



راهنمای امنیت دیجیتال برای وسایل الکترونیکی

بخش اول



OUTRIGHT
ACTION INTERNATIONAL



راهنمای امنیت دیجیتال برای وسایل الکترونیکی

بخش اول



Every day around the world, LGBTIQ people's human rights and dignity are abused in ways that shock the conscience. The stories of their struggles and their resilience are astounding, yet remain unknown—or willfully ignored—by those with the power to make change. OutRight Action International, founded in 1990 as the International Gay and Lesbian Human Rights Commission, works alongside LGBTIQ people in the Global South, with offices in six countries, to help identify community-focused solutions to promote policy for lasting change. We vigilantly monitor and document human rights abuses to spur action when they occur. We train partners to expose abuses and advocate for themselves. Headquartered in New York City, OutRight is the only global LGBTIQ-specific organization with a permanent presence at the United Nations in New York that advocates for human rights progress for LGBTIQ people.

hello@OutRightInternational.org
<https://www.facebook.com/outrightintl>
<http://twitter.com/outrightintl>
<http://www.youtube.com/lgbthumanrights>
<http://OutRightInternational.org/iran>

OutRight Action International
80 Maiden Lane, Suite 1505, New York, NY 10038 U.S.A.
P: +1 (212) 430.6054 • F: +1 (212) 430.6060

This work may be reproduced and redistributed, in whole or in part, without alteration and without prior written permission, solely for nonprofit administrative or educational purposes provided all copies contain the following statement:

© 2018 OutRight Action International. This work is reproduced and distributed with the permission of OutRight Action International. No other use is permitted without the express prior written permission of OutRight Action International. For permission, contact hello@OutRightInternational.org.



جدول محتوا

I. مقدمه.....

۱. امنیت خریدنی نیست.....
۲. امنیت دیجیتال را عادت خود کنید.....
۲. بازنگری.....
۳. چه زمان (تاوب استفاده) از این وسایل الکترونیکی و ارتباطی و شبکه های مجازی استفاده می کنم؟.....
۳. برآورد.....
۴. ارزیابی خطرات متوجه دستگاه های الکترونیکی.....
۵. ارزیابی خطر.....
۵. پیاده سازی.....
۷. نکات ایمنی هنگام استفاده از رایانه.....
۸. اطمینان از سلامت نرم افزارهایی که نصب میکنید.....
۹. آشنایی با تنظیمات امنیتی ویندوز ۱۰.....
۱۰. نگهداری از اطلاعات و فایل های مهم.....
۱۰. فایل ها و اطلاعات شما پاک نمیشود.....
۱۰. خطر استفاده از تلفن همراه هوشمند و وسایل تصویر و صدا برداری.....
۱۱. نکات مهم برای وسایل الکترونیکی، دسترسی به شبکه، ارتباطات و نرم افزار.....
۱۶. لازم است بدانید IP چیست و چگونه کار میکند.....

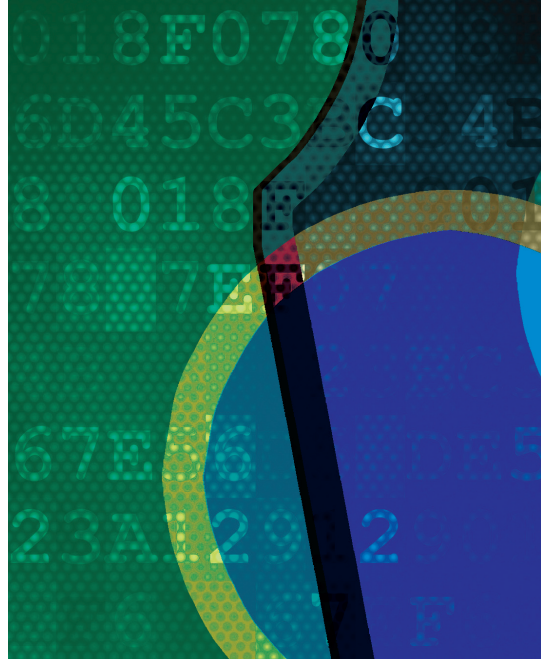
II. منابع و مآخذ.....

۲۰. مطالعه آنلاین.....

III. واژه نامه.....







مقدمه

هدف از گردآوری این مجموعه، بالا بردن امنیت اطلاعات شخصی و حرفه ای شما در فضای مجازی و شبکه‌های اجتماعی است. امیدواریم این راهنمای آموزشی بتواند شما را از تاثیر ردپای دیجیتالی و وسایل الکترونیکی بر امنیت شخصی و حرفه ای آگاه سازد.

امنیت خریدنی نیست

حملات و تهدیدات دیجیتالی، همواره نقاط ضعف امنیتی شما را هدف قرار می دهند. برای همین تمرکز برنامه های امنیتی بر کاهش خطر این نوع تهدیدات و حملات است.

چه از رایانه شخصی استفاده کنید یا از رایانه مشترک (محل کار، منزل، کافی نت) یا اینکه بیشتر فعالیت های اینترنتی خود را روی تبلت یا گوشی هوشمند انجام دهید، راهنمای حاضر شما را در برآوردن نیازها، انتخاب ابزارهای امنیتی و به کارگیری عادت های ایمنی و تضمین امنیت شخصی و حرفه ای برخط و برون خط (آنلاین و آفلاین)، یاری خواهد کرد.

این راهنما به دو بخش تقسیم شده است:

- تمرکز بخش اول بر امنیت دیجیتال از منظر شخصی و حرفه ای است. این بخش کمک می کند تا شبکه و جوامع دیجیتالی خود را شناسایی و بازبینی کرده و بر امنیت و راهکارهای پیشگیرانه تمرکز کنید.
- تمرکز بخش دوم بر امنیت و پیشگیری از تهدیدات متوجه وسایل الکترونیکی، گردآوری اطلاعات از طریق اینترنت، شبکه های اجتماع و ابلیکشن های دوستیابی است.

تعريف امنيت ديڃيٽال

امنیت دیجیتال به حفاظت از اطلاعات و منابع دیجیتالی در برابر تهدیدات داخلی، خارجی، عمدی و تصادفی گفته می شود. برای نهادها و افراد، امنیت دیجیتال به معنی شناسایی، پیشگیری و پاسخگویی به تهدیدات از طریق اعمال سیاست های امنیتی، استفاده از نرم افزار و خدمات فناوری اطلاعات است.

راهنمای حاضر با فرض موارد زیر نگاشته شده است:

- شما به صورت روزمره از رایانه و تلفن همراه برای ارتباطات یا کار استفاده می کنید.
- تلاش ما بر پیشنهاد راهکارهای موثر و کم هزینه است اما توجه داشته باشید که برخی از راهکارهای رایگان، پر مخاطره هستند. بیشتر تمرکز ما بر سیستم عامل های مایکروسافت و اندروید است که رواج بیشتری در سطح جهانی دارند.
- از آنجا که تکنولوژی (فناوری) همواره در حال تغییر است، تلاش ما بر آن بوده که این مجموعه را به صورت انعطاف پذیر تنظیم کنیم (تا در شرایط مختلف قابل استفاده باشد) زیرا باید به طور مستمر در عادات امنیتی خود بازنگری کنید.



امنیت دیجیتال را عادت خود کنید

بازنگری -----> برآورد -----> بکارگیری

این سه مرحله را به صورت ماهانه، هر دوماه یک بار، فصلی، هر شش ماه یک بار یا سالانه تکرار کنید.

بازنگری

از چه وسایل الکترونیکی استفاده می کنید و چه کسانی به آنها دسترسی دارند؟

اولین گام در محافظت از خود، بازنگری در وضعیت دارایی ها و اطلاعات دیجیتال ذخیره شده در وسایل الکترونیکی، شبکه ها، ارتباطات و شبکه های اجتماعی است. این کار شبیه محافظت از خانه است. مثلا پس از خروج از منزل، از خود می پرسید: آیا در و پنجره و ... را قفل کردم؟

یکی از روش های بازنگری استفاده از نظرسنجی است. می توانید سوالات زیر را از خود، خانواده، دوستان و یا همکارانی که بر اطلاعات دیجیتال شما تاثیر دارند (مثلا والدین، خواهر و برادر، همسر و ...) پرسید:

- وسایل الکترونیکی و ارتباطی و شبکه های مجازی که استفاده می کنم را نام ببرید.

• چه کسانی به این وسایل الکترونیکی و ارتباطی و شبکه های مجازی دسترسی دارند؟

• این وسایل الکترونیکی و ارتباطی و شبکه های مجازی کجا قرار دارند؟

چه زمان (تناوب استفاده) از این وسایل الکترونیکی و ارتباطی و شبکه های مجازی استفاده می کنم؟

• چطور از این وسایل الکترونیکی و ارتباطی و شبکه های مجازی استفاده می کنم؟

• چرا از این وسایل الکترونیکی و ارتباطی و شبکه های مجازی استفاده می کنم؟

ورودی های دیجیتال خود را بشناسید

بازنگری به این دلیل لازم است که به شما یادآوری کند از چه وسایل الکترونیکی استفاده می کنید، چه نرم افزارهایی را اجرا می کنید، و چه کسانی به این دو دسترسی دارند. این راهکار در کشف نقاط ضعف احتمالی که می توانند زمانی به تهدید تبدیل شوند، موثر است.

با شناسایی راه های دسترسی به وسایل الکترونیکی و اطلاعات خود از طریق

این پرسشنامه، می توانید وضعیت امنیت خود را ارزیابی کرده و برای محافظت از اطلاعات راهکارهای موثر بکار گیرید.

برآورد

پس از شناسایی دستگاه هایی که نیاز به محافظت دارند، گام بعدی ارزیابی موارد تحت کنترل شما و خطراتی است که زمان استفاده از وسایل الکترونیکی و نرم افزارها متوجه شما می شود.

راه های مختلفی برای ارزیابی وجود دارد. جدول زیر یکی از نمونه های رایج سیستم های رده بندی امنیتی است که متخصصان از آن برای اولویت بندی تاکتیک های امنیتی استفاده می کنند.

خطرات	موارد قابل کنترل	آسیب پذیری	تهدیدات
چگونه تهدیدات از نقاط ضعف شما سو استفاده کرده تا به اموال شما دسترسی پیدا کرده و آن را تخریب یا نابود کنند.	مواردی که تحت کنترل شماست یا به آن دسترسی دارید و می توانید به نحوی از آن برای محافظت یا پیشگیری استفاده کنید.	هر نقطه ضعفی یا خلا امنیتی در محافظت از اموال و اطلاعات.	هر چیزی که از خود در برابر آن محافظت می کنید.

این دسته بندی ذره بینی است که به شما برای ارزیابی وسایل و اطلاعات دیجیتال کمک می کند. برای این کار می توانید از جدول یا برگه گسترده (spreadsheet) استفاده کنید. انجام این کار روش درست یا غلطی ندارد. هدف از انجام این ارزیابی یافتن راهکارهای مناسب برای شناسایی، پیشگیری و پاسخگویی به تهدیدات است. نحوه بکارگیری این راهکارها به شما یا سازمانتان بستگی دارد.

ارزیابی خطرات متوجه دستگاه های الکترونیکی

اهمیت امنیت فیزیکی دستگاهی که به صورت روزمره برای ذخیره سازی اطلاعات استفاده می شود، به اندازه ی امنیت مجازی آن است. چه در مورد امنیت شخصی و چه در مورد امنیت سازمانی باید به هر دو توجه کرد.

در بخش بازبینی از شما خواسته شد دستگاه هایی که برای دسترسی به اینترنت و ارتباط با دیگران استفاده می کنید را نام ببرید. از این فهرست برای بازنگری تهدیدات، آسیب پذیری ها، موارد قابل کنترل و خطرات، استفاده کنید.

تمام دستگاه های الکترونیکی متداول در جدول زیر فهرست و سپس هر یک از منظر موارد چهارگانه ی فوق بررسی شده است. جدول زیر یک نمونه محافظه کارانه از حداقل موارد نیازمند بررسی است:

خطرات	موارد قابل کنترل	آسیب پذیری	تهدیدات	دستگاه
متوسط رو به پایین	محافظت از خانه / ایمنی، دسترسی به رایانه ، تنظیمات، نرم افزار، تجهیزات جانبی	دسترسی، دزد زدن، تعداد کاربران (خانواده یا افرادی که در فضای مشترک زندگی می کنند)، افزایش ناگهانی جریان برق، اتصالات / شبکه ها، دسترسی خط یا کابل تلفن، نرم افزار	حمله ناگهانی پلیس، سرقت، حریم خصوصی	رایانه محل کار/ خانگی
متوسط	تجهیزات جانبی، تنظیمات رایانه ای برای دسترسی ، گذرواژه ورود به سیستم ، نرم افزار	ضبط قضایی، گم کردن، زاویه دید، طول عمر باتری، وای فای، بلوتوث، شکستگی / افتادن، دسترسی به اینترنت، نرم افزار، امنیت شخصی	سرقت، حریم خصوصی، پلیس، سفر	لپ تاپ
متوسط رو به بالا	تجهیزات جانبی، تنظیمات رایانه ای برای دسترسی ، گذرواژه ورود به سیستم ، نرم افزار	ضبط قضایی، گم کردن، زاویه دید، طول عمر باتری، وای فای، بلوتوث، شکستگی / افتادن، دسترسی به اینترنت، نرم افزار، امنیت شخصی	سرقت، حریم خصوصی، پلیس، سفر	تبلت
متوسط رو به بالا	تجهیزات جانبی، تنظیمات رایانه ای برای دسترسی ، گذرواژه ورود به سیستم ، نرم افزار	ضبط قضایی، گم کردن، زاویه دید، طول عمر باتری، وای فای، بلوتوث، شکستگی / افتادن، دسترسی به اینترنت، نرم افزار، امنیت شخصی	شرکتهای مخابراتی، سرقت، حریم خصوصی، پلیس، سفر	تلفن همراه
نامعلوم	تجهیزات جانبی، تنظیمات رایانه ای برای دسترسی ، گذرواژه ورود به سیستم ، نرم افزار	ضبط قضایی، گم کردن، زاویه دید، طول عمر باتری، وای فای، بلوتوث، شکستگی / افتادن، دسترسی به اینترنت، نرم افزار، امنیت شخصی، اطلاعات تولید کننده، قوانین	شرکت های تولید کننده، شبکه ها، سرقت، حریم خصوصی، پلیس	تلویزیون و ساعت هوشمند، پخش کننده های موسیقی، خانه یا لوازم خانگی هوشمند

این جدول نقطه‌ی شروعی برای شناسایی بزرگترین خطرات و تهدیدات مختص موقعیت، برنامه‌ها و محیط شما است.

این نمونه فقط به عنوان مثال ذکر شده و بسیار محافظه کارانه است. کلید انجام این کار استفاده از جزییات مربوط به شرایط خاص شما است. اگر خطری برای شما مشخص نیست، ایرادی ندارد که از گزینه «نامعلوم» استفاده کنید. چرا که هدف کاهش تهدیدات و افزایش آگاهی شما است. به یاد داشته باشید که موارد تحت کنترل شما با منابع موجود قابل مدیریت هستند. تهیه فهرست مواردی که می‌توان مدیریت یا کنترل کرد، به شناسایی سطح تهدیدات و تلاش برای کاهش آن کمک می‌کند. این به طراحی یک استراتژی دفاع و پیشگیری خوب منجر می‌شود.

ارزیابی خطر

یکی از مدل‌های رایج برای ارزیابی خطرات و تهدیدات در تصویر ۱ آمده است. این مدل بر اساس شدت و تناوب تهدیدات طراحی شده است. تغییر در آسیب پذیری و میزان کنترل می‌تواند منجر به کاهش یا افزایش احتمال وقوع تهدید شود. شدت تهدیدها یا به عبارت دیگر آنچه سعی می‌کنید از خود در برابر آن محافظت کنید، به فرد یا سازمان بستگی دارد.

حال با استفاده از جدول فوق، به عنوان نمونه به ارزیابی خطرات کلی متوجه تلفن‌های همراه می‌پردازیم. می‌توان گفت دستگاه‌هایی که افراد معمولاً همراه خود دارند، بیشتر آسیب پذیرند، بیشتر در معرض تهدید قرار دارند و امکان کنترل شان کمتر است.

بنابراین خطرات متوجه تلفن‌های همراه با رایانه‌های خانگی و محل کار که از لایه‌های امنیتی بالاتری برخوردار هستند، فرق می‌کند. برای مثال شما برای ورود به منزل احتیاج به کلید و برای ورود به محل کار احتیاج به کارت هوشمند دارید. این امر تناوب و شدت تهدیدات و آسیب پذیری رایانه‌های خانگی و محل کار را کاهش داده و قدرت دفاعی را بالا می‌برد.

پیاده سازی

امنیت و پیشگیری

پایه و اساس دفاع و مقابله و پیشگیری از حملات، ریشه در عادت‌ها و رفتارهای افراد و سازمان‌ها هنگام استفاده از دستگاه‌های دیجیتال برای ذخیره و تبادل اطلاعات دارد.

با در نظر داشتن اطلاعات فوق، گام بعدی باید تصمیم‌گیری درباره تاکتیک‌ها و چگونگی پیاده‌سازی برنامه دفاعی باشد. طراحی یک برنامه دفاعی متناسب با نیازهای شما ضروری است. اگر زمانی برای شما و یا اطلاعات تان اتفاقی بیفتد، داشتن یک چنین برنامه‌ای حیاتی است.

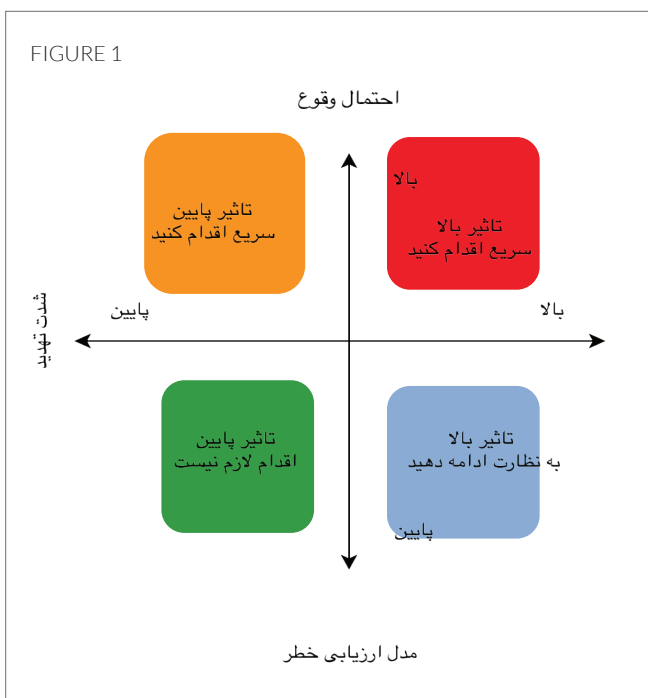
فناوری اطلاعات دائماً در حال تغییر است. بنابراین باید به طور مداوم امنیت خود را ارزیابی کنید. این ارزیابی نباید فقط در واکنش به یک اتفاق باشد، بلکه باید حداقل سالی یکبار انجام شود. بخش‌های بعدی حاوی نکات ایمنی، تنظیمات دستگاه، تنظیمات نرم افزار و تنظیمات شبکه‌های اجتماعی برای حفظ حریم خصوصی و امنیت است.

نکات ایمنی عمومی برای امنیت دیجیتال

امروزه حجم زیادی از اطلاعات خصوصی بر روی بیشتر دستگاه های قابل حمل مانند تلفن همراه، تبلت، فیت بیت و لپ تاپ ذخیره می شود. بنابراین آگاهی از راهکارهای امنیت شخصی و به کارگیری آن بسیار مهم است.

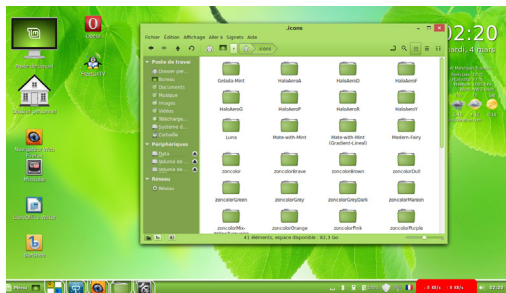
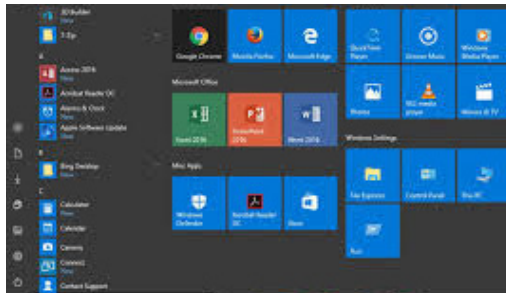
فهرست زیر شامل نکات ایمنی عمومی برای حمل وسایل الکترونیکی است:

- هنگام استفاده از وسایل الکترونیکی مراقب اطراف خود باشید. یعنی به طور مداوم به اطراف خود نگاه کرده و توجه کنید چه کسانی در نزدیکی شما حضور دارند. با این افراد دوستانه رفتار کنید. برخی افراد به دوربین های مدار بسته و جاذبه های اطراف خود نیز توجه می کنند تا در صورت نیاز بتوانند در آینده از این اطلاعات استفاده کنند. وقتی دستگاهی دزدیده شود، سارقان به اطلاعات آن دسترسی پیدا می کنند.
- در حالت توقف از دستگاه خود استفاده کنید. استفاده از دستگاه در حین راه رفتن توجه شما را از اطراف دور می کند. در صورت امکان، برای استفاده از دستگاه خود در جایی توقف کنید که کسی نتواند از پشت به شما نزدیک شود. در اماکن عمومی، توجه کنید دیگران می توانند محتوای صفحه شما را مشاهده کنند یا نه.
- اگر احساس می کنید تحت نظر هستید، دستگاه الکترونیکی خود را خاموش کرده و باتری آن را خارج کنید. دستگاه خود را به جایی نبرید که در آنجا حریم خصوصی برای امنیت فردی شما ضروری است.
- مکان یاب (gps) دستگاه خود را خاموش کرده و فقط در صورت نیاز آن را روشن کنید. حتی وقتی مکان یاب خاموش است، اپراتورهای مخابراتی می توانند موقعیت مکانی شما را پیدا کنند. با این حال خاموش کردن مکان یاب کار افرادی که شما را تعقیب می کنند، سخت تر می کند. خود را خاموش کرده و هرگز اجازه ندهید که دستگاه شما به صورت خودکار به شبکه هایی که پیدا می کند وصل شود WiFi.
- در صورت امکان سعی کنید با شخص دیگری مسافرت کنید که تنها نباشید. اگر تحت نظر بودن برای شما معضل شده است، حداقل در ساعت های معین با افراد مورد اعتماد تماس بگیرید و جزئیات سفر خود را با ایشان در میان بگذارید.



- مسیرهای سفر خود را تغییر دهید. همیشه از یک مسیر نروید. این کار به شما کمک خواهد کرد تا شناخت بهتری از منطقه بدست آورید و نیز با دیگر اعضای جامعه تان آشنا شوید. این تمهید می تواند به شما کمک کند از تحت تعقیب بودن خود آگاه شوید. برخلاف مسیرهای ثابت همیشگی، وقتی در یک مسیر جدید حرکت می کنید افرادی که شما را تعقیب می کنند، همزمان با شما تغییر مسیر می دهند و از این رو تشخیص آنها ممکن می شود.
- رفتار. تحت نظر گرفتن افراد تنها برای دسترسی به اطلاعات آنها نیست بلکه رفتارهای فرد هم تحت نظر است. برای همین افزایش ناگهانی اقدامات امنیتی می تواند مشکل ساز شود چون به کسانی که فرد را تحت نظر دارند می رساند، خبری شده است. به عنوان مثال استفاده از VPN ها در ایران، روسیه و چین معمول است، اما در سایر نقاط دنیا، افزایش ناگهانی استفاده از VPN می تواند هشدار به شرکت ها و سازمان های دولتی باشد.

هدف ایمنی است. اگر احساس می کنید که عادت های روزانه جدید و تغییر عادات قدیمی کافی نیست و امنیت شخصی شما همچنان در خطر است، با افراد و سازمان های مورد اعتماد مشورت کنید.



نکات ایمنی هنگام استفاده از رایانه

در بازار ایران نسخه های مختلف ویندوز و سیستم عامل های دیگر با قیمت ارزان و مارک های مختلف به فروش میرسد. باید توجه داشته باشید که ممکن است این سیستم عاملها به صورت عمدی یا غیر عمدی دارای مشکلات امنیتی باشند. برای مثال، ممکن است بخشهایی از سیستم عامل که باید امنیت رایانه شما را حفظ کند، دستکاری یا حذف شده باشد یا ویروسهایی بر روی این سیستم عامل نصب شده باشد. بر فرض ممکن است در این سیستم عامل حفره امنیتی ایجاد شده باشد یا آلوده به انواع ویروس و بدافزار شده باشد. در این صورت، بلافاصله پس از نصب چنین سیستم عاملی در معرض خطر قرار خواهید گرفت.

سه نوع سیستم عامل رایج وجود دارد:

ویندوز نسخه ۱۰

اپل MacOS High Sierra

لینوکس مینت

توصیه می شود خودتان سیستم عامل رایانه خود را نصب کنید. راهنمای نصب سیستم عامل، در اینترنت موجود است. از راه های میانی استفاده نکنید چرا که این کار اوضاع را پیچیده تر کرده و مجبور به فرمت هارد دیسک می شوید.

امروزه می توان سیستم عامل را بطور مستقیم از سرور شرکت سازنده دانلود کرد. حتما اگر به ارتباط امن اینترنت دسترسی دارید مستقیما از سرور خود شرکت، سیستم عامل دانلود کنید. مطمئن شوید که سیستم عامل را از سایت اصلی مایکروسافت، اپل یا لینوکس و نه سایت یک فروشنده داخلی خریداری می کنید. پس از خرید سیستم عامل، شرکت سازنده برای شما لینک دانلود مستقیم یا تورنت (torrent) آن را ارسال می کند. قبل از دانلود مطمئن شوید که نام شرکت سازنده در آدرس اینترنتی (url) لینکی که برایتان ارسال شده آمده است.

در زمان نصب، سیستم عامل جهت ساختن حساب کاربری از شما اطلاعات شخصیتان را می خواهد. اگر احساس می کنید وارد کردن اطلاعات شخصی تان شما را در معرض خطر قرار می دهد، پیشنهاد می شود از نام مستعار و آدرس ایمیل جعلی استفاده کنید. به خاطر داشته باشید که اگر اطلاعات وارد شده را فراموش کنید ممکن است دیگر نتوانید به این حساب کاربری وارد شوید. به هر صورت داشتن یک نام مستعار دم دستی به محافظت از هویت شما کمک می کند.

دانلود فایل های تورنت و نرم افزارهای قفل شکسته (کرک شده)

بسیاری از برنامه هایی که به صورت قفل شکسته (کرک شده) مورد استفاده قرار میگیرند، آلوده به بدافزار هستند. زمانی که این نرم افزارها را روی رایانه خود نصب می کنید، گاهی حتی ضد ویروسها هم نمیتوانند جلوی آلوده شدن رایانه شما را بگیرند. بنابراین، تا جایی که امکان دارد، این نرم افزارها را بر روی رایانه ای که ایمنی برای شما مهم است، نصب نکنید و از نرم افزارهای اصل یا رایگانی استفاده کنید که قابل دانلود از سایت اصلی هستند.

اطمینان از سلامت نرم افزارهایی که نصب میکنید

ویروسهای رایانه ای برنامه هایی هستند که میتوانند به رایانه شما و اطلاعات داخل آن صدمه زننده آنها را از بین ببرند. همچنین ویروسها قابلیت انتقال از یک رایانه به رایانه دیگر از طریق CD، DVD، هارد دیسکهای قابل حمل، فلش و هرگونه وسیله انتقال دادهی دیگر و نیز شبکه های رایانه ای و تلفنهای همراه را دارند.

برای در امان ماندن از خطر ویروسها

سعی کنید برای انتقال اطلاعات کمتر از فلش درایو هارد دیسکهای قابل حمل استفاده کنید؛ در صورت امکان، بهتر است رایانه ای را که بر روی آن اطلاعات حساس دارید، به صورت مجزا و ایزوله ۹ چگونه با تهدیدات اینترنتی مقابله کنیم نگه دارید و برای تفریحات و کارهای روزمره، از یک رایانه دیگر استفاده کنید.

یک ضد ویروس مطمئن و کارآمد بر روی رایانه خود نصب کنید. ضد ویروس می تواند در کنار ساختارهای امنیتی پیش فرض سیستم عامل باشد. اندپوینت (Endpoint Security) یکی از ضد ویروس های متداول برای سیستمهای مک (Mac) است.

Webroot نرم افزاری سبک و کم هزینه است که با همه سیستم های رایانه ای و

تلفن همراه سازگار است. اما هر ضد ویروسی که انتخاب کردید، مراقب باشید که خود این نرم افزار آلوده به ویروس نباشد؛ ضد ویروس را هم مانند سایر نرم افزارها از یک منبع مورد اعتماد دریافت کنید.

بعضی از بدافزارها به اطلاعات شما صدمه نمیزنند، ولی بر روی رایانه شما جاسوسی می کنند و اطلاعات ذخیره شده بر روی آن یا هرگونه اطلاعات دیگری را که بتوانند جمع آوری کنند، برای یک منبع دیگر ارسال میکنند. این بدافزارها حتی ممکن است میکروفون یا وبکم رایانه شما را روشن کنند و صدا و تصویر شما را به منبع دیگری بفرستند. برخلاف ویروسها که به اطلاعات شما صدمه میزنند و ممکن است رایانه شما را از کار بیاندازند، این بدافزارها (نرم افزارهای جاسوسی) معمولا هیچ اشکال در استفاده شما از رایانه ایجاد نمی کنند و ممکن است بدون آنکه متوجه شوید، رایانه شما مدتها به یک بدافزار آلوده باشد. معمولا برنامه های ضد ویروس این بدافزارها را شناسایی میکنند. این بدان معنی است که شما باید بطور مستمر ضد ویروس خود را به روز رسانی (update) کنید.

برخی بدافزارها به رایانه یا اطلاعات

صدمه نمی زنند بلکه بدون متوجه شدن شما اطلاعات حساسی که روی رایانه ذخیره کرده اید را به منبع دیگری ارسال می کنند.

امنیت ویندوز

روشن کنید:

Windows Firewall

Windows Defender

خاموش کنید:

Windows Backup (پشتیبانی گیری ویندوز)

کورتانا (برای Mac سیری)

قابلیت تکمیل خودکار فرم (Autofill) و ذخیره ی سابقه مرور خاموش کنید:

Windows Backup (پشتیبانی گیری ویندوز)

کورتانا (برای Mac سیری)

قابلیت تکمیل خودکار فرم (Autofill) و ذخیره ی سابقه مرور

آشنایی با تنظیمات امنیتی ویندوز ۱۰

در عصری که هیچ کس شرایط استفاده از خدمات نرم افزارها Terms of Service (Agreement) ToS را نمی خواند، بهتر است این شرایط را مطالعه کنید. امروزه تکنولوژی های مختلف می توانند اطلاعات شخصی را بدون آگاهی شما به سهولت گردآوری کنند.

برخی از تنظیمات ویندوز که بهتر است بلافاصله پس از نصب نسبت به غیر فعالسازی آن اقدام کنید، به شرح زیر است:

غیر فعال کردن موقعیت مکانی :

ابتدا وارد تنظیمات privacy شوید. برای این کار به مسیر زیر بروید:

Start > Settings > Privacy

از منوی Privacy می توانید انتخاب کنید رایانه ی شما چگونه از اطلاعات موقعیت مکانی، دوربین، میکروفون و ... استفاده کند.

حالا که در منوی Privacy هستید روی Feedback and Diagnostic هم کلیک کرده و تغییرات زیر را اعمال کنید:

برای Feedback Frequency گزینه ی Never را انتخاب کنید.

برای Diagnostic and Usage Data گزینه ی Basic را انتخاب کنید.

انجام این مراحل مانع گردآوری اطلاعات شما توسط مایکروسافت می شود.

از سابقه ی مرور (Browser History) خود محافظت کنید

مرورگر اج (Edge) - که بصورت پیش فرض بر روی ویندوز ۱۰ نصب شده است- سابقه مرور شما را برای کورتانا (Cortana) ارسال می کند تا این دستیار صوتی ویندوز ۱۰ بتواند تجربه شما را شخصی سازی کند. برای پیشگیری از این امر ابتدا روی دکمه سه نقطه در گوشه بالا سمت راست اج کلیک کرده و سپس به مسیر زیر بروید:

Settings > Advanced Settings > View Advanced Settings

در بخش Privacy and Services گزینه Have Cortana Assist Me in Microsoft Edge را خاموش کنید.

حالا که در Privacy and Service هستید گزینه "use page prediction to speed up browsing, improve reading, and make my overall experience better" را هم خاموش کنید.

نگهداری از اطلاعات و فایل‌های مهم

با نگهداری اطلاعات آلوده به ویروس روی حافظه خارجی مانند CD ، Flash Drive و DVD یا انواع دیگر هارد دیسک های قابل حمل، این بدافزارها به CD و DVD هم منتقل می شود و برای همیشه باقی میماند و حتی برنامه‌های ضد ویروس هم نمیتواند آنها را پاکسازی کند.

اگر اطلاعاتی دارید که میخواهید مخفی بماند و در صورت لزوم بتوانید آنها را از بین ببرید یا همچنین مخفی نگه دارید، بهتر است آن اطلاعات را بر روی حافظه های خارجی مانند CD ، Drive Flash یا انواع دیگر هارد دیسک‌های قابل حمل ذخیره کنید تا در صورت لزوم، بتوانید آن وسایل را به سرعت در جایی مخفی یا منهدم کنید.

فایل‌ها و اطلاعات شما پاک نمیشود

برخلاف تصور رایج، هنگامی که شما برای مثال یک فایل را از روی رایانه خود پاک می کنید و Recycle Bin را هم خالی می کنید، هنوز امکان بازیابی آن فایل وجود خواهد داشت. زمانی که شما یک فایل را پاک میکنید، سیستم عامل شما، آن قسمت از حافظه داخلی خود را که برای نگهداری آن فایل اشغال شده بوده است، آزاد میکند و به این ترتیب شما دیگر آن را نخواهید دید و با روش‌های معمول، به اطلاعات آن فایل دسترسی نخواهید داشت. هرچند تا زمانی که اطلاعات جدیدی بر روی این حافظه آزاد شده ذخیره نشود، اطلاعات قدیمی همچنین در جای خود باقی خواهد ماند و با استفاده از نرم افزارهای خاصی می توان آن را بازیابی کرد. برای جلوگیری از بازیابی اطلاعات پاک شده، می توانید از نرم افزارهایی که اطلاعات فایل را پس از پاک شدن به صورت کامل از بین میبردند - برای مثال «Shredder File» یا «Eraser» استفاده کنید. با این حال، این نرم افزارها هم نمی توانند از بین رفتن فایل‌ها را کاملاً تضمین کنند. اگر نگران بازیابی اطلاعات خود هستید، حافظه رایانه را کامل تخریب کنید یا از افراد معتمد متخصص در این زمینه کمک بگیرید.

خطر استفاده از تلفن همراه هوشمند و وسایل تصویر و صدا برداری

برای دسترسی به سرویس هایی که روی آنها اطلاعات مهمی دارید و می تواند برای شما جنبه امنیتی داشته باشد، از تلفن‌های همراه هوشمند استفاده نکنید. در مجموع بهتر است اگر نگرانی امنیتی خاصی دارید و از سوی عوامل حکومتی در معرض خطر هستید، چنین استفاده‌های از تلفن‌های هوشمند نکنید.

با آنکه به نظر میرسد اطلاعاتی که روی حافظه این تلفنها دارید، پس از پاک شدن از دسترس خارج می شود، اما همانطور که پیشتر در مورد سایر رایانه ها توضیح داده شد، ممکن است هنوز هم قابل بازیابی باشد. اطلاعات حساس، چه از نوع عکس، فیلم، نوشته، پیامک یا گذرواژه ها، به راحتی قابل پاک شدن نیستند. این اصل در مورد دوربین‌های عکاسی و فیلمبرداری و وسایل ضبط صدا یا هر وسیله الکترونیکی مشابه دیگری هم صدق میکند.

پیشنهاد می شود یک اپلیکیشن دکمه دلهره (پنیک باتن) دانلود کنید. این اپلیکیشن ها معمولاً دو کارکرد دارند:

- ۱- بطور مداوم از اطلاعات شما پشتیبانی می گیرند - این کار به شما امکان می دهد فایل‌های تان را حذف یا مستقیماً در کلود ذخیره کنید.
- ۲- با اجرای یک فایل ویروس، اطلاعات تلفن همراه شما را آلوده کرده و از بین می برند. با این اپلیکیشن می توانید سریع اطلاعات روی تلفن همراه را نابود کنید.

اگر فرد متخصصی در این زمینه نیستید، در مورد تلفنها برای اینکه مطمئن شوید اطلاعات مورد نظرتان کاملاً از بین رفته و به هیچ طریقی قابل بازیابی

نخواهد بود، احتمالاً چاره‌ای نخواهید داشت جز تخریب کامل دستگاه - و در مورد دوربینها و وسایل ضبط صدا، تخریب کامل حافظه در صورتی که قابل تعویض باشد. یا می‌توانید از فردی متخصص در این زمینه کمک بگیرید.

اگر امکان تخریب برای شما وجود ندارد، پس از پاک کردن حافظه مراحل زیر را انجام دهید:

- تلفن همراه خود را به تنظیمات کارخانه بازگردانید (Factory reset).
- سپس تمام ظرفیت حافظه را با فایل‌های غیر مهم پر کنید؛ این کار احتمال امکان بازیابی فایل‌های پاک شده شما را کاهش میدهد.

نکات مهم برای وسایل الکترونیکی، دسترسی به شبکه، ارتباطات و نرم افزار

به یاد داشته باشید که دستگاه‌های الکترونیکی پر از اطلاعات خصوصی شما است. این اطلاعات شامل لیست مخاطبین، افرادی که به تازگی با آنها تماس گرفته‌اید، پیامک‌های ارسالی، عکس، ویدیو، اطلاعات GPS، سابقه مرور، گذرواژه‌ها، اطلاعات شبکه‌های اجتماعی و سابقه گفتگوهای اینترنتی (چت) است. بنابراین جلوگیری از دسترسی به این اطلاعات ضروری است.

به یاد داشته باشید که راهنماهای کاربری و سایت شرکت‌های سازنده، برای مطلع شدن از آخرین تنظیمات، به روز رسانی‌های امنیتی و تغییرات در دستگاه الکترونیکی شما ابزاری ارزشمند است.

گذرواژه/کلید ورودی امن و احراز هویت دو مرحله‌ای

اگر احتمال دستگیری شما در خیابان یا فرودگاه زیاد است و یا ممکن است منزل شما مورد بازرسی نیروهای امنیتی قرار گیرد، جلوگیری از دسترسی به وسایل الکترونیکی شما حیاتی است.



از روش‌های معمول برای جلوگیری از دسترسی به اطلاعات، استفاده از گذرواژه یا کلید

ورودی امن USB key و یا تلفیقی از هر دو است.

نکات مهم برای تولید و استفاده از گذرواژه در وسایل الکترونیکی مانند تلفن همراه و تبلت:

- از گذرواژه و یا کدی که بیش از چهار کاراکتر و یا حتی بیش از شش کاراکتر باشد، استفاده کنید.

- از شناساگر اثر انگشت یا تاج آیدی و شناساگر تشخیص چهره استفاده نکنید زیرا این تکنولوژی ها قابل دور زدن است.
- نمایش مدیریت هشدار (نوتیفیکیشن) تلفن همراه خود را خاموش کنید تا هنگامی که صفحه تلفن شما قفل است، نمایش داده نشود. برای انجام این مرحله به راهنمای کاربری تلفن همراه مراجعه نمایید.
- به یاد داشته باشید که در برخی کشورها سیم کارت شما باید به ثبت برسد. قوانین مربوطه را مطالعه کرده تا مطمئن شوید از بهترین گزینه برای تضمین امنیت خود استفاده می کنید. برای در امان ماندن از خطرات، راهکارهای اینترنتی و امنیتی مختلفی وجود دارد. برای یافتن راهکارهای جایگزین حتما به منابع معتبر رجوع کنید.
- قبل از خرید اشتراک اینترنت به سابقه ی شرکت های رساننده خدمات اینترنتی مخصوصا به روابط آنها با دولت دقت کنید چون بر راهکارهایی که برای امنیت خود، وسایل الکترونیکی و مدیریت اطلاعات تان انتخاب می کنید، تاثیر می گذارد.

نکات مهم برای تولید و استفاده از گذرواژه در رایانه و نرم افزار



- از احراز هویت دو مرحله ای استفاده کنید.
- گذرواژه باید حداقل ۸ کاراکتر باشد ولی هر چه بیشتر باشد، بهتر است.
- از تلفیقی از حروف کوچک، بزرگ، کاراکترهای خاص و اعداد استفاده کنید.
- گذرواژه خود را به طور مداوم عوض کنید. اگر این کار را نمی کنید، حداقل زمانی که احساس کردید حساب کاربری شما در معرض خطر است، گذرواژه خود را سریعاً عوض کنید.
- برای اطلاعات مهم خود مانند حساب بانکی از گذرواژه های مختلف استفاده کنید
- توصیه می شود برای احراز هویت از کلید ورودی امن USB key استفاده کنید.
- توصیه می شود از نرم افزار مدیریت گذرواژه استفاده کنید. تحت هیچ شرایطی گذرواژه ی مربوط به برنامه مدیریت گذرواژه های خود را در اختیار فرد دیگری قرار ندهید چون این کار تمامی گذرواژه های شما را در اختیار شخص سوم قرار می دهد.

احراز هویت دو مرحله ای چیست؟

یک اقدام امنیتی اضافی است. در این روش علاوه بر نام کاربری و گذرواژه اطلاعات دیگری که تنها کاربر می داند یا می تواند فراهم کند درخواست می شود. پیامک و کلید ورودی امن USB Key معمول ترین شیوه های احراز هویت دو مرحله ای است. می توانید از این روش برای محافظت از حساب های کاربری دیجیتال خود مانند حساب بانکی، ایمیل و غیره استفاده کنید. از این روش برای لپ تاپ و رایانه هم می توان استفاده کرد.



از اطلاعات خود پشتیبانی بگیرید

پشتیبانی گرفتن از اطلاعات، بهترین راه مبارزه با از دست رفتن اطلاعات به دلیل گم شدن، دزدیده شدن و یا ضبط شدن است. اطلاعات پشتیبانی گیری شده منبع ارزشمندی است چون به شما یادآوری می کند چه چیزهایی ضبط شده و قدم بعدی شما برای دفاع و امنیت شخصی تان چه باید باشد.

رمزنگاری Encryption --. اگر احتمال دستگیری شما در خیابان یا فرودگاه زیاد است و یا ممکن است منزل شما مورد بازرسی نیروهای امنیتی قرار بگیرید، یک روش متداول برای محافظت از اطلاعات روی تلفن همراه یا رایانه و وسایل الکترونیکی دیگر، رمزنگاری است. شرکت های سازنده وسایل الکترونیکی، رمزنگاری را به عنوان یک گزینه اختیاری در راهنمای کاربری خود ارائه می دهند. برخی تلفن های همراه مانند آیفون و گوشیهای سامسونگ جدید بصورت پیش فرض رمزنگاری شده اند. اگر خطری که متوجه شما شده به قدری شدید است که تلفن همراه خود را رمزنگاری کرده اید، قدم بعدی شما باید رمزنگاری ارتباطات تان باشد.

رمزنگاری ایمیل

پیشنهاد می شود ایمیل های خود را به صورت End-to-End رمزنگاری کنید. این بدان معناست که هر دو طرف برای تضمین امنیت خود باید از رمزنگاری استفاده کنند. از ایرادهای رمزنگاری End-to-End آگاه باشید. مثلاً عنوان ایمیل شما بنا به قوانین و پروتکل های ایمیل رمزنگاری نمیشود. البته سرویس های ایمیل تحت وی مانند Protonmail وجود دارند که کاملاً رمزنگاری شده اند. برای اطلاعات بیشتر به بخش منابع مراجعه کنید.



رمزنگاری پیامک و پیام رسان

از سرویس های پیام رسان رمزنگاری شده بر روی تلفن همراه خود استفاده کنید. بهتر است این سرویس ها را به دوستان خود نیز پیشنهاد دهید. اگر هر دو طرف از پیام رسان رمزنگاری شده استفاده کنند، تمام پیام ها به صورت End-to-End رمزنگاری می شود. هنگام انتخاب پیام رسان، داشتن قابلیت رمزنگاری را ملاک خود قرار دهید. Signal و WhatsApp دو پیام رسان کاملاً رمزنگاری شده اند.

دسترسی به شبکه

از هر وسیله ای که برای دسترسی به اطلاعات دیجیتالی خود استفاده می کنید، توجه داشته باشید که چه اشخاص دیگری به این شبکه ها و Wifi شما دسترسی دارند. شناخت اپراتور شبکه تلفن همراه و اینترنتی که استفاده می کنید، بسیار مهم است. زیرا نوع رابطه ی این شرکت ها با دولت، نیروهای امنیتی و مشتریان شان بر امنیت شما تاثیر مستقیم می گذارد.

بطور کلی خوب است که :

- شرایط استفاده از خدمات را مطالعه نموده تا از مسئولیت های شرکت که در قرارداد قید شده، مطلع شوید.
- فقط برای پرداخت قبض به سایت شرکت مراجعه نکنید. بلکه با مراجعه به سایت می توانید از آخرین اخبار شرکت مثلاً قرارداد با دولت برای تولید تکنولوژی جدید و یا هر چیز دیگری که به امنیت شما مربوط میشود، مطلع شوید.
- درباره روتر هایی که شرکت های اینترنتی برای خانه و محل کار پیشنهاد میدهند تحقیق کنید- با افراد متخصص در این زمینه مشورت کنید و راهنما های کاربری را مطالعه کنید.
- VPN- اگر به VPN دسترسی دارید حتماً استفاده کنید. VPN به شما شناسه اینترنتی موقت می دهد و شناسه حقیقی شما را از تمامی سایت ها و ایمیل هایی که به آن متصل می شوید مخفی می کند و معمولاً رمزنگاری شده است. استفاده از VPN به مخفی ماندن هویت و امنیت شما کمک می کند. نکته: قابل اعتماد بودن VPN به قابل اعتماد بودن سرویس دهنده آن بستگی دارد. برای اطلاعات بیشتر درباره VPN به بخش بعدی مراجعه کنید.



دسترسی به WiFi

هنگامی که از WiFi استفاده نمی کنید آن را خاموش کنید. توصیه های دیگر:

- از شبکه های باز استفاده نکنید. شبکه باز شبکه ای است که برای دسترسی به آن نیازی به گذرنامه نیست.
- زمان استفاده از شبکه هایی که به آن اعتماد ندارید و یا صاحبشان را نمی شناسید را محدود کنید. افرادی که به شبکه ی WiFi شما دسترسی دارند می توانند به وسایل الکترونیکی شما هم دسترسی پیدا کنند.
- گزینه دریافت هشدار پیش از اتصال به شبکه ی WiFi را روی رایانه خود فعال کنید. این گزینه می تواند حجم اطلاعاتی که اجازه دسترسی به آن داده می شود را محدود کند.



WiFi Tethering

به استفاده از تلفن همراه به عنوان مودم جهت دسترسی به اینترنت، Tethering گفته می شود. چند نکته برای استفاده از این قابلیت:

- قرارداد تلفن همراه خود را مطالعه کنید زیرا استفاده از این قابلیت ممکن است هزینه اضافه دربرداشته باشد.
- Tethering را به صورتی راه اندازی کنید که نیاز به گذرنامه داشته باشد، هرگز از قابلیت دسترسی باز استفاده نکنید.
- گذرنامه Tethering خود را فقط در اختیار اشخاص قابل اعتماد بگذارید.
- به یاد داشته باشید که همیشه پس از استفاده، Tethering را خاموش کنید.
- کنشگران از Tethering برای ارتباط با هم از طریق یک شبکه شناخته شده در حین تظاهرات و برنامه های زنده، استفاده می کنند.

بلوتوث Bluetooth

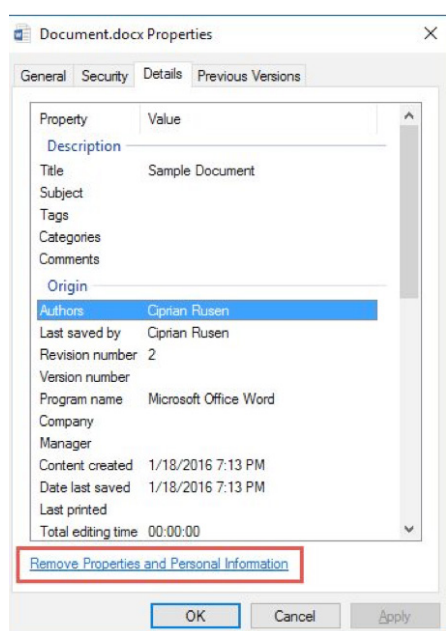


- از تمامی نکات ایمنی مربوط به WiFi، این جا هم استفاده کنید. نکات اضافه:
- دستگاه های جدید مجهز به آخرین نسخه بلوتوث، همه رمزنگاری شده اند. اگر از بلوتوث های نسخه قدیمی مثل ۱.۰، ۲.۰ or LE-۴۰۰ که نرم افزار آن را نمی توان بروز رسانی کرد، استفاده می کنید به یاد داشته باشید که نرم افزار شما رمزنگاری شده نیست و پیشنهاد می شود آن را خاموش کنید.
- بسیاری از هدفون های بی سیم با بلوتوث کار میکنند. مطمئن شوید که همیشه آخرین نسخه نرم افزار را استفاده می کنید. همیشه پس از استفاده، بلوتوث خود را خاموش کنید زیرا از این وسایل میتوان برای شنود استفاده کرد.
- برای استفاده از این وسایل همیشه از احراز هویت استفاده کنید. حتی بهتر است در صورت فقدان این گزینه، از رمز عبور استفاده کنید.
- دستگاه های بلوتوث گرم شده یا به سرقت رفته ای که با وسایل الکترونیکی شما جفت شده اند را از روی وسایل الکترونیکی خود حذف کنید.

مرورگرها

از مرورگرها برای دسترسی به اینترنت استفاده می شود. هر وسیله ای که قابلیت اتصال به اینترنت داشته باشد، به صورت پیش فرض یک مرورگر دارد مثلاً اپل از مرورگر سافاری استفاده می کند و ویندوز از مرورگر اج . به دلیل تنوع، هنگام انتخاب مرورگر چند نکته کلیدی را رعایت کنید:

- درباره توسعه دهندگان مرورگر تحقیق کنید تا بفهمید تا چه حد درباره نرم افزاری که تولید کرده اند، شفافیت دارند . از اطلاعاتی که مرورگر ردیابی می کند مطلع باشید.
- قبل از دانلود و نصب هر مرورگر، تمام اطلاعات مربوط به آن را بررسی کنید.
- به مرورگر اجازه ذخیره سابقه مرور و کوکی ها را ندهید.
- بهتر است برای کارهای مختلف از مرورگرهای مختلف استفاده کنی. به عنوان مثال از مرورگر کروم برای ایمیل و از فایرفاکس برای تحقیق برای سفر استفاده کنید.
- بوک مارک ها (لینک های ذخیره شده) را به صورت مداوم بررسی و حذف نمایید. حذف سابقه مرور، لینک های ذخیره شده را پاک نمیکند.



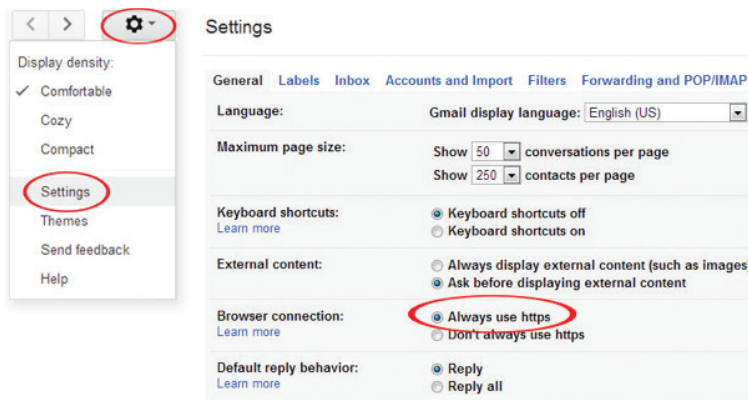
داده‌ها یا متادیتا (تصویر نمونه متادیتا است)

متادیتای چیست؟ به اطلاعات ذخیره شده درون فایل های رسانه ای مانند فرمت، طول فایل، اطلاعات فنی، تعاریف متنی نظیر اطلاعات شخصی، کلید واژه، محدودیت های امنیتی، موقعیت جغرافیایی و غیره، متادیتا گفته می شود. توجه به متادیتا به این دلیل مهم است که:

- فایل ها بسته به منبع و تولیدکننده شان، حاوی اطلاعات مختلف هستند. برای اطلاعات بیشتر به استانداردهای متادیتا مراجعه کنید.
- با مراجعه به راهنمای کاربری وسایل الکترونیکی مانند دوربین یا هر وسیله ای دوربین دار می توانید نوع اطلاعاتی که در متادیتا ذخیره می شود را تعیین کنید.
- قبل از فرستادن فایل به اشخاص دیگر متادیتای آن را مرور کنید. با این کار می فهمید چه اطلاعاتی قابل رویت و چه اطلاعاتی غیر قابل رویت است.
- نکته: نرم افزارهای ویرایش تصویر مانند فتوشاپ متادیتا را ویرایش می کنند و اطلاعات جدید برگرفته از نرم افزار را جایگزین اطلاعات اصلی می کنند.
- از لحظه شروع به کار با یک دستگاه جدید که اطلاعات کاربری خود را به آن اضافه کرده اید، گردآوری متادیتا آغاز می شود. به این دلیل برخی افراد به دستگاه های خود نام مستعار داده و فایل های خود را فقط بر روی هارد دیسک های قابل حمل ذخیره می کنند تا در صورت نیاز بتوان به راحتی آن را از بین برد.

برای کاهش خطر و افزایش امنیت خود و سازمان تان راهکارهای متفاوتی وجود دارد. عملی بودن و راحتی ممکن است در اولویت باشند، اما این نباید باعث نادیده گرفتن امنیت شود. امنیت باید توأم با احترام به حریم شخصی، قانون و حقوق بشر باشد.

اگر از نظر امنیتی به شدت احساس خطر می کنید، با اشخاص و سازمان های قابل اعتماد مشورت کرده و درخواست کمک کنید.



دنیای مجازی بر پایه اعتماد استوار است. این یعنی کار های ما در فضای مجازی همواره با عنصری از خطر همراه است. همیشه این نکته را در مسائل امنیتی مربوط به خود و افرادی که روی شما حساب می کنند، به یاد داشته باشید.

لازم است بدانید IP چیست و چطور کار میکند

هنگام اتصال به شبکه، به هر کاربر اینترنت یک شناسه اینترنتی (IP) تعلق میگیرد. هنگامی که در اینترنت به یک آدرس مراجعه میکنید، IP شما به آن آدرس متصل میشود. در هر صورت، هنگام هرگونه استفاده از اینترنت، IP شما برای وب سایت یا نرم افزار مقصد آشکار خواهد بود. با استفاده از امکانات دولتی و شرکت هایی که به شما اتصال اینترنت می فروشند و همچنین دسترسی به اطلاعات سایت یا سرویسی که شما به آن متصل شده اند، میتوان متوجه شد که این شناسه اینترنتی یا IP متعلق به چه شخص و محلی است و به این ترتیب، هویت شما میتواند آشکار شود. بنابراین، هنگامی که به صورت مستقیم به یک آدرس اینترنتی مراجعه می کنید، باید متوجه باشید که از خود ردپا به جا میگذارد. به یاد داشته باشید که ممکن است برخلاف تصوراتان، در اینترنت هنگام استفاده از سرویسهای اینترنتی ناشناس باقی نمانید.

به سایتهای ایرانی فروشنده راهکارهای عبور از فیلتر اعتماد نکنید

راهکارهای متعددی برای عبور از فیلترینگ وجود دارد که الزاما امنیت شما را تامین نمی کنند بلکه حتی ممکن است به شما آسیب بزنند. بعضی از سایتهایی که راهکار عبور از فیلتر مانند وی.پی.ان یا انواع دیگر Proxy را به کاربران ایرانی می فروشند، تمام اطلاعات رد و بدل شما را کنترل و ثبت میکنند؛ پس باید از سرویس هایی استفاده کنید که به آن اطمینان کامل دارید.

از HTTPS استفاده کنید

هنگام استفاده از پروتکل https، درخواست های شما برای ارتباط با صفحات وب و نتایج ارسال سرورهای اینترنتی به مرورگر شما، رمزنگاری و رمزگشایی می شود. استفاده از پروتکل https جلوی حملات شنود و مرد میانی را میگیرد.

بیشتر بانکها و سازمانهای مردم نهاد (NGO) بخاطر امنیت کاربران و سرویس های میزبانی از پروتکل https استفاده می کنند. اگر سایتی که قصد بازدید از آن را دارید امکان دسترسی به https ندارد، وارد آن سایت نشوید. آگاه باشید که فیلترهای فایروال ایرانی کمتر از بیست درصد سرعت شبکه را به ترافیک اینترنتی https اختصاص می دهند. اصولا ترافیک رمزنگاری شده تعددا کند تر است. به همین دلیل https از http کند تر است.

Settings

General Labels Inbox Accounts and Import Filters Forwarding and POP/IMAP Chat	
Language:	Gmail display language: English (US) Show all
Maximum page size:	Show 50 conversations per page Show 250 contacts per page
Keyboard shortcuts:	☒ Keyboard shortcuts off Learn more ☐ Keyboard shortcuts on
External content:	☐ Always display external content (such as images) sent by ☒ Ask before displaying external content
Browser connection:	☒ Always use https ☐ Don't always use https Learn more

امنیت email

از سرویسهای ایمیل مطمئن، به خصوص Gmail استفاده کنید

حتماً با آدرسهای https ایمیل خود را باز کنید. در نوار بالای مرورگر شما که آدرس اینترنتی را نمایش میدهد، باید بتوانید https را در اول آدرس ببینید؛ برای مثال https:// mail.google.com در صورتی که از

سرویس Gmail استفاده میکنید، روی دکمهای که در تصویر زیر نمایش داده شده کلیک کنید، سپس روی Settings کلیک کنید:

در صفحه بعد از آن، مانند تصویر زیر مطمئن شوید که گزینه Always https use انتخاب شده باشد؛ سپس در پایین صفحه روی دکمه Save Changes کلیک کنید:

- گذرواژه (password) ایمیل خود را فقط برای ایمیل استفاده کنید. برای مثال، اگر می خواهید در سایت دیگری ثبت نام کنید، دقت کنید که گذرواژه ای که در نظر میگیرید با گذرواژه ایمیل شما یکی نباشد.
- هرگز گذرواژه ایمیل خود را در اختیار سایتهای دیگر قرار ندهید. بسیاری از سایتهای معتبری مانند Facebook از شما میخواهند که گذرواژه ایمیل خود را وارد کنید تا دوستان شما را پیدا کنند. هرگز نباید چنین درخواست هایی را - به خصوص در مورد سایتهایی که شناخته شده و معتبر نیستند - بپذیرید.
- هنگامی که ایمیلی را باز می کنید، حتی اگر ایمیل را از طرف یک فرد آشنا دریافت کرده باشید، روی پیوندهایی که داخل ایمیل به سایتهای دیگر وجود دارد تا حد امکان کلیک نکنید. اگر فایلی به ایمیل ضمیمه شده و نمی دانید چیست، آن را باز نکنید.
- فریب کلاهبرداری های ایمیلی را نخورید، به ایمیل هایی که به شما میگویند برنده جایزه شده اید، توجهی نکنید و به ایمیل هایی که از شما نظرخواهی می کنند، به خصوص اگر فرستنده را نمی شناسید، پاسخ ندهید.
- حتماً چند ایمیل برای کارهای مختلف داشته باشید. برای مثال، می توانید یک ایمیل با اسم واقعی خود برای کارها و ۲۸ چگونه با تهدیدات اینترنتی مقابله کنیم مکاتبات رسمی درست کنید، یک ایمیل برای فعالیتهایی که حس می کنید، ممکن است برای شما خطر آفرین باشد یک ایمیل جداگانه هم برای کارهای تفریحی مانند ثبت نام کردن در سایتهای مختلف.
- دیدن تصاویر و دسترسی به فایلها و پیوندهایی که در داخل متن ایمیل (نه قسمت پیوستها یا Attachments) است، میتواند IP شما را برای منابع دیگر لو بدهد. نخست دقت کنید که در اینجا از فایلها و تصاویری که به ایمیل شما پیوست (Attach) شدهاند صحبت نمی کنیم؛ فایلها و عکسهای پیوست شده این مشکل را ندارد، ولی این امکان وجود دارد که از طریق تصاویر احتمالی در داخل متن ایمیل شما که قابل دیدن باشند یا با کلیک کردن بر روی پیوندهایی که در داخل ایمیل وجود دارند، شناسایی شوید. سرویس Gmail به صورت پیشفرض این مشکل را حل کرده و شما تصاویر را در داخل متن ایمیل نمی بینید، مگر آنکه در متن ارسال شده روی گزینه «Display w images» کلیک کنید؛ در این صورت، به راحتی می توان «آی پی» شما (دارنده ایمیل) و از آن طریق، شما را شناسایی کرد.

محافظت از وسایل الکترونیکی که با آن به شبکه های اجتماعی و اپلیکیشن های دوست یابی متصل می شوید تا حد امکان از وسایلی که با آن به شبکه های اجتماعی و اپلیکیشن های دوست یابی متصل می شوید، محافظت کنید. باید به دقت لایه های امنیتی را در نظر بگیرید و از آن غفلت نکنید. برخی از نکات زیر ممکن است تکراری باشند اما می توانید موارد متناسب با نیازهای خود را انتخاب و استفاده نمایید.



سیم کارتهای ثبت شده تلفن همراه

در ایران سیم کارت ها باید ثبت شوند. هنگام سفر به ایران برای ثبت سیم کارت باید پاسپورت و ویزای خود را نشان دهید. حجم سانسور در ایران بالاست. بسیاری از وب سایت ها در دسترس نمی باشند و محدودیت هایی برای تماس های تلفنی اینترنتی و استفاده از برخی پیام رسان ها وجود دارد. مراقب مطالبی که در پیام رسان ها، Facebook و Twitter می نویسید

باشید چون تحت نظارت حکومتی است. به یاد داشته باشید مطالبی که در شبکه های اجتماعی می نویسید ممکن است منجر به بازداشت، اخراج از کشور یا موارد بدتر شود. برای استفاده از اینترنت در ایران توصیه می شود از VPN استفاده کنید.



استفاده از WiFi در تلفن همراه

در آوردن سیم کارت و استفاده از WiFi برای اتصال به شبکه های اجتماعی و اپلیکیشن های دوست یابی یک راهکار رایج دیگر است. در ایران WiFi به راحتی در دسترس است اما با استفاده از یک سیستم فیلترینگ پیچیده از سوی دولت کنترل می شود. برای همین در بخش بعدی به VPN ها پرداخته ایم.

علاوه بر بستن سایت های خاص، شبکه اینترنت ایران ترافیک را بر اساس محتوای فیلتر می کند. ترافیکی که با پروتکل SSH رمزگذاری شده (https) با کمتر از ۲۰ درصد از سرعت کامل شبکه حرکت می کند (عمدتا ترافیک رمزگذاری شده به سرعت مورد هدف قرار می گیرد). گزارشی در سال ۲۰۱۳ توسط دو ایرانی و یک استاد دانشگاه میشیگان منتشر شد که جزئیات بیشتری در مورد نحوه سانسور اینترنت در ایران دربر دارد. فایل pdf این گزارش را می توانید از طریق لینک زیر دریافت کنید:

<https://jhalderm.com/pub/papers/iran-foci13.pdf>.

رمزنگاری

- رمزنگاری نکردن داده ها در وسایل الکترونیکی درست مانند قفل نکردن درب ورودی خانه، کاری خطرناک است. جدا توصیه می شود که داده های موجود در وسایل الکترونیکی خود را رمزنگاری کنید.
- اگر دستگاه خود را رمزنگاری نکرده اید یا مطمئن نیستید که دستگاه شما رمزنگاری شده است یا نه، دفترچه ی راهنمای کاربر تلفن همراه خود را مطالعه کنید. محبوب ترین تلفن های همراه یعنی آیفون و سامسونگ گزینه هایی برای رمزگذاری دارند:
- آی فون: اگر از آی فون ۳GS یا مدل جدیدتر، آی پاد لمسی نسل ۳ به بعد، و یا هر نوع آی پدی استفاده می کنید، می توانید محتویات

دستگاه خود را با رمزنگاری محافظت می کند.

- گوشی های جدید سامسونگ و دستگاه های اندروید در زمان راه اندازی، گزینه رمزنگاری را پیشنهاد می دهند. همه وسایل الکترونیکی در دفترچه راهنمای کاربر خود اطلاعاتی درباره ی نحوه رمزنگاری دارند.

چت کردن و استفاده از Messengerها

در بیشتر نرم افزارهایی که برای گفتگوی اینترنتی یا «چت» کردن مورد استفاده قرار میگیرند، IP شما برای شخصی که با او چت میکنید، قابل دیدن خواهد بود و به این ترتیب، این امکان وجود دارد که هویت شما به راحتی شناسایی شود. بخصوص باید توجه داشته باشید که بسیاری از راهکارهای امنیتی که هویت شما را مخفی میکنند و راهکارهای فیلترشکن در مورد نرم افزارهایی که برای چت کردن استفاده می شود، بی تاثیر خواهد بود، زیرا بسیاری از راهکارهای امنیتی فقط در مورد «مرورگر وب» کارایی دارند. برای مثال، نرم افزار Browser Tor نمیتواند امنیت شما را هنگام استفاده از Messenger Yahoo یا Skype تامین کند. تشخیص اینکه آیا هنگام استفاده از نرم افزارهای گفتگوی متنی، صوتی و تصویری اینترنتی امنیت دارد یا نه، برای افراد غیر متخصص کار دشواری است و بهتر است در این مورد از یک فرد متخصص کمک بگیرید. ولی در مجموع، پروکسی و VPNهایی که تمام ارتباطات اینترنتی شما را پوشش میدهند (نه فقط مرورگر وب را) این امکان را دارند که امنیت شما را هنگام چت کردن بالا ببرند. همچنین، مراقب فایلهایی باشید که از طریق نرم افزارهای چت برای شما فرستاده میشود. ممکن است یک فایل در ظاهر شبیه به یک عکس باشد، ولی در واقع یک ویروس یا بدافزار جاسوسی باشد. در مورد پیوندهایی که هنگام چک کردن برای شما فرستاده میشود و نوشته هایی که در ظاهر مربوط به خود نرم افزار به نظر میرسند، دقت کنید و ندانسته روی چیزی کلیک نکنید. در صورتی که معنی و مفهوم یک پیام یا پیام خطا را درست متوجه نمی شوید، روی هیچ یک از گزینه ها کلیک کنید و سعی کنید نرم افزار را ببندید. مهم! اگر با VPN به اپلیکیشن های دوست یابی، پیام رسان و یا شبکه های اجتماعی فیلتر شده وصل شده اید، بدانید که میزان خطر متوجه شما متوسط رو به بالاست. به حس امنیت کاذبی که VPN به شما می دهد، اطمینان نکنید. مراقب باشید و احتیاط کنید!



منابع و مآخذ

مطالعه آنلاین

بهداشت روانی و فضای مجازی

http://iran.outrightinternational.org/interview-article/mental_security/

- تفاوت میان امنیت فیزیکی و روانی و نمونه های آن،
- ساز و کارهای پذیرش از طرف اطرافیان چیست و چگونه آن را تغییر دهیم؟
- تمایل به پذیرش و دوست داشته شدن -
- تمایز بین هویت و هویت مجازی

نحوه محافظت از داده ها

http://iran.outrightinternational.org/interview-article/saving_data/

- امنیت دیجیتال چیست؟
- امنیت دستگاه شما چقدر است؟
- گزینه های مختلف برای ذخیره کردن داده ها (از جمله گزینه های محلی و کلود)
- چگونه داده های خود را بدون خطر ذخیره کنید

امنیت دیجیتال

<http://iran.outrightinternational.org/interview-article/digisecurity/>

- معنای «امنیت» برای مردم طول تاریخ چه بوده و چرا به آن نیاز داشته ایم (به اختصار)؟

- چه راهکارهایی برای محافظت از خود در برابر آسیب دیجیتال وجود دارد؟
- حمله سایبری چیست و روش های متداول این حملات چیست؟ (به طور مثال بدافزارها، باجافزار واناکرای، مهندسی اجتماعی، فیشینگ)
- دقیقاً با چه راهکارهای می توانیم از خود محافظت کنیم؟

مدیریت گذرواژه

http://iran.outrightinternational.org/interview-article/pass_manage/

- اهمیت آن چیست؟
- چطور می توان مانع این تهدید شد
- گذرواژه
- ارتباط با اپلیکیشن های دیگر
- ایجاد فضای شخصی
- فضای عمومی، امن است یا نه ؟
- فیشینگ
- توضیح رمزنگاری end-to-end توسط Protonmail.
- مرورگرهای جدید مانند DuckDuckGo جمع آوری غیرفعال اطلاعات را محدود می کنند.
- دفاع از خود در شرایطی که تحت نظر هستید تدوین شده توسط بنیاد حریم الکترونیک
- دفاع از خود در شرایطی که تحت نظر هستید تدوین شده توسط Intercept
- دفاع از خود در شرایطی که تحت نظر هستید تدوین شده توسط Equality Labs
- نوزده منبع فناوری به فارسی ASL
- Access Now - تمرکز بر حقوق دیجیتال کاربران در معرض خطر در سطح جهانی
- سیستم های اوپن ویسپر (Open Whisper Systems)
- شبکه های توری (Mesh Networks) - شبکه های توری، دسترسی مستقیم به اینترنت را بدون استفاده از شرکت های رساننده خدمات اینترنتی ممکن می سازند.



واژه نامه

فن آوری اطلاعات - استفاده از سیستم ها (به خصوص رایانه ها و مخابرات) برای ذخیره سازی، بازیابی و ارسال اطلاعات.
امنیت (در فناوری اطلاعات (IT)) - به معنی دفاع از اطلاعات دیجیتال و منابع فناوری اطلاعات در برابر تهدیدهای داخلی و خارجی، مخرب و تصادفی است.

کنترل - آنچه در دسترس و حیطه کنترل است و می تواند برای دفاع و پیشگیری استفاده شود تا خطرات امنیتی متوجه دارایی ها، اطلاعات و دستگاه ها به حداقل برسد.

احراز هویت دو مرحله ای - یک لایه اضافی امنیتی است که علاوه بر گذرواژه و نام کاربری، نیازمند چیزی است که فقط کاربر می داند یا می تواند فراهم کند.
دو مورد از رایج ترین مراحل احراز هویت دو مرحله ای، تایید از طریق پیامک یا کلید های امن USB Key است.

رمزنگاری - به معنی مخدوش کردن پیام یا اطلاعات به گونه ای است که فقط طرفین مجاز، به آن دسترسی داشته و افراد غیر مجاز به آن دسترسی نداشته باشند.

داده های حسگر - داده هایی است که توسط حسگر هایی مانند دوربین و میکروفون در مکان های عمومی، خانه های خصوصی و دستگاه های تلفن همراه ایجاد می شود.

فراداده یا متادیتا - اطلاعات ذخیره شده در فایل هایی است که توسط حسگرها ایجاد شده اند.

Torrent - به یک فایل رایانه ای گفته می شود که دارای متادیتای حاوی اطلاعات مختلف است. فایل تورنت به طور معمول دارای پسوند torrent است و شامل محتوای اصلی نیست. برای باز کردن این فایل / لینک نیاز به یک نرم افزار BitTorrent است.

فایروال - یک سیستم امنیت شبکه است که براساس قوانین امنیتی معین، ترافیک ورودی و خروجی شبکه را نظارت و کنترل می کند. ویروس رایانه ای - نوعی کد یا برنامه مخرب است که برای تغییر نحوه عملکرد رایانه و سرایت از یک رایانه به رایانه دیگر، طراحی شده است. ویروس با آلوده کردن برنامه های رایانه ای و یا اتصال به فایل های پشتیبان ماکرو نویسی، کد خود را اجرا می کند. ویروس می تواند از طریق خراب کردن یا از بین بردن داده به نرم افزار سیستم آسیب زده و اثرات غیر منتظره یا مخربی داشته باشد.

بدافزار - یک «نرم افزار مخرب» است. این نرم افزارها مخصوص آسیب زدن به رایانه ها سرقت اطلاعات بدون اطلاع فرد، طراحی شده اند. انواع مختلف بدافزار عبارتند از: جاسوسافزار، باجافزار، ویروس ها، کرم ها، اسب های تروجان، ابزارهای تبلیغاتی مزاحم (آگهیافزار) یا هر نوع کد مخرب که در رایانه نفوذ می کند.

Format - فرمت کردن درایو (هارد دیسک، دیسک قابل حمل، فلش درایو و غیره) به معنای آماده کردن بخشی از درایو که به سیستم عامل اختصاص داده شده، است. فرمت کردن تمام داده ها را از روی درایو پاک کرده و فایل سیستم را نصب می کند.

شبکه خصوصی مجازی یا VPN - VPN با گسترش برد شبکه خصوصی، به کاربران اجازه می دهد تا از طریق شبکه های مشترک یا عمومی به تبادل اطلاعات بپردازند. فعالیت VPN بگونه ای است که انگار رایانه ها به طور مستقیم به یک شبکه خصوصی وصل هستند. برنامه هایی که تحت VPN اجرا می شوند می توانند از کارکرد، امنیت و مدیریت شبکه خصوصی بهره مند شوند.

TOR چیست؟ یک شبکه پیازی (onion router) یا چند لایه است که ترافیک اینترنت را از طریق یک شبکه همپوشان داوطلب و رایگان جهانی هدایت می کند. این شبکه دارای بیش از ۷ هزار رله (رایانه هایی که اجزا کوچک اطلاعات از آنها عبور می کند) است. این شبکه پیازی مکان و محتوای اطلاعات کاربران را از هر کسی که نظارت شبکه یا تجزیه و تحلیل ترافیک انجام می دهد، پنهان می کند.

TTPS (HTTP over SSL or HTTP Secure) به معنی استفاده از لایه سوکتهای امن (Secure Socket Layer- SSL) یا پروتکل امنیتی لایه انتقال (Transport Layer Security-TLS) تحت HTTP است. HTTPS درخواست های صفحه کاربر و نیز صفحاتی که مرورگر از سرور وب دریافت کرده را رمزنگاری و رمزگشایی می کند. استفاده از HTTPS مانع از استراق سمع و حملات مرد میانی می شود.





