دست‌رسی داشته باشد؟
- آیا نشانه‌هایی مبنی بر دست‌رسی فیزیکی به آن مشاهده می‌شود؟

برای کمک بیش‌تر در مورد انواع تهدیدها به بخش راهنمای دفاع شخصی در برابر نظارت مراجعه کنید.

اگر مدت زیادی دستگاه خود را در اختیار نداشته‌اید و احتمال می‌دهید که چیزی روی آن نصب‌شده باشد مسائل زیر را در نظر بگیرید:

- رایانه: سیستم‌عامل را به طورکلی و از اول نصب کنید. مدارک خود را از آخرین فایل‌های پشتیبانی بازیابی کنید و پس از آن با نرم‌افزار ضد ویروس بررسی (Scan) کنید. برای راهنمایی‌های بیش‌تر به زیر بخش تمیز کردن دستگاه خود در بخش بدافزارها نگاه کنید.
- تلفن همراه و تبلت: بسته به سطح خطر و شرایطی که در آن تلفن همراه یا تبلت خود را از دست داده‌اید، ممکن است بهتر باشد دیگر از وسیله‌ی خود استفاده نکنید. در صورت امکان، از همه‌ی اطلاعات و فایل‌های روی دستگاه خود پشتیبان بگیرید و پس از خرید دستگاه دیگری به آن منتقل کنید. اگر فکر می‌کنید امنیت دستگاه شما خدشه‌دار شده اما نمی‌توانید آن را تعویض کنید مواظب باشید و از دستگاه خود برای ارتباطات و فایل‌های حساس استفاده نکنید. در هنگام رفتن به ملاقات‌های حساس و یا هنگام گفتگوهای حساس آن را همراه نداشته باشید.

کار هنوز تمام نشده! گام‌های مهم بعدی:

چه دستگاه خود را پس گرفته باشید چه نه، گام‌های زیر را دنبال کنید:

- گام اول: فکر کنید که به چه منظور از این دستگاه استفاده کرده‌اید، آیا اطلاعات حساس مانند فهرست افراد در ارتباط با شما، محل‌ها و یا محتوای پیغام‌های شما روی این دستگاه است؟ آیا این اطلاعات می‌توانند برای شما یا دوستانتان مشکل‌ساز شوند؟
- گام دوم: شبکه‌ی دوستان خود را از این اتفاق مطلع کنید. به افراد و سازمان‌های کلیدی و در معرض خطر بالا که با آن‌ها کارکرده‌اید به طور خصوصی اطلاع دهید. اگر صلاح می‌دانید، فهرستی از حساب‌های خود را که به طور بالقوه در معرض خطر قرارگرفته‌اند تهیه کرده و روی تارنما یا حساب شبکه اجتماعی خود منتشر کنید.
- گام سوم: آیا در حساب‌ها و دستگاه‌های دیگر هم از همان رمز عبور استفاده کرده‌اید؟ در این صورت همین کارها را بری آن دستگاه‌ها و حساب‌ها هم انجام دهید. ممکن است آن‌ها هم درخطر باشند.

- گام چهارم: در صورت امکان تاریخچه اتصالات و فعالیت همه‌ی حساب‌های متصل به آن دستگاه را بررسی کنید (این امکان روی فیس‌بوک و گوگل و دیگر سرویس‌دهندگان رایانامه وجود دارد). بررسی کنید که آیا حسابتان هنگامی‌که شما آنلاین نبوده‌اید مورداستفاده قرارگرفته است؟ آیا کسی از یک IP و مکان نامعلوم به حساب شما ورود شده است؟ برای اطلاعات بیش‌تر به بخش دزدی حساب کاربری مراجعه کنید.
- گام پنجم: تنظیمات همه‌ی حساب‌های کاربری متصل به این دستگاه را بررسی کنید. آیا تغییر کرده‌اند؟ برای حساب‌های رایانامه(ایمیل)تان، فورواردهای خودکار، هماهنگ‌سازی با دستگاه‌های دیگر مانند تلفن همراه و رایانه و تبلت و یا حق دست‌رسی به برنامه‌ها را بررسی کنید.
- گام ششم: بررسی فعلی حساب/تاریخچه‌ی اتصال را حداقل برای یک ماه و هفته‌ای یک بار تکرار کنید تا مطمئن شوید که حساب شما فعالیت‌های عجیبی نشان نمی‌دهد. در غیر این صورت به بخش بدافزار مراجعه کنید.

در برابر حمله‌کنندگان، اقدامات احتیاطی اضافی در پیش گیرید:

پیش‌گیری کلید کاهش خطر دزدیده شدن، گم‌شدن یا ضبط شدن دستگاه شماست. با این وجود، اقداماتی ساده می‌تواند از اطلاعات شما به هنگام از دست دادن دستگاهتان محافظت کند. به رمزگذاری، رمز عبور، رمز ورود تلفن‌های همراه، ابزاری که پاک کردن اطلاعات از راه دور را میسر می‌کنند، نصب زنگ خطر نرم‌افزار به هنگام دزدیده شدن فکر کنید. Prey Anti-Theft ابزار ردگیری متن‌بازی است که این امکان‌ها را در اختیار شما قرار می‌دهد.

تحقیق کنید

اگر دستگاه شما توسط فرد سومی دزدیده و یا ضبط‌شده، خوب است که بدانید چه اتفاقی افتاده است. فکر می‌کنید چه کسی ممکن است شما یا سازمانتان را مورد هدف قرار دهد؟ آیا این تهدید به کار شما مربوط است؟ در بخش منابع مفید پیوندهایی وجود دارد که پیشنهادها و حقه‌هایی برای پیش‌گیری از موارد اورژانسی دیجیتالی و فعال بودن شما در امنیتتان ارائه می‌دهد.

پیوندها و منابع مفید

امنیت در جعبه

الگوهای تهدید و دفاع شخصی در برابر نظارت

بدافزارها

بدافزار یک نرم‌افزار مخرب است که تصاحب بی‌اجازه دستگاه شما توسط یک کاربر دیگر، دولت و یا یک شخص سوم را برای شنود و نظارت، ضبط صدا، ویدیو و غیره را ممکن می‌سازد.

درحالی‌که بیش‌تر بدافزارها برای استفاده مجرمان طراحی‌شده‌اند، کارگزاران دولتی به طور فزاینده در حال استفاده از بدافزارها برای نظارت و شنود، جاسوسی و خراب‌کاری هستند. بدافزارها برای مقاصد مختلفی چون کسب کنترل دستگاه قربانی طراحی می‌شوند. گاهی بدافزارها از دست‌رسی به دستگاه برای فرستادن هرزنامه (اسپم)، دزدیدن اعتبارات شبکه‌های اجتماعی و رایانامه (ایمیل) و یا حساب بانکی، مسدود کردن تارنماها و جمع‌آوری اطلاعات حیاتی از روزنامه‌نگاران، مدافعان حقوق بشر، سازمان‌های غیردولتی کنش‌گران و وبلاگ‌نویسان استفاده می‌کنند. اگر احتمال می‌دهید که دستگاه شما به یک بدافزار آلوده شده باشد، اقدامات زیر می‌تواند کمک‌کننده باشد:

با پاسخ به چند سؤال کوچک آغاز کنید:

- آیا مطمئن هستید که این دزدی حساب یا به خطر افتادن رمز عبور نیست؟برای اطلاعات بیش‌تر به بخش دزدی حساب مراجعه کنید.
- نشانه‌های خطری که شما را تهدید می‌کند چیست؟ برای اطلاعات بیش‌تر ادامه‌ی متن را بخوانید.

نشانه‌های خطر چیست؟

دلایل زیادی وجود دارند که شما به وجود یک بدافزار در دستگاهتان شک کنید. به این دلایل «نشانه‌های خطر» می‌گویند. این نشانه‌ها ممکن است شامل موارد زیر باشند:

- شما یک فایل ضمیمه‌شده یا پیوندی را بازکرده‌اید که فکر می‌کنید مخرب بوده است.
- دوربین دستگاهتان -وقتی از آن استفاده نمی‌کنید- روشن می‌شود.
- حساب‌های شما چندین بار مورد خطر قرار گرفته‌اند حتا بعد از تغییر رمز عبور.

ممکن است دلایل زیر نیز علت شک شما به وجود بدافزار باشد:

- دستگاه شما ضبط شده سپس برگردانده شده است.
- کسی بی‌اجازه وارد خانه‌ی شما شده و دستگاه شما را دست‌کاری کرده است.
- بعضی از اطلاعات شخصی شما که تنها در دستگاه خودتان موجود بوده به صورت عمومی منتشرشده است.
- گروه شما مورد هدف دولت، مراجع قانونی و یا یک کارگزار با امکانات غیرعادی قرارگرفته است.

گام‌های نخست برای کاهش مشکل

بعد از آن که مطمئن شدید که قضیه‌ی دزدی حساب نیست و نشانه‌های واضح خطر را مشاهده کردید دو رویکرد عملی وجود دارد: پاک‌سازی دستگاهتان، یا یافتن دلیل مشکل/حمله و سپس پاک‌سازی دستگاهتان. اولویت اول شما احتمالاً پاک‌سازی و قابل استفاده کردن دستگاهتان است. فهمیدن خود اتفاق و پیدا کردن عامل اتفاق ممکن است در درجه‌ی دوم اهمیت باشد. با این وجود، دریافتن اطلاعاتی دقیق از دشمنتان، توانائی‌های فنی آن‌ها و این که آیا حمله‌کننده‌ی احتمالی (دولتی یا فرد سوم) دارای فناوری نظارت اینترنتی است یا نه بسیار مهم خواهد بود. اگر دریافتن دلیل حمله و شناسایی حمله‌کننده به وضعیت شما مربوط است، لازم است که قبل از پاک‌سازی دستگاه به جمع‌آوری و تحلیل اطلاعات در مورد بدافزار احتمالی بپردازید. برای جمع‌آوری اطلاعات و تحلیل بدافزار به بخش گام‌های احتمالی برای تحلیل‌گر سطح اول مراجعه کنید، در غیر این صورت به بخش زیر بروید.

پاک‌سازی دستگاه

اگر انتخاب کردید که بدون دریافتن دلیل حمله و بدافزار دستگاه خود را پاک‌سازی کنید مسائل زیر را در نظر بگیرید.

1. هیچ راه حل سریع و قاطعی برای پاک‌سازی دستگاه شما وجود ندارد. حتا پس از کامل کردن گام‌های پیش رو، یک بدافزار سطح بالا (مانند FinFisher) می‌تواند هم‌چنان فعال باشد. با این وجود این گام‌ها برای از بین بردن بیش‌تر بدافزارها که شما با آن روبه‌رو هستید کافیند مگر این که مورد هدف یک حمله‌کننده‌ی بسیار پیشرفته قرارگرفته باشید.

2. اگر فکر می‌کنید که هدف یک حمله‌ی دولتی قرارگرفته‌اید و نشانه‌های خطر بعد از پاک‌سازی ویروس توسط گام‌های زیر هم‌چنان باقی ماندند، دستگاه را از اینترنت جدا کرده، خاموش، از برق کشیده، در صورت امکان باتری را درآورید و از یک حرفه‌ای کمک بگیرید. می‌توانید به فهرستی که در بالا به آن اشاره شده اعتماد کنید.

نرم‌افزار ضد ویروس (Anti-Virus)

نرم‌افزار ضد ویروس می‌توانند یک گام اولیه‌ی مؤثر برای محافظت دستگاه‌ها در برابر در صد بالایی از بدافزارها بردارد. با این وجود، نرم‌افزارهای ضد ویروس همیشه در برابر حمله‌های هدف‌دار، مخصوصاً توسط عاملان دولتی، غیر مؤثرند. با این حال، این نرم‌افزار هم‌چنان یک ابزار دفاعی ارزشمند علیه حمله‌های غیر هدف‌دار (و البته هم‌چنان خطرناک) است. در زیر لیست غیر کاملی از انتخاب‌های ممکن تهیه شده است. پیش از آن دقت داشته باشید که تصور غلطی بین کاربران وجود دارد و آن این است که سیستم‌عامل‌های مک (شرکت اپل) یا لینوکس نیازی به ضد ویروس ندارند.

- برای ویندوز: Microsoft Safety Scanner یا F-Secure یا Kaspersky یا ClamAV یا TrendMicro
- برای مک: ClamXav یا Avast
- برای لینوکس: ClamAV یا Avast یا MacAfee

وقتی از نرم‌افزار ضد ویروس استفاده می‌کنید، مطمئن شوید که به روز است. اگر ویروسی شناسایی شد، گام‌های زیر پیشنهاد می‌شوند.

- گام اول: از به روز بودن نرم‌افزار ضد ویروس اطمینان حاصل کنید.
- گام دوم: از پیغام‌ها اسکرین‌شات بگیرید.
- گام سوم: به قدم‌های توصیه‌شده برای از بین بردن ویروس عمل کنید.
- گام چهارم: پس از انجام راهنمایی‌های بخش ارتباط امن‌تر در بالا، اسکرین‌شات را به یک فرد متخصص امنیت بفرستید.

هنوز تمام نشده! گام‌های مهم بعدی را دنبال کنید:

اگر شک دارید که موردحمله‌ی یک عامل دولتی قرارگرفته‌اید و یا می‌خواهید در مورد حمله یا حمله‌کنندگان بدانید، مهم است که تا حد ممکن اطلاعات قانونی/قضایی جمع کنید؛ لطفاً به بخش گام‌های توصیه‌شده برای تحلیل‌گر سطح اول مراجعه کنید. در بعضی از رایانه‌ها می‌شود هارد دیسک را تعویض کرده، هارددیسک آلوده را برای تحلیل نگه دارید و با هارد دیسک جدید کارکنید.

- از فایل‌های خود پشتیبان تهیه کرده و سیستم‌عاملتان را دوباره نصب کنید. امکان ندارد از نابودی کامل ویروس مطمئن شد. حمله‌کنندگان پس از نصب یک بدافزار معمولاً بدافزارهای دیگری نیز نصب می‌کنند؛ بنابراین، همیشه توصیه می‌شود که بعد از یک پاک‌سازی کامل هارد دیسک، یک سیستم‌عامل جدید نیز نصب شود. در صورت امکان، تحقیق کنید ببینید جایگزین کردن هارد دیسک امکان‌پذیر است یا نه.

- بی‌شک پس از باز-نصب سیستم‌عامل می‌خواهید به فایل‌های خود دست‌رسی داشته باشید. در نظر بگیرید که بدافزار ممکن است فایل‌های شما را هم آلوده کرده باشد. پس از باز-نصب سیستم‌عامل، گام‌های زیر را بردارید:
- در صورت امکان، مدارک خود را که قبل از آلودگی از آن‌ها پشتیبان گرفته‌اید بازیابی کنید.
- اگر نمی‌دانید دستگاه شما چه زمانی به بدافزار آلوده‌شده است، یا اگر فکر می‌کنید مدارک و فایل‌های خاصی به بدافزار آلوده هستند، چند کار می‌تواند انجام دهید:
- فایل‌های قابل‌اجرای خود را از یک منبع موثق دریافت کنید.
- اگر عامل حمله توسط یک متخصص فنی شناسایی‌شده و بدافزار در حال آلوده کردن مدارک دیگر است، یک راه حل می‌تواند بارگذاری و باز کردن آن‌ها در Google Docs و دریافت دوباره آن‌ها ازآنجا باشد. در بیش‌تر موارد باز کردن یک مدرک مشکوک در Google Docs راه حل خوب است. مدارک و فایل‌ها، رایانه‌ی شما را آلوده نخواهند کرد و قابل ویرایش خواهند بود.
- یک راه حل دیگر کپی مدارک روی یک حافظه‌ی USB و باز کردن آن‌ها در نرم‌افزار پاک‌ساز حافظه‌ی CIRCLean است. با استفاده از این دستگاه بدافزاری به حافظه‌ی USB جدید کپی نخواهد شد، اما مدارک به یک تصویر یا پی‌دی‌اف، در یک فرمت تنها قابل‌خواندن و ویرایش ناپذیر تبدیل می‌شود.

گام‌های توصیه‌شده برای یک تحلیل‌گر سطح اول

گام‌های در پیش رو باید تنها توسط فردی با مقداری تجربه در زمینه‌ی امنیت اجرا شود. اگر شما تجربه‌ی لازم برای دنبال کردن گام‌های زیر را ندارید لطفاً از یک متخصص کمک بگیرید. در صورت امکان، از طریق کانال‌های امن و با استفاده از راهنمایی‌های بخش ارتباطات امن‌تر با آن‌ها تماس بگیرید.

گام‌های اول:

- اگر نشانه‌های خطر یک رایانامه (ایمیل) است، سرآیندها (Header) را جمع‌آوری کرده و بررسی کنید. گوگل یک ابزار ساده برای انجام خودکار این بررسی آماده کرده است.
- در صورت امکان، خود بدافزار را به روشی امن به دست بیاورید و با جستجوی Hash این فایل در سامانه Virus Total بررسی کنید که آیا این فایل تاکنون بارگذاری شده است یا خیر.
- اگر فایل محرمانه نیست، می‌توانید آن را در سامانه Malwr بارگذاری کرده و نتیجه را بررسی کنید.
- اگر فایل مشکوک از یک پیوند آمده است، URL را گرفته و در سامانه‌های URLQuery یا Wepawet بررسی کنید.

گام بعدی چیست؟

گام اول: جمع آوری اطلاعات برای تحلیل بیش‌تر

اطلاعات زیر برای تحلیل بیش‌تر، توسط شما یا هر شخص دیگری مورد نیاز است. توصیه می‌شود بیش‌تر -یا در حد امکان همه‌ی- اطلاعات زیر را برای تحلیل بیش‌تر جمع‌آوری کنید.

- اطلاعات روی سیستم (سخت‌افزار، جزئیات سیستم‌عامل، شامل نسخه و وضعیت به‌روزرسانی)
- محل قربانی و اطلاعات محلی سیستم (منبع IP، کشور، زبان کاربر)
- فهرست کاربرانی که از دستگاه استفاده می‌کنند
- در مورد رایانامه (ایمیل) مشکوک: سرآیند (Header) کامل
- در مورد پیوند مشکوک: پیوند کامل، برچسب زمانی و اسکرین‌شات
- داشتن یک کپی از صفحه ی وب و اطلاعات دزدیده شده مربوط به آن صفحه، مفید خواهد بود.
- رونوشت از حافظه. (خودآموز رونوشت گرفتن از حافظه را در این پیوند بیابید)
- یک شبیه‌سازی از حافظه‌های ذخیره‌سازی (Disk images). (خودآموز شبیه‌سازی حافظه ذخیره‌سازی را در این پیوند بیابید)
- نتایج ابزار بررسی یک‌پارچگی (اگر استفاده شده است)

- ارزیابی امکان جمع‌آوری از راه دور اطلاعات مستدل و قابل استفاده در دادگاه و در صورت امکان، برقراری یک راه ارتباطی مناسب

گام دوم: تحلیل بدافزار

اگر دارای مهارت‌های لازم برای پردازش اطلاعات نیستید، آن را به یک متخصص بدافزار آموزش‌دیده و مورد اعتماد یا یکی از سازمان‌های زیر منتقل کنید:

- EFF؛ info@eff.org https://www.eff.org/
- Citizen Lab؛ info@citizenlab.org http://citizenlab.org/
- CIRCL؛ info@circl.lu http://www.circl.lu/

در برابر حمله‌کنندگان، اقدامات احتیاطی اضافی در پیش گیرید:

بدافزار به صورت بالقوه خطرناک‌ترین حمله به یک کنش‌گر است، زیرا دست‌رسی آسان به اطلاعات حساب و مدارک شخصی و کاری مرتبط را فراهم می‌سازد. هیچ راه ساده و منحصر به فردی برای محافظت شما در برابر بدافزارها وجود ندارد، اما می‌توانید خود را به یک حریف سخت‌تر تبدیل کنید.

اما در نظر بگیرید که بدافزارهای هدف‌دار و تخصصی توسط بهترین نرم‌افزار ضد ویروس‌ها هم شناسایی نخواهند شد. گام اول و دوم شما را در برابر بدافزارهای قدیمی‌تر محافظت می‌کنند، اما تنها با تغییر رفتار خود می‌توانید مقاومت خود را بهبود بخشید.

- گام اول: به‌روزرسانی نرم‌افزارها را به طور مداوم است، مخصوصاً سیستم‌عامل و مرورگر.
- گام دوم: یک نرم‌افزار ضد ویروس نصب و تنظیم کنید و اطمینان حاصل کنید که به طور مداوم و خودکار به‌روزرسانی می‌شوند. بعضی نرم‌افزارهای ضد ویروس پس از تمام شدن دوره‌ی امتحانی متوقف می‌شوند.
- گام سوم: رفتار خود را تغییر دهید. رایانامه (ایمیل) و فایل‌های پیوست در هنگام گفت‌وگوی اینترنتی با دیگران از متداول‌ترین عاملان حمله هستند. در چنین مواقعی است که رایانه‌ی آلوده‌ی یک دوست به صورت خودکار پیوست‌های مخرب و آلوده به رایانه‌ی دیگر دوستان می‌فرستد. از دوستان خود بخواهید که تا جای ممکن مدارک و فایل‌ها را به صورت متن ساده بفرستند. هرگز فایل‌های پیوست غیر منتظره را بدون اطمینان از این که فرد فرستنده قصد فرستادن داشته است را باز نکنید. جنبش تبت در Detach from Attachments توصیه‌های بیش‌تری دارد. استفاده از یک سرویس سوم مانند Google Docs برای باز کردن فایل‌های Office به شما امکان خواندن و ویرایش محتوای آن با کم‌ترین خطر در برابر هجوم یک بدافزار را می‌دهد.
- گام چهارم: محافظت‌های بیش‌تر با اضافه کردن افزونه‌هایی مانند HTTPS Everywhere یا NoScript به مرورگر.

تحقیق کنید

اگر دستگاه شما توسط تهدید یا حمله‌ی هدف‌دار قرار گرفته، مهم است که بدانید چرا و توسط چه کسی هدف قرار گرفته شده‌اید.

چرا مورد حمله قرار گرفته‌اید؟ فکر می‌کنید چه کسی ممکن است بخواهد شما یا سازمانتان را مورد هدف قرار دهد؟ آیا به کار شما مربوط است؟ در بخش منابع مفید پیوندهایی وجود دارد که شما را برای پیش‌گیری از شرایط بحرانی دیجیتالی و فعال بودن در امنیت دیجیتالی‌تان راهنمایی می‌کنند.

توسط چه کسی: توانائی‌های فنی دشمنانتان در چه حدی است؟ آیا حمله‌کننده‌ی احتمالی (یک ارگان دولتی یا یک شخص سوم) شناخته‌شده در زمینه‌ی نظارت اینترنتی است؟ در بخش گزارش حمله‌های بدافزاری دولتی، اطلاعات بیش‌تری در مورد راه‌های مختلفی که دولت‌ها از بدافزار برای حمله‌های هدف‌دار استفاده کرده‌اند پیدا می‌کنید.

مستندسازی: به یادآوردن جزئیاتی چون زمان و تاریخ کلیک روی یک پیوند مشکوک مشکل خواهد بود. بنابراین، توصیه می‌کنیم یک دفتر یادداشت کنار رایانه خود برای یادداشت زمان و تاریخ اتفاقات عجیب داشته باشید. در بعضی موارد متخصصان توانسته‌اند یک نوع خاص بدافزار را با ربط دادن زمان و تاریخ حمله و ویژگی‌های خاص یک حمله و یا یک نشانه خطر احتمالی شناسایی کنند.

گزارش‌های حمله‌های بدافزاری دولتی

- گزارش‌های سوریه
- گزارش‌های ویتنام
- گزارش فینفیشر
- گزارش کت آی
- گزارش Hacking Team

منابع مفید

- Detach from Attachments
- مرورگر گوگل کروم و نسخه متن‌باز آن، کرومیوم، اطلاعات بسیار خوبی در مورد تارنماهای مشکوک ارائه می‌کنند.
- اطلاعات بیش‌تری در مورد ویروس‌ها و جاسوس ابزارها

کاهش اثرات مخرب حملات گسترده عدم سرویس‌دهی (DDoS)
یک تهدید علیه روزنامه‌نگاران مستقل، تارنماهای خبری و وبلاگ‌نویسان، خاموش شدن صدای آن‌ها به دلیل در دست‌رس نبودن یا تغییر شکل (deface) تارنماشان است. در بسیاری موارد، ممکن است این یک مشکل خسته‌کننده ولی بی‌ضرر باشد ولی بعضی وقت‌ها، ممکن است به خاطر یک حمله‌ی «عدم سرویس‌دهی» یا تصاحب تارنما باشد. این بخش بسته‌ی کمک‌های اولیه دیجیتال، شما را با چند گام ساده اولیه برای شناسایی مشکل احتمالی آشنا می‌کند. اگر تارنمای شما مورد حمله‌ی «عدم سرویس‌دهی» قرارگرفته، تعدادی راه حل فوری پیشنهاد می‌شود.

به طور کلی، مهم است بدانید که برای در دست‌رس نبودن تارنمایتان دلایل متعددی وجود دارد. در بیش‌تر موارد، علت اشتباهات برنامه‌نویسی یا مشکلات فنی شرکت میزبان است. بعضی مواقع، مشکلات دیگر مانند چالش‌های قانونی ممکن است یک سرویس میزبان را وادار به پائین آوردن یک تارنما کند. اگر تجربه‌ی میزبانی نداشته باشید، پیدا کردن مشکل و راه حل‌های احتمالی سخت و زمان‌بر خواهد بود. بنابراین اولین گام تماس با یک فرد مورد اطمینان است که می‌تواند به شما در مورد تارنمایتان کمک کند، خواهد بود؛ کسانی مثل مدیر تارنمایتان، کسانی که در راه اندازی تارنمایتان به شما کمک کردند و شرکت میزبان تارنمایتان.

پس از بررسی چالش‌های معمول زیر، تماس با مدیر تارنمایتان و شرکت سرویس میزبانی می‌تواند راه حل خوبی باشد. ممکن است مشکل شما هنوز به آن‌ها گزارش نشده باشد، مشکل موقتی باشد و یا تارنمای میزبان هنوز از مشکل مطلع نشده باشد. یک رابطه‌ی خوب با سرویس‌دهندگان بسیار به کار خواهد آمد. شفاف و مؤدب باشید و نتایج بررسی‌های خود را با استفاده از این سؤالات، در اختیار آن‌ها قرار دهید تا به آن‌ها در عیب‌یابی سریع کمک کنید.

با پاسخ به چند سؤال کوچک آغاز کنید

اطلاعات‌پایه

- چه کسی تارنمای شما را راه‌اندازی کرده است؟ آیا به آن‌ها برای کمک دست‌رسی دارید؟
- سرویس‌دهنده‌ی میزبان شما کیست؟ سرویس‌دهنده‌ی میزبان یا Hosting Company شرکتی است که سرور تارنمای شما را تأمین می‌کند. اگر نمی‌دانید از این ابزار استفاده کنید.
- آیا جزئیات ورود و خروج حساب خود را دارید؟
- دامنه‌ی خود را از کدام شرکت خریده‌اید؟ در بعضی موارد این تارنما میزبان شما نیز هست، اما می‌تواند شرکت دیگری هم باشد.
- آیا جزئیات ورود و خروج برای خدمات نام دامنه‌ی خود را نیز دارید؟ اگر نه، پیدا کردن این جزئیات اولین گام شما برای بازیابی تارنمایتان است.
- چه کسی به این جزئیات حساب امکان دست‌رسی داشته است؟

اطلاعات تشخیصی

دلایل مختلفی برای در دست‌رس نبودن تارنمای شما وجود دارد. ممکن است از شبکه تا سیاست‌گذاری، میزبانی، مسدود شدن، نرم‌افزار، تغییر شکل و مشکلات عمل‌کردی باشد. بخش زیر هر کدام از این مشکلات و نحوه‌ی تشخیص آن‌ها را توضیح داده است.

- آیا میزبان شما کار می‌کند ولی تارنما شما از دست‌رس خارج‌شده؟ به تارنمای «آیا تنها من مشکل دارم» سری بزنید. ممکن است که تارنمای در دست‌رس باشد ولی شما آن را نبینید. این مشکل شبکه‌ی شماست. ممکن است که اتصال اینترنتتان مشکل داشته باشد یا شرکت خدمات دهنده‌ی اینترنت یا دولت دست‌رسی شما به تارنمایتان را مسدود کرده باشند. هم‌چنین ممکن است به معنی از کار انداخته شدن حساب کاربری‌تان باشد.
- آیا پیغامی از طرف سرویس میزبانی تارنمایتان مشاهده می‌کنید؟ ممکن است که تارنمای شما ممکن است به خاطر عدم پرداخت صورت‌حساب، حق نشر یا دلایل قانونی پائین آمده باشد. این مشکل سیاست‌گذاری است. نخست از به‌روز بودن اطلاعات صورت‌حسابتان و عدم وجود بدهی پرداخت نشده روی سرویس میزبانی یا نام دامنه‌تان اطمینان حاصل کنید. اگر پیغام مربوط به یک

مسئله‌ی حقوقی یا قانونی است، این منبع تهیه شده توسط EFF، برای یادگیری بیش‌تر مکان مناسبی هستند.

- آیا تارنمای شما به هیچ عنوان باز نمی‌شود؟ ممکن است مشکل از سرویس میزبانی باشد، که در ین صورت شما دچار مشکل میزبانی هستید. آیا می‌توانید تارنمای شرکت میزبان خود را ببینید؟ توجه کنید که منظور بخش مدیریت تارنما خودتان نیست، بلکه متعلق به شرکت یا سازمانی است که تارنما شما را میزبانی می‌کند. دنبال یک صفحه‌ی وضعیت سرورهای شرکت میزبان بگردید (مانند status.dreamhost.com). هم‌چنین می‌توانید در توییتر دنبال کاربرانی که مشکل مشابه دارند بگردید. یک جستجوی ساده «در دست‌رس بودن (اسم شرکت)» مشخص می‌کند که آیا دیگران هم این مشکل رادارند یا نه.
- آیا قادر به دیدن تارنماهای دیگر با محتوای مشابه تارنمای خود هستید؟ دیدن تارنماهای مرتبط با تارنمای شما و پوشش دهنده‌ی مسائل مشترک را امتحان کنید. هم‌چنین تارنمای خود را با تور یا سایفون امتحان کنید، اگر جواب داد شما با مشکل مسدود شدن مواجه هستید یعنی برای دیگر نقاط جهان آنلاین هستید اما در کشور خودسانسور شده‌اید.
- آیا پیغام‌های خطا می‌بینید؟ ممکن است یک مشکل نرم‌افزاری باشد. به هر تغییری که خودتان یا تیمتان به تازگی ایجاد کرده‌اید توجه کرده و با مدیر تارنمایتان تماس بگیرید. فرستادن یک اسکرین‌شات، پیوند صفحه‌ی مشکل‌دار و هر پیغام خطایی می‌تواند به مدیر تارنمایتان برای پیدا کردن دلیل مشکل کمک کند. هم‌چنین می‌توانید پیغام خطا را کپی و جستجو کنید و ببینید آیا مشکل به راحتی قابل حل است یا نه.
- آیا تارنماهای دیگر را می‌بینید (مانند یک تارنمای خبری: BBC یا رادیو فردا)؟ ممکن است اینترنتتان دچار مشکل شده باشد و امکان دیدن هیچ صفحه‌ای را نداشته باشید. در این صورت باید با شرکت سرویس‌دهنده‌ی اینترنت تماس بگیرید. گاهی اوقات با راه‌اندازی مجدد دستگاهتان مشکل حل می‌شود.
- آیا از مرورگرتان اخطارهایی در مورد وجود بدافزار روی تارنمایتان می‌بیند؟ ممکن است یک مشکل تغییر شکل (defacement) باشد. گام‌های زیر را دنبال کنید؛ باید با سرویس میزبانتان تماس بگیرید و بخش دزدی حساب کاربری را مرور کنید.
- آیا تارنمایتان با وقفه و به کندی باز می‌شود؟ تارنما شما ممکن است به خاطر تعداد بالای تقاضا برای سر زدن به مشکل برخورده باشد، این مشکل عمل‌کرد است. این یک خبر خوب است به این دلیل که تارنمای شما محبوب شده است و تنها به مقداری بهینه‌سازی برای پاسخ بهتر به خوانندگان احتیاج دارد. برای یک برنامه بلندمدت بهبودسازی با تحلیل‌گر تارنمایتان تماس بگیرید. هم‌چنین می‌توانید با مدیر تارنما یا سرویس میزبانی‌تان برای راهنمایی بیش‌تر تماس بگیرید. بسیاری از سرویس‌های وبلاگ‌نویسی و سامانه‌ی مدیریت محتوای محبوب (جوملا، وردپرس، دروپال و دیگران) پلاگین‌هایی برای ذخیره کردن محلی تارنمایتان و یک‌پارچه کردن CDNها دارند که عمل‌کرد و مقاومت تارنما را بهبود می‌بخشند. بسیاری از راه حل‌های زیر می‌توانند مشکلات عمل‌کردی را نیز بهبود ببخشند.

اولین گام‌ها برای کاهش مشکل

وقتی دچار مشکل حمله‌ی «عدم سرویس‌دهی» هستید

اگر تشخیص‌های بالا کمکی نکرد (یا شما یک مشکل عمل‌کرد شدید را تجربه می‌کنید) تارنما شما ممکن است قربانی حمله «عدم سرویس‌دهی» باشد. این اتفاق زمانی رخ می‌دهدکه یک یا چند کاربر بد نیت سعی می‌کنند تارنما را مداوم و با استفاده از ابزار اتوماتیک، بازدید کنند. با این کار کاربران حقیقی را از تارنمایتان محروم می‌کنند. بعضی مواقع یک حمله‌کننده سعی دارد این کار را انجام دهد که معمولاً مشکل بزرگی نمی‌تواند ایجاد کند مگر این که برای پهنای باندی که پرداخت می‌کنید. حمله‌ی گسترده‌ی «عدم سرویس‌دهی» جایی معنا می‌دهد که حمله‌کننده از هزاران ماشین تحت کنترلش برای مورد هدف قرار دادن یک تارنما استفاده کند.

- گام اول: با یک فرد مطمئن که می‌تواند به شما کمک کند تماس بگیرید.
- گام دوم: با شرکتی که دامنه را از آن خریداری کرده‌اید تماس بگیرید (مانند EasyDNS، Network Solutions، GoDaddy) و «Time to Live» یا TTL را به یک ساعت تغییر دهید. این تغییر می‌تواند به شما کمک کند که بعد از این حمله تارنمایتان را سریع‌تر هدایت کنید. (زمان

پیش‌فرض ۷۲ ساعت یا ۳ روز است). این قسمت از تنظیمات، بیش‌تر اوقات در قسمت امکانات پیشرفته دامنه شما قرار دارد و بعضی مواقع به عنوان بخشی از SRV و یا Service records.

- گام سوم: تارنمای خود را به یک سرویس کاهش حملات گسترده عدم سرویس‌دهی منتقل کنید. فهرست کامل را ببینید. این مقاله به شما کمک می‌کند تا یک خدمات‌دهنده‌ی خوب پیدا کنید.
- گام چهارم: به محض بازپس‌گیری کنترل، نیازهای خود را بازبینی کنید و بین یک سرویس میزبانی امن و یا ادامه دادن با سرویس کاهش حملات گسترده عدم سرویس‌دهی تصمیم بگیرید.
- گام نهایی: خدماتی چون دیفلکت، این خدمت گوگل یا کلادفلر می‌توانند به شما کمک کنند که حد قابل قبولی این مشکل را برای همیشه حل کنید.

وقتی دچار مشکل تغییر شکل تارنما (Defacement) شده‌اید

- گام اول: تحقیق کنید که آیا وب سایت از روی سو نیت تصاحب شده است یا نه. یک کار تاسف آور اما قانونی، خریدن یک اسم دامنه است که به تازگی منقضی شده. این کار به اسم این انجام میشود که ترافیکی که تارنمای قبل برای مصارف تبلیغاتی داشته است را بگیرند. بسیار مهم ست که مبلغ نام دامنه خود را به طور منظم پرداخت کنید.
- گام دوم: اگر تارنمای شما تغییر شکل پیدا کرده است، اول کنترل ورود حساب تارنمای خود را به دست بیاورید و رمز عبور را تغییر دهید، به بخش دزدیده شدن حساب کاربری نگاه کنید.
- گام سوم: از تارنما تغییر شکل داده‌شده پشتیبان تهیه کنید که بتوانید برای تحقیق از آن استفاده کنید.
- گام چهارم: موقتاً تارنمای خود را غیر فعال کنید، از یک صفحه‌ی اصلی ساده یا صفحه موقت استفاده کنید.
- گام پنجم: ببینید تارنمای شما چگونه هک شده است. سرویس میزبانی‌تان ممکن است بتواند کمک کند.
- گام ششم: فایل‌های نسخه‌ی اصلی را از پشتیبان بازیابی کنید. اگر شما و شرکت میزبانی‌تان پشتیبان ندارید، ممکن است مجبور به بازسازی تارنمایتان از نقطه‌ی صفر باشید. هم‌چنین در نظر داشته باشید که اگر تنها پشتیبان شما در سرویس میزبانی باشد، یک حمله‌کننده می‌تواند آن‌ها را در هنگام کنترل تارنمایتان حذف کند پس پشتیبان گرفتن را فراموش نکنید.
- گام هفتم: به یک سیستم کاهش حملات گسترده عدم سرویس‌دهی (مانند دیفلکت) یا یک سرویس‌دهنده‌ی میزبانی امن (مانند VirtualRoad یا Qurium) نقل‌مکان کنید.

کار هنوز تمام نشده! گام‌های مهم بعدی را دنبال کنید

پیش از موردحمله قرار گرفتن اقدام کنید. همه سرویس‌های فهرست شده به شما برای بهبودی سریع در حین و بعد از یک حمله کمک می‌کنند، اما همین‌الان، قبل از موردحمله قرار گرفتن، می‌توانید از خودتان محافظت کنید. این کار با پائین آوردن استفاده از پهنای باند هزینه‌های شما را کاهش می‌دهد و شما را در هنگام حمله، پا بر جا نگه می‌دارد. اگر مورد حمله قرار بگیرید و نتوانید از پس آن بر بیاید سه روز طول می‌کشد تا آدرس تازه و امنتان ثبت و مورد استفاده قرار گیرد، پس تقریباً در همه‌ی موارد بهتر است آماده باشید و از همین‌الان شروع کنید.

1. اگر در حال تغییر سرویس میزبانی هستید، سرویس‌های میزبانی امن از شما می‌خواهند که تارنمای خود را کاملاً به سرور آن‌ها منتقل کنید. بسیاری از آن‌ها می‌توانند به شما کمک کنند. فایده‌ی این کار در این است که سرویس میزبان معمولاً ویژگی‌های حفاظتی دیگری در اختیار شما قرار میدهند. نکته منفی این ممکن است هزینه باشد (بسته به هزینه‌ای که شما همین‌الان می‌پردازید) و کنترل؛ شما نیاز دارید که به میزبان دامنه‌تان اعتماد داشته باشید زیرا کنترل بسیاری روی تارنما شما خواهد داشت.
نکات مثبت:
- خدمات مرکزی برای بیش‌تر، اگرنه همه، نیازهای تارنما شما فراهم می‌آورد.
- خدمات حفاظتی برای حملات گسترده عدم سرویس‌دهی، هک و حمله‌های هرزنامه‌ای فراهم می‌آورد.
- معمولاً خدمات و مشاوره‌های ثانویه بسیاری، حتا در بعضی موارد دفاع قانونی محدود را شامل می‌شوند.
- تیم‌های پشتیبانی کامل معمولاً برای کمک فراهم هستند.
نکات منفی

- شما باید تارنمایتان را با خدمات و موازین آن شرکت میزبانی کنید.
- شما باید به شرکت برای اداره‌ی تارنمایتان و حمایت از حقوقتان اعتماد کنید.
- این خدمات معمولاً بسیار گران‌تر هستند (اما شما مجبور به پرداخت دیگر هزینه‌های میزبانی و خدمات DNS نیستید)

2. خدمات کاهش حملات گسترده عدم سرویس‌دهی به شما این امکان را می‌دهند که تارنمای خود را از هرکجا که بخواهید میزبانی کرده و فقط نحوه‌ی استفاده و دست‌رسی دیگران به تارنمایتان را کنترل می‌کنند. استفاده از این خدمات بسیار ساده‌تر از انتقال میزبانی است. این خدمات، سرورهایی در سراسر دنیا دارند و شما هستید که کنترل کامل تنظیمات میزبانی و تارنمای خود را در دست دارید. یک چالش خدمات دارای نماینده این است که تارنماهای بسیار پیچیده ممکن است با ورود و خروج کاربرانی که مدیر نیستند و حوزه تعاملی/جاوا اسکریپت پیچیده دچار مشکل شوند. این مشکل را با مدیر تارنما و سرویس پروکسی‌تان در میان بگذارید؛ بسیاری از این مشکلات به آسانی حل می‌شوند.

نکات مثبت:

- هزینه‌هایی پائین تر (اغلب با یک سطح رایگان)
- برپایی راحت و سریع
- مجبور به تغییر میزبان تارنما فعلی خود نیستید
- می‌توانید سرویس را در هر زمانی قطع کنید یا تغییر دهید

نکات منفی:

- اختیارات پشتیبانی کم‌تر
- تمرکز عمده بر کاهش حملات گسترده عدم سرویس‌دهی؛ لزوماً شامل کمک در زمینه‌ی بدافزارها و فرستندگان هرزنامه نمی‌شود
- ترافیک رمزگذاری شده‌ی SSL به مدت کوتاهی توسط سرور پروکسی برای انتقال ترافیک از روی پروکسی خودشان به سرور شما رمز گشایی و دوباره کد گذاری می شود.

3. از یک خدمات دهنده خاص استفاده کنید. برای هر خدماتی باید با خدمات دهنده‌ی خود احساس راحتی کنید. این مربوط به اعتماد و هم‌چنین فهم مدل تجاری آن‌ها می‌شود: آیا شیوه آن‌ها، پول در برابر خدمات است؟ اگر نسخه رایگانی وجود دارد، آیا پشتیبانی کم‌تری دریافت می‌کند؟ آیا هزینه‌اش توسط دولت پرداخت می‌شود؟ بهتر آن است که از اول تا حد امکان از جزئیات مطلع باشید تا بعداً غافل‌گیر نشوید.

برای هر خدمتی که قصد استفاده از آن را دارید، سؤال‌های زیر را از خودتان بپرسید:

- ساختار شرکت/سازمان خدمات‌دهنده چیست و چگونه نگه‌داری می‌شود؟ آن‌ها ملزم به ارائه‌ی چه بررسی‌ها و گزارش‌هایی هستند؟ آیا این گزارش‌ها منجر به شکستن حریم خصوصی شما یا سازمانتان نمی‌شود؟ آیا چنین کمک‌هایی جز مرام سازمانتان است؟
- در چه کشور یا کشورهایی حضور حقوقی دارند و ملزم به رعایت قوانین و دیگر خواسته‌های حقوقی کجا هستند؟
- چه logهایی تولید می‌شوند و برای چه مدتی قابل‌دست‌رسی هستند؟
- آیا محدودیت‌هایی در مورد نوع محتوایی که سرویس میزبانی/پروکسی می‌کند وجود دارد؟ و آیا این محدودیت‌ها اثری روی تارنما شما خواهند داشت؟
- آیا محدودیت‌هایی در زمینه‌ی کشورهایی که به آن‌ها خدمات می‌دهند وجود دارد؟
- آیا فرمی از پرداخت را که برای شما مناسب باشد دارند؟ هزینه‌ی خدمات آن‌ها به جیب شما می‌خورد؟
- ارتباطات امن؛ باید بتوانید امن وارد شوید و با خدمات‌دهندگانتان خصوصی ارتباط برقرار کنید.
- آیا امکانی برای احراز هویت دو مرحله‌ای برای بهتر کردن امنیت دست‌رسی مدیر وجود دارد؟ این امکان و دیگر سیاست‌گزاری‌های مربوط به امنیت، خطر دیگر انواع حمله به تارنمایتان را کاهش می‌دهند.
- به چه نوع پشتیبانی مداوم دست‌رسی خواهید داشت؟ آیا یک هزینه‌ی اضافی باید برای پشتیبانی پرداخت کنید و آیا در صورت رایگان بودن، پشتیبانی کافی دریافت خواهد کرد؟
- آیا می‌توانید تارنمای خود را قبل از انتقال، از طریق یک تارنمای آزمایشی بررسی کنید؟

سؤال‌هایی برای خدمات میزبانی امن

- آیا آن‌ها در انتقال تارنمایتان به سرویسشان پشتیبانی کامل ارائه می‌دهند؟
- آیا خدمات، بهتر یا به همان اندازه خدمات میزبان کنونی شما، حداقل در ابزار/خدمات است؟ مسائل مهم:
  - بخش مدیریت مانند Cpanel
  - حساب‌های کاربری رایانامه (ایمیل) (تعداد، حجم، دسترسی از طریق SMTP و IMAP)
  - پایگاه داده (تعداد، انواع، دسترسی)
  - دسترسی از راه دور از طریق SFTP و SSH
  - پشتیبانی از زبان برنامه‌نویسی (PHP، Perl، دسترسی cgi-bin) یا سامانه مدیریت محتوا (Drupal، WordPress، Joomla) که تارنمای شما از آن استفاده می‌کند.

سؤال‌هایی برای خدمات کاهش حملات گسترده عدم سرویس‌دهی

- اگر از SSL استفاده می‌کنید (که به نام ترافیک امن شبکه نیز شناخته می‌شود)، از نحوه‌ی مدیریتی که بر SSL دارند سؤال کنید. در بعضی تنظیمات، آسان‌تر است که کلید SSL خصوصی خود را به آن‌ها بدهید. اگر این کار را می‌کنید، باید به خدمات دهنده‌ی خود اعتماد بالایی داشته باشید، زیرا آن‌ها می‌توانند خود را به عنوان تارنمای شما جا بزنند (در واقع این چیزی است که از شما با در اختیار گذاشتن پروکسی خود از آن‌ها می‌خواهید انجام دهند)
- در مورد اداره‌ی ورود و خروج کاربران تارنما (مدیر تارنما و ویراستار و مدیریت صفحات) بپرسید.
- در مورد قسمت‌های تعاملی تارنمایتان صحبت کنید (کاربرهایی که وارد می‌شوند، نظرات، نیازهای مدیریتی و ویراستاری، هم کنشی مجموعه صفحات و جاوا اسکریپت و پویانمایی). سرویس‌های پروکسی مختلف این‌ها را به انواع مختلف مدیریت می‌کنند، پس قبل از انتقال کامل، این موارد را امتحان کنید.

خدمات خاص کاهش آسیب

خدمات خاص در این پیوند همراه با تبصره‌های بیش‌تر فهرست شده‌اند. در نظر داشته باشید که این لیست کامل نیست و خدمات و سرویس‌های بیش‌تری هم وجود دارد. با این حال، این خدمات نقطه‌های شروع مناسب را نشان می‌دهند و توسط دیگران در رسانه‌های مستقل، حقوق بشری و انجمن‌های آزادی بیان استفاده شده‌اند. موارد زیر برای پوشش‌دهی فوری هستند:

خدمات میزبانی امن:

- Qurium (formerly Virtual Road)
- The Positive Internet Company
- Greenhost

خدمات پیش‌گیری از حمله‌ی گسترده عدم سرویس‌دهی:

- دیفلکت
- سامانه زره گوگل
- پروژه گالیله کلادفلر

در برابر حمله‌کنندگان، اقدامات احتیاطی اضافی در پیش گیرید.

حتا اگر دچار حمله‌ی عدم سرویس‌دهی نشده‌اید، این راهنما قدم‌هایی را برای آمادگی قبلی پیشنهاد می‌کند که امیدواریم ازکارافتادگی تارنمای شما پیش‌گیری کند. به بخش پاسخ‌گویی به یک حمله‌ی عدم سرویس‌دهی مراجعه کنید تا راه حل‌های معمول قابل‌استفاده برای الآن (قبل از حمله) را بررسی کنید. در بخش منابع مفید می‌توانید راهنمایی‌هایی برای سر پا نگه‌داشتن تارنمایتان پیدا کنید.

- فایل‌های پشتیبانی: همیشه مطمئن شوید که فایل‌های پشتیبانی دارید (که در جایی غیر از تارنمایتان ذخیره کرده‌اید!). بسیاری از سرویس‌های میزبانی و سامانه‌ها این مسئله را به عنوان بخشی از خدماتشان ارائه میدهند، اما بهتر است که نسخه‌های غیر آنلاینی از تارنمایتان هم داشته باشند.
- به روزرسانی: اگر از سامانه مدیریت محتوا (CMS) مانند وردپرس، جوملا یا دروپال استفاده می‌کنید، از به‌روز بودن فناوری تارنمای خود به آخرین نسخه اطمینان حاصل کنید، مخصوصاً اگر به دلایل امنیتی به‌روزرسانی شده باشند. اگر از نرم‌افزارهای سفارشی استفاده می‌کنید به انتقال به یک سرویس مدیریت محتوا که به صورت منظم به روز می‌شود فکر کنید.
- نظارت: خدمات بسیاری هستند که می‌توانند به طور منظم تارنمای شما را بررسی کنند و با رایانامه (ایمیل) و پیام کوتاه در هنگام در دست‌رس نبودن تارنمایتان با شما در تماس باشند. این مقاله ده تا از محبوب‌ترین‌ها را فهرست کرده است. در نظر بگیرید که رایانامه (ایمیل) یا شماره تلفنی که برای نظارت از آن استفاده می‌کنید مشخصاً به مدیریت تارنما ارتباط پیدا می‌کند.

تحقیق کنید

اگر قربانی عدم سرویس‌دهی یا تغییر شکل شده‌اید، مهم است که بدانید چرا موردحمله قرارگرفته‌اید و چرا حالا مورد چنین حمله‌ای قرار گرفته‌اید.

چرا موردحمله قرارگرفته‌اید و چرا حالا: چه کسی ممکن است بخواهد تارنما یا سازمان شما را مورد هدف قرار دهد؟ آیا به تازگی موردی مشکوک در تارنما خود دیده‌اید، آیا این تهدید به کار شما مربوط است یا تارنما شما ترافیک بالایی دارد و یا آیا نام دامنه شما منقضی شده است؟ چرا حالا؟ آیا تغییر تازه‌ای شما را به هدفی برای حمله‌های تغییر شکل (deface) یا عدم سرویس‌دهی تبدیل کرده است؟ در بخش منابع مفید پیوندهایی وجود دارد که شما را برای پیش‌گیری از شرایط بحرانی دیجیتالی و فعال بودن در امنیت دیجیتالی‌تان راهنمایی می‌کنند.

منابع مفید

- تارنمای من در دست‌رس نیست
- تارنمای خود را سرپا نگه‌دارید
- امنیت در جعبه
- الگوهای تهدید و دفاع شخصی در برابر نظارت

اعتمادسازی

در بخش ارتباطات امن ما راه‌هایی اولیه و اساسی برای آغاز اعتمادسازی بین جویای کمک و کمک‌کننده ذکر کرده‌ایم. این بخش اضافه کردن یک‌لایه فنی اعتماد و فهم ابزاری که به شما در داشتن یک ارتباط امن با تنها کسی که قصد ارتباط با او را دارید را هم در بردارد. گر چه این بخش بیش‌تر فنی است اما همه‌ی سعی خود را به کار بگیرید تا همه‌ی توصیه‌های آن را به کار ببندید؛ بدون شک استفاده از ابزار رمزگذاری از استفاده نکردن آن بهتر است.

ابزار رمزگذاری مانند OTR (خلاصه‌ی Off The Record) و PGP (خلاصه‌ی Pretty Good Privacy) مزایای بسیاری دارند. فایل‌ها و یا پیغام‌های رمزگذاری شده در برابر هرکسی که بخواهد به آن‌ها مخفیانه دست‌رسی پیدا کند -یا در آن‌ها اخلال ایجاد کند- دست خالی به خانه باز می‌گرداند. در واقع این فایل‌ها و پیام‌ها را از زمان خروج از رایانه‌ی شما تا رسیدن به مقصد، محافظت می‌کنند. مشکل اما دانستن دقیق مقصد نهایی واقعی است.

برای استفاده از چنین ابزاری باید آدرس صحیح و واقعی را برای فرستادن پیغام رمزگذاری شده بدانید. این تنها شامل آدرس رایانامه (ایمیل) یا اسم مستعار پیام فوری (IM) نمی‌شود، بلکه به اطلاعات بیش‌تری مثل کلید رمزگذاری مربوط به آن حساب کاربری نیز نیاز است. بیش‌تر این‌ها توسط رایانه‌تان انجام می‌شود، اما شما باید امضای نهایی را انجام دهید! ازلحاظ نظری، اگر شما سعی در ایجاد یک ارتباط امن با کسی دارید، حمله‌کننده می‌تواند آن اطلاعات رمزگذاری خاص را با اطلاعات خودشان جابه‌جا کرده و پیغام شما را بخواند. برای جلوگیری از این چند حیله وجود دارد.

اعتماد در تارنما

تارنماهای امن (آن‌هایی که با HTTPS شروع می‌شوند) دارای ساختاری هستند که مرورگرها تنها به تعداد محدودی شرکت قابل‌اعتماد برای کار کردن استناد می‌کنند. این امر کار را برای کاربران نسبتاً آسان می‌کند، اما اگر امنیت هرکدام از آن شرکت‌ها خدشه‌دار شده باشد (که تابه حال اتفاق افتاده است) و یا اگر این شرکت‌ها حاضر به همکاری با دولت‌هایی که ممکن است برای شما تهدید محسوب شوند شده باشند، همه‌ی شبکه اعتماد مشکل‌دار خواهد شد. این مدل برای یک نوع خاصی از امنیت رایانامه (ایمیل) که S/MIME نام دارد نیز استفاده می‌شود.

اعتماد در ابزار ارتباطی

برای رایانامه (ایمیل)، گفت‌وگو و تماس‌های تلفنی امن، قضیه سرراست‌تر است. موقعیت ایده‌آل است که شخص را شخصاً ملاقات کنید و اطلاعات اثر انگشت را مبادله کنید. مشخص است که این راه همیشه ممکن نیست. ابزارهای مختلف، راه‌های مختلفی برای حل این مشکل‌دارند. امنیت در جعبه یک بخش کامل برای ارتباطات خصوصی دارد.

گفت‌وگو با ویژگی OTR

در گفت‌وگو یا پیغام فوری، استاندارد کنونی برای اعتماد OTR یا Off The Record است. این Off the History موجود در هنگ‌آوت (سرویس پیام‌رسان گوگل) به این معنی که گوگل مکالمات را به صورت دائم ذخیره نمی‌کند، نیست. OTR نه تنها مزایای اساسی بالا (امنیت نقطه به نقطه و مقابله با دست‌درازی را ارائه می‌دهد، بلکه یک لایه‌ی اضافی امنیت هم دارد. هر جلسه‌ی ارتباط به صورت جداگانه محافظت می‌شود. این بدین معناست که اگر کسی توانسته باشد همه‌ی مکالمات خصوصی گفت‌وگو شما را ذخیره کند، شکستن رمز یک گفت‌وگو، خواندن گفت‌وگوهای دیگر را ممکن نمی‌سازد. به علاوه OTR یک درجه‌ی انکارپذیری را به مکالمه‌ها اضافه می‌کند. برای نمونه وقتی مکالمات شما محافظت و احراز هویت شوند، هیچ راهی برای اثبات این که آن مکالمه‌ها از طرف شما بوده‌اند وجود ندارد. OTR در نرم‌افزارهای Adium و Jitsi و Pidgin کار می‌کند.

برای بهره‌مندی از همه‌ی این‌ها، شما باید راهی برای «احراز هویت» کسی که با او گفت‌وگو می‌کنید داشته باشید. برای هر تماس امن در هر دستگاه، تنها یک بار مجبور به این کار هستید (می‌توانید از برنامه‌هایی مثل

KeySync استفاده کنید). ساختن کلید مشترک یک اعتماد دیجیتالی با کسی است که او را می‌شناسید و از طریق پرسیدن سوآلی انجام می‌شود که فقط شما دو نفر جواب آن را بدانید. برای امنیت بیش‌تر می‌توانید به هم زنگ بزنید و مستقیماً یک کد مخصوص حساب‌های کاربری خود را با هم مقایسه کنید، یا از همان روش پرسش و پاسخ در مورد چیزی که تنها شما دو نفر از آن اطلاع دارید استفاده کنید.

منابع

- احراز هویت در OTR
- جزییات فنی OTR

رایانامه (ایمیل) با PGP

PGP (یا Pretty Good Privacy) و معادل متن‌باز آن GPG (یا Gnu Privacy Guard) به شما این امکان را می‌دهند که رایانامه (ایمیل)ها و فایل‌های خود را برای خود و یا فرستادن به دیگران، رمزگذاری کنید. با افزونه‌هایی مانند Enigmail برای تاندربرد یا GPGOL برای Outlook می‌توانید به طور مؤثر از PGP برای محافظت از محتوای رایانامه (و نه عنوان و نام گیرنده‌ی رایانامه) استفاده کنید.

برای فرستادن یک رایانامه (ایمیل) رمزگذاری شده توسط PGP به کلیدهای PGP خود نیاز دارید. کلیدهای PGP جفتی هستند، یکی عمومی و یکی خصوصی. کلید عمومی مثل یک آدرس خانه است که هرکسی می‌تواند بداند اما تنها کسی با داشتن کلید خصوصی می‌تواند به پیغام‌های فرستاده‌شده به آن آدرس دست‌رسی داشته باشد، صاحب آن است. با جادوی PGP، فقط کسی که دارای آن کلید خصوصی آن آدرس است می‌تواند از آن آدرس پیغام بفرستد (که با کلید عمومی تائید می‌شد). به منابع فهرست شده در زیر برای بحث‌های بیش‌تر پیرامون عمل‌کرد PGP نگاه کنید.

البته مسئله پیدا کردن آدرس کلید عمومی است؛ دفتر تلفن‌های دیجیتالی برای کلیدهای PGP وجود دارد که می‌توانید با جستجوی نام یا رایانامه آن‌ها را پیدا کنید (sks-keyservers و pgp.mit محبوب‌اند) اما هیچ مرجعی ضمانت نمی‌کند که این شخص و کلید، همان فرد مورد نظر شما باشد. کاملاً ممکن است که کسی با بارگذاری کلید خود و رایانامه‌ی جعلی، خود را جای کسی دیگری جا زده باشد.

دوباره مسئله این است که باید راه دیگری از درست بودن کلید اطمینان حاصل کنید. بسیاری روی کارت ویزیت خود یا تکه کاغذهایی «اثر انگشت» کلید خود را نوشته‌اند و با هم رد و بدل می‌کنند یا آن‌ها را در تارنما یا حساب توییتر خود قرار می‌دهند (بعضی از این‌ها را می‌توانید در بخش ابتدایی این نوشته مشاهده کنید) اما این روش تنها برای گروه‌های کوچک دوستان کار می‌کند و نه در مقیاس شبکه‌ی جهانی.

می‌توانید کلید عمومی کسانی که در لیست خود دارید و به آن‌ها نسبتاً امنیت دارند را «امضا کنید». با این کار می‌تواند مشکل اعتماد را با به وجود آوردن یک «شبکه‌ی اعتماد» حل کند. برای نمونه اگر کلید کسی را تصدیق کرده‌اید و به آن‌ها برای تصدیق کلید دیگران اعتماد کرده‌اید، می‌توانید به کلیدهایی که آن‌ها تصدیق کرده‌اند هم اعتماد کنید. فراموش نکنید که با این کار به دیگران نشان می‌دهید که چه کسانی در لیست دوستانتان قرار دارند. به طورکلی تا زمانی که مطمئن باشید که کلید و آدرس رایانامه‌ی صحیح کسی را که می‌خواهید با او تماس بگیرید را دارید و به هرگونه تغییر مشکوک باشید، مسئله‌ی شبکه‌ی اعتماد مشکل بزرگی نیست و به سادگی می‌توانید از آن بگذرید.

منابع

- رمزگذاری چه طور کار می‌کند؟
- رمزنگاری چیست؟

صدای رمزگذاری شده: ZRTP

ZRTP از بسیاری جهات شبیه OTR است، برای هر مکالمه تغییر می‌کند و تاریخچه ارتباطاتتان را محافظت می‌کند. ZRTP در تماس‌های تلفنی رمزگذاری شده استاندارد است. با استفاده از Jitsi یا RedPhone یا Signal یا Silent Circle این رمزگذاری انجام می‌شود. برخی از این نرم‌افزارها از شما می‌خواهد که مجموعه‌ای از کاراکترهایی را برای کسی که با آن صحبت می‌کنید بخوانید تا تماسی که با صدای شما می‌آید را با مخلوطی از ویژگی‌های خاص تائید کند.

منابع

- راهنمای Jitsi
- راهنمای Silent Circle

منابع مفید

منابع مربوط به شرایط اورژانسی دیجیتالی

- بنیاد جبهه‌ی الکترونیک (EFF)
- مشارکت مدافعان دیجیتالی (Digital Defenders Partnership)
- مدافعان خط مقدم (Front Line Defenders)
- اینترنیوز (Internews)
- خانه آزادی (Freedom House)
- دسترسی (Access)
- کمیته‌ی حمایت از روزنامه‌نگاران (CPJ)
- گزارشگران بدون مرز (RSF)
- تیم امنیتی ایران (IranSec)

راهنماهای امنیت دیجیتال

- امنیت در جعبه
- دفاع شخصی در برابر نظارت
- امنیت اطلاعات برای روزنامه‌نگاران
- امنیت ارتباطات
- راهنمای کوتاه امنیت تلفن همراه

راهنماهای میزبانی امن و کاهش آسیب حمله‌ی گسترده «عدم سرویس‌دهی»

- تارنما من در دسترس نیست؛ مدارک و راهنما برای مقابله با حمله‌های گسترده عدم سرویس‌دهی
- اگر در حال تحقیق هستید که چگونه تارنما خود را در برابر حمله‌هایی که آن را آفلاین می‌کند مقاوم بسازید، اول این راهنمای بنیاد جبهه الکترونیک را بخوانید.
- AccessNow یک راهنمایی عمیق با منابع و روش‌های کاهش آسیب، به انگلیسی، فارسی، عربی و روسی تهیه‌کرده است. به این صفحه رفته و در سمت راست روی DoS کلیک کنید و یا نسخه‌ای از آن را از این آدرس دریافت کنید.

منابع مرتبط به موارد اورژانسی غیر دیجیتال

- مدافعان خط مقدم: برای مدافعان حقوق بشر که به موارد اورژانسی روبه‌رو شده‌اند، پشتیبانی فراهم می‌آورد
- S.A.F.E Initiative: آموزش‌های یک پارچه‌ی امنیت که امنیت را از طریق دیدگاه هویت دیجیتال، آگاهی‌رسانی فیزیکی و مراقبت روانی به شاغلین رسانه‌ها، ترکیب و تأمین می‌کند.
- Media Legal Defence Initiative: پشتیبانی از روزنامه‌نگاران، بلاگرها و رسانه‌های مستقل تحت خطر حقوقی
- کمیته حمایت از روزنامه‌نگاران (CPJ): کمک مستقیم به روزنامه‌نگاران درخطر و خانواده‌هایشان را فراهم می‌آورد
- کمیته حمایت از روزنامه‌نگاران (CPJ): راهنمای امنیت روزنامه‌نگاران

واژه‌نامه

- حمله‌ی گسترده عدم سرویس‌دهی (DDoS): حمله‌ی «عدم سرویس‌دهی» وقتی است که یک یا چند کاربر مخرب مانع از استفاده از یک سرویس مثل تارنما یا یک سرور گفت‌وگو می‌شوند. بعضی مواقع یک «حمله‌کننده» سعی دارد این کار را انجام دهد که به خودی‌خود معمولاً مشکلی برای تارنمای شما ایجاد نمی‌کند؛ مگر این که برای پهنای باند خود که برایش پول پرداخت می‌کنید. در حمله‌ی گسترده عدم سرویس‌دهی معمول‌تر است که یک حمله‌کننده از هزاران ماشین تحت کنترل خود یک تارنما را مورد هدف قرار می‌دهد.
- مقادیر DNS: مقادیر DNS مانند لیست تماس‌های اصلی یک دفتر تلفن در اینترنت است. همه‌ی سرورهای تارنما به وسیله یک سری حروف (نام دامنه) یا اعداد (آدرس IP) شناسایی می‌شوند؛ برای نمونه IP گوگل ۷۴.۱۲۵.۲۲۸.۶۹ است. با تغییر دادن این مقدار، می‌توانید یک آدرس IP دیگر برای یک تارنما بدهید، برای نمونه آدرس یک میزبان جدید یا یک پروکسی برای تارنما اصلی‌تان.
- نام دامنه (Domain Name): نام قابل خوانده شدن تارنمای شما. برای نمونه Google.com
- رمزگذاری نقطه به نقطه (end-to-end): بدین معنا است که پیغام‌ها و فایل‌ها، دستگاه شما را رمزگذاری شده ترک می‌کنند و تا رسیدن به مقصد موردنظرتان رمزگذاری شده باقی می‌مانند.
- خواب زمستانی (Hibernate): پروسه‌ای که به وسیله‌ی آن رایانه تلاش خواهد کرد که از حداقل انرژی استفاده کند درحالی‌که امکان راه‌اندازی سریع را فراهم می‌کند. مانند حالت Sleep سیستم نمایشگر، هارد دیسک و دستگاه‌های اتصال از دور خاموش هستند، اما به اندازه کافی انرژی برای روشن شدن سریع را فراهم می‌آورند. این کار را رایانه با نوشتن محتوای حافظه روی یک فایل در دیسک انجام می‌دهد. در بعضی رایانه‌ها پروسه‌ی Hibernate می‌تواند امنیت رایانه را پائین بیاورد.
- خواب (sleep): سیستم‌عامل، صفحه‌نمایش، هارددیسک و دستگاه‌های کنترل از راه دور را خاموش می‌کند ولی هم‌چنان انرژی کافی به رایانه برای روشن شدن سریع را می‌دهد. برخلاف Hibernate محتوای حافظه روی دیسک نوشته نمی‌شود.
- پیغام فوری (IM): مثال‌های پیام فوری گفت‌وگوهای در گوگل هنگ‌آوت و گفت‌وگوهای در فیس‌بوک می‌باشند. در حالت کلی هر سرویسی که از روش XMPP Jabber استفاده می‌کند.
- سرور نام (Nameserver): وقتی یک مرورگر بخواهد یک تارنما را پیدا کند ابتدا به یک NameServer وصل می‌شود. این به مرورگر می‌گوید که نام دامنه را به آدرس اینترنتی (آدرس IP) به وسیله‌ی مقادیر DNS متصل کند. با تغییر دادن یک مقدار DNS در یک سرور نام، می‌توانید مرورگر را به یک سرور متفاوت متصل کنید. ازلحاظ فنی مرورگر پیش از رفتن سراغ DNS، فایل hosts را چک می‌کند این گونه است که افراد می‌توانند دست‌رسی به فیس‌بوک را در رایانه‌ی خود با منتقل کردن facebook.com به یک آدرس IP دیگر، مسدود کنند. این کار هم‌چنین برای دست‌رسی به بعضی تارنماهایی که از طریق DNS مسدود شده‌اند قابل‌استفاده است.
- مقدار سرویس (Service record) یا SRV: یک مقدار ذخیره‌شده در سیستم نام دامنه است که محل (نام میزبان و شماره‌ی درگاه) سرورها را برای یک سرویس خاص تعریف می‌کند.
- مدل‌سازی تهدید: راهی است برای ارزیابی تهدیدهایی که با آن روبه‌رو هستید، مبدأ تهدید و دارایی‌هایی که می‌خواهید از آن‌ها محافظت کنید. تهدید بسته به محلش کار شما و کسانی که با آن‌ها کار می‌کنید متفاوت است.
- SSL: به توضیح رمزگذاری لایه انتقال یا ویکی پدیا نگاه کنید.
- رمزگذاری لایه انتقال (Transport Layer Encryption): پروتکل‌های رمزنگاریی هستند، امنیت لایه‌ی انتقال (TLS) و لایه سوکت امن (SSL)، که برای ارائه‌ی مسیرهای امن ارتباطی در اینترنت طراحی‌شده‌اند.
- بررسی (Vettin2g): پروسه‌ی انجام بررسی سابقه روی یک فرد یا یک سازمان قبل از درگیری در روابط مالی و سرویس یا دیگر روابط با آن‌هاست.
- میزبان تارنما (Website host): سروری که تارنما شما و فایل‌ها/ پایگاه داده‌هایش در آن ذخیره‌شده‌اند.
- هم‌چنین به واژه‌نامه‌ی امنیت در جعبه نگاه کنید.