امنیت در دنیای مجازی

دوره آموزش الکترونیک

مقدمه

بدون مراقبت‌های کافی، دیگران می‌توانند بی‌اجازه مکالمات و فعالیت‌هایتان را تحت نظر بگیرند. شاید همه ندانند این کار چگونه انجام می‌شود، اما دولت ایران (در کنار بسیاری دول دیگر) به پیشرفته ترین تجهیزات شنود و فیلترینگ اینترنت مجهز است و این اقدامات را در سطح گسترده انجام می‌دهد. اگر هنگام استفاده از اینترنت تدابیر لازم را به‌کار نگرفته باشید هر کسی می‌تواند از فعالیت‌های‌تان باخبر شده، به محتوای مکالمات‌تان دسترسی پیدا کند یا از طرف شما به دیگران پیام بفرستند. علاوه بر این، بدون حفظ تدابیر امنیتی، داده و اطلاعات‌تان نیز از خطر دستبرد در امان نخواهد ماند.

خوشبختانه، عادت به رفتار امن در فضای مجازی کار سختی نیست. پیش از هرچیز می‌بایست تهدیدهای پیش رو را شناخته، دانش و ابزارهای مقابله با آن تهدیدات را به روز نگه دارید.

هدف این دوره بررسی روش‌هایی است که با استفاده از آن هویت کاربران اینترنتی، به‌خصوص خبرنگاران، کنشگران اجتماعی و حقوق بشری افشا شده، می‌توان آنان را زیر نظر گرفت. آگاهی از این روش‌ها گام نخست در مسیر حفاظت از حریم خصوصی در محیط اینترنت است.

این دوره آموزشی شامل چهار درس است:

- شناخت تهدید.
- ایمن‌سازی کامپیوتر و دیگر وسائل الکترونیکی هوشمند.
- حفاظت از داده و اطلاعات.
- ایمن‌سازی ارتباطات اینترنتی.

درس یک: شناخت تهدید

فهرست عنواین

مقدمه

تهدیدها در فضای مجازی کدامند؟

تهدید های اینترنتی دو دسته هستند:

i. **گروه اول** تهدیدهایی‌اند که **فعالیت‌هایتان** را تحت تاثیر قرار می‌دهند. اگر امنیت سیستم‌تان به خطر بیافتد، داده و اطلاعات‌تان آسیب دیده، به دست افراد ناشایست افتاده یا در اطلاعات ارسالی/دریافتی‌تان و وب‌سایت‌هایی که بازدید می‌کنید دست برده می‌شود.
ii. **گروه دوم** تهدیدهایی هستند که به **شخص شما** آسیب می‌رسانند. بدون رعایت احتیاط، امکان دارد هویت، محل کار و یا دیگر اطلاعات شخصی‌تان افشا شده، امنیت‌تان به طور جدی به خطر بیافتد.

این دو دسته تهدید، نه همواره، اما اغلب با یکدیگر مرتبط هستند. برای مثال، ممکن است دولت بدون آن‌که هویت‌تان را بداند، عمل‌کرد رایانه‌ای که با آن کار می‌کنید را مختل کند. با این حال، بهتر است فرض را بر این بگذارید که اگر فعالیت‌تان در معرض خطر است، امنیت شخصی‌تان نیز به خطر خواهد افتاد.

ممکن است شما هدف اصلی تهدید نباشید، اما حمله‌کنندگان از طریق شما به هدف اصلی (دوستان یا همکاران‌تان) حمله کنند. از سوی دیگر، ممکن است در اثر حمله، کنترل شناسه کاربری‌تان را از دست داده، یا شناسه کاربری‌تان کاملا نابود شود.
حمله‌کنندگان ممکن است شبکه افرادی را که با آنان در ارتباط هستید را شناسائی کرده یا نشانی و اطلاعات تماس آنان را از طریق هک کردن حساب کاربری شما به دست آورند.

تهدیدها چگونه عمل می‌کنند؟

روش‌های حمله به کنش‌گران و خبرنگاران در محیط‌های آنلاین بسیار است، هرچند برخی از همه مشهورتر هستند. در پایان این درس، شما با سه نوع معمول از این روش‌ها آشنا خواهید شد: جعل اینترنتی(فیشینگ)، بدافزار و حملات باواسطه.
جنبه دیگر تهدیدها ناشی از فعالیت در شبکه‌های اجتماعی یا ناشی از عدم رعایت موارد ایمنی توسط افرادی است که شما با آنان در ارتباط هستید. به این موارد در درس‌های چهار و پنج خواهیم پرداخت.

بیشتر بخوانید:

این درس به تهدیدهایی می‌پردازد که خبرنگاران و کنشگران اینترنتی در ایران با آن روبرو هستند. برای درک بهتر این موضوع که چرا دانستن این مطالب برای شما اهمیت دارد می‌بایست با روش هایی که دولت ایران برای فیلترینگ، نظارت، و ایجاد محدودیت های قانونی در محیط مجازی به کار می گیرد آشنا شوید.

پیش از ادامه، مطالعه لینک‌هایی زیر را پیشنهاد می‌کنیم:

- جرائم کامپیوتری در ایران - رفتارهای اینترنتی مخاطره آمیز (فارسی)
- آزادی در اینترنت - گزارش سال ۲۰۱۴ خانه آزادی (انگلیسی)
- دشمنان اینترنت: ایران - فضای مجازی آیت‌الله‌ها (انگلیسی)
- دشمنان اینترنت - ایران (گزارش ۲۰۱۴) : سپاه پاسداران انقلاب اسلامی، شورای عالی فضای مجازی، کارگروه تعیین مصادیق محتوای مجرمانه (فارسی)

تهدید شماره یک: جعل اینترنتی (فیشینگ)

جعل اینترنتی (فیشینگ) چیست؟

در این نوع حمله اینترنتی، حمله کننده وانمود می‌کند که شخص یا وبسایتی است که شما به آن اعتماد دارید. هدف او از این کار دریافت گذرواژه (پسورد) یا نصب بدافزار روی رایانه شما است. البته این کار بدون آن‌که شما متوجه آن شوید انجام خواهد شد.(در ادامه، درباره بدافزار بیشتر توضح داده خواهد شد.)

چرا آگاهی از این نوع حمله اهمیت دارد؟

نفوذگران اینترنتی می‌توانند با استفاده از گذرواژه به محتوای ایمیل، حساب بانکی، یا هر حساب کاربری دیگری که در اینترنت داشته باشید دسترسی پیدا کنند. به بیانی دیگر، با داشتن گذرواژه می‌توانند ایمیل‌هایی را که می‌فرستید بخوانند، نام افرادی که با آن‌ها در ارتباط هستید را ببینند، به حساب بانکی‌تان دسترسی پیدا کنند، و حتی خودشان را به جای شما جا بزنند. هرکسی که در اینترنت از گذرواژه استفاده می‌کند، در معرض این نوع حمله قرار دارد.

این حمله چگونه انجام می شود؟

نفوذگران اینترنتی اغلب با کمک آدرس‌های ایمیل مشابه، یا نشانی وبسایت‌هایی شبیه اسامی آشنا، خودشان را به جای اشخاص معتبر جا می‌زنند. برای مثال ممکن است ایمیلی با شناسه کاربری دوستان یا همکاران‌تان ارسال کنند که از سرویس ایمیل دیگری فرستاده شده باشد، یعنی به جای xxxxx@gmail.com از آدرس ایمیل xxxxx@yahoo.com استفاده کنند. یا لینکی برای‌تان ارسال کنند که شما را به صفحه‌ای هدایت می‌کند که نشانی‌اش بسیار شبیه آدرس وبسایت‌های مورد اطمینان‌تان است. برای مثال، آدرس سایت‌هایی مانند facebook یا Gmail اما با اندکی تفاوت در طرز قرار گرفتن حروف (faceboook.com به جای facebook.com). حتی همان‌طور که در تصویر بالا دیده می‌شود، متن نمایش داده شده ممکن است کاملا درست باشد، حال آن‌که آدرس واقعی پشت لینک شما را به جای دیگری هدایت خواهد کرد. این تفاوت‌ها آنقدر ظریف‌اند که افراد کمی ممکن است متوجه آن شوند. همین نقطه قوت نفوذگران است.

نبض‌ایران
تقویت صدای ایرانیان

رعایت نکات زیر را به همه کاربران توصیه می‌کنیم:

- ✓ همیشه نشانی ایمیل فرستنده را چک کنید.
- ✓ محتوای ایمیل‌های دریافتی را با دقت بررسی کنید، ممکن است بی‌ربط یا غلط باشد. ایمیل‌های فیشینگ معمولا از شما می‌خواهند که هرچه زودتر کاری را انجام دهید یا روی لینکی کلیک کنید. ایمیل ممکن است دقیقا نام و نام خانوادگی شما را ذکر نکرده باشد.
- ✓ نشانی لینک‌های درون ایمیل را پیش از کلیک کردن روی آن حتما چک کنید. آیا همان است که انتظار دارید؟
- ✓ آیا اطلاعات ارائه شده درون ایمیل صحیح است؟
- ✓ آیا منتظر چنین ایمیلی بوده‌اید؟

نمونه‌های واقعی حمله در ایران

در پاییز سال ۱۳۹۰، یک نفر با ربودن مجوزهای امنیت دیجیتالی، برای مقامات امنیتی ایران این امکان را فراهم ساخت تا صفحات جعلی ورود به حساب کاربری گوگل و برخی سایت‌های دیگر را شبیه‌سازی کنند. این مجوزهای دیجیتالی نفوذگران را قادر ساخت تا صفحه ایمیل گوگل (mail.google.com) را بازسازی کرده، ردیابی حمله را بسیار دشوارتر سازند.

نمونه دیگر، گزارش Citizen Lab از حملات پیشرفته فیشینگ علیه کاربران ایرانی و بین‌المللی فعال در زمینه ایران است که با هدف هک کردن رمز عبور دو مرحله‌ای انجام شده. در این نوع حملات، حمله‌کنندگان با کمک اطلاعات و دانش پیش گردآوری شده در مورد قربانیان، روابط و فعالیت‌های آنان سعی می‌کرده‌اند تا حساب‌های کاربری که از رمز عبور دو مرحله‌ای استفاده می‌کردند را هک کنند.
گزارش فارسی سیتیزن‌لب در مورد این حملات را اینجا بخوانید. گزارش انگلیسی از طریق این لینک قابل دسترسی است.

نبض ایران
تقویت صدای ایرانیان

ایمیل واقعی بود یا جعلی؟

آیا می‌توانید تشخیص دهید که این ایمیل واقعی است یا جعلی؟ روی لینک کلیک کنید تا پاسخ آن را بیابید.

Subject: Balatarin Account Verification
Date: Fri, xxxxxxxxxxxx
From: "Balatarin" <accounts@balatarin.com>
Reply-To: accounts@balatarin.com
To:

کاربر گرامی،
بنا به دلایلی معتقدیم که گذرواژه یا اطلاعات حساب کاربری شما احتمالا رخنه پذیر شده و ایمن نیست.
خواهشمند است از طریق لینک زیر اقدام فرمائید:
http://arribba.cgi3.balatarin.com/aw-cgi/balatarinISAPI.dll?UpdateInformationConfirm&bpuser=1

لطفا اطلاعات مورد نیاز را در فرم ارائه شده وارد کنید. دریافت این اطلاعات برای ارائه خدمات امن به شما کاربر گرامی توسط بالاترین الزامی است.
با تشکر
مدیریت حساب‌های کاربری
طبق توافقنامه کاربری، سایت بالاترین هر چند وقت یکبار گزارشی از تغییرات ایجاد شده و بهبود کارآئی وبسایت برای شما ارسال می‌کند.
پاسخ به پرسش‌های خود دراین باره را در صفحه توافقنامه کاربری و سیاست حریم خصوصی بیابید.

این یک حمله فیشینگ است.

همان‌طور که احتمالا متوجه شدید، با نگه داشتن ماوس روی نشانی وب، لینک مربوطه شما را به سایت بالاترین هدایت نمی‌کند - بلکه به آدرسی کاملا متفاوت می‌برد. این یکی از روش‌های رایج در حملات فیشینگ است، که باید به آن توجه داشت.

تهدید شماره ۲: بدافزار

بدافزار چیست؟

بدافزار اصطلاحی کلی است برای برنامه‌های رایانه‌ای مخرب نظیر انواع ویروس‌ها، کرم‌ها، و برنامه‌های مشابه آن. بدافزار می‌تواند به چند روش به شما ضربه بزند؛ ممکن است با ربودن گذرواژه‌های‌تان - یا هر چیز دیگری که تایپ می‌کنید - به حساب‌های کاربری‌تان دسترسی پیدا کند یا از رایانه‌تان به اینترنت وصل شده و به دیگر رایانه‌ها حمله کند. بدافزار حتی می‌تواند فایل‌های‌تان را بازرسی کرده یا اطلاعاتی که روی رایانه ذخیره کرده‌اید را به جای دیگری ارسال کند.

برخی گونه‌های اصلی بدافزار عبارتند از:

- **ویروس، کِرم و بات**. این گونه بدافزارها بسیار به یکدیگر نزدیکند و به همین دلیل اغلب با یکدیگر اشتباه می‌شوند. از نظر فنی، یک ویروس برای انتقال از رایانه‌ای به رایانه دیگر نیازمند اقدام کاربر است؛ مثلا، ارسال مجدد ایمیل، اما کِرم به‌طور خودبه‌خودی گسترش می‌یابد. با این حال، همه انواع بدافزار به‌طور بالقوه از امکان انتشار و تخریب مؤثر برخوردارند.
- **اسب تروِیا**. این گونه بد افزار برنامه مخربی است که خود را درون نرم افزارهای به‌ظاهر بی‌خطر پنهان می‌کند؛ همانطور که در افسانه اسب تروِیا اشاره شده. این نوع بدافزار در آغاز به نظر بی‌خطر می‌آید یا اصلا تشخیص داده نمی‌شود. او منتظر می‌ماند و در موقع مناسب با آغاز حمله تهدیدش را عملی می‌سازد.

چرا باید درباره این نوع حمله هشیار باشم؟

بدافزار راه مناسبی برای رخنه‌گران است تا برنامه‌های نظارتی‌شان را به منظور جمع‌آوری اطلاعات درباره شما یا شناسائی فعالیت‌های‌تان اجرا کنند. هر کاربر اینترنتی در معرض آسیب‌دیدن از سوی بدافزار است.

این حمله به چه صورتی انجام می شود؟

بدافزار می‌تواند شکل‌های متفاوتی به خود بگیرد؛ ممکن است از راه برنامه‌هایی با منابع نامطمئن ،همچون نرم افزارهای قفل‌شکسته، به رایانه‌تان منتقل شود. در ضمن این امکان وجود دارد که بدافزار از راه‌های زیرکانه‌ای به رایانه‌تان نفوذ کند؛ برای مثال، صفحه‌ای که همچون یک اخطار امنیتی طراحی شده باشد. علاوه بر این، بدافزارها می‌توانند از راه ابزارهای ذخیره‌سازی مثل یو.اس.بی درایو یا انتقال فایل از طریق شبکه منتقل شوند. برخی وب‌سایت‌های دانلود رایگان توسط هکرها مدیریت می‌شوند. این وب‌سایت‌ها (که در ایران نیز بسیار پرطرفدار هستند) به کاربر امکان دانلود مجانی نرم‌افزارها را می‌دهند، اما به‌طور پنهانی بدافزار روی رایانه نصب می‌کنند.

آیا از این تهدید در ایران نیز علیه کاربران استفاده شده؟

یک نمونه استفاده از بدافزار علیه ایرانیان دگراندیش، اسب تروای سیمرغ است. محققان در دانشگاه تورنتو متوجه شدند که یک برنامه فیلترشکن پرطرفدار در میان کاربران از سوی هکرها تغییر شکل یافته تا اطلاعات موجود در رایانه کاربران را به منبعی دیگر منتقل کند. این نمونه بدافزار به ویژه از آن رو خطرناک بود که خود را به عنوان ابزاری برای ارتقاء آزادی دیجیتال معرفی می‌کرد. این مثال خوبی از این واقعیت است که فارغ از شکل و کاربردی که برنامه‌ها ارائه می‌کنند، همواره می‌بایست در برابر تهدیدهای امنیتی بالقوه گوش به زنگ ماند.

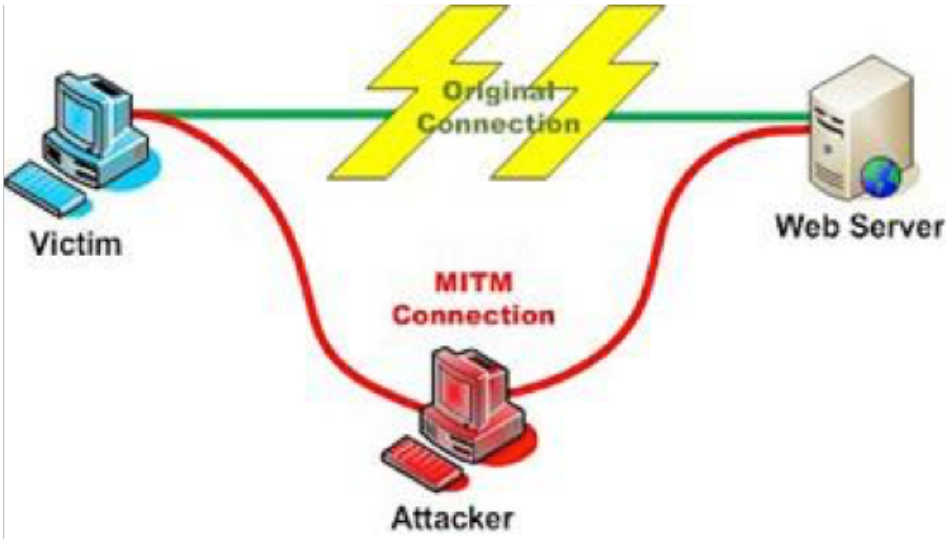
تهدید شماره ۳: حمله فرد میانی، نظارت گزینشی، و فیلترینگ

حمله فرد میانی به حمله‌ای گفته می‌شود که شخص ثالثی اطلاعات ارسالی/دریافتی‌تان از طریق اینترنت را برباید. هنگام اتصال به اینترنت، در تک‌تک گره‌های ارتباطی مسیر انتقال اطلاعات، ممکن است چنین حمله‌ای رخ دهد. گره ارتباطی یعنی نقاط اتصال شبکه اینترنت؛ از مودم منزل یا محل کار گرفته تا شبکه خدمات دهنده اینترنت، شرکت مخابرات و غیره. حلمه فرد میانی وقتی اتفاق می‌افتد که یکی از گره‌های طول مسیر، با هدف جاسوسی، اقدام به جمع آوری اطلاعات کرده، اطلاعات عبوری را تغییر داده یا به شما اطلاعات دروغین تحویل دهد.

در نوع دیگری از حمله فرد میانی، تمرکز بر نظارت بر کلمات کلیدی است. در این نوع حمله، به‌جای بررسی همه اطلاعات رد و بدل شده، گره ارتباطی حمله‌کننده، یا تنها بر کلمات کلیدی از پیش تعریف شده‌ای تمرکز می‌کند که ارزش اطلاعاتی دارد، یا بر ارتباطات شخص مورد نظر نظارت می‌کند. در این روش ممکن است جریان اطلاعاتی که مورد تأیید نظارت‌گران نیست قطع شود؛ به زبان دیگر محتوای مورد نظر ما فیلتر می‌شود.

به خاطر داشته باشید

به‌طور معمول، در حمله فرد میانی، شخص ثالثی با دستکاری رایانه‌تان جریان داده را تغییر می‌دهد. اما همچنین ممکن است شبکه میزبان یا ارائه کننده خدمات اینترنتی نیز از جایگاه خود سوء استفاده کرده، کد ارتباطاتی را بشکنند یا به نحوه دیگری ارتباطات‌تان را دستکاری کند.



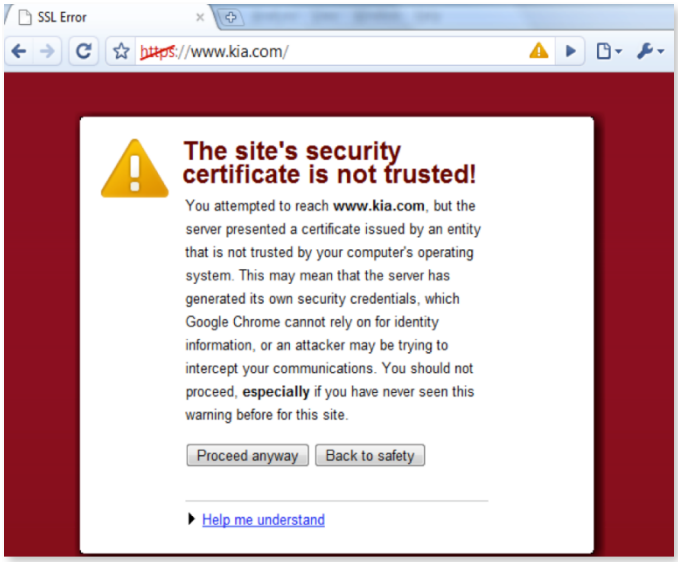
چرا باید نسبت به این نوع حمله هشیار باشیم؟

حمله فرد میانی، بیشتر در شبکه‌های بی‌سیم عمومی (Public Wifi) رخ می‌دهد، جایی که کاربران می‌توانند ارتباطات دیگر کاربران را رصد کرده یا مختل سازند. هرچند در دیگر گره‌های ارتباطی نیز ممکن است رخ دهد.

علاوه بر خواندن و رصد اطلاعاتی که رد و بدل می‌شود، صاحبان کافی‌نت‌ها یا ارائه دهندگان خدمات اینترنتی نیز می‌توانند دسترسی به سایت‌های مورد نظر را محدود سازند. فیلترینگ ممکن است براین اساس انجام شود که شما چه کسی هستید، به چه سایتی قصد دارید مراجعه کنید، یا به دنبال چه محتوایی می‌گردید. فیلترینگ ممکن است همه دامنه وب را از کار بیاندازد، یا تنها صفحات مشخصی را بر مبنای کلماتی کلیدی از دسترس خارج کند.
نکته مهم در مورد فیلترینگ این است که همچون حمله فرد میانی کسی به محتوای اطلاعاتی که رد و بدل می‌کنید دسترسی دارد. یعنی می‌بیند که شما از چه وب‌سایت بازدید می‌کنید، یا به متن مکالمات (رمزگذاری نشده) شما دسترسی دارد.

این حمله به چه شکل انجام می‌شود؟

متاسفانه، کشف حمله فرد میانی گاه بسیار دشوار است. یک نشانه مهم اخطار مجوز سایت است. هنگامی که به سایتی سر می‌زنید که حاوی اطلاعات حساس است، رایانه شما مجوز سایت را به‌طور خودکار، مرور و تأیید می‌کند. کسی که جریان اطلاعات را دستکاری کرده باشد نمی‌تواند از آن مجوز استفاده کرده، شما اخطاری شبیه این دریافت خواهید کرد: (توجه داشته باشید که سایت‌های بدون گواهینامه امنیتی چنین اخطاری نشان نمی‌دهند و شما هنگام بازدید از آن وب‌سایت‌ها احتمالا متوجه نخواهید شد که تحت نظر قرار گرفته‌اید.)



چگونه این تهدید در ایران به کار گرفته شد؟

یک نمونه از حمله فرد میانی در ایران هنگامی روی داد که هکرها برای گوگل، مجوز تقلبی طراحی کردند. این حمله که در ماه مرداد ۱۳۹۰ کشف شد به هکرها اجازه داده بود تا به محتوای جستجوی‌های اینترنتی کاربران ایرانی که از مرورگرهائی غیر از گوگل کروم استفاده کرده بودند، دسترسی پیدا کنند.

ارزیابی میزان خطر: قسمت ۱

تا اینجا کلیاتی در خصوص تهدیدهای اصلی در فضای مجازی ارائه شد. طرز استفاده از اینترنت از فردی به فرد دیگر فرق می‌کند؛ به همان میزان هم نقطه ضعف‌های افراد و ملاحظاتی که می‌بایست در نظر بگیرند متفاوت است. این نکته بسیار اهمیت دارد، زیرا می‌بایست با تهدیدهای خاص مربوط به نوع استفاده‌ای که از اینترنت می‌کنید آشنا شوید.

پرسشنامه زیر سعی می‌کند تا تصویر بهتری ترسیم کند از خطرهایی که در کمین‌تان نشسته‌اند. هنگام پاسخ به این پرسش‌ها یک روز عادی از را به خاطر بیاورید که در آن از رایانه و اینترنت استفاده می‌کنید. بدین ترتیب به فهرست تهدیدهایی خواهید رسید که احتمالا برخی برای‌تان ناآشنا هستند. در ضمن، فهرستی بدست خواهید آورد از اقدامات امنیتی لازم برای فعالیت در فضای مجازی. در درس‌های بعد، شما را در تکمیل این فهرست بیشتر یاری خواهیم کرد.

برای تکمیل فرم ارزشیابی به کاغذ و قلم نیاز خواهید داشت.

الف. ابزار، حساب ها، و شبکه‌ها: ترسیم تهدیدهای پیش روی

I. بگذارید با یک روز عادی هفته شروع کنیم. روز شما از چه فعالیت‌هایی تشکیل شده؟ منظور زمانی است که به کار، خانواده و دوستان اختصاص می‌دهید. زمان‌بندی یک روز عادی را در جدولی روی کاغذ ترسیم کنید.
II. حال به جدولی که کشیده‌اید نگاه کنید. در چه موقعیت‌هایی از روز به اینترنت وصل می‌شوید؟ برای مثال، آیا در راه رسیدن به محل کار، ایمیل‌تان را چک می‌کنید؟ یک فهرست کلی تهیه کنید شامل همه مواقعی از روز که آنلاین هستید.
III. حال در فهرستی که تهیه کرده‌اید، ببینید از چه وسائلی برای اتصال به اینترنت (رایانه شخصی، تبلت، ...) استفاده می‌کنید؟ فهرست آن را نیز تهیه کنید.
IV. کجا از این وسائل استفاده می‌کنید؟ از چه شبکه‌هایی برای اتصال به اینترنت استفاده می‌کنید؟ آیا آنها عمومی هستند (مانند کافی‌نت‌ها) یا خصوصی (مانند خانه یا محل کار)؟ چه کسی هر کدام از این شبکه‌ها را اداره می‌کند؟ همه این موارد را نیز فهرست‌بندی کنید.
V. در پایان، از چه حساب‌های کاربری برای دسترسی به اینترنت استفاده می‌کنید؟ این پرسش شامل همه موارد از قبیل ایمیل، کد دسترسی به رایانه شخصی، حساب بانکی و غیره می‌شود. همه را یادداشت کنید.

حال نقشه‌ای در دست دارید که موارد تهدیدهای امنیتی را به شما نمایش می‌دهد. شاید باور نکنید، اما هر ابزار دسترسی و حساب کاربری که حاوی اطلاعاتی از شما باشد، رخنه‌پذیر بوده، به‌طور بالقوه می‌تواند مورد تهدید واقع شود. همچنین سطح امنیتی هر یک از این ابزارها و حساب‌ها به‌طور مستقیم به شبکه‌ای بستگی دارد که شما برای اتصال به اینترنت از آن استفاده می‌کنید. درباره این‌که چگونه از ابزارهای ارتباطی خود محافظت کرده، شبکه‌های امن‌تری انتخاب کنید، در درس‌های بعد بیشتر توضیح داده خواهد شد.

ب. کاربری: تحلیل مخاطراتی که در فضای آنلاین با آن مواجه هستید

اکنون می خواهیم به‌طور مشخص تهدیدات مرتبط با هریک از وسائل مورد استفاده را تحلیل کنیم. از آنجایی که این پرسش‌ها به مسائل جزئی‌تر می‌پردازند، به همراه هر پرسش، توضیحاتی درباره روش امن استفاده نیز ارائه شده.

درس‌های آینده به تفصیل به هر یک از این موارد خواهد پرداخت.

- فهرست رایانه‌ها، تبلت‌ها و موبایل‌هایی که با آن کار می‌کنید را در نظر بگیرید. آیا **سیستم‌عامل‌های**[1] این رایانه‌ها ثبت شده و قانونی‌اند؟ یا از سیستم‌عامل‌های قفل[1]شکسته استفاده می‌کنید؟ برای هر دستگاه، پاسخ به این پرسش را جلوی نام آن یادداشت کنید. اگر از سیستم‌عامل‌های «قفل‌شکسته» استفاده می‌کنید، باید در نظر داشته باشید که این نسخه‌ها، احتمالا حامل ویروس‌های از پیش جاسازی شده هستند. سیستم‌عامل و دیگر نرم‌افزارها را تا حد امکان از وب‌سایت رسمی یا توزیع کنندگان معتبر تهیه کنید. در ایران فروشگاه‌های لوازم رایانه‌ای به صورت گسترده نرم‌افزارهای قفل‌شکسته عرضه می‌کنند. این نرم‌افزارها غالبا آلوده به انواع بدافزارهایی‌اند که برخی از آن‌ها برای جاسوسی از رایانه‌ها طراحی شده‌اند. روش‌های پاک کردن نرم افزار از ویروس در درس‌های پیش‌رو توضیح داده خواهد شد.

- هنگام استفاده از اینترنت از چه **مرورگری** استفاده می‌کنید؟ فایرفاکس، گوگل کروم، یا مرورگرهای دیگر؟ برخی مرورگرها نسبت به حملات اینترنتی آسیب پذیری بیشتری دارند. هر دو مرورگر فایرفاکس و گوگل کروم از از این نظر امن‌تر از بقیه‌اند. برای مثال، مرورگر کروم راه یک سری حملات به خدمات جی‌میل را سد می‌کند. در نتیجه این مرورگر برای کسانی که از جی‌میل زیاد استفاده می‌کنند مناسب‌تر است. اگر از رایانه‌های موجود در مکان‌های عمومی (مانند کافی‌نت) استفاده می‌کنید و در آن امکان استفاده از گوگل کروم یا فایرفاکس وجود ندارد، تا حد امکان از وبسایت‌های حاوی اطلاعات حساس پرهیز کنید. با این حال، بدون رعایت نکات ایمنی دیگر، مرورگرها به تنهایی قادر به تضمین امنیت شما نیستند.

- آیا از **افزایه‌ها (پلاگین)** در مرورگرتان استفاده می‌کنید؟ برخی افزایه‌ها ممکن است ناقل بدافزار باشند. همیشه سعی کنید افزایه‌ها را از منابع قابل اطمینان، همچون وب‌سایت رسمی‌شان بگیرید.

- آیا در وبسایت‌ها و برنامه‌های مختلف از **گذرواژه‌های متفاوت** استفاده می‌کنید؟ بکارگیری یک گذرواژه برای حساب‌های کاربری متفاوت ممکن است به‌خاطر سپردن‌اش را ساده‌تر کند، اما بسیار خطرناک است. اگر فردی گذرواژه‌تان را به دست

---

[1] **سیستم‌عامل نرم‌افزاری است** که مدیریت منابع رایانه را به عهده گرفته و بستری را فراهم می‌سازد که نرم‌افزار کاربردی اجرا شده و از خدمات آن استفاده کنند. منبع: ویکیپدیا سیستم‌عامل‌های معروف عبارتند از MS Windows، OSX، IOS و Linux.

آورد می‌تواند به دیگر حساب‌های‌تان نیز دسترسی بیابد. درس دو اطلاعات بیشتری درباره ذخیره‌سازی گذرواژه ارائه کرده، راه‌های ساده‌ای را برای تسهیل مدیریت گذرواژه‌ها آموزش می‌دهد.

- آیا **گذرواژه‌های‌تان از ترکیب حروف و اعداد و علائم نوشتاری** ساخته شده‌اند؟ حدس زدن گذرواژه‌ای که شامل ترکیب حروف، اعداد و علائم نوشتاری باشد دشوارتر است. سعی کنید گذرواژه‌هایی یکتا و منحصربفردی بسازید که به سادگی قابل حدس‌زدن نباشند.

- آیا با کمک **رمزگذاری از حریم ارتباطاتی‌تان** محافظت می‌کنید؟ رمزگذاری یکی از بهترین راه‌ها برای محافظت از مکالمات در محیط اینترنت است. در این باره در درس‌های بعد بیشتر توضیح داده خواهد شد.

- آیا برای **دسترسی به ایمیل‌های‌تان** از وب‌سایت استفاده می‌کنید یا از نرم‌افزار ایمیل؟ شبکه‌های اجتماعی چطور؟ آیا دسترسی به آن‌ها نیز با واسطه است؟

- آیا از **ضد بدافزار و فایروال (دیوار آتش)** استفاده می‌کنید؟ و آیا این نرم‌افزارها به روز هستند؟بسیار مهم است که از آخرین ترتیبات امنیتی برای حساب‌های کاربری و ابزارهای واسطه‌ای که استفاده کنید. به این موضوع بیشتر خواهیم پرداخت.

- آیا از **VPN، فیلترشکن** یا دیگر انواع ابزارها برای دور زدن فیلترینگ استفاده می‌کنید؟ از کجا آن‌ها را به دست آورده‌اید؟ فیلترشکن‌ها و VPN ها خود می‌توانند عامل توزیع بدافزار باشند. شما می‌بایست از اعتبار منبع تأمین کننده فیلترشکن‌ها آگاه باشید. به خاطر داشته باشید که تنها وب‌سایت رسمی تولیدکنندگان چنین ابزارهایی قابل اطمینان است.

- آیا **دیگران** نیز از رایانه‌تان استفاده کنند؟ اگر پاسخ مثبت است، این افراد چه کسانی هستند؟ آیا به حساب‌های کاربری‌تان نیز دسترسی دارند؟ برای حفظ امنیت خود و آنان، می‌بایست از محرمانه بودن اطلاعات دسترسی به حساب‌های کاربری اطمینان حاصل کنید. این موضوع به‌خصوص وقتی اهمیت پیدا می‌کند که افراد مختلفی از یک رایانه استفاده کنند.

اقدامات عملی

حال که حوزه‌های خطر را شناسائی کردید وقت آن رسیده تا فهرستی از اقدامات عملی تهیه کنید که به کمک آن بتوانید از خود و فعالیت‌های‌تان حفاظت کنید.

(برپایه پاسخ‌هایی که به پرسش‌های ارائه شده فراهم کردید گام‌های مرتبط را از فهرست زیر انتخاب کنید. ممکن است همه این‌ها به کار شما نیاید، پس سعی کنید گزینه‌هایی را انتخاب کنید که به نظرتان مناسب می‌آید.)
تا این‌جا که این آموزش را تکمیل کرده‌ام:

- ✓ میزان امنیت و قابل اطمینان بودن شبکه‌هایی که از آن استفاده می کنم را بررسی کرده‌ام.
- ✓ به منظور افزایش سطح امنیت، گذرواژه‌ها را تغییر داده‌ام.
- ✓ سیستم‌عامل رایانه‌ام را به نوع رسمی و گواهینامه‌دار تغییر داده‌ام.
- ✓ دسترسی افراد به رایانه و حساب‌های کاربری‌ام را محدود ساخته‌ام.
- ✓ مطمئن هستم همه برنامه‌های واسطه‌ای که برای دریافت ایمیل، چت، و دیگر ارتباطات اینترنتی از آن استفاده می‌کنم قابل اعتماد و به روزشده هستند.
- ✓ مطمئن هستم فیلترشکنی که از آن استفاده می‌کنم از منبعی قابل اعتماد دریافت شده، یا درحال جستجو برای یافتن یک فیلترشکن جایگزین هستم.
- ✓ از مرورگر اینترنت ایمن‌تری استفاده می‌کنم.
- ✓ همه افزایه‌ها (پلاگین‌ها)ی نصب‌شده روی مرورگرم را غیرفعال ساخته‌ام.
- ✓ ضدبدافزار و فایروال مناسب نصب کرده و آن‌ها را به روز نگه دارید.

مطالعه بیشتر:
اصول اولیه امنیت دیجیتال - بالاویزیون (فارسی)

نبض‌ایران
تقویت صدای ایرانیان

درس دو: ایمن‌سازی رایانه

فهرست عنواین

مقدمه

به درس دو از مجموعه امنیت در فضای مجازی از نبض‌ایران خوش آمدید. در درس پیشین، به برخی تهدیدها پرداختیم که کاربران اینترنت همه روزه با آن مواجه هستند. همچنین به تاثیراتی اشاره شد که این تهدیدات ممکن است بر امنیت و کار افراد داشته باشد.

حال وقت آن است تا کمی بیشتر درباره روش‌های محافظت از داده و اطلاعات صحبت کنیم. امنیت مناسب در فضای دیجیتال شیوه‌های مختلفی را در بر می‌گیرد. این درس به‌طور عمده به محافظت در برابر حملات خارجی از طریق ایمن‌سازی رایانه یا "دشوارسازی" دسترسی به اطلاعات، اختصاص داده شده است.

اغلب مباحث این درس از سایت Security in a Box گرفته شده که به زبان فارسی نیز منتشر می‌شود. ما مطالعه مطالب این سایت را به شما توصیه می‌کنیم، اما توجه داشته باشید که بخش فارسی این وب‌سایت گاه به اندازه بخش انگلیسی آن به روز نیست.

رایانه و دیگر ابزارهای دیجیتالی که از آن استفاده می‌کنید، همچون پلی می‌مانند به جهان اطلاعات، اما هم‌زمان می‌توانند دروازه‌ای باشند به دنیای تهدیدهای اینترنتی. به همین دلیل، بسیار مهم است تا از ابزارهای‌تان در برابر حملات مختلف محافظت کنید. ممکن است شما نتوانید همه ابزارها و روش های لازم را به درستی فرا بگیرید یا حتی استفاده از روش‌های تازه به دلیل قدیمی بودن رایانه‌تان امکان‌پذیر نباشد. با این حال، وقت و تلاشی که صرف می‌کنید تا بر دانش‌تان در زمینه روش‌های حفاظت در برابر تهدید نفوذگران در دنیای مجازی بیافزائید، ارزش‌اش را دارد. آگاهی از این موارد موجب می‌شود تا به صورت ناخودآگاه به سطحی از هشیاری دست یابید و شاید در آینده گام‌های مناسب‌تری برای بهبود امنیت خود بردارید.

در پایان این درس، از شما سؤالاتی پرسیده خواهد شد درباره آنچه از رایانه خود می‌دانید. تا آن هنگام، شما خواهید آموخت که چگونه از خود در فضای مجازی محافظت کنید. همچنین با پیروی از توصیه‌های ارائه شده امنیت رایانه‌ای که هم اکنون مشغول کار با آن هستید نیز بهبود خواهد یافت.

سیستم‌عامل

در سال‌های اخیر تنوع وسائل رایانه‌ای (تلفن‌های هوشمند، تبلت‌ها و لپ‌تاپ) موجب شده انواع سیستم‌عامل و نرم‌افزارهای مرتبط با آن نیز گوناگونی بیشتری پیدا کند. متاسفانه در ایران به دلیل تحریم‌های بین‌المللی و محدودیت‌های داخلی، بازار نرم‌افزارهای قفل‌شکسته داغ‌تر از همیشه است و این خود یکی از مهم‌ترین مشکلات امنیتی برای کاربران ایرانی به شمار می‌رود. سازمان‌های اطلاعاتی، شرکت‌ها و افراد سودجو خیل عظیم نرم‌افزارهای قفل‌شکسته را بهترین راه برای نفوذ به رایانه و تلفن هوشمند کاربران می‌یابند زیرا: ۱. وقتی قفل یک نرم‌افزار شکسته شد همه جور برنامه جانبی را نیز می‌توان به درون آن تزریق کرد، بدون آن‌که ردپائی به جای گذاشته شود. ۲. معمولاً شرکت‌های تولیدکننده نرم‌افزار از نسخه‌های قفل‌شکسته حمایت نمی‌کنند و نسبت به امنیت کاربران آنان تعهدی ندارند.

اردیبهشت سال ۹۴ خبر رسید که شرکت‌های همراه اول و ایرانسل بدون اجازه مشترکان تلفن، روی تلفن‌های هوشند آنان نرم‌افزاری را نصب می‌کنند که امکان استراق صمع مکالمات و پیامک‌های آنان را فراهم کرده، صدا و تصویر محیط را بدون اجازه مشترکان به شرکت مخابرات ارسال می‌کند. این بدافزار حتی مکان مشترک تلفن همراه را نیز به مرکز گزارش می‌دهد. بیشتر بخوانید: سرقت اطلاعات مشترکان توسط اپراتورهای تلفن همراه در ایران

سیستم‌عامل چیست؟

سیستم‌عامل در هر رایانه یا وسیله هوشمند، نرم‌افزاری پایه‌ای است که «مدیریت منابع رایانه را به عهده گرفته و بستری را فراهم می‌سازد که نرم‌افزار کاربردی اجرا شده و از خدمات آن استفاده کنند[2].» ویندوز، گنو لینوکس و OSX از سیستم‌عامل‌های مشهور و شناخته شده برای رایانه‌ها به شمار می‌روند.

سیستم‌عامل مناسب کدام است؟

به‌طور کلی می‌توان سیستم‌عامل‌ها را به دو دسته تقسیم کرد. سیستم‌عامل دستگاه‌های هوشمند مانند تلفن همراه هوشمند یا تبلت و سیستم‌عامل رایانه‌ها.

[2] منبع ویکیپدیا: سیستم‌عامل

سیستم‌عامل رایانه

به‌طور سنتی در ایران از سیستم‌عامل‌های ویندوز استفاده می‌شده، هرچند در سال‌های اخیر کاربران ایرانی با ورد رایانه‌های شرکت اپل از سیستم‌عامل‌های مک نیز بیشتر استفاده می‌کنند. متأسفانه همان‌طور که پیشتر اشاره شد، تقریبا تمام این سیستم‌عامل‌ها در ایران به صورت قفل شکسته در اختیار کاربران قرار می‌گیرند (بجز مواردی که به صورت نصب شده توسط لپ‌تاپ‌ها ارائه می‌شود). در مواردی که سیستم‌عامل قفل شکسته نباشد، ممکن است شرکت سازنده به دلیل تحریم‌های بین‌المللی از ثبت‌نام کاربر ایرانی جلوگیری کند.
عدم ثبت‌نام سیستم‌عامل موجب می‌شود که کاربر از دریافت به‌هنگام‌سازی‌های امنیتی محروم شود.

از سوی دیگر و با رشد فناوری‌های کد-باز که جنبه تجاری کمتری دارند، این نرم‌افزارها روز به روز پیشرفته‌تر و امن‌تر شده، رابط کاربری کاربرپسندتر و ساده‌تری ارائه می‌کنند. از آن نمونه می‌توان به سیستم‌عامل گنو لینوکس اشاره کرد. این سیستم‌عامل به صورت مجانی قابل بارگیری و نصب روی همه انواع رایانه و دستگاه‌های هوشمند است.

خبر خوش این‌که نسخه‌های کد-باز معمولا زبان فارسی را به خوبی و گاه بهتر از سیستم‌عامل‌های تجاری پشتیبانی می‌کنند.

سیستم‌عامل دستگاه‌های هوشمند

دستگاه‌های هوشمند ارائه شده در ایران معمولا از سه سیستم‌عامل مختلف بهره می‌گیرند، IOS برای محصولات شرکت اپل، ویندوز و Andriod. همچون رایانه‌ها، شرایط تحریمی برای دستگاه‌های هوشمند نیز کاربران و فروشندگان ایرانی را به دنبال نرم‌افزارهای قفل‌شکسته فرستاده. در این میان، شرکت گوگل، تولیدکننده سیستم‌عامل Android تحریم کاربران ایران را برای برنامه‌های مجانی ارائه شده در فروشگاه آنلاین گوگل برداشته.
برخی دستگاه‌های هوشمند نیز از سیستم‌عامل‌های متن-باز همچون اوبونتو فون استفاده می‌کنند.

توصیه ما این است که حتی‌الامکان سیستم‌عامل‌ها ونرم‌افزارها را خودتان از وب‌سایت تولیدکنندگان آن تهیه و روی رایانه یا دستگاه هوشمندتان نصب کنید.

از آن‌جا که سیستم‌عامل‌های Android و Ubuntu Phone به‌صورت مجانی برای کاربران ایرانی قابل دسترس است و برنامه‌های آن را نیز می‌توان به صورت مجانی بارگیری کرد، استفاده از این سیستم‌عامل‌ها را به کاربران ایرانی توصیه می‌کنیم.

به خاطر داشته باشید

بدافزارهای نصب‌شده روی سیستم‌عامل‌های قفل‌شکسته را شاید حتی نتوان با بهترین ضدویروس‌های موجود شناسائی و خنثی کرد. به‌خصوص اگر سیستم‌عامل به هنگام‌سازی نشود.

تمرین امنیت دیجیتال: چگونه تهدیدهای امنیتی را شناسایی کنیم؟

همه وسایلی که برای دسترسی به اینترنت به کار برده می‌شوند در برابر حمله آسیب پذیرند. در ادامه این درس با ابزارهای مختلفی آشنا خواهید شد که برای مقابله با حملات اینترنتی به کار می‌آیند، اما دست آخر، تنها یک ابزار است که در برابر ویروس ها، جاسوس‌افزارها و دیگر حملات دنیای مجازی می‌تواند از شما دفاع کند: **آن ابزار خود شما هستید.**

آیا ضدویروس‌ها مفید هستند؟ البته، هرچند، این برنامه‌ها به دور از خطا هم عمل نمی‌کنند. به عنوان کسی که روزانه با رایانه، تلفن همراه یا تبلت‌تان کار می‌کنید، شما بهتر از همه از عملکرد آنها آگاهی دارید. شما می‌بایست به هر تغییری که در عمل‌کرد این دستگاه‌ها مشاهده می‌کنید توجه نشان دهید؛ بخصوص رفتارهای غیرعادی، مثل کند شدن برنامه‌ها یا وجود سایت‌ها و یا برنامه‌های جدیدی که از وجودشان خبر نداشته‌اید. توجه به این موارد ممکن است مسائلی را برملا کند که برنامه‌های ایمنی قادر به یافتن‌شان نباشند. چگونه می‌توانید مهارت‌های‌تان در کشف تهدیدات را تقویت کنید؟ به بیانی دیگر، چطور می‌توان تشخیص داد که هدف کدام یک از حملاتی قرار گرفته‌اید که در درس یک به آن پرداختیم؟

بیایید بیشتر در این‌باره صحبت کنیم.

تهدیدهای ناشی از اینترنت

برنامه‌های مخرب می‌توانند از راه ایمیل یا صفحه‌های وب به رایانه‌تان نفوذ کنند. ایمیل هم خود ممکن است عامل انتقال ویروس و دیگر بدافزارها باشد و هم نفوذگران از آن برای فریب‌دادن‌تان استفاده کنند تا هویت‌تان را کشف کرده یا اطلاعات‌تان را بربایند. به همین دلیل، بگذارید کمی درباره روش‌های شناسائی ایمیل‌های خطرناک صحبت کنیم. پس از آن به شیوه‌های امن کار با ایمیل خواهیم پرداخت.

احتمالا، از درس یک به یاد دارید که ایمیل فیشینگ خود را به جای یک منبع قابل اعتماد جا زده تا اطلاعات حساسی را از شما به سرقت ببرد یا برنامه مخربی را روی رایانه‌تان نصب کند. موارد زیر روش‌هایی را توضیح می‌دهد که به کمک آن می‌توان به جعلی بودن یک ایمیل پی برد:

- **به نظر می‌رسد که ایمیل از موسسه یا شرکتی آمده که شما از قبل با آن آشنا هستید یا به آن اعتماد دارید،** مثلا بانک، نهاد دولتی، یا سایت شبکه‌های اجتماعی.
- **غالبا، پیام چنین ایمیل‌هایی عمومی است و شخص شما را مخاطب قرار نمی‌دهد.** چنین ایمیلی ممکن است به جای نام یا نام خانوادگی‌تان، با «مشتری گرامی»، «دوست عزیز» یا «سلام» آغاز شود. دلیل آن این است که برخلاف نهادها و اشخاص قابل اعتماد، فرستندگان چنین ایمیل‌هایی احتمالا اسم شما را نمی‌دانند. به‌طور کلی، به ایمیلی که با نام شما آغاز نشده یا در متن آن به‌طور مشخص نام شما ذکر نشده شک کنید.
- حتی اگر ایمیلی از لوگوی یک شرکت معتبر یا امضای افراد مورد اعتماد استفاده کرده باشد، **متن ایمیل را به دقت مطالعه کنید و ببینید آیا به طور واضح نوشته شده** و قابل اعتماد است؟
- ممکن است از شما خواسته شود تا **اطلاعات حساب کاربری‌تان** را با پاسخ دادن به آن ایمیل ارسال کرده یا مثلاً، نام خانوادگی، گذرواژه یا دیگر اطلاعات شخصی‌تان را از طریق لینک ارائه شده در ایمیل تأیید نمایید. به عنوان نمونه به متن زیر توجه کنید: «ما فکر می‌کنیم بدون اجازه شما از حساب کاربری‌تان استفاده می‌شود. برای اطمینان از این‌که حساب‌تان مورد رخنه قرار نگرفته، لطفاً روی لینک زیر کلیک کنید تا هویت‌تان تأیید شود.»
- پیام ارسال شده **حاکی از امر فوری** باشد. مانند: «اگر ظرف ۴۸ ساعت به این ایمیل پاسخ ندهید حساب کاربری‌تان پاک خواهد شد.»

در ضمن، توجه داشته باشید که امروزه بسیاری از شرکت‌های اینترنتی بین‌المللی مانند گوگل، فیس‌بوک و تویتر، برای ارتباط با کاربران ایرانی‌شان از زبان فارسی استفاده می‌کنند. این موضوع، کار نفوذگران را برای جعل ایمیل‌های شبه واقعی ساده‌تر کرده.

حمله فیشینگ ممکن است از راه‌هایی غیر از ارسال ایمیل انجام شود. یک روش مرسوم ظاهر شدن پنجره‌ای در صفحه مرورگر وب است. این نوع حمله نیز مانند ایمیل‌های جعلی با هدف کسب اطلاعات از شما انجام می‌شود؛ بدین منظور، این پنجره‌ها به شکل وبسایت‌هایی که شما می شناسید طراحی می‌شوند.

برخی نشانه‌ها برای تشخیص حملات فیشینگ از طریق وبسایت‌ها یا پنجره‌های بازشونده از این قرارند:

- ✓ ممکن است از نظر محتوا یا شکل ظاهری با برنامه یا وبسایتی که می‌خواهد از آن تقلید کند تفاوت داشته باشد. مانند ایمیل فیشینگ، پنجره فیشینگ نیز می‌تواند شبیه به سرویس وب یا سازمانی طراحی شده باشد که شما آن را می‌شناسید. گاه تفاوت‌های جزئی در نوع قلم یا شکل ظاهری قابل تشخیص است، یا ممکن است از شما چیزی بخواهد که با آن‌چه سرویس وب مورد اعتمادتان به‌طور معمول مطالبه می‌کند فرق داشته باشد. (به مثال. ۱ توجه کنید.)
- ✓ ممکن است که همچون همتای ایمیلی‌اش، پیام این پنجره‌ها نیز حاوی نوعی فوریت باشد.
- ✓ ممکن است از شما اطلاعات شخصی بخواهد.
- ✓ ممکن است به شکل پیامی از نیروی انتظامی، یا دیگر نهادهای رسمی کشوری طراحی شده باشد.

راه‌های مقابله با این نوع تهدید

امروزه، برخی نهادها با همکاری دیگر کاربران و روش‌های جمع‌سپاری فعالیت کنونی و سوابق وب‌سایت‌های مختلف را مورد پایش قرار می‌دهند. این سرویس‌ها به شما امکان می‌دهند تا وب‌سایت مورد نظرتان را از نظر آلوده بودن به بدافزار یا تلاش برای حمله فیشینگ بررسی کنید.

- وب‌سایت **Phishtank** یک نمونه از این سرویس‌ها است. Phishtank با کمک روش‌های جمع‌سپاری وب‌سایت مورد نظر شما را بررسی می‌کند. پس از ثبت یک وب‌سایت در Phishtank دیگر کاربران شروع به رأی دادن می‌کنند که آیا این سایت حاوی حمله فیشینگ است یا خیر. گاه نیز وب‌سایت مورد نظرتان پیشتر اضافه شده و شما می‌توانید وضعیت آن را ملاحظه کنید.
- ضدویروس نورتن امکانی دارد تحت نام Safeweb. این ابزار هم به عنوان بخشی از نرم‌افزار نورتن قابل نصب است و هم می‌توان از طریق **وب‌سایت** از آن استفاده کرد. اگر از نسخه نصب‌شده آن استفاده می‌کنید، این ابزار به‌طور خودکار دسترسی شما را به وب‌سایت‌های آلوده قطع می‌کند. نسخه وب آن با جستجو در بانک اطلاعات نورتن وضعیت امنیتی وب‌سایت مورد نظرتان را مشخص می‌کند.
- **URL Void** سرویس دیگری است که سوابق امنیتی وب‌سایت‌ها را ارائه می‌کند. اگر وب‌سایتی پیشتر به بدافزار آلوده بوده یا از طریق آن حمله فیشینگی صورت گرفته باشد، از طریق این سرویس می‌توان آن را ردیابی کرد.
- **Google Chrome, Google account password alert**. این افزایه ساخت شرکت گوگل است و تنها روی مرورگر گوگل کروم کار می‌کند. اگر صفحه‌ای غیر از صفحه ورود به حساب کاربری شرکت گوگل اطلاعات حساب کاربری گوگل و جی‌میل شما را درخواست کند، این افزایه به شما اخطار امنیتی می‌دهد. از این راه، احتمال حمله فیشینگ علیه حساب کاربری گوگل بسیار کاهش خواهد یافت.

اگر فکر می‌کنید که به سایتی زده‌اید یا ایمیلی دریافت کرده‌اید که در واقع یک حمله فیشینگ بوده، برای محافظت از خود و اطلاعات تان باید به سرعت اقدامات احتیاطی خاصی رادر پیش بگیرید:

- پیش از هر چیز، تمام رایانه‌تان را با ضد ویروس و ضدجاسوس‌افزار اسکن کنید.
- سپس گذرواژه حساب کاربری‌تان را عوض کنید.

اگر هنوز مطمئن نیستید که سیستم‌های‌تان از تهدید رها شده‌اند، و به خدمات اورژانس دیجیتالی نیاز دارید، بهتر است یک سری به **بسته کمک‌های اولیه دیجیتالی** بزنید.

راه‌های پیشگیری

- پیش از هر چیز، به ایمیل‌های مشکوک **پاسخ ندهید**. پاسخ دادن به این ایمیل‌ها خطرناک است.
- هیچ‌گاه پرونده‌های ضمیمه ایمیل‌های مشکوک را باز یا **دانلود نکنید**.
- روی لینک‌های موجود در در ایمیل‌های مشکوک **کلیک نکنید**.

به عنوان یک قاعده کلی، حتی‌الامکان روی هیچ لینکی که در ایمیل وجود دارد کلیک نکنید. یک راه خوب آن است که روی لینک موجود (در ایمیل‌هایی که از صحت آن اطمینان دارید)، کلیک راست کرده، نشانی آن را کپی و در صفحه جدیدی در مرورگرتان باز کنید. لینک‌های مشکوک معمولا شما را به نشانی‌هایی غیر از وب‌سایت مورد نظرتان راهنمایی می‌کنند که از این طریق قابل کشف است. اگر نشانی کپی شده با آن‌چه در ایمیل نمایش داده شده فرق داشته باشد، این یک حمله فیشینگ است.

- تحت هیچ شرایطی، **اطلاعات حساس**، همچون گذرواژه، اطلاعات کارد اعتباری، یا اطلاعات شخصی مهم را از طریق ایمیل ارسال نکنید. شرکت‌های معتبر مانند گوگل، یاهو، فیس‌بوک، تویتر و غیره، هیچ‌گاه چنین چیزی از شما نخواهند خواست. هر نوع درخواست اینچنینی حتما یک حمله فیشینگ است.
- به **پنجره‌های جهنده در مرورگر** که به شکل خودکار ظاهر می‌شوند توجه کنید. به‌جای کلیک بر گزینه‌های "بله" یا "اوکی" آنها را با دقت بخوانید. اگر تردید دارید، می‌بایست این پنجره‌ها را با کلیک بر «X» در گوشه سمت راست بالای پنجره ببندید، نه از طریق انتخاب گزینه "Cancel" که ممکن است درون فرم باشد. گاه نیز با قراردادن ماوس بر روی گزینه "کنسل" می‌توانید ببینید که لینک پنهان شده در زیر آن، شما را به کجا هدایت می‌کند - اما روی آن کلیک نکنید. گاه نفوذگران لینک‌های موردنظرشان را در بخش‌هایی از یک پنجره مخفی می‌کنند. این عمل، تشخیص حمله را مشکل‌تر می‌سازد. به این دلیل، تا حد امکان از تعامل با پنجره‌های بازشونده خودداری کرده، هرچه زودتر آن‌ها را ببندید.

بیشتر مرورگرها امکان Pop-up blocker را در بخش تنظیمات ارائه می‌کنند. این امکان جلوی باز شدن خود به خودی پنجره‌های جهنده را می‌گیرد. حتما آن را فعال نگه دارید.

- مرورگرهای گوگل کروم، فایرفاکس و اوپرا امکان **مسدودسازی javaScript** را فراهم می‌کنند. حتما آن را فعال کنید. این روش امکان ورود بدافزار از طریق حمله‌های فیشینگ را نیز سد تا حد بسیاری کاهش خواهد داد.
- هنگام **بازکردن پرونده‌های ضمیمه ایمیل** بسیار محتاط باشید.

کاربران جی‌میل (و برخی دیگر از خدمات ایمیل) می‌توانند به جای دانلود پرونده‌های ضمیمه از گزینه "View" استفاده کنند. این گزینه به آنان امکان می‌دهد درون پرونده را از چشم مرورگر ببینند. بدین وسیله از اجرا شدن بد افزار احتمالی در رایانه جلوگیری می‌شود. پس از مشاهده درون پرونده، در صورتی که محتوای آن، همان باشد که انتظار داشته‌اید می‌توانید آن را دانلود کرده از آن استفاده کنید. جی‌میل همچنین این امکان را به کاربران می‌دهد که برخی پرونده‌ها را در Google Drive ذخیره کرده، بدون دانلود کردن و به صورت آنلاین از آن استفاده کنند. در این مورد بیشتر توضیح خواهیم داد.

به خاطر داشته باشید

حتی ایمیل دریافتی از افرادی که به آنها اعتماد دارید می‌تواند ناقل ویروس باشد؛ پرونده‌های ارسالی از رایانه‌های آلوده به احتمال زیاد خود آلوده هستند. به‌طور کلی، از بازکردن پرونده ضمیمه ایمیل از منابع ناشناس خودداری کنید. اگرمی‌بایست پرونده ضمیمه را باز کنید، توصیه ما این است که ابتدا آن را بر روی رایانه‌تان ذخیره کرده، پس از اسکن با برنامه ضدویروس از آن پرونده استفاده کنید.

یواس‌بی، سی دی، و دیگر ابزار خارجی

یواس‌بی فلش درایو، سی دی، و دیگر ابزارهای خارجی حمل و نقل داده و اطلاعات همگی می‌توانند ناقل بدافزار باشند؛ به‌ویژه اگر منبع تهیه آن‌ها نامطمئن باشد.

در ایران، معمولاً نرم‌افزارهای مختلف (قفل شکسته یا نرم‌افزارهایی که از اینترنت دانلود شده‌اند) به صورت گسترده از این طریق تبادل می‌شوند. توصیه ما این است که نرم‌افزارهای مورد نیازتان را خود از وب‌سایت‌های مرجع دانلود کرده، تا حد امکان از نرم‌افزارهای کد-باز (Open source) استفاده کنید که نیازی به شکستن قفل آن نباشد. در این زمینه بیشتر توضیح داده خواهد شد.

برای مقابله با انتقال ویروس و بدافزار از طریق ابزارهای خارجی انتقال اطلاعات، راه‌کارهای حفاظتی چندی موجود است. اقدامات لازم در این زمینه، به فراخور نوع رایانه متفاوت خواهد بود. در این‌جا اقدامات لازم جهت محافظت از سیستم‌های ویندوز و مک توضیح داده می‌شود.

ویندوز

اگر یک ابزار ذخیره خارجی حامل پرونده مانند سی‌دی، دی‌وی‌دی یا یواس‌بی‌درایو را به رایانه‌تان متصل کنید، بیشتر سیستم‌های ویندوز ممکن است به‌طور خودکار پرونده اجرائی اصلی موجود در آن را باز کند. مشکل هنگامی پیش می‌آید که آن پرونده آلوده به بدافزار باشد. برای این‌کار می‌بایست گزینه AutoPlay یا AutoRun را در ویندوز غیرفعال کنید. روش انجام این کار بسته به نسخه ویندوز متفاوت است. اگر از ویندوز ۲۰۰۰ یا XP[3] استفاده می‌کنید، توصیه می‌کنیم راه‌نمای شرکت مایکروسافت برای غیرفعال کردن این گزینه را **اینجا** بخوانید. برای نسخه‌های ویندوز ویستا و ۷ **اینجا** را مطالعه کنید.

[3] به یاد داشته باشید که شرکت مایکروسافت پشتیبانی از ویندوز XP را متوقف کرده. این بدان معنی است که دیگر ایرادات امنیتی این نسخه از ویندوز به طور مجانی برطرف نخواهد شد. ما توصیه می‌کنیم که اگر هنوز از این نسخه از ویندوز استفاده می‌کنید، هرچه زودتر آن را به نسخه بالاتری که به صورت قانونی از شرکت مایکروسافت خریداری شده ارتقاء داده، یا آن را با سیستم‌عامل مجانی و کد-باز گنو لینوکس جایگزین کنید.

سیستم های Mac

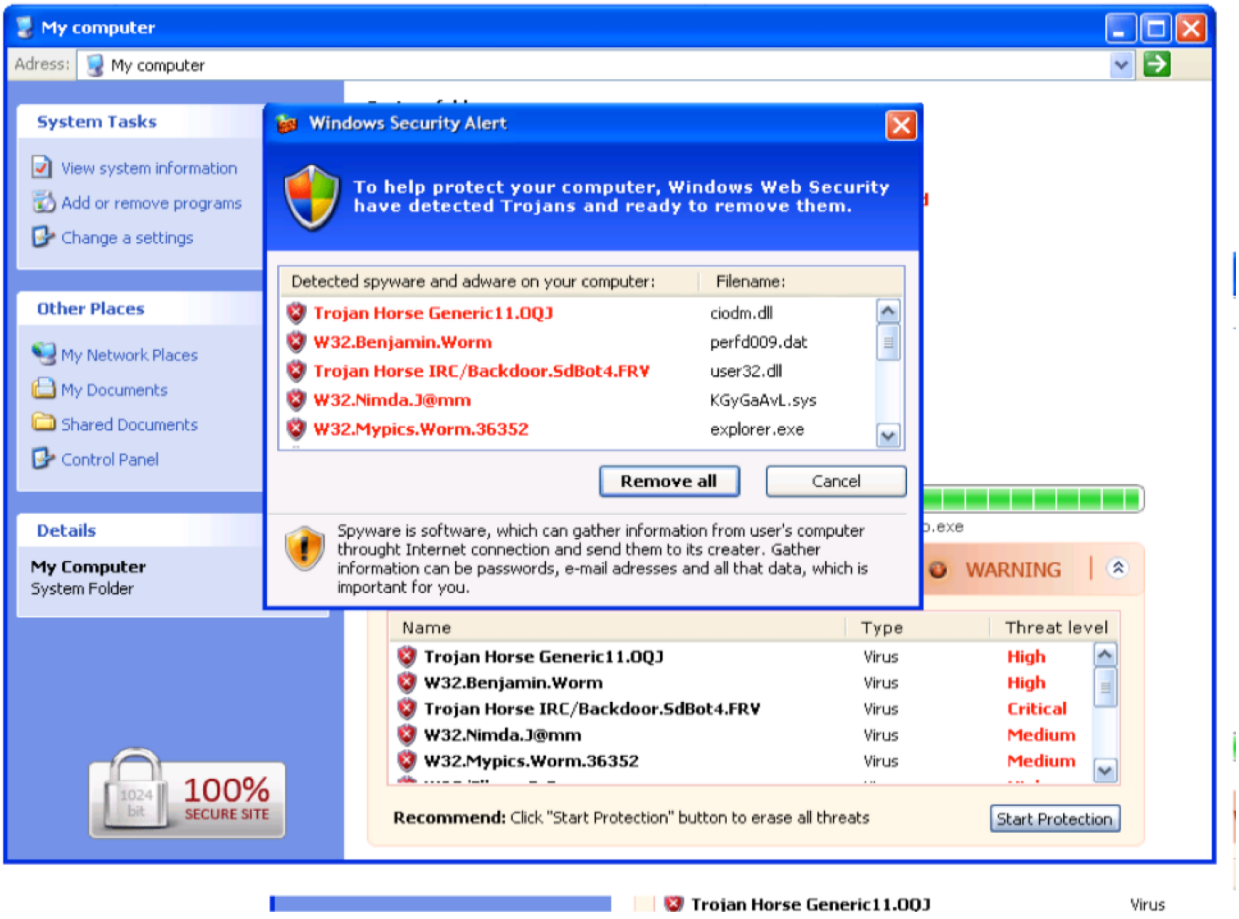
خوشبختانه رایانه‌های مک گزینه اجرای خودکار یواس‌بی را ندارند. با این‌حال بدافزارها همچنان می‌توانند از طریق سی‌دی یا دی‌وی‌دی به این رایانه‌ها وارد شوند. به این شکل از خود حفاظت کنید:

گزینه Autoplay را روی درایو (CD/DVD) غیر فعال کنید. برای انجام این کار به بخش ، به System Preferences رفته و بر "CDs & DVDs" کلیک کنید. پنجره باز شده به شما امکان می‌دهد واکنش سیستم هنگام ورود سی‌دی یا دی‌وی‌دی به رایانه را انتخاب کنید. شما می‌توانید به تفکیک یکی از دو گزینه "Ignore" یا "Ask me what to do" را برای سی‌دی و دی‌وی‌دی انتخاب کنید.

در هر دو حالت استفاده از سیستم‌های مک یا ویندوز توصیه می‌کنیم پیش از استفاده از ابزارهای ذخیره خارجی، حتما آن‌ها را با نرم‌افزار ضدویروس اسکن کنید.

مثال ۱:

این نمونه‌ای از یک پنجره مشکوک است. چطور می‌توان تشخیص داد که این هشدار واقعی نیست؟ خوب، نخست اینکه چندین هشدار ترسناک به‌طور هم‌زمان ظاهر شده و همزمان از شما می‌خواهد با یک کلیک مجوز کارهای مختلفی را صادر کنید. بهتر آن است که این پنجره را ببندید ورایانه‌تان را با برنامه ضدویروس اسکن کنید.

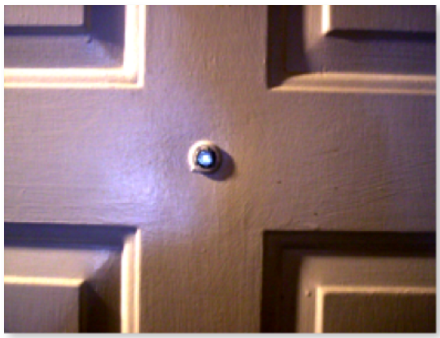


حفاظت از خود در برابر بدافزارها و هکرها

بحث محافظت از خود در فضای مجازی بسیار گسترده است. خوشبختانه در این زمینه ابزارها و راهکارهای متنوعی نیز در دست است که به ما برای دفاع از خود کمک می‌کنند.

رایانه را می‌توان مانند بنایی تصور کرد که اطلاعات در آن ذخیره می‌شود. همچون یک ساختمان، رایانه نیزاز طرق مختلف نفوذپذیر است. در این بخش، به ابزارها و روش‌هایی می‌پردازیم که برای حفاظت از رایانه در برابر نفوذگران به دردتان می‌خورد. سپس راه‌های استفاده از آن را در عمل بررسی خواهیم کرد.

نرم‌افزارهای ضدویروس و ضدجاسوس‌افزار: دو وسیله مفید برای نظارت بر وضعیت امنیتی رایانه



ویروس‌ها و به زبان کلی‌تر همه بدافزارها مدام برای رایانه شما مزاحمت ایجاد می‌کنند. از آن‌جا که شیوه عمل بدافزارها با یکدیگر متفاوت است، برای خنثی سازی آن‌ها پیش از آن‌که به رایانه‌تان آسیب رسانده باشند به ابزارهای گوناگونی نیاز دارید. استفاده درست از این ابزارها به شما کمک می‌کند تا اکثر تهدیدات را پیش از به اجرا در آمدن متوقف سازید.

ضدویروس

ضدویروس همان‌طور که از اسمش پیداست به‌طور مشخص برای مقابله با انواع ویروس و کرم رایانه‌ای طراحی شده. این نوع برنامه رایانه را برای یافتن کدهای مخرب پایش می‌کند. از آن‌جا که همه روزه ویروس‌های تازه‌ای به عرصه می‌آیند، ضدویروس‌ها نیز می‌بایست به طور مداوم به روز رسانی شوند.

توجه داشته باشید که نرم‌افزارهای ضدویروس بسته به شرایط و تنظیمات انجام شده، اقدامات مختلفی انجام می‌دهند. اگر بدافزاری در رایانه‌تان پیدا شد ضدویروس آن را قرنطینه کرده یا کد آلوده را پاک می‌کند. اما اگر بد افزار در یک منبع خارجی متصل به رایانه (مانند یواس‌بی یا دی‌وی‌دی) پیدا شود، از آن‌جا که به احتمال زیاد ضدویروس قادر به تغییر محتوای آن نیست، کار زیادی از او ساخته نیست. در این حالت، بهترین گزینه خارج کردن یا قطع اتصال منبع خارجی از رایانه است.

به خاطر داشته باشید

تحت هیچ شرایطی از ضدویروس‌های قفل شکسته استفاده نکنید. همیشه ضدویروس‌تان را ثبت کنید تا به‌طور مداوم به روز رسانی شود.

تنظیمات سیستم‌تان را با موارد زیر محک بزنید:

- **دو برنامه ضدویروس را به‌طور هم‌زمان نصب یا اجرا نکنید**. چنین کاری موجب ارتقاع امنیت رایانه نشده، ممکن است سرعت رایانه‌تان را به شدت پایین آورده یا آن را قفل کند. قبل از نصب ضدویروس جدید، ضدویروس قدیمی را به‌طور کامل پاک کنید.
- **حتما ضدویروس را همیشه به روز نگه دارید**. این کار شما را در برابر آخرین ویروس‌ها ایمن نگاه می‌دارد. بیشتر نرم‌افزارها برای به روز شدن باید پس از نصب روی رایانه در وب‌سایت تولیدکننده آن ثبت شوند؛ این امر شامل نرم‌افزارهای کد-باز که مجانی در دسترس هستند نیز می‌شود. همه نرم‌افزارهای پیشنهاد شده در این دوره به‌طور مجانی ثبت و به روز رسانی می‌شوند. ضدویروس‌ها به‌طور معمول، هنگام اتصال به اینترنت توسط یک پنجره جهنده به شما یادآوری می‌کنند که زمان به‌روزرسانی فرارسیده.

توجه: پیشتر در این درس گفتیم نسبت به پنجره‌های فیشینگ که به‌طور ناگهانی ظاهر می‌شوند هشیار باشید. اگر به پیامی که می‌گوید وقت به روز رسانی ضدویروس فرارسیده شک دارید، بهتر آن است که با رجوع به وب‌سایت مربوطه چک کنید آیا واقعا زمان به روز رسانی است یا نه. همچنین می‌توانید پرونده‌های به روز رسانی نرم‌افزار را خودتان از وب‌سایت ضدویروس بارگیری و نصب کنید.

- **اگر ضدویروس‌تان دارای گزینه «Always On» است، آن را فعال کنید**. نرم‌افزارهای متفاوت ممکن است از نام‌های مختلفی برای این گزینه استفاده کنند، اما اغلب چنین گزینه ای را ارائه می‌دهند. برخی نام‌های دیگر برای این گزینه: «Real Resident Protection»، «Time Protection».
- **رایانه‌تان را به‌طور منظم اسکن کنید**. نیازی نیست که این کار را هر روز انجام دهید (به ویژه اگر برنامه ضدویروس شما همان‌طور که در بالا گفته شد دارای گزینه «همیشه روشن» باشد.) اما هرچند وقت یک‌بار می‌بایست این کار را انجام دهید. زمان‌بندی اسکن‌ها به شرایط کاری بستگی دارد. اگر به تازگی رایانه‌تان را به شبکه‌های بی‌سیم عمومی (Public Wifi) یا دیگر شبکه‌های نامطمئن وصل کرده‌اید؛ از حافظه یواس‌بی برای انتقال پرونده از رایانه دیگران استفاده کرده‌اید؛ یا به تازگی پرونده ضمیمه نامتعارفی که از طریق ایمیل دریافت بودید را باز کرده‌اید؛ یا این‌که رایانه یکی از آشنایان‌تان که با او پرونده رد و بدل می‌کرده‌اید، به تازگی مشکل ویروسی داشته؛ در همه این موارد می‌بایست رایانه‌تان را با ضدویروس اسکن کنید.

ضد جاسوس‌افزار

ضد جاسوس‌افزار (Anti-Spyware) ابزاری است که علیه جاسوس‌افزارها به کار گرفته می‌شود. این ابزار به‌جای تمرکز بر ویروس‌ها، دیگر برنامه‌های خطرناک از جمله برنامه‌های جاسوسی و نظارتی را کشف و خنثی می‌کند. (جهت یادآوری؛ ویروس‌ها ماهیتی تخریبی دارند اما جاسوس‌افزارها ممکن است چیزی را خراب نکنند و تنها به جمع‌آوری اطلاعات بپردازند.) طرز عمل ضدجاسوس‌افزارها با ضدویروس‌ها متفاوت است. یک طرح امنیت دیجیتالی مناسب می‌بایست هردونوع نرم‌افزار را در بر بگیرد. همچون ضدویروس‌ها، ضدجاسوس‌افزارها نیز می‌توانند در کار یکدیگر تداخل ایجاد کنند و نمی‌بایست از بیش از یک ضدجاسوس‌افزار روی رایانه‌تان استفاده کنید. برای دست‌یابی به امنیت بهتر، ضدجاسوس‌افزار نیز می‌بایست همیشه به روزرسانی شود.

وب‌گردی امن: در و پنجره‌ها را محکم ببندید

مرورگر اینترنت همچون دروازه ورود به فضای مجازی عمل می‌کند. همان‌طور که شما از این راه به اینترنت وارد می‌شود، غریبه‌ها نیز می‌توانند از طریق آن به رایانه شما راه یابند. به این خاطر، مرورگر اینترنت هدف دلخواهی برای تهدیدات امنیتی به حساب می‌آید.

انتخاب مرورگر مناسب

توانایی مرورگرها در مقابله با برنامه‌های القوه خطرناک متفاوت است. به همین دلیل، بسیار اهمیت دارد که از قوی‌ترین مرورگر موجود استفاده کنید؛ ابزاری که بهتر از دیگر نمونه‌ها از رایانه‌تان حفاظت کند.

از این نظر، مرورگرهای گوگل کروم و فایرفاکس بهترین گزینه‌های موجود هستند که از آن میان فایرفاکس با داشتن ویژگی کد-باز و استقلال از شرکت‌های تجاری گزینه ارجح به شمار می‌رود. زیرا جامعه بسیار فعالی از کنشگران و برنامه‌نویسان در سرتاسر جهان به‌طور مداوم در حال بررسی و بهبود کد این مرورگر هستند و اشکالات آن را به‌طور مستمر شناسائی و برطرف می‌کنند.
اطلاعات بیشتر در مورد مرورگر FireFox را در صفحه ویژه آن در امنیت در یک جعبه دنبال کنید.

به خاطر داشته باشید

همیشه مرورگرتان را به طور مستقیم از وبسایت اصلی آن دانلود کنید. هیچگاه مرورگرها را از روی سی‌دی‌هایی که در بازار به فروش رسیده یا دست به دست می‌گردد نصب نکنید.

توجه: مرورگر اینترنت اکسپلورر شرکت مایکروسافت در سال‌های اخیر تلاش کرده تا امنیت خود را در مقابله با حمله بدافزارها بهبود بخشد. با این حال، همچنان یکی از اصلی‌ترین هدف‌ها برای حمله‌کنندگان به شمار می‌رود. دوره‌های به روز رسانی این مرورگر طولانی‌تر است و به تازگی شرکت مایکروسافت اعلام کرده که برای برخی نسخه‌های ویندوز دیگر از این مرورگر استفاده نخواهد کرد. ما نیز استفاده از این مرورگر را به کاربران توصیه نمی‌کنیم. برای کاربران اپل، مرورگر سافاری کماکان از گزینه‌های قابل اطمینان است، هرچند که از نظر سطح امنیت پایین‌تر از گوگل کروم و موزیلا قرار دارد.

بستن جاوا اسکریپت

جاوا اسکریپت زبانی رایج در برنامه‌نویسی رایانه است که کمک می‌کند وبسایت‌ها قابلیت تعاملی پیدا کنند؛ یعنی بتوانند به‌صورت پویا به درخواست‌های کاربران واکنش دهند. از سوی دیگر، جاوا اسکریپت راه سهل و آسانی در اختیار بدافزارها و جاسوس‌افزارها می‌گذارد تا بی سر و صدا به محتویات رایانه دسترسی پیدا کنند. صفحاتی که قابلیت جاوا اسکریپت برای آن‌ها فعال شده همچون در و پنجره‌های قفل نشده‌ای می‌مانند که نفوذگران از راه آن وارد می‌شوند.

امروزه، اغلب مرورگرها امکان غیرفعال کردن جاوا اسکریپت را ارائه می‌دهند.

دیوار آتش: حفاظ امنیتی شما

رایانه شما، برای حفاظت از خود در برابر تهدیدهای خارجی به دیوار آتش (Firewall) نیاز دارد. دیوار آتش همچون حصاری به دور رایانه‌تان عمل می‌کند. این‌که چه نوع اطلاعاتی می‌تواند به رایانه وارد یا از آن خارج شود را می‌بایست در دیوار آتش تنظیم کنید. دیوار آتش پیش از دیگر برنامه‌ها، تمام اطلاعات ورودی به رایانه‌تان را پایش کرده، در مسیر خروج اطلاعات از رایانه نیز در آخرین مرحله قرار می‌گیرد و آن را اسکن می‌کند.

یک دیوار آتش مناسب، از دسترسی هکرها و نفوذگران به اطلاعات رایانه جلوگیری می‌کند و جلوی بدافزارها را در ارسال اطلاعات به بیرون می‌گیرد. اوایل ممکن است کمی زمان ببرد تا همه تنظیمات متناسب با نوع استفاده شما از رایانه انجام شود، اما پس از آن، دیوار آتش بدون نیاز به دخالت شما، به کار خود ادامه خواهد داد.

آموخته‌هایتان را در عمل به کار بگرید

حال ببینیم چگونه می توانید برای حفاظت بیشتر از رایانه‌تان اطلاعات ارائه شده در این درس را به‌کار گرفت. با ما همراه شوید تا ابزارهای مناسب برای این کار را انتخاب کرده، راه‌های درست استفاده از آن را بررسی کنیم.

نرم‌افزارهای ضدویروس و ضدجاسوس‌افزار

ضدویروس

درباره استفاده از نرم‌افزارهای ضدویروس پیشتر توضیح دادیم. ممکن است شما هم اکنون نیز روی رایانه‌تان ضدویروس داشته باشید، اما آیا ضدویروس‌تان به اندازه کافی امنیت‌تان را تأمین می‌کند؟ آیا تنظیمات آن متضمن بهترین کارآیی لازم است؟ اگر پاسخ به هردو پرسش مثبت نیست، همین الان برای جایگزینی ضدویروس‌تان دست به کار شوید و یا تنظیمات رایانه‌تان را اصلاح کنید.

اگر هرکدام از موارد زیر شامل حال‌تان می‌شود، شما می‌بایست در مورد ایمنی رایانه خود تجدید نظر کنید:

- ضدویروس نصب شده روی رایانه، لپ‌تاپ، موبایل یا تبلت‌تان قفل شکسته است یا از منبعی به غیر از وب‌سایت اصلی یا نمایندگی رسمی آن به دست‌تان رسیده؛
- به‌طور کلی، ضدویروس ندارید؛ یا
- همین حالا هم شک دارید که رایانه‌تان آلوده شده باشد.

برای حفاظت از رایانه‌تان به ضدویروسی نیاز دارید که ثبت شده باشد و به طور مرتب به روز رسانی شود.
ما ضد ویروس !avast را پیشنهاد می‌کنیم. این برنامه را می توانید از این پیوند دریافت کنید. این ضدویروس مجانی است و به طور متناوب به‌روزرسانی می‌شود. همچنین نصب آن ساده است و زمان زیادی نمی‌برد.
طریقه نصب ضدویروس !avast را در وب‌سایت امنیت در یک جعبه دنبال کنید.

علاوه بر !avast ضدویروس AVG نیز نسخه رایگان ارائه می‌کند. اخیراً، این ضد ویروس صفحه زبان فارسی برای مشترکات ایرانی راه‌اندازی کرده. دیگر گزینه مجانی قابل اطمینان Avira AntiVir Personal Edition است.

اگر فکر می‌کنید رایانه‌تان به ویروس آلوده شده (سیستم‌های ویندوز)، می‌بایست از سی‌دی‌های نجات در مواقع اضطراری استفاده کنید. این پرونده‌ها را می‌توان در قالب ISO دانلود کرد. ISO قالب استاندارد برای تولید سی‌دی و دی‌وی‌دی است. سی‌دی‌های نجات در مواقع اضطراری AVG Rescue CD و Kaspersky Rescue Disk را می‌توانید به صورت مجانی از وب‌سایت‌های آن‌ها (پیوندهای ارائه شده) بارگیری کنید.

برای استفاده از این دیسک‌های نجات دهنده، مراحل زیر را دنبال کنید:

I. پرونده ISO را از یکی از پیوندهای بالا بارگیری کنید.

II. پرونده بارگیری شده را با کمک نرم‌افزار تولید سی‌دی مثل ImgBurn روی یک سی‌در کپي کنید. سی‌دی را در رایانه آلوده شده قرار دهید و رایانه را restart کنید تا از روی سی‌دی بالا بیاید. برای این منظور، به محض روشن شدن مجدد رایانه، کلید F۱۰ یا F۱۲ روي صفحه کلید را فشار دهید. باقی مراحل را از طریق دستوراتی که روی صفحه نمایشگر ظاهر می‌شود دنبال کنید. پس از آن سی‌دی شروع به پاک‌سازی رایانه خواهد کرد. بعد از راه‌اندازي مجدد، رایانه را به اینترنت وصل کنید تا در صورت نیاز ضدویروس و ضدجاسوس‌افزار به روزرسانی شوند. برای اطمینان همه رایانه را به‌طور کامل اسکن کنید.

هیچ‌گاه از پرونده‌های نجات اضطراری که از طریق سی‌دی‌های آماده به فروش می‌رسد استفاده نکنید.

ضد جاسوس‌افزار

ضد جاسوس‌افزار Spybot Search & Destroy را می‌توانید به‌طور مجانی از وب‌سایت آن بارگیری و روی رایانه خود نصب کنید. این نرم‌افزار برای کشف و خنثی‌سازی انواع بدافزار و جاسوس‌افزار گزینه مناسبی است. این برنامه رایانه شما را در برابر بدافزارها و جاسوس‌افزارها ایمن می‌سازد و از آلوده شدن آن در آینده جلوگیری خواهد کرد.
جزییات درباره این برنامه و روش نصب آن را در صفحه مربوطه در امنیت در یک جعبه دنبال کنید (به زبان فارسی).

Google Drive

همانطور که پیشتر اشاره شد، گوگل درایو راه امنی برای ذخیره‌سازی و باز کردن پرونده‌های دریافتی از اینترنت فراهم می‌کند. اگر از نسخه وب این ابزار استفاده می‌کنید، همه پرونده‌ها پیش از قرار گرفتن در آن محیط توسط ضدویروس اسکن می‌شوند. میان ابزارهای به اشتراک گذاری پرونده، گوگل درایو یکی از امن‌ترین سرویس‌ها را ارائه می‌کند. هرچند توصیه ما این است که کماکان حین استفاده از این ابزار نکات عمومی ایمنی را رعایت کنید.

وبگردی امن

همانطور که قبلا اشاره شد، برای مرور وب بهتر است تا از مرورگر فایرفاکس استفاده کنید. این مرورگر از حفره‌های امنیتی بسیار کمتری نسبت به دیگر نمونه‌های تجاری برخوردار است و از طریق افزونه‌ها (Plugin) به کاربران امکان گسترش امکانات خود را می‌دهد. یکی از افزونه‌های بسیار کارا، NoScript نام دارد. این افزونه برای کاربران امکان مسدود سازی جاوا اسکریپت در وب‌سایت‌های ناشناخته را فراهم می‌سازد. اطلاعات بیشتر در مورد شیوه نصب و استفاده از این افزونه را در وب‌سایت امنیت در یک جعبه دنبال کنید.

دیوارآتشین (Firewall)

اگر از سیستم عامل‌های مک یا گنو لینوکس استفاده می‌کنید. این سیستم‌ها مجهز به دیوار آتشین قدرتمند و قابل اطمینان مختص به خود هستند. می‌بایست اطمینان حاصل کرد که تنظیمات مربوطه به درستی انجام شده باشند. برای انجام این تنظیمات در گنو لینوکس رابط کاربری GUFW توصیه می‌شود. همچنین برای کاربران مک رابط کاربری NoobProof یا IPSecuritas را توصیه می‌کنیم. سیستم‌عامل‌های ویندوز نیز گرچه با دیوارآتشین عرضه می‌شوند اما کماکان به نصب برنامه‌های خارجی برای مراقبت از خود نیاز دارند. ما دیوار آتشین کومودو (Comodo) را به کاربران ویندوز پیشنهاد می‌کنیم. شیوه نصب و استفاده از این نرم‌افزار را در وب‌سایت امنیت در یک جعبه دنبال کنید.

منابع مفید

- فهرستی از ویروس‌های رایانه‌ای شناخته شده (ویکی‌پدیا).
- پاسخ به پرسش‌های متداول پیرامون بدافزارها (موسسه .(SANS
- چگونه از رایانه خود در برابر حمله بدافزارها و هکرها محافظت کنید (Security in a box)(انگلیسی).
- امنیت دیجیتال و حریم خصوصی برای مدافعان حقوق بشر(انگلیسی).
- امنیت فضای دیجیتالی و حریم خصوصی مدافعان حقوق بشر (فارسی).
- برنامه کمک هزینه‌های امنیتی برای مدافعان حقوق بشر (فارسی).
- خودآموز امنیت و حفاظت برای مدافعان حقوق بشر (فارسی).
- کمک اضطراری خط مقدم به مدافعان حقوق بشر در زمینه امنیت دیجیتالی (فارسی).
- جعبه کمک‌های اولیه دیجیتالی (انگلیسی).

درس سه: ایمن‌سازی ذخیره اطلاعات

فهرست عنواین

مقدمه

به درس سه از دوره امنیت در فضای مجازی نبض‌ایران خوش آمدید. در دو درس پیش به شناخت تهدیدها و امنیت رایانه پرداختیم. حال وقت آن رسیده تا کمی درباره امنیت اطلاعات و داده‌های موجود در رایانه و دستگاه‌های هوشمند صحبت کنیم. چه کنشگر اجتماعی/سیاسی باشید یا خبرنگار و یا یک شهروند عادی، دستگاه‌های رایانه‌ای که استفاده می‌کنید حاوی اطلاعات سودمندی در مورد کار یا زندگی‌تان است و احتمالا نفوذگرانی آن بیرون مایل به در اختیار گرفتن آن اطلاعات هستند. به همین دلیل، شما می‌بایست از اطلاعات و داده‌های‌تان محافظت کنید.
ربایندگان از دو راه کلی ممکن است به اطلاعات شما دسترسی پیدا کنند.

I. نخست به صورت فیزیکی، یعنی رایانه یا دستگاه هوشمندتان را به سرقت ببرند یا آن را ضبط کنند.
II. دوم، از طرق الکترونیک، مثلاً از طریق اینترنت یا راه‌های ارتباطی دیگر.

یک طرح امنیتی مناسب می‌بایست هر دو این موارد را در نظر بگیرد. شما می‌بایست هم از رایانه خود چنان مراقبت کنید که نفوذ از راه دور را هرچه بیشتر برای ربایندگان دشوار سازید و هم با مخفی‌سازی و رمزگذاری اطلاعات، تا حد امکان دسترسی به آن را در صورت در اختیار گرفتن رایانه توسط شخص ناصالح مشکل کنید.

یک طرح امنیتی مناسب، مکان نگهداری اطلاعات را نیز به دقت مورد توجه قرار می‌دهد. بسته به نوع استفاده و نگرانی‌های امنیتی، شما می‌توانید اطلاعات را در رایانه شخصی، حافظه‌های قابل حمل یا در ابرهای اینترنتی ذخیره سازید. هریک از این راه‌حل‌ها نقاط قوت و ضعف خاص خود را دارد، به گونه‌ای که تنها با سبک و سنگین کردن وضعیتی که در آن قرار دارید می‌شود گزینه مناسب را انتخاب کرد.

برای مطالعه مفصل پیرامون تهیه طرح امنیتی، خودآموز امنیت و محافظت برای مدافعان حقوق بشر، راهنمای مناسبی است. هرچند که نگاه این سند به مبحث امنیت بسیار کلی‌تر از مورد امنیت دیجیتالی است.

داده، اطلاعات و پرونده

نخست بگذارید کمی در مورد تفاوت میان داده، اطلاعات و پرونده در دنیای رایانه صحبت کنیم.

داده واقعیت خام است. قطعاتی از اطلاعات که هنوز به هم نپیوسته و شکل داده نشده‌اند. داده می‌تواند در اشکال گوناگون ظاهر شده و به راه‌های مختلفی ذخیره شود. فهرست شاگردان یک کلاس، فهرست دمای گزارش شده از ایستگاه‌های هواشناسی، فهرست درآمد اقشار مختلف کشور و فهرست نشانی کافه‌های تهران همه نمونه‌هایی از داده هستند.
گاه به دلیل آن‌که داده سخت به دست آمده و یا قابلیت تبدیل شدن به اطلاعات حساسی را داراست، ارزش بسیار پیدا می‌کند، اما به‌طور کلی، داده تا پیش از تبدیل شدن به اطلاعات شکل و مفهوم ندارد.

اطلاعات مجموعه داده‌ای است که به شکل منسجمی ساختار یافته تا مفهوم خاصی را ارائه دهد. اطلاعات می‌تواند شخصی یا حرفه‌ای باشد. درز اطلاعات شخصی ممکن است، هویت، حرفه یا فعالیت فرد یا گروه خاصی را به خطر انداخته یا آنان را آسیب‌پذیر سازد. نفوذگران تنها با دانستن نام، نام خانوادگی و نشانی ایمیل‌تان می‌توانند خود را جای شما جا زده، دوستان و آشنایان‌تان را فریب دهند.

پرونده، سامانه‌های رایانه‌ای داده و اطلاعات را در قالب‌های گوناگونی به صورت پرونده‌های جداگانه ذخیره‌سازی می‌کنند. پرونده ممکن است داده، متن، صدا یا تصویر را در خود جای دهد. از این رو حفاظت از پرونده‌ها اهمیت بسیار زیادی دارد.
نفوذگران و رباینده‌گان ممکن است به داده، اطلاعات یا پرونده‌های متعلق به شما علاقمند باشند. یک طرح امنیتی مناسب می‌بایست حفاظت فیزیکی و دیجیتالی از همه این اقلام را در بر بگیرد.

مراقبت فیزیکی از رایانه و دستگاه‌های هوشمند

همان‌طور که پیشتر توضیح داده شد، رایانه و دستگاه‌های هوشمندی که امروزه با خود همراه داریم حاوی اطلاعات ارزشمندی هستند که برای رباینده‌گان، سازمان‌های امنیتی و رقبای کاری جذابیت دارد. نخستین خطر علیه این اطلاعات، سرقت یا ضبط فیزیکی رایانه، دستگاه‌های هوشمند یا حافظه‌های قابل حمل است.

به خاطر داشته باشید

اگر رایانه یا دستگاه هوشمندتان که به سرقت رفته بود یا توسط نیروهای امنیتی ضبط شده بود را دوباره به دست آوردید، احتمال دارد روی آن برنامه‌های استراق سمعی نصب شده باشد که در آینده اطلاعات، پرونده‌ها و حتی مکالمات روزمره و مکان‌تان را به بیرون گزارش دهد.

در این فصل به روش‌های ایمن‌سازی فیزیکی و دیجیتالی دستگاه‌ها می‌پردازیم. اما پیش از آن توجه داشته باشید که بهترین راه برای محافظت از اطلاعات آن است که از حمل غیرضروری آن خودداری کنید. اگر چیزی برای دزدیده شدن نداشته باشید، نگران آن هم نخواهید بود.

دسترسی به رایانه، تلفن همراه و دیگر دستگاه‌های هوشمند

شاید بدیهی به نظر برسد، اما سالیانه تعداد بسیاری زیادی لپ‌تاپ به سرقت می‌رود، علاوه بر آن، تقریباً همیشه نیروهای امنیتی موقع بازداشت افراد رایانه و دستگاه‌های هوشمند (تفلن همراه، تبلت و ..) آن‌ها را ضبط و مورد بازرسی قرار می‌دهند. موارد ایمنی زیر به شما در محافظت فیزیکی از دستگاه‌های هوشمندتان کمک خواهد کرد:

- هیچ‌گاه لپ‌تاپ یا تلفن همراه‌تان را در مکان‌های عمومی رها نکنید.
- در صورت امکان از کابل ایمنی لپ‌تاپ استفاده کنید (هرچند این کار متضمن حفظ امنیت لپ‌تاپ نیست).
- همیشه از گذرواژه مناسب برای ورود به دستگاه‌های هوشمند استفاده کنید. گذرواژه می‌بایست حداقل از ۱۲ حرف تشکیل شده باشد و به سادگی قابل حدس زدن نباشد. کمی بعد در مورد گذرواژه بیشتر صحبت خواهیم کرد.
- از گذرواژه‌های یکسان برای دستگاه‌های مختلف استفاده نکنید.
- گذرواژه دستگاه‌ها (و حساب‌های کاربری)تان را به دیگران ندهید.
- اگر در خانه یا محل کار، روی داده خاصی کار می‌کنید، یا اطلاعات و پرونده‌های ارزشمندی در دست دارید، به امنیت فیزیکی آن فکر کنید. آیا مکان نگهداری آن از دست‌برد سارقان یا یورش مأموران امنیتی در امان است؟ یک طرح امنیتی مناسب این موضوع را به دقت مد نظر خواهد گرفت.
- برخی نرم‌افزارهای ارتباط آنلاین (مانند اسکایپ) مکالمات متنی (یا حتی صوتی و تصویری) را روی رایانه ذخیره می‌کنند. این مکالمات در پرونده‌هایی ذخیره می‌شوند که به راحتی قابل دسترس و خواندن است. اگر از این نرم‌افزارها برای انجام مکالمات حساس استفاده می‌کنید، امنیت پرونده‌های مربوط به مکالمات‌تان را نیز درطرح امنیتی در نظر بگیرید.

طرح امنیتی

یک طرح امنیتی مناسب، جنبه‌های گوناگون تهدیدات پیش رو را مورد توجه قرار داده، برای هرکدام چاره‌ای پیشنهاد می‌کند. چه به عنوان یک فرد و چه در قالب یک سازمان، می‌بایست طرح امنیت دیجیتالی جامع و کاملی را در دست داشته باشید. هرچند لازم نیست این طرح روی کاغذ آورده شده باشد، اما نوشتن آن به درک بهتر حفره‌های امنیتی و یافتن راه‌حل برای آن کمک می‌کند.

برای مطالعه بیشتر پیرامون طرح امنیتی خودآموز امنیت و محافظت برای مدافعان حقوق بشر، تهیه شده توسط frontlinedefenders.org را توصیه می‌کنیم. این راهنما بحث امنیت و طرح امنیتی را به صورت موشکافانه مدنظر قرار داده، شیوه تهیه طرح امنیت فردی و سازمانی را به تفصیل شرح می‌دهد.

مطالعه بیشتر: برنامه‌ریزی برای امنیت (انگلیسی)

انتخاب مکان مناسب برای ذخیره‌سازی

داده، اطلاعات، متن، صدا، عکس و فیلم در دنیای رایانه به شکل پرونده (file) ذخیره می‌شود. نخستین گام در راه حفاظت از پرونده‌ها، ذخیره‌سازی آن در مکانی امن است. انواع مکان‌های ذخیره‌سازی را می‌توان به سه دسته تقسیم‌بندی کرد:

I. رایانه یا دستگاه هوشمند از قبیل تلفن‌های هوشمند، تبلت و غیره.
II. حافظه قابل حمل، یواس‌بی درایو، سی‌دی، دی‌وی‌دی و غیره.
III. ابر اینترنتی، شامل انواع خدمات ذخیره‌سازی آنلاین از قبیل، یوتیوب، اپل، گوگل درایو، آمازون درایو و غیره.

هر کدام از این روش‌های ذخیره‌سازی مزایا و معایب خاص خود را دارد که در یک طرح امنیتی مناسب باید به دقت بررسی شده و در نظر گرفته شوند. به‌طور کلی، فایل‌های ذخیره شده در محیط‌های ابر اینترنتی از تخریب یا سرقت فیزیکی در امان هستند. شرکت‌های ارائه دهنده این خدمات همه تدابیر لازم برای حفاظت فیزیکی از این فایل‌ها را در نظر می‌گیرند. هرچند، فایل‌های ذخیره‌شده در محیط‌های ابر اینترنتی گاه به گاه مورد بازبینی و دسترسی مقامات دولتی قرار گرفته، یا هکرها به سیستم‌های امنیتی آن رخنه می‌کنند. اگر از گذرواژه امن استفاده کرده و دیگر ملاحظات امنیت دیجیتالی را رعایت می‌کنید و در کشوری هستید که امکان بازرسی فیزیکی از محل کار و اقامت‌تان وجود دارد، استفاده از سیستم‌های ابر اینترنتی شاید بهترین راه برای حفاظت از پرونده‌های‌تان باشد. همیشه به این فکر کنید که شرکت ارائه دهنده خدمات ابر اینترنتی در کجا واقع شده. اگر شرکت در همان کشوری است که شما می‌خواهید اطلاعات‌تان را از تفتیش دولتی محفوظ نگه دارید، آن سرویس برای کار شما مناسبت نیست.

به خاطر داشته باشید:

اگر برای ذخیره‌سازی پرونده‌های حساس از سیستم‌های ابر اینترنتی استفاده می‌کنید، در انتخاب شناسه کاربری بسیار محتاط باشید. شناسه کاربری که قابل حدس زدن بوده، یا به هر نوعی بتوان آن را به شما ربط داد گزینه مناسبی نیست. برای مثال، از نام واقعی خود در انتخاب شناسه کاربری استفاده نکنید.

نگهداری پرونده در رایانه یا حافظه قابل حمل نیاز به مراقبت‌های ویژه دارد، زیرا همیشه امکان تخریب فیزیکی، سرقت یا ضبط آن توسط مقامات وجود دارد. رعایت نکات امنیت دیجیتال در هیچ‌یک از این موارد به تنهایی کارساز نخواهد بود و بسته به نوع پرونده و میزان اهمیت آن می‌بایست تدابیر مراقبتی مناسب اتخاذ گردد. با این حال، در این مورد نیز، رعایت نکات امنیت دیجیتال بسیار ضروری است. نفوذگران همیشه می‌توانند از طرق مختلف، حتی بدون دسترسی فیزیکی به محل نگهداری پرونده، آن را به سرقت برده یا تخریب کنند. مخفی‌سازی و رمزگذاری اطلاعات دو روش مؤثر برای مقابله با این تهدیدات هستند.

مخفی‌سازی و رمزگذاری اطلاعات

خانه‌تان را در نظر بگیرید، کجا بهترین جا برای نگهداری از مدارک مهم یا جواهرآلات است؟ البته یک گاوصندوق امن که جائی مخفی شده باشد. گاوصندوق محیط امنی را برای‌تان ایجاد می‌کند که تنها با یک رمز قابل دسترس است. درست مانند یک گاوصندوق، ابزارهای رمزگذاری اطلاعات نیز محیطی در رایانه یا حافظه قابل حمل‌تان ایجاد می‌کنند که پرونده‌های داخل آن تنها با گذرواژه قابل دسترس هستند. همچون یک گاوصندوق، برای دسترسی به پرونده‌های رمزگذاری شده، نخست می‌بایست آن‌ها را رمزگشائی کرده، و پس از اتمام کار، حتما دوباره رمزگذاری نمود.

بیشتر بخوانید:

- تاریخچه رمزگذاری از دوران باستان تا به امروز (انگلیسی).
- رمزگذاری چیست؟ (انگلیسی).
- جاسوسی که از کد در آمد، داستان فیلم‌سازی که به‌طور تصادفی مشخصات افرادی که با او همکاری کرده بودند را در اختیار نیروهای امنیتی سوریه قرار داد (انگلیسی).

به خاطر داشته باشید:

تعیین گذرواژه برای ورود به سیستم ویندوز (یا دیگر سیستم‌عامل‌ها)، باعث رمزگذاری و حفاظت از پرونده‌های درون رایانه نمی‌شود. راه‌های بسیاری برای ورود به رایانه و دور زدن این مانع وجود دارد. با این حال، ما استفاده از گذرواژه برای دسترسی به رایانه، و دستگاه‌های هوشمند را توصیه می‌کنیم زیرا تا حدی از دسترسی افراد، بدون اجازه شما به سیستم جلوگیری می‌کند.

ابزارهای رمزگذاری

نرم‌افزار TrueCrypt ابزار کد-باز و قابل اطمینانی است که معمولا توسط متخصصین امنیت توصیه می‌شده. متأسفانه این نرم‌افزار از میانه سال ۲۰۱۴ بدین‌سو دیگر توسط تولیدکنندگان آن پشتیبانی نمی‌شود. با این حال، کارشناسانی هستند که کماکان استفاده از آن را توصیه می‌کنند. نبض‌ایران با پیروی از یک قاعده کلی، استفاده از نرم‌افزارهایی که دیگر پشتیبانی نمی‌شوند را به کاربران خود توصیه نمی‌کند. ابزارهای جایگزینی برای TrueCrypt وجود دارد که شاید از نظر کارآیائی به پای آن نرسند، اما از سطح امنیت قابل اطمینانی برخوردارند. چند نمونه از این قرار است:

- زیرشاخه‌های TrueCrypt. کد برنامه TrueCrypt برای عموم باز است؛ یعنی هر کسی می‌تواند به اصل کد آن دسترسی داشته باشد. حال که این پروژه متوقف شده، گروه‌های دیگری از برنامه‌نویسان با پایه قراردادن کد TrueCrypt اقدام به تولید ابزارهای رمزگذاری تازه‌ای کرده‌اند. دو نمونه موفق از این دست:
  - CipherShed، یکی از زیرشاخه‌های TrueCrypt است. این نرم‌افزار هنگام نگارش متن این درس، هنوز در حال آماده‌سازی بوده.
  - VeraCrypt، نمونه دیگری از زیرشاخه‌های TrueCrypt است. این نرم‌افزار مجانی، کد-باز بسیاری از قابلیت های TrueCrypt را به کاربران ارائه داده، برخی ایرادات امنیتی آن را نیز برطرف کرده.
- BitLocker، محصولی از شرکت مایکروسافت است. این ابزار به کاربران ویندوز امکان رمزگذاری دیسک سخت، یا بخش‌هایی از آن را می‌دهد. BitLocker قابلیت نصب روی تمام نسخه‌های ویندوز را ندارد.
- FileVault، محصول شرکت اپل است که به همراه نسخه‌های اخیر سیستم‌عامل رایانه‌های این شرکت ارائه می‌شود.

اگر درباره نصب یا استفاده از هر یک از این ابزارها سؤالی دارید می‌توانید با ایمیل info at nabz-iran.com تماس بگیرید.

بیشتر بخوانید:
چگونه دستگاه ویندوز خود را رمزگذاری کنید (انگلیسی).
چگونه گوشی آی‌فون‌تان را رمزگذاری کنید (انگلیسی).

مخفی‌سازی پرونده‌ها

همچون مثال گاوصندوق، اگر از ابزارهای رمزگذاری استفاده می‌کنید یعنی شما چیزی برای مخفی کردن دارید. در برخی کشورها حتی ارائه، یا استفاده از ابزارهای رمزگذاری، خود یک جرم محسوب می‌شود. در موارد دیگر نیز، کشف پرونده‌های رمزگذاری شده در رایانه‌تان، ممکن است شک و ضن را نسبت به فعالیت‌های‌تان برانگیخته، مأموران امنیتی یا نفوذگران کنجکاو شوند که محتوای آن پرونده‌ها چیست. نکته دیگر این‌که، همچون نمونه گاوصندوق، پرونده‌های رمزگذاری شده نیز به نفوذگران نشان می‌دهد که اطلاعات مهم را کجا ذخیره می‌کنید.

به این دلائل، می‌بایست پرونده‌های رمزگذاری شده را جائی مخفی کنید. نرم‌افزارهایی همچون TrueCrypt راه حل این مسئله را ارائه می‌کنند. اگر به دنبال جایگزینی برای TrueCrypt می‌گردید، حتما به این موضوع توجه داشته باشید.

پنهان‌نگاری (Steganography)، دانش و فناوری پنهان ساختن یک پرونده درون یا تحت نام پرونده دیگری است، با هدف مخفی ساختن آن پرونده. نرم‌افزار TrueCrypt و برخی از شاخه‌های آن، چنین امکانی را برای کاربران فراهم می‌کنند. گاوصندوقی را در نظر بگیرید که داخل جعبه خود، فضائی مخفی داشته باشد. در این صورت، حتی اگر نفوذگری به رمز گاوصندوق دسترسی پیدا کرد، متوجه وجود فضای مخفی درون آن نخواهد شد.

معمولاً، روش‌های غیر فنی برای بدست آوردن گذرواژه نرم‌افزارهای رمزگذاری وجود دارد، از جمله تهدید و ارعاب، بازجوئی، شکنجه، باج‌گیری و .. اما حالتی را در نظر بگیرید که اصلاً پرونده رمزگذاری شده‌ای در رایانه‌تان پیدا نشود؛ به این روش انکار باورپذیر (Plausible deniability) گفته می‌شود. یعنی اگر شما می‌گویید چیزی برای مخفی کردن ندارم، پرونده مخفی شده‌ای هم در رایانه‌های‌تان کشف نشود. نرم‌افزار TrueCrypt پا را این نیز فراتر گذاشته، امکان آن را می‌دهد تا پرونده‌ها را درون فضای رمزگذاری شده، مخفی‌سازی کرد؛ درست مانند حالت فضای مخفی درون گاوصندوق. در این حالت، حتی اگر فرد تحت فشار گذرواژه TrueCrypt را لو داده، پرونده‌هایش رمزگشائی شوند، هنوز پرونده‌های با اهمیت خیلی بالا از چشم نفوذگران دور می‌ماند.

پس چطور می‌توان خود نرم‌افزار رمزگذاری را مخفی کرد؟ TrueCrypt راه حلی برای این مسئله نیز ارائه می‌دهد. نرم‌افزار TrueCrypt را می‌توان به‌جای نصب روی رایانه، از روی یواس‌بی‌درایو اجرا کرد. با این روش هیچ اثری از آن روی رایانه باقی نخواهد ماند.

به خاطر داشته باشید

نکته دیگر خود نرم‌افزار رمزگذاری است. به یاد بیاورید که در برخی کشورها، بارگیری، نصب یا استفاده از نرم‌افزارهای رمزگذاری جرم شناخته می‌شود. در موارد دیگر، وجود نرم‌افزار رمزگذاری خود نشانه‌ای خواهد بود از وجود پرونده‌های رمزگذاری شده.

بیشتر بخوانید:

از پرونده‌های حساس در رایانه‌تان مراقبت کنید

چگونه با TrueCrypt یک فضای رمزنگاری شد ایجاد کنید؟

راهنمای استفاده از TrueCrypt به همراه جزئیات بیشتری در مورد روش‌های رمزگذاری و پنهان‌نگاری (به زبان انگلیسی).

پرسشگان TrueCrypt، پاسخ بسیاری از پرسش‌هایی که ممکن است در ذهن‌تان پیش آمده باشد یا در عمل با آن مواجه شده باشید را فراهم می‌کند.

چگونه داده خود را امن نگهدارید (انگلیسی).

راهنمای نصب DiskCryptor برای رمزگذاری ویندوز (انگلیسی).

نابودسازی پرونده‌ها و اطلاعات

بهترین راه برای جلوگیری از دسترسی دیگران به اطلاعات و پرونده‌ها، نابودسازی آنان است. نسخه‌های قدیمی پرونده‌ها، نسخه‌های پشتیبانی که تاریخ‌شان سپری شده، پرونده‌های موقتی و غیره، نمونه‌هایی هستند از مواردی که می‌بایست به دقت نابود شوند. اما نابودساختن پرونده‌ها در دنیای مجازی کار ساده‌ای نیست.

دانش نرم‌افزاری گسترده‌ای لازم نیست تا پرونده‌های حذف شده در یک رایانه را بازیابی کرد. در محیط اینترنت کار از این نیز سخت‌تر است. در محیط‌های آنلاین، تقریبا هیچ چیز نابود نمی‌شود. وقتی شما، ایمیلی را پاک می‌کنید یا عکسی را از صفحه فیس‌بوک‌تان حذف می‌کنید، آن پرونده دیگر برای شما (و احتمالا برای دیگر کاربرانی که به پروفایل‌تان دسترسی دارند) قابل دسترس نخواهد بود، اما اصل پرونده ممکن است حتی سال‌ها پس از حذف شدن، در سرورهای شرکت ارائه‌دهنده ایمیل یا شبکه اجتماعی باقی بماند.

در دنیای اطلاعات، به این روش، حذف منطقی می‌گویند، یعنی به‌جای این‌که پرونده به صورت فیزیکی نابود شود، تنها دسترسی افراد به آن از بین می‌رود، هرچند که پرونده دست نخورده باقی خواهد ماند. بیشتر سرویس‌دهندگان اینترنتی از این روش برای حذف استفاده می‌کنند. این مشابه آن است که به جای نابود کردن یک نامه، آن را در سطل آشغال بیاندازید. کسی که به زباله‌ها دسترسی داشته باشد می‌تواند اصل نامه‌تان را پیدا کند.

به همین دلیل، هیچ‌چیزی که ممکن است در آینده برای‌تان مشکل‌ساز شود را در اینترنت قرار ندهید، حتی اگر سطح دسترسی به آن را محدود تعریف کرده باشید.

به خاطر داشته باشید

این ممکن است با سیاست نگهداری اطلاعات و داده‌های حساس در ابرهای اینترنتی در تضاد به نظر برسد. موقع استفاده از چنین سرویس‌هایی باید در نظر داشته باشید که در صورت لو رفتن حساب کاربری، چه اطلاعاتی از شما یا دیگران نیز لو خواهد رفت و می‌بایست حد می‌توان از بارگذاری آن اطلاعات جلوگیری کرد.

به خاطر داشته باشید

پس به یاد داشته باشید که حذف فیزیکی پرونده‌ها و اطلاعات تنها در رایانه شخصی و برخی حافظه‌های قابل حمل، جایی که شما همه دسترسی‌های ممکن را دارید امکان‌پذیر است. هرچند ممکن است به آن سادگی‌ها عملی نباشد؛ برای این‌کار به نرم‌افزارهای خاصی نیاز دارید.

همان‌طور که اشاره شد، در سیستم‌های الکترونیکی، حذف به صورت منطقی انجام می‌شود، یعنی فقط ایندکس مربوط به پرونده مورد نظر از فهرست ایندکس‌ها حذف می‌گردد. در حالی که خود پرونده به صورت فیزیکی دست نخورده باقی خواهد ماند تا وقتی‌که نرم‌افزار دیگری شروع به نوشتن در محل نگهداری پرونده در حافظه رایانه کند. همچون نوشتن با مداد، در دنیای رایانه نیز حتی بعد از پاک کردن و دوباره نوشتن هنوز اثر نوشته قبلی باقی می‌ماند و قابل بازیافت است. علاوه بر این، معمولاً در رایانه‌تان پرونده‌هایی وجود دارد که حاوی اطلاعات حساس هستند و احتمالا شما از وجودشان هیچ اطلاعی ندارید.

برای مثال، وقتی روی یک پرونده Word کار می‌کنید، ویندوز به صورت خودکار نسخه‌های پشتیبانی از آن پرونده تهیه می‌کند تا در مواقع ضروری بتواند آن را بازیابی کرده، کار شما را نجات دهد.

هر بار که پرونده را ذخیره می‌کنید، یک نسخه پشتیبان جدید تولید می‌شود. پس از مدتی، نسخه‌های بسیاری از پرونده در حال تکمیل شما در دیسک سخت (Hard disk) رایانه ذخیره شده، که با کمی تلاش و جستجو قابل بازیابی است. هرکدام از این نسخه‌ها، درصدی از تکامل پرونده‌تان را در خود ذخیره دارد. بجز Word، دیگر نرم‌افزارهای Office، مرورگر فایرفاکس، ابزارهای ایمیل و دیگر نرم‌افزارها نیز ردپاهایی از این دست در رایانه‌تان به جا می‌گذارند. به علاوه، خود ویندوز هم، گاه گذرواژه‌ها و نسخه‌هایی از پرونده‌ها، سابقه مرور وب و دیگر اطلاعات حساس از فعالیت‌های‌تان را روی رایانه برجای می‌گذارد.

بیشتر بخوانید:

- نابودسازی اطلاعات حساس از وب‌سایت امنیت در یک جعبه (انگلیسی).
- چگونه اطلاعات را به شیوه‌ای امن حذف کنیم (سامانه‌های گنو لینوکس)(انگلیسی).
- چگونه اطلاعات را به شیوه‌ای امن حذف کنیم (سامانه‌های اپل)(انگلیسی).
- چگونه اطلاعات را به شیوه‌ای امن حذف کنیم (سامانه‌های ویندوز)(انگلیسی).
- پاکسازی امن اطلاعات - بالاویزیون (فارسی)

دو ابزار کارآمد در این زمینه وجود دارد؛ Eraser و CCleaner. ابزار نخست، Eraser، به شما کمک می‌کند که یک پرونده خاص را از روی دیسک سخت یا حافظه یواس‌بی پاک کنید. همچنین، این ابزار به کاربر امکان می‌دهد تا همه پرونده‌هایی را که به‌طور ناخواسته روی دیسک یا حافظه وجود دارند پاک کرد. به این ترتیب می‌توانید اطمینان حاصل کنید که جایی دور از چشم‌تان پرونده‌ای با اطلاعات حساس مخفی نشده باشد.

مطالعه بیشتر:

- راهنمای نصب Eraser در ویندوز (انگلیسی).

- حذف اطلاعات به شیوه امن از حافظه‌های مغناطیسی و حالت جامد (انگلیسی).

ابزار به درد بخور دیگر در این زمینه، CCleaner نام دارد. در حالی که Eraser به شما کمک می‌کند پرونده‌های مورد نظر یا نسخه‌های مربوطه را هر وقت لازم شد پاک کنید، CCleaner وظیفه پاک کردن خودکار، پرونده‌های موقتی، نسخه‌های موقتی، سابقه مرور وب و دیگر فعالیت‌های شما در رایانه که ممکن است اطلاعات حساسی در خود نگهداری کنند را بر عهده می‌گیرد.
بدین‌ترتیب، شما مجبور نخواهید بود، هربار پس از استفاده از اینترنت یا دیگر نرم‌افزارها، Eraser را اجرا کنید. ما ترکیب استفاده از این دو نرم‌افزار با هم را به شما پیشنهاد می‌کنیم.

بیشتر بخوانید:

- نصب CCleaner در سیستم‌عامل ویندوز - حذف پرونده به شیوه امن (انگلیسی).
- پاسخ به برخی پرسش‌های متداول پیرامون CCleaner.

پاک کردن، حافظه‌های قابل حمل مانند سی‌دی، دی‌وی‌دی و غیره از این هم پیچیده‌تر است. بهترین راه، شاید نابودی کامل حافظه توسط قیچی یا وسیله مشابه باشد. ما به دلیل ملاحظات سلامت و محیط زیستی، سوزاندن را توصیه نمی‌کنیم.
اگر در زمینه، نابودی اطلاعات و یا نصب و استفاده از هر یک از ابزارهای معرفی شده پرسشی داشته باشید می‌توانید آن را از طریق نشانی ایمیل: info@nabz-iran.com با ما در میان بگذارید.

نبض ایران
تقویت صدای ایرانیان

درس چهار: ایمن‌سازی ارتباطات

فهرست عنوان

مقدمه

به درس چهار از دوره امنیت در فضای مجازی نبض‌ایران خوش آمدید. در درس‌های پیش به انواع خطراتی پرداختیم که هنگام آنلاین بودن، شما را تهدید می‌کنند. همچنین در مورد حافظت از اطلاعات رایانه‌تان صحبت شد. حال به اطلاعاتی می‌پردازیم که شما از رایانه خود به اینترنت می‌فرستید.

همچنین به‌طور کلی‌تر به امنیت مکالمات و ارتباطات از طریق اینترنت خواهیم پرداخت.
اگر اطلاعاتی که ارسال یا دریافت می‌کنید کدگذاری شده و یا به‌صورت رمزنگاری شده، پنهان و ارسال شوند، دسترسی و خواندن آن برای دیگران بسیار دشوار خواهد شد. ایمن‌سازی ارتباطات آنلاین (ارسال و دریافت اطلاعات در اینترنت) مهمترین گام در راستای محافظت از خود در فضای مجازی است.

در خاتمه این درس شما خواهید توانست از حساب‌های کاربری‌تان در اینترنت به شیوه‌ای درخور محافظت کرده، اطلاعات شخصی‌تان را از دسترس دیگران محفوظ نگه دارید. همچنین یاد خواهید گرفت که چگونه با کمک رمزگذاری ارتباطات اینترنتی، مکالمات و مکاتبات‌تان را مخفی نگه دارید.

همچون درس‌های پیشین، در انتهای این درس نیز بخشی با عنوان به‌کارگیری آن‌چه آموخته‌اید وجود دارد، که در آن کاربرد عملی موارد ارائه شده در این درس را بررسی خواهیم کرد.

امنیت حساب کاربری

تقریباً استفاده از تمام سرویس‌های اینترنتی موجود مستلزم ایجاد حساب کاربری است. این حساب‌ها اطلاعات شخصی، مانند نام، نام خانوادگی، تاریخ تولد، آدرس محل سکونت و غیره را از کابران مطالبه می‌کنند. بسته به نوع سرویس، گاه ممکن است این سرویس‌ها حاوی اطلاعات بیشتری از کاربران نیز باشند؛ مواردی همچون: سوابق مکاتبات، ارتباطات شخصی و کاری، شبکه اجتماعی، حساب بانکی و غیره. بنگاه‌های ارائه دهنده این سرویس‌ها حداکثر تلاش خود را برای محافظت از این اطلاعات می‌کنند. اما در این میان نقش اصلی را شما بازی می‌کنید. انتخاب گذرواژه مناسبی که به سادگی قابل حدس زدن نبوده و در جای دیگری نیز استفاده نشده باشد کار شماست.

به‌طور کلی، دو روش برای هک کردن حساب کاربری وجود دارد که شما می‌بایست مراقب هر دوی آن باشید:

I. روش نخست، هک توسط یک شخص حقیقی است. بدین گونه که هکرها سعی می‌کنند با استفاده از اطلاعات خصوصی که از شما در دست دارند، یا از طریق گول زدن شما، گذرواژه مورد نظر را حدس بزنند. برای مقابله با این روش، شما نمی‌بایست از عبارات قابل حدس زدنی، همچون تاریخ تولد، نام افراد خانواده یا هرگونه اطلاعات شخصی که بتوان به سادگی (مثلا با استفاده از شبکه‌های اجتماعی) بدست آورد استفاده کنید. گذرواژه‌ها را طوری انتخاب کنید که برای دیگران قابل حدس‌زدن نباشد. در صورت امکان، همیشه از گزینه ورود دو مرحله‌ای برای مراقبت از حساب‌های کاربری‌تان استفاده کنید. در این زمینه بیشتر توضیح خواهیم داد.
II. روش دوم، هک توسط روبات یا برنامه‌های رایانه‌ای است. هکرها بدین منظور از الگوریتم‌های رمزشکن استفاده می‌کنند. این الگوریتم‌ها، حروف و اعدادی که احتمال استفاده از آن در گذرواژه شما وجود داشته باشد را به صورت تصادفی امتحان کرده، تا آن را حدس بزنند. مقابله با این روش کمی دشوارتر است، هرچند که از آن نیز کمتر استفاده می‌شود. برای مقابله با این تهدید، بهتر است از عبارت‌های طولانی که از حروف، اعداد و نشانه‌ها تشکیل شده باشد استفاده کنید. همچنین گزینه ورود دو مرحله‌ای نیز راه خوبی برای سد کردن چنین تهدیدی است.

برای حساب‌های کاربری مختلف، از گذرواژه‌های یکسان یا مشابه استفاده نکنید. این کار باعث می‌شود در صورت لو رفتن یکی از گذرواژه‌ها، دیگر حساب‌های کاربری نیز به خطر بیافتند. درضمن، هر از گاهی می‌بایست گذرواژه حساب‌های کاربری‌تان را تغییر دهید.

به حساب ایمیل یا فیس‌بوک خود فکر کنید، آیا موارد بالا در مورد آن‌ها رعایت شده؟ غالبا، به خاطر سپردن گذرواژه‌های طولانی و پیچیده کار ساده‌ای نیست و از این رو بسیاری کاربران این نکته را رعایت نمی‌کنند. با این حال، ابزارهای سودمندی برای حل این مسئله وجود دارد؛ ابزارهایی که به شما در تولید و نگهداری امن گذرواژه یاری می‌رسانند. یکی از این ابزارها، KeePass نام دارد. در بخش به‌کارگیری آن‌چه آموخته‌اید در مورد این ابزار بیشتر صحبت خواهیم کرد.

امنیت ارتباط از طریق رمزگذاری

رمزگذاری چیست؟

رمزگذاری فرآیند امنیتی است که با تغییر ساختار اطلاعات آن را برای دیگران غیرقابل خواندن می‌کند. بدین صورت، هیچ کس به جز شخص گیرنده‌ای که "کلید" رمزگشائی خاص خود را دارد، قادر به درک محتوای پیام نخواهد بود. کلید رمزگشایی به گیرنده کمک می‌کند تا اطلاعات (متن، صدا یا تصویر) را به شکل اولیه آن باز گردانده به محتوای آن دسترسی پیدا کند.

آنچه در بستر اینترنت می‌خوانید یا می‌نویسید به‌صورت متن خام انتقال می‌یابد که برای همه قابل دسترس است. هر صفحه اینترنتی که باز می‌کنید و یا متنی که روی سایتی قرار می‌دهید، در طول مسیر انتقال از وب‌سایت مربوطه به رایانه شما و برعکس، برای شرکت مخابرات، و دیگر سرورهای سر راه قابل رؤیت است. در ایران بیشتر سرویس‌دهندگان اینترنت و مدیران شبکه‌ها، فعالیت‌های شما را ردیابی کرده و بر آن نظارت می‌کنند.

از سوی دیگر، زمانی که از شبکه‌های بیسیم (Wifi) غیررمزگذاری شده استفاده می‌کنید، یا از جایی به اینترنت متصل می‌شوید که به‌طور اخص ردیابی و نظارت بر مکالمات انجام می‌شود تعداد بیشتری به فعالیت‌های اینترنتی‌تان دسترسی پیدا کرده، "رمزگذاری ارتباطات" حتی مهم‌تر هم می‌شود. رمزگذاری ارتباطات باعث حفظ حریم خصوصی‌تان شده، مانع نظارت دیگران بر فعالیت‌های‌تان شوید. این امر شامل ارتباطات از طریق دستگاه‌های هوشمند مانند گوشی تلفن همراه وتبلت نیز است.

شبکه Wifi

امروزه تقریبا همه از شبکه‌های بی‌سیم یا Wifi برای اتصال به اینترنت در خانه، محل کار یا مکان‌های عمومی استفاده می‌کنند. وسائل مختلف از قبیل رایانه قابل حمل، گوشی تلفن همراه و تبلت همگی امکان اتصال به این شبکه‌ها را دارند. ارتباط بی‌سیم به این معنی است که در محدوده پوشش شبکه، هرکسی می‌تواند به آن متصل شده، به رایانه‌های موجود در شبکه دسترسی پیدا کند. این یک حفره بزرگ امنیتی برای شماست. برای این منظور می‌بایست همیشه از ارتباط رمزگذاری شده برای اتصال به شبکه‌های Wifi استفاده کنید. معمولا رایانه شما هنگام اتصال به شبکه علامت یک قفل را کنار نام شبکه‌های رمزگذاری شده نمایش می‌دهد.
هنگام اتصال به شبکه‌هایی که اتصال رمزگذاری شده فراهم نمی‌کنند مواظب فعالیت‌های خود باشید. در این مواقع، به صفحه ایمیل خود سر نزنید و از حساب بانکی یا کارت اعتباری‌تان استفاده نکنید. در خانه نیز همیشه از ارتباط رمزگذاری شده استفاده کنید.
مطالعه بیشتر:

- ایمن‌سازی شبکه Wifi - ویدئوی آموزشی گوگل (انگلیسی)

امنیت در وب‌گردی

برخی وب سایت‌ها اطلاعات رد و بدل شده و صفحات‌شان را هنگام بازدید کاربران رمزگذاری می‌کنند. بدین ترتیب، دیگران نمی‌توانند ببینند که یک کاربر خاص چه مطلب از آن وب‌سایت را می‌خواند یا چه نوع فعالیتی در آن وب‌سایت انجام می‌دهد.
برای این‌کار می‌بایست از اعتبارنامه‌های اینترنتی استفاده کرد. اعتبارنامه اینترنتی ابزاری است که هویت واقعی فرستنده اطلاعات را مشخص کرده، معلوم می‌کند که آیا او واقعا کسی است که ادعا می‌کند. تنها مراکز بین‌المللی معتبر قادر به صدور اعتبارنامه هستند و به همین این دلیل می‌شود به آن اعتماد کرد. اعتبارنامه اینترنتی به کاربر امکان می‌دهد تا با وب‌سایت مربوطه به صورت رمزگذاری‌شده ارتباط برقرار کند. روش کار بدین صورت است که اطلاعات فرستاده شده، تنها توسط دارنده اعتبارنامه قابل رمزگشائی است، بنابراین از دسترس دیگران به دور می‌ماند. برای برقراری چنین ارتباطی به پروتکل اینترنتی خاصی به نام HTTPS نیاز است.

تمام اینترنت را یک شبکه پستی جهانی در نظر بگیرید. نامه از مبداء به مقصد، از مسیر دفاتر پست عبور می‌کند و پستچی‌ها نیز در این میان نامه را دست به دست خواهند کرد. هرکس در طی این مسیر می‌تواند پاکت نامه را باز کرده، متن آن را بخواند. حال روشی را در نظر بگیرید که نامه با کدهای خاصی رمزگذاری شده باشد که تنها برای فرستنده و گیرنده قابل رمزگشائی است. در این حالت، اگر کسی پاکت نامه را باز کند، از محتوای آن چیزی دستگیرش نخواهد شد.

وب‌سایت‌ها برای ارائه خدمات HTTPS می‌بایست از یکی از سازمان‌های معتبر ارائه کننده اعتبارنامه دیجیتالی، اعتبارنامه خریداری کنند. پس از آن، این اعتبارنامه به همراه امضای دیجیتالی آن وب‌سایت، به مرورگرها ابلاغ شده، مرورگر وب‌سایت مربوطه را با آن امضا خواهد شناخت. این فرآیند به صورت خودکار انجام می‌شود و شما لازم نیست برای آن کاری انجام دهید. از آن پس، مرورگرعلیه مکالمات امضا نشده با آن وب‌سایت اخطار امنیتی خواهد داد.
البته به یاد داشته باشید که استفاده از اعتبارنامه معتبر الزاما به معنی قابل اطمینان بودن یک وب‌سایت نیست. بلکه تنها می‌توان مطمئن بود که ارتباط میان شما و آن وب‌سایت برای دیگران قابل شنود نیست.

HTTPS از چه محافظت می‌کند؟

HTTPS اطلاعاتی که بین رایانه شما و یک سایت رد و بدل می‌شود را رمزگذاری می‌کند. در واقع، HTTPS هرچه شما به آن سایت می‌فرستید یا در آن مشاهده می‌کنید را از نظر دیگران مخفی می‌کند.

HTTPS از چه محافظت نمی کند؟

- نشانی وب‌سایتی که از آن بازدید می‌کنید را مخفی نمی‌سازد.
- اگر رایانه‌تان آلوده به جاسوس‌افزاری باشد که فعالیت‌های‌تان را رصد می‌کند، HTTPS نمی‌تواند جلوی آن را بگیرد و ممکن است اطلاعات حساسی از قبیل گذرواژه را که تایپ می‌کنید به سرقت ببرد.
- اگر وب‌سایت مربوطه هک شده باشد، HTTPS نمی‌تواند از اطلاعات شما که قبلا روی سرور آن سایت قرار گرفته بود محافظت کند.
- در مواردی، صاحبان سایتی که شما از آن استفاده می‌کنید (سرویس‌دهنده ایمیل یا شبکه اجتماعی)، بنا به قانون موظف به ارائه اطلاعات شخصی‌تان به مقامات دولتی هستند. شرکت‌هایی مثل گوگل و فیسبوک در کشورهایی که دفاتر رسمی دارند، در برابر درخواست‌های قانونی برای ارائه اطلاعات کاربران‌شان چنین عمل می‌کنند.
    - همینطور می‌توان از شبکه‌های اجتماعی و سرویس‌دهندگان وبلاگ در ایران نام برد. آنان نیز بنا به قوانین جمهوری اسلامی ملزم به در اختیار نهادن همه اطلاعات مربوط به کاربران‌شان به نهادهای امنیتی هستند.

تشخیص HTTPS

با مشاهده علائم زیر می‌توان از ارائه سرویس HTTPS توسط یک سایت اطمینان حاصل کرد:

- آدرس سایت با https:// شروع شود.
- پیش از آدرس وب‌سایت، مرورگرتان علامت یک قفل را قرار داده باشد.

اگر روی این قفل کوچک کلیک کنید، می‌توانید اطلاعات مربوط به اعتبارنامه امنیتی وب‌سایتی که از آن بازدید می‌کنید را به دست بیاورید. این اطلاعات شامل آدرس وب‌سایت، تاریخ صدور و انقضاء اعتبارنامه و روش رمزگذاری اطلاعات توسط HTTPS در این سایت می‌شود.

اعتبارنامه‌های جعلی

همان‌طور که پیشتر توضیح داده شد، اعتبارنامه‌ها می‌بایست از مراکز معتبر بین‌المللی خریداری شوند. در سال ۲۰۱۱، دو شرکت ارائه دهنده این اعتبارنامه‌ها مورد حمله هکرهای ایرانی قرار گرفت. بدین ترتیب، هکرها توانستند به اعتبارنامه‌های اصیلی دسترسی پیدا کنند که آنان را قادر می‌ساخت خود را جای وب‌سایت‌های معتبر دیگر جا بزنند. در نتیجه، آنان از حملات فیشینگی استفاده کردند که هیچ ابزار امنیتی یا فرد متخصصی قادر به تشخصی آن نبود. آنان توانستند با بازسازی صفحه ورودی GMail به سرقت گذرواژه‌های کاربران ایرانی دست بزنند.

البته پس از تشخیص این حمله توسط شرکت‌های مسئول، اعتبارنامه‌های دزدیده شده لغو و مرورگرها از ارائه خدمات به آن اعتبارنامه‌ها باز داشته شدند. با این‌که خطر این نوع حمله اکنون برطرف شده، اما همیشه احتمال تکرار آن در آینده وجود دارد. متأسفانه از کاربران معمولی اینترنت کاری در این زمینه بر نمی‌آید. HTTPS امن‌ترین راه ارتباط است و ما همه به آن وابسته‌ایم.

اما اگر در اخبار چیزی از هک شدن دوباره شرکت‌های ارائه‌دهنده اعتبارنامه امنیتی شنیدید، گوش‌های‌تان تیز شوند و هرچه زودتر، مرورگرتان را به روز رسانی کنید. به روزرسانی مرورگر باعث می‌شود که اعتبارنامه‌های جعلی بی‌اعتبار شده، در صورت وجود حمله به شما اخطار داده شود.

VPN چیست؟

VPN یا Virtual Private Network به کاربر امکان می‌دهد در محیط اینترنت از یک شبکه خصوصی مجازی برای وب‌گردی استفاده کند. یعنی، به جای استفاده از خدمات شرکت ارائه‌دهنده اینترنت، به صورت امن به سرور مشخصی که ممکن است در آن سوی دنیا باشد متصل شده، از خدمات آن استفاده کنید. بدین شکل، دیگر شرکت ارائه‌دهنده اینترنت، مخابرات یا مقامات دولتی قادر به شنود ارتباطات، یا فیلترکردن دسترسی شما به سایت‌ها و سرویس‌های اینترنتی نخواهند بود. VPN یکی از امن‌ترین راه‌های دسترسی به اینترنت است. با این حال، امنیت VPN بستگی دارد به اعتماد شما به سرویس‌دهنده آن. اگر یکی از دوستان خارج نشین‌تان، شرکت‌ها و سازمان‌های معتبر یا شرکت یا سازمانی که برای‌اش کار می‌کند سرویس VPN برای‌تان فراهم کرده باشد، این سرویس امن است.

به خاطر داشته باشید

در ایران گاه کدهای اتصال به شبکه‌های *VPN* دست به دست می‌شود، بدون آن‌که کسی بداند سرویس‌دهنده آن کیست. گاه این سرویس‌ها را سازمان‌های امنیتی، افراد سودجو یا هکرها راه‌اندازی می‌کنند تا به اطلاعات شخصی شما دسترسی پیدا کنند. اگر به سرویس‌دهنده *VPN* اعتماد داشته باشید، استفاده از آن امنیت ارتباطات‌تان را تا حد قابل ملاحظه‌ای افزایش خواهد داد. یکی از معتبرترین سرویس‌های *VPN* توسط *RiseUP VPN* ارائه می‌شود.

فرق بین VPN و HTTPS چیست؟

VPN کل ارتباط شما در اینترنت را از مجرائی جدا از ارائه‌دهنده‌ای که از طریق آن متصل شده‌اید فراهم می‌سازد. HTTPS ارتباط رمزگذاری‌شده‌ای میان شما و وب‌سایتی که از آن بازدید می‌کنید ایجاد می‌کند.

امنیت پست الکترونیک

امنیت سرویس‌های ایمیل آنلاین همچون دیگر وب‌سایت‌ها بستگی به رمزگذاری ارتباطات دارد. اگر از سرویس‌های ایمیل آنلاین (مانند هات‌میل، جی‌میل و امثال آن)استفاده می‌کنید، HTTPS امنیت ارتباطتان با سرور ارائه دهنده خدمات را تأمین می‌کند. در غیر این صورت، متن ایمیل‌ها در مسیر ارسال یا دریافت، قابل خواندن خواهد بود. اگر بین گیرنده و فرستنده یک ایمیل تنها یکی از HTTPS استفاده کند، متن ایمیل هنگام ارسال یا دریافت توسط طرف بدون HTTPS برای دیگران قابل رؤیت خواهد بود.

مثلاً اگر کسی از جی‌میل به یاهو ایمیل بفرستد، گیرنده ایمیل که از یاهو استفاده می‌کند، ارتباطش امن نیست و متن ایمیل قابل رؤیت خواهد بود. سرویس ایمیل جی‌میل، HTTPS را به صورت پیش‌فرض برای همه کاربران فعال ساخته است. بدین ترتیب، بدون نیاز به تنظیم خاص، کاربران جی‌میل می‌توانند با آرامش خیال بیشتر ایمیل‌های خود را چک کنند. ما نیز استفاده از این سرویس را به شما توصیه می‌کنیم. شما نیز می‌توانید از آشنایان و همکاران‌تان بخواهید که برای حفظ امنیت خود، از جی‌میل یا سرویس‌های مشابه که ارتباط امن برای کاربران‌شان فراهم می‌کنند استفاده کنند. **امنیت مکاتبه‌های ایمیلی‌تان زمانی تأمین می‌شود که کسانی که با آنان مکاتبه می‌کنید نیز موارد امنیتی را رعایت کنند.**

چند توصیه برای امن‌تر کردن جی‌میل:

- ✓ **ورود دو مرحله‌ای:** حتما از روش ورود دو مرحله‌ای برای دسترسی به حساب کاربری‌تان استفاده کنید. ورود دو مرحله‌ای به معنی استفاده از پیامک، یا ابزار مخصوص گوگل برای تلفن‌های هوشمند و تبلت در کنار استفاده از گذرواژه است؛ تا مشخص شود که حتما خود شما هستید که وارد می‌شوید. بدین ترتیب، اگر کسی به گذرواژه‌تان دسترسی پیدا کند، هنوز برای ورود به حساب کاربری به کدی که برای شما از طریق پیامک ارسال می‌شود یا در تلفن هوشمندتان از طریق ابزار گوگل دریافت می‌کنید نیاز خواهد داشت.
- ✓ **آخرین استفاده از حساب کاربری:** جی‌میل به کاربران خود امکان می‌دهد که آخرین استفاده از حساب کاربری‌شان را به همراه تاریخچه استفاده و اطلاعات مربوط به آن ملاحظه کنند. بدین‌ترتیب، کاربران می‌توانند از دسترسی دیگران به حساب کاربری‌شان باخبر شوند. شما می‌توانید در قسمت پایین، سمت راست صفحه ایمیل روی عبارت «Last account activity» کلیک کرده تا تاریخچه ورود به حساب کاربری‌تان را ملاحظه کنید. مثلا اگر کسی از مکان دیگری به‌جز خانه یا محل کارتان به ایمیل شما دسترسی پیدا کرده باشد در اینجا مشخص خواهد شد. البته این روش موارد استفاده از POP و IMAP، که در ابزارهای ایمیل‌خوان همچون MS Outlook یا Thunderbird استفاده می‌شود را نشان نخواهد داد. همچنین در نظر داشته باشید که در صورت استفاده از VPN، Proxy یا دیگر انواع فیلترشکن ممکن است اتصال شما به حساب کاربری‌تان از مکان‌هایی غیر از محل واقعی‌تان گزارش شود.

- ✓ **ارسال ایمیل به‌طور خودکار**: یکی از ابزارهای جی‌میل امکان ارسال خودکار ایمیل‌های دریافتی به آدرس ایمیل دیگری است. برای مثال، می‌توان جی‌میل را طوری تنظیم کرد که همه ایمیل‌های کاری‌تان را به‌طور خودکار به ایمیل شخصی‌تان ارسال کند. متأسفانه این امکان می‌تواند خود به یک تهدید امنیتی بدل گردد. اگر کسی بدون اجازه شما به حساب کاربری‌تان دسترسی پیدا کند، ممکن است ایمیل خود را در بخش تنظیمات قرار داده، از آن پس یک نسخه از هر آن‌چه شما دریافت می‌کنید برای او نیز ارسال خواهد شد. مقابله با این تهدید مشکل نیست. شما می‌بایست در بخش تنظیمات (settings) حساب جی‌میل‌تان، قسمت Forwarding and POP/IMAP را چک کرده از صحیح بودن تنظیمات آن مطمئن شوید. ما توصیه می‌کنیم، هر از گاهی این بخش را دوباره بازرسی کنید.
- ✓ **بایگانی چت**: جی‌میل و بسیاری دیگر از سرویس‌های چت اینترنتی، گپ‌های اینترنتی را بایگانی می‌کنند. اگر نیازی به بایگانی نباشد، بهتر است این امکان را غیر فعال کنید. در قسمت Setting با انتخاب Never Save Chat History می‌توانید این کار را انجام دهید.

رمزگذاری متن ایمیل

رعایت نکات بالا به شما کمک می‌کند تا امنیت ارتباطات ایمیلی‌تان را بالا ببرید. بدین ترتیب، شنود ارتباطات برای نفوذگران مشکل‌تر خواهد شد. با این حال، متن اصلی ایمیل‌تان کماکان متن خامی است؛ برای همه قابل خواندن. مثلا، اگر نفوذگران موفق شوند به حساب کاربری‌تان دسترسی پیدا کنند، یا اگر آن سوی خط، طرف مکاتبه شما، موارد امنیتی را به‌طور کامل رعایت نکرده باشد و هکرها بتوانند به حساب کاربری‌اش نفوذ کنند، آن‌گاه متن مکاتبات‌تان قابل رؤیت است.

به خاطر داشته باشید

هرچند این روش رمزگذاری معتبرترین روش مرسوم رمزگذاری است، اما نمی‌تواند در موارد زیر از شما محافظت کند:

- کلید خصوصی به هر شکلی لو رفته باشد.
- اگر متن ایمیل، پیش یا پس از رمزگذاری شنود شده باشد. مثلا، اگر در رایانه فرستنده یا گیرنده(گان) ایمیل جاسوس‌افزاری برای تصویربرداری از صفحه مانتیور یا ثبت فعالیت صفحه‌کلید نصب شده باشد.

در این موارد، راه محافظت از مکاتبات ایمیلی استفاده از رمزگذاری متن ایمیل است. از این طریق، متن ایمیلی که ارسال می‌کنید، تنها و تنها برای شخص گیرنده ایمیل که کلید رمزگشائی آن را در دست دارد قابل خواندن خواهد بود. روش کار ساده است. با کمک ابزارهای مخصوص، هرکس برای خود دو کلید رمزگذاری تهیه می‌کند. یکی کلید خصوصی و دیگری کلید عمومی. کلید خصوصی را به هیچ وجه نباید در اختیار کس دیگری قرار دهید. کلید عمومی را می‌بایست به کسانی داد که می‌خواهند برای‌تان ایمیل رمزگذاری شده بفرستند؛ در بخش امضای ایمیل، روی کارت ویزیت، صفحه وبلاگ شخصی و غیره. اگر ایمیلی توسط کلید عمومی که شما در اختیار دیگران قرار می‌دهید رمزگذاری شود، تنها و تنها یک نفر قادر به رمزگشائی آن است. آن شخص شما هستید که کلید خصوصی را در اختیار دارید. شما نیز برای ارسال ایمیل رمزگذاری شده به دیگران به کلید عمومی آنها نیاز دارید.

برای استفاده از رمزگذاری کلید-عمومی یا رمزگذاری نامتقارن، می‌بایست از نرم‌افزارهای ایمیل همچون Thunderbird و افزونه‌های مربوطه استفاده کنید. روش نصب و راه‌اندازی این ابزارها را می‌توانید از طریق لینک‌های زیر بیاموزید:

- چگونه Thunderbird را دانلود و نصب کنید؟ (فارسی)
- چگونه ایمیل‌تان را در Thunderbird اضافه کنید؟ (فارسی)
- چگونه GPG را دانلود و نصب کنید؟ (فارسی)
- چگونه Enigmail را دانلود و نصب کنید؟ (فارسی)
- چگونه Public Key و Private Key ایجاد کنید؟ (فارسی)
- ایمیل امن - شیوه نصب و راه‌اندازی Thunderbird، Enigmail و OpenGPG در ویندوز (انگلیسی)
- استفاده از PGP در سامانه‌های مک (انگلیسی)

امنیت چت (گپ اینترنتی)

چت یا گپ اینترنتی یکی از ابزارهای پرطرف‌دار ارتباط از طریق اینترنت است. متأسفانه تنها تعداد معدودی از سرویس‌دهندگان گپ اینترنتی از رمزگذاری ارتباط برای سرویس خود استفاده می‌کنند. بدین ترتیب، بیشتر گپ‌های اینترنتی ناامن است. از آن بدتر این‌که برخی از ابزارهای ارتباط آنلاین، همچون Skype، تاریخچه گپ‌های اینترنتی‌تان را در پرونده‌ای ذخیره می‌کنند که به راحتی قابل دسترس و خواندن است.

یک راه امن برای برقراری ارتباط از طریق گپ اینترنتی، استفاده از برنامه Pidgin است. این برنامه، امکان برقراری ارتباط از طریق حساب‌های کاربری موجود، همچون Yahoo، Gmail و غیره را به شیوه‌ای امن فراهم می‌سازد. Pidgin افزونه‌ای دارد به نام OTR که کاربر را قادر می‌سازد با دیگر کاربران ارتباط امن رمزگذاری شده برقرار کند.

ما نیز این سرویس را برای برقراری ارتباط امن به شما توصیه می‌کنیم.
روش نصب و راه‌اندازی Pidgin و افزونه مربوطه را از طریق لینک زیر بیاموزید:

- ارسال پیامک به شیوه امن - راهنمای نصب و راه‌اندازی Pidgin با افزونه OTR در ویندوز (انگلیسی)
- استفاده از OTR در سامانه‌های مک (انگلیسی)
- استفاده از OTR در سامانه‌های ویندوز (انگلیسی)

نکته: ارتباط شما امن خواهد بود اگر همه طرفین ارتباط نکات ایمنی را در نظر گرفته باشند. از مهم‌ترین این نکات می‌توان به برقراری ارتباط رمزگذاری شده و پاک کردن تاریخچه گپ اینترنتی توسط همه طرفین اشاره کرد.

امنیت مکالمات اینترنتی

Voice Over Internet Protocol پروتکل اینترنتی است که امکان برقراری ارتباط صوتی/تصویری از طریق اینترنت را فراهم می‌سازد. با فن‌آوری موجود، سطح امنیت این پروتکل پایین‌تر از امنیت ارتباط متنی رمزگذاری شده است. بدین ترتیب، هنگام برقراری مکالمات صوتی، تصویری، همیشه امکان شنود مکالمه وجود دارد، هرچند با در نظر گرفتن تدابیری می‌توان سطح امنیت مکالمات را افزایش داد.

Skype ابزار بسیار پرطرفدار برقراری ارتباط صوتی/تصویری از طریق اینترنت است. اما با وجود ادعای این شرکت مبنی بر رمزگذاری ارتباطات، از آن‌جا که کد این برنامه باز نیست، امکان بازبینی بی‌طرفانه آن وجود ندارد. مشکل دیگر این‌که نسخه‌های هک شده این نرم‌افزار از طریق سی‌دی دست به دست شده یا از طریق وب‌سایت‌های دیگر هم‌رسانی می‌شود. این نسخه‌ها قابل اعتماد نیستند و احتمال دارد که روی آن جاسوس‌ابزاری نصب شده باشد که به مقامات امکان شنود مکالمات‌تان را بدهد.
توصیه ما این است که در صورت استفاده از Skype حتما نرم‌افزار آن را از وب‌سایت اصلی به نشانی:http://www.skype.com بارگیری و نصب کنید. ممکن است در مواردی سایت Skype فیلتر شده باشد. در این صورت از فیلترشکن مناسب برای دسترسی و بارگیری Skype استفاده کنید. این هشدار ایمنی در مورد نسخه‌های موبایل و تبلت Skype نیز صادق است.

Jitsi ازمعدود ابزارهای ارتباط صوتی/تصویری از راه اینترنت است که از رمزگذاری مکالمات استفاده می‌کند و کد آن به‌صورت مستقل بازبینی شده. Jitsi، امکان اجرا روی سیستم‌ها مختلف از جمله، ویندوز، مک و گنو لینوکس را دارد. شما می‌توانید با حساب کاربری بسیاری از سرویس‌دهنده‌های گپ اینترنتی، از جمله، Google Talk، Yahoo و غیره از Jitsi استفاده کنید. فایده استفاده از Jitsi این است که با این کار یک لایه امنیتی اضافه به حساب کاربری‌تان افزوده می‌شود. همان‌طور که پیشتر گفته شد، بسیاری از سرویس‌های گپ اینترنتی و تقریبا همه سرویس‌های ارتباط صوتی/تصویری اینترنتی نا امن و رمزگذاری نشده هستند. Jitsi حین استفاده از همان سرویس‌ها، ارتباط میان دو طرف را رمزگذاری می‌کند. البته این وقتی صورت می‌گیرد که همه طرفین ارتباط از Jitsi استفاده کنند. بدین ترتیب، مکالمات و گپ همه رمزگذاری‌شده انجام خواهند شد و حتی شرکت‌های ارائه دهنده خدمات، یعنی، گوگل، یاهو، مایکروسافت و غیره نیز قادر به رمزگشائی مکالمات شما نخواهند بود.

برای کسب اطلاعات بیشتر در مورد این ابزار و روش نصب و راه‌اندازی آن، لینک‌های زیر را توصیه می‌کنیم:

- راهنمای بارگذاری، نصب و استفاده از Jitsi در وب‌سایت امنیت در یک جعبه (انگلیسی)
- همه اطلاعات پیرامون Jitsi در سایت بی‌خوف (فارسی)

بیشتر بخوانید:

مقایسه سطح امنیت ابزارهای مکالمه اینترنتی (انگلیسی)

تلفن همراه و تلفن و دستگاه‌های هوشمند

تلفن همراه

امروزه، گوشی تلفن همراه وسیله‌ای رایج برای مکالمه و ارتباط میان مردم است. تلفن‌های همراه امکان برقراری ارتباط صوتی و متنی (پیامک) را فراهم می‌سازند. اما این وسائل قابل حمل، امکانات دیگری نیز دارند که ممکن است به تهدید امنیتی علیه شما تبدیل شود.

تلفن همراه، به‌طور خودکار و برای استفاده از خدمات شبکه‌های مخابراتی، مرتباً مکان خود را به شرکت مخابرات گزارش می‌دهد. این بدان معنی است که اگر شما تحت نظر باشید، افرادی که به امکانات شبکه تلفن همراه دسترسی داشته باشند می‌توانند مکان شما را پیدا کنند؛ حتی اگر دستگاه تلفن همراه خاموش باشد، هنوز مکان شما را گزارش می‌دهد. از سوی دیگر، برخی از دستگاه‌های تلفن همراه را می‌توان از راه دور به گونه‌ای فعال ساخت که به نظر خاموش بیاید. بدین ترتیب، دستگاه به وسیله‌ای برای شنود مکالمات در محدوده میکروفون آن تبدیل می‌شود.

همه مکالمات و مکاتبات (پیامک‌ها) توسط تلفن همراه قابل شنود و ناامن است. تا به امروز، روش قابل اطمینانی برای برقراری ارتباط امن و رمزگذاری شده با تلفن همراه در دسترس عموم نیست.

اپراتورهای تلفن همراه و کسانی که به امکانات آن دسترسی داشته باشند، می‌توانند شما را از طریق شماره تلفن همراه، شماره سیم‌کارت و شماره دستگاه تلفن همراه شناسائی کنند. هنگام برقراری ارتباط توسط تلفن همراه، همه این اطلاعات به اپراتور فرستاده شده و در پایگاه داده آن به نام شما ثبت می‌شود.

اگر در جلسه‌ای شرکت می‌کنید که می‌بایست مخفی بماند، بهترین کار این است که تلفن همراه‌تان را در مکان امنی، غیر از محل جلسه، خاموش کرده، باتری آن را در بیاورید و همان‌جا رها کنید. بهتر است آن را تا پس از بازگشت از جلسه روشن نکنید. طبیعی است که دیگر شرکت‌کنندگان نیز می‌بایست همین کار را انجام دهند.

برای مطالعه بیشتر پیراون امنیت تلفن همراه، مطلب زیر را به شما توصیه می‌کنیم: استفاده امن‌تر از تلفن همراه (انگلیسی)

تلفن و دیگر دستگاه‌های هوشمند

تلفن هوشمند ابزاری است که کم‌کم جای خود را در کنار دیگر دستگاه‌های هوشمند مانند انواع تبلت‌ها در میان وسائل شخصی‌مان باز کرده. همه مطالبی که در این فصل پیرامون تلفن هوشمند ارائه می‌شود، در مورد دیگر دستگاه‌های هوشمند نیز صادق بوده، بهتر است که در نظر گرفته شوند.

تلفن هوشمند در واقع دستگاه رایانه بسیار قدرتمند و فشرده‌ای است که امکان برقراری تماس تلفنی را در کنار دسترسی به اینترنت، ضبط صدا و تصویر و اعلام مکان دقیق خود ارائه می‌دهد. مجموعه این امکانات کاربر را قادر می‌سازد همه‌جا و همه وقت به گستره عظیمی از اطلاعات، خدمات و ابزارهای ارتباطی دسترسی پیدا کرده، حتی خود تبدیل به ماشین تولید اطلاعات گردد. شهروند-خبرنگاران همه روزه موارد نقض حقوق شهروندان و دیگر مسائل مهم را توسط دوربین‌های تلفن هوشمندشان ضبط و در شبکه‌های اجتماعی منتشر می‌کنند. خانواده‌ها با کمترین هزینه، توسط برنامه‌های ارتباط متنی، VoIP و غیره با عزیزان‌شان در آن سوی جهان در تماس هستند و بنگاه‌های تجاری همه روزه بهترین خدمات را به ساده‌ترین شکل از طریق تلفن‌های همراه به مشتریان‌شان ارائه می‌کنند.

از سوی دیگر، همین امکانات گستره تازه‌ای از تهدیدها را با خود به همراه آورده. مکان‌تان در هر لحظه با خطای کمتر از یک متر ثبت (و می‌تواند گزارش شود)، صدا و تصویرتان با بهترین کیفیت قابل شنود است و اطلاعات خصوصی‌تان بدون اجازه و حتی آگاهی‌تان در اختیار بنگاه‌های خصوصی و مقامات دولتی قرار می‌گیرد. تلفن هوشمند قادر است به آسان‌ترین شکل اطلاعات حساب‌های شخصی خود و آشنایان‌تان را در اختیار دیگران بگذارد. از این رو، امنیت تلفن همراه از اهمیت بسیار برخوردار است؛ هم امنیت فیزیکی و هم دیجیتالی.

امنیت فیزیکی

سرقت هر وسیله‌ای از آدم، تجربه سختی است، اما سرقت تلفن هوشمند نه تنها یک ضرر مالی بلکه تهدیدی بالقوه خطرناک علیه شخص شما یا فعالیت‌های‌تان نیز به شمار می‌رود. کمی به این موضوع فکر کنید، چه اقلامی در تلفن هوشمندتان ممکن است پیدا شود:

- عکس و فیلم های خصوصی از دوستان و آشنایان.
- دسترسی مستقیم به همه ایمیل‌ها، شبکه‌های اجتماعی و ابزارهای ارتباطی همچون واتس‌آپ و اسکایپ و سوابق ارتباطات از آن.
- دفترچه تلفن الکترونیکی، شامل شماره تلفن‌های تماس، ایمیل و آدرس اشخاص.
- دسترسی به حساب بانکی، و دیگر حساب‌های کاربری مهم.
- و غیره.

بدتر آن‌که تلفن همراه، دسترسی به این اقلام را به صورت تعاملی و پویا برقرار می‌کند که از این نظر، حتی می‌تواند خطرناک‌تر از گم شدن یا به سرقت رفتن کلید منزل یا کیف پول باشد.
پس امنیت فیزیکی تلفن هوشمند بسیار مهم است. شما به هیچ وجه نمی‌بایست تلفن هوشمندتان را از خود دور کرده، یا به دست غریبه‌ها بدهید. علاوه بر این، شما می‌بایست از گذرواژه‌های مناسب برای دسترسی به تلفن هوشمندتان استفاده کنید و این گذرواژه را با هیچ‌کس در میان نگذارید. توصیه‌های ما برای تولید، و محافظت از گذرواژه خوب و غیرقابل حدس‌زدن اینجا هم صدق می‌کند.

اگر اطلاعات حساسی روی دستگاه تلفن هوشمندتان وجود دارد، شاید بهترین کار رمزگذاری همه اطلاعات موجود روی گوشی تلفن هوشمند باشد. برای این‌کار، گوشی شما می‌بایست نخست ROOT شده باشد. پس از آن با نصب و راه‌اندازی LUKS Manager می‌توانید به سادگی همه محتوای گوشی‌تان را رمزگذاری کنید.
بیشتر بخوانید: چگونه محتوای iPhone تان را رمزگذاری کنید (انگلیسی)

امنیت دیجیتالی

همان‌طور که پیشتر اشاره شد، تهدیدها علیه تلفن هوشمند ممکن است از راه دور و از طریق شبکه مخابرات یا اینترنت عمل کند. تهدیدها علیه تلفن هوشمندتان ممکن است از منابع مختلف اعمال شوند، مهم‌ترین منابع تهدید عبارت است از:

سیستم‌عامل تلفن همراه

تلفن همراه نیز مانند دیگر رایانه‌ها برای کار به سیستم‌عامل نیاز دارد. معروف‌ترین سیستم‌عامل‌های موجود عبارتند از Android، iOS و Windows. در این میان، Android به دلیل کد-باز و مجانی بودن در ایران بسیار طرفدار دارد و اکثر تلفن‌های هوشمند از آن استفاده می‌کنند. شرکت‌های تولیدکننده تلفن و همچنین شرکت‌های ارائه‌دهنده خدمات تلفن همراه، معمولا کد سیستم‌عامل تلفن‌های همراه را پیش از فروش به کاربر دستکاری می‌کنند تا بر مبنای منافع و سیاست‌های تجاری - امنیتی‌شان، برخی امکانات سیستم‌عامل را غیرفعال کرده یا ابزارهای مورد نظرشان را به آن اضافه کنند. از جمله این ابزارها می‌تواند ابزارهای شنود مکالمات باشد. اخیرا در ایران افشا شد که شرکت‌های همراه اول و ایرانسل بدون اجازه مشترکان‌شان، چنین ابزارهایی را روی تلفن‌های هوشمند نصب می‌کنند.

بیشتر بخوانید: سرقت اطلاعات مشترکان توسط اپراتورهای تلفن همراه در ایران (فارسی)

از سوی دیگر، سیستم‌عامل‌های قفل‌شکسته آی‌فون و ویندوز نیز خطرات خود را دارند. این نرم‌افزارها معمولا از مجاری غیرقابل اعتماد به دست می‌آیند. همیشه به یاد داشته باشید که کسی که قفل یک نرم‌افزار را می‌شکند قادر است تغییرات مورد نظرش را در آن اعمال کرده بدون این‌که ردی از خود برجای بگذارد.

یک راه مقابله با این مشکل نصب نسخه‌های جایگزین اندروید است که توسط ناظران بین‌المللی امنیت مورد تأیید قرار گرفته‌اند. برای مثال می‌توان از CyanogenMod نام برد. CyanogenMod نسخه تقویت‌شده‌ای از سیستم‌عامل اندروید است که با نصب آن روی دستگاه هوشمندتان می‌توانید از شر دستکاری‌های شرکت‌های تولیدکننده تلفن همراه و اپراتورهای موبایل راحت شوید. در ضمن، CyanogenMod یک سیستم VPN نیز با خود دارد که می‌تواند به شما برای وب‌گردی‌های امن و دور زدن فیلتر کمک کند. از طریق این صفحه می‌توانید چک کنید که آیا این سیستم‌عامل قابل نصب شدن روی دستگاه هوشمندتان است یا خیر. ما به‌طور اکید توصیه می‌کنیم که حتما این سیستم‌عامل را خودتان یا شخصی که به او اعتماد کامل دارید از وب‌سایت اصلی بارگیری کند، نسخه‌هایی که در سی‌دی‌ها ممکن است دست به دست بگردد یا در فروشگاه‌ها به فروش برسند قابل اعتماد نیست.

نرم‌افزارهای نصب شده روی تلفن همراه

دیگر منبع اصلی تهدید علیه امنیت تلفن همراه، نرم‌افزارهایی است که روی آن نصب می‌کنید. این نرم‌افزارها به دو دلیل اصلی ممکن است منبع خطر باشند:

۱. **نرم‌افزارهای قفل شکسته**. همانند سیستم‌عامل، نرم‌افزارهای قفل شکسته نیز در معرض انواع بدافزارها و جاسوس‌افزارها هستند. فراموش نکنید که هیچ چیز مجانی به دست نمی‌آید، مخصوصا اگر قفل‌شکسته باشد. در ایران به دلیل تحریم‌ها گاه دسترسی و استفاده از نرم‌افزارها، حتی اگر مجانی نیز باشند، با مشکل روبرو است و این امر کاربران را تشویق به استفاده از نرم‌افزارهای قفل‌شکسته که از طریق دیگر وب‌سایت‌ها قابل دسترس است یا حتی خرید نرم‌افزار (مجانی) از فروشگاه‌های سی‌دی‌فروشی می‌کند. هرچند مدتی است که شرکت گوگل برای کاربران در ایران امکان بارگذاری نرم‌افزارهای مجانی را فراهم ساخته، راه‌حل دیگر می‌تواند استفاده از نرم‌افزاری به نام F-Droid باشد. F-Droid کاربران را قادر می‌سازد تا نرم‌افزارهای مجانی کد-باز را پیدا، بارگذاری و نصب کنند. البته می‌بایست همیشه در ذهن داشته باشید که کد-باز بودن نشانه‌ای برای قابل اعتماد بودن نرم‌افزارها نیست و می‌بایست هنگام نصب هر نرم‌افزار تازه‌ای از این موضوع اطمینان حاصل کرد.

۲. **نرم‌افزارهایی که کارکردی غیر از آن‌چه ادعا می‌کنند دارند**. هرچند سیستم‌های اپل و اندروید به منظور نظارت بهتر بر تولید و ارائه نرم‌افزارها (Appها) نصب آن را منوط به استفاده از فروشگاه‌های آنلاین خود می‌کنند، با این حال، این نظارت خالی از اشکال هم نیست. خوشبختانه، سیستم‌عامل‌های اندروید و اپل به کاربر امکان می‌دهد که سطح دسترسی نرم‌افزارها را به امکانات تلفن هوشمندشان تعیین کنند. مثلا، شما می‌توانید دسترسی واتس‌آپ را به اطلاعات دفترچه تلفن موبایل‌تان ببندید تا این app اطلاعات تماس موجود در آن را به شرکت واتس‌آپ نفرستد. توصیه ما این است که اگر نرم‌افزاری قصد دسترسی به امکاناتی را داشته باشد که بی‌مورد به نظر می‌رسد از آن نرم‌افزار استفاده نکنید. مثلا، اگر یک app خبرخوان قصد دسترسی به مکان جغرافیائی شما یا دفترچه تلفن‌تان را داشته باشد، آن را از گوشی تلفن همراه‌تان پاک کنید.

۳. **سهل‌انگاری و بی‌دقتی در استفاده از امکانات دستگاه هوشمند**. تلفن‌های هوشمند امکانات بسیار متنوعی ارائه می‌کنند که همان‌طور که اشاره رفت ممکن است در مواقعی به تهدید بدل شوند. برای مثال، بسیاری از شبکه‌های اجتماعی مکان شما هنگام ارسال مطلب به آن شبکه‌ها را آشکار می‌کنند. دوربین تلفن‌های همراه، نمونه دیگری از ابزارهایی است که مکان کاربر را آشکار می‌کند. معمولا، هنگام عکس‌برداری یا فیلم‌برداری توسط تلفن همراه، مکان گرفته شدن عکس و فیلم نیز ذخیره می‌شود. در برخی مواقع این امکان ممکن است یک خطر امنیتی به حساب بیاید. برای مثال، اگر در جلسه یا مهمانی عکس گرفته باشید ممکن است مکان برگزاری آن از این طریق لو برود.

همچنین، برخی ابزارهای ارتباطی مانند اسکایپ ممکن است به‌طور خودکار جواب دهند. در این صورت، اگر کسی به اسکایپ شما زنگ بزند، تلفن همراه بدون اجازه شما ارتباط را برقرار کرده، صدا و تصویر محیط را ارسال می‌کند. همیشه به بخش حریم خصوصی (privacy) دستگاه هوشمند خود سر بزنید و وضعیت تنظیمات آن را چک کنید. در این بخش می‌توانید تصمیم بگیرید که چه برنامه‌هایی می‌توانند به دفترچه تلفن، مکان جغرافیایی، میکروفن و دوربین دستگاه‌تان دسترسی داشته باشد. به appهای نصب شده، بیش از آن‌چه نیاز دارند دسترسی ندهید.

مطالعه بیشتر:

- مبانی امنیت در گوشی‌های اندروید.
- ANDROID PRIVACY GUARD، ابزاری برای رمزگذاری ایمیل‌ها و پرونده‌ها در گوشی‌های اندروید.

ارتباط از طریق اینترنت ارائه شده روی تلفن همراه (3G و غیره)

به‌طور کلی می‌توان گفت استفاده از شبکه‌های Wifi امن و مورد اعتماد از امنیت بالاتری برخوردار است، زیرا ردپایی که به‌طور مستقیم به شما مرتبط شود از خود برجای نمی‌گذارد؛ البته اگر موارد امنیتی را رعایت کرده باشید. پروتکل‌های شبکه‌های موبایل ممکن است توسط شرکت‌های مختلف با سیاست‌ها و نیازهای تجاری و سیاسی‌شان منطبق شده باشد که از چشم مشترکان به دور می‌ماند. این بدان معنی است که شرکت‌های مخابراتی متناسب با سیاست‌های تعیین شده ممکن است امکان دسترسی و نظارت بر ارتباطات کاربران را برای نهادهای دیگر فراهم سازند.

ما نصب و استفاده از دو نرم‌افزار OrBot و OrWeb را برای افزایش سطح امنیت ارتباطات از طریق تلفن هوشمند و مخفی ماندن از چشم پایشگران، به شما توصیه می‌کنیم.

بیشتر بخوانید:

- شیوه نصب و راه‌اندازی OrBot (انگلیسی)
- شیوه نصب و راه‌اندازی OrWeb (انگلیسی)

شبکه‌های Wifi ناامن

تمام موارد امنیتی که در مورد رایانه‌ها و اتصال آن‌ها به اینترنت مطرح شد، در مورد دستگاه‌های هوشمند نیز صدق می‌کند. هنگام استفاده از شبکه‌های Wifi در مکان‌های عمومی، همیشه مواظب اطلاعات رد و بدل شده از گوشی تلفن هوشمندتان باشید. بسیاری از appهای نصب شده روی گوشی، از پروتکل‌های امن برای ارتباط استفاده نمی‌کنند، در ضمن ممکن است نفوذگرانی که در کافه‌های اینترنتی، فرودگاه‌ها و دیگر مکان‌های عمومی به کمین نشسته‌اند به اطلاعات تلفن همراه یا ارتباطات شما دسترسی پیدا کنند.

شنود ابزارهای مکالمه و پیامک، همچون واتس‌آپ، وایبر، اسکایپ و غیره

به عنوان یک قاعده کلی می‌بایست فرض را بر این بگذارید که هیچ‌کدام از ابزارهای ارتباطی، پیامک، صوتی یا تصویری امن نیستند، به‌خصوص روی گوشی تلفن هوشمند. در ایران، واتس‌آپ و وایبر از محبوبیت بسیار برخوردار هستند. هنگام استفاده از این ابزارها توجه داشته باشید که ارتباط صوتی (تلفنی) رمزگذاری شده نیست و قابل شنود است. ارتباط متنی نیز امن و قابل اطمینان نیست. یک نکته مهم در استفاده از چنین سرویس‌هایی، ارسال پیام به گروه است. توجه داشته باشید که این روش گاه ممکن است همه اعضای گروه را به خطر بیاندازد. حکومت جمهوری اسلامی و سپاه پاسداران با استفاده از طرحی به نام عنکبوت، سعی در شناسائی کنشگران در شبکه‌های اجتماعی و گروه‌های آنلاین دارند. رعایت نکات ایمنی می‌تواند شما و دیگر دوستان‌تان را تا حد زیادی محفوظ نگاه دارد.

یک توصیه به دارندگان دستگاه‌های هوشمند، استفاده از VPNهای امن است. توجه داشته باشید که امروزه سرویس‌های متنوع VPN در ایران وجود دارد، اما همه آن‌ها امن و قابل اعتماد نیستند. برخی از این سرویس‌ها توسط نهادهای امنیتی/نظامی برای شناسائی کنشگران اینترنتی و آنلاین راه‌اندازی و ارائه شده‌اند، هرچند ممکن است این‌طور به نظر نرسد. RiseUp یکی از سرویس‌های امن VPN در جهان است.

مطالعه بیشتر در این زمینه:

- چگونه از گوشی تلفن همراه به شیوه‌ای امن، خصوصی و آزاد استفاده کنیم؟ (انگلیسی)
- آیا برنامه WhatsApp قابل هک شدن است؟ (فارسی)
- تا حد امکان از تلفن‌های هوشمند به شیوه‌ای امن استفاده کنید (انگلیسی)
- Signal ابزاری نسبتا امن برای ارسال پیامک و ارتباط تلفنی توسط گوشی‌های اندروید (انگلیسی)
- Signal معادل اپل RedPhone است که امکان ارتباط با آن را نیز فراهم می‌کند.
- نصب و راه‌اندازی Signal (انگلیسی)
- نصب و راه‌اندازی ChatSecure، ابزار ارسال پیامک برای گوشی‌های آی‌فون و اندروید (انگلیسی)
- CSipSimple، ابزار بسیار قدرتمند با امنیت نسبتا بالا برای اندروید است. مکالمات از طریق این نرم‌افزار به‌طور کامل رمزگذاری‌شده‌اند.

به‌کارگیری آن‌چه آموخته‌اید

خوب، تا بدین‌جا با انواع تهدیدها در دنیای ارتباطات مجازی و برخی راه حل‌ها برای مقابله با آن آشنا شدید. حال وقت آن رسیده تا ببینیم در عمل کدام راه حل‌ها گزینه مناسب را فراهم کرده، چه سبک رفتاری متضمن تأمین امنیت شما در دنیای مجازی است.

HTTPS

پیشتر اشاره شد که HTTPS صفحه‌های اینترنتی را رمزگذاری می‌کند تا دیگران به محتوای آن‌چه در محیط وب انجام می‌دهید دسترسی پیدا نکنند. اما همه وب‌سایت‌ها این سرویس را ارائه نمی‌کنند. یک راه‌حل خوب در این زمینه استفاده از افزایه HTTPS Anywhere است. این افزایه قابلیت نصب در مرورگرهای گوگل کروم، فایرفاکس و اوپرا را دارد و به کاربر امکان می‌دهد تا همیشه نسخه رمزگذاری شده وب‌سایت‌ها را مشاهده کند. این ابزار به‌طور خودکار لینک‌ها به صفحات دیگر را چک کرده به نسخه رمزگذاری شده تبدیل می‌کند.
بیشتر بخوانید: HTTPS Anywher (انگلیسی)

حساب کاربری

پیشتر در مورد اهمیت محافظت از حساب کاربری از طریق تولید و حفاظت از گذرواژه‌های مناسب صحبت کردیم. حال به روش‌های عملی آن می‌پردازیم. گذرواژه خوب باید پیچیده باشد و تکراری نباشد. یعنی شما می‌بایست تعداد زیادی گذرواژه تولید کنید و همه آن را نیز به خاطر بسپارید. در ضمن، بهتر است هر چند وقت یکبار گذرواژه‌ها را تغییر دهید. چگونه همه این کارها را می‌توان انجام داد؟

روش تولید گذرواژه مناسب

یک روش خوب برای تولید گذرواژه پیچیده‌ای که خودتان به سادگی به خاطر بیاورید، استفاده از عباراتی است که برای شما خاطره برانگیز است، اما دیگران از آن خبر ندارند. بخشی از یک شعر یا ضرب‌المثل، نقل قولی از بزرگان، کلماتی طنزآمیز یا ترکیبی از لغات که ممکن است برای دیگران بی معنا به نظر برسد. مثلا: baniadamazayehamand.

راه‌هایی وجود دارد که این گذرواژه را پیچیده‌تر کرد. برای مثال می‌توانید از ترکیب حروف کوچک و بزرگ استفاده کنید، یعنی: BaniaDaMaZAyehamanD. یک مرحله پیچیده‌تر استفاده از نشانه‌هاست: B@n!aDaMaZ4y€hamand. حتی می‌توان گذرواژه‌های بسیار پیچیده‌ای تولید کنید که از ترکیب عباراتی از زبان‌های مختلف عربی، فارسی (فینگلیشی)، ترکی و .. ساخته شده‌اند. هدف آن است که گذرواژه‌ای ساخته شود که برای خودتان به یادماندی و برای دیگران غیر قابل حدس زدن باشد.

دست آخر، تعداد حساب‌های کاربری روز به روز درحال افزایش است و با فرض این‌که هر چندوقت یک‌بار می‌بایست گذرواژه‌ها را تغییر داد، به خاطر سپردن همه این عبارات کار ساده‌ای نیست. اما خوشبختانه برای آن راه حل‌هایی وجود دارد. ابزارهایی هستند که به شما را در مدیریت گذرواژه‌ها کمک می‌کنند؛ یعنی گذرواژه حساب‌های کاربری‌تان را به تفکیک و به صورت رمزگذاری شده نگهداری کرده، در ساخت گذرواژه‌های پیچیده به شما یاری می‌رساند.

یک نمونه کارآمد از این‌گونه ابزارها، KeePass نام دارد. KeePass نرم‌افزاری مجانی و کد-باز است که برای مدیریت حساب‌های کاربری ساخته شده. این ابزار را می‌توان روی سیستم‌های گوناگون رایانه، و دستگاه‌های هوشمند نصب کرد و ما نیز برای مدیریت حساب‌های کاربری استفاده از آن را به شما توصیه می‌کنیم.

برای مطالعه بیشتر درباره این نرم‌افزار، نحوه نصب، راه‌اندازی و کاربرد آن لینک‌های زیر را مطالعه کنید:

- راهنمای نصب KeePass روی سیستم‌های ویندوز (انگلیسی).
- KeePass برای گوشی‌های اندروید (انگلیسی).
- کاربرد KeyPass (انگلیسی).
- راهنمای نصب و اجرای KeePass (فارسی).
- گذرواژه (انگلیسی).
- استحکام گذرواژه (انگلیسی).
- شکستن گذرواژه (انگلیسی).

ورود دو مرحله‌ای

در صورتی که سرویس‌دهنده ایمیل، یا شبکه اجتماعی امکان ورود دو مرحله‌ای را فراهم سازد، حتما از آن استفاده کنید. در حال حاضر، جی‌میل، فیس‌بوک و دراپ‌باکس این امکان را فراهم می‌کنند. توجه داشته باشید که ورود دو مرحله‌ای سعی در حصول اطمینان از عدم دسترسی دیگران به حساب کاربری شما دارد. اما در گذشته نفوذگران با گول زدن افراد کد دوم را که از طریق تلفن همراه ارسال می‌شود را به دست آورده و وارد حساب کاربری افراد شده‌اند.

بیشتر بخوانید: هکرها تلفن می زنند، لطفا فریب نخورید (فارسی)

ایمیل

همان‌طور که اشاره شد، به‌طور کلی دو روش برای استفاده از سرویس‌های ایمیل وجود دارد. استفاده از سرویس‌های آنلاین، مانند هات‌میل، جی‌میل و یاهو و استفاده از نرم‌افزارهای خاص برای دسترسی به این سرویس‌ها. هرکدام از این موارد سود و زیان‌های خاص خود را دارد. توصیه کلی ما این است که در هر دو صورت، اطمینان حاصل کنید که ارتباط شما با سرور ارائه دهنده ایمیل امن و رمزگذاری شده است. در مورد سرویس‌های آنلاین کار ساده است. ببینید که آیا نشانی صفحه ایمیل‌تان در مرورگر وب با HTTPS شروع می‌شود یا خیر. اگر پاسخ منفی است از آن سرویس استفاده نکنید.
در مورد نرم‌افزارهای خواندن ایمیل نیز در قسمت تنظیمات حساب کاربری، Connection Security بایداز نوع SSL باشد تا ارتباط با سرور امن برقرار شود.

یک نکته مهم این‌که، امنیت ارتباطات از طریق ایمیل بستگی به رعایت نکات امنیتی در هر دو سوی فرستنده و گیرنده دارد. اگر یکی از دو طرف موارد امنیتی را رعایت نکند طرف دیگر نیز به خطر می‌افتد. البته این موضوع را می‌بایست در همه انواع ارتباطات در نظر داشت.

سرویس‌های ایمیل بسیار امنی مانند RiseUp وجود دارند که تا حد بسیار بالائی، امنیت کاربران‌شان را تضمین می‌کنند. اما استفاده از چنین خدماتی ممکن است سوء ظن‌ها را نسبت به فعالیت‌های‌تان برانگیزد، زیرا که استفاده از چنین خدماتی خود نشانی از آن است که شما درگیر فعالیت‌های کنشگری هستید یا چیزی برای مخفی کردن دارید. در این‌گونه موارد شاید بهترین کار آن باشد که نشانی ایمیلی که برای خود انتخاب می‌کنید تا حد امکان ارتباطی با شخص یا شغل شما نداشته باشد. مثلا، از نام واقعی خود در نشانی ایمیل استفاده نکنید.
بیشتر بخوانید: امنیت ایمیل - بالاویزیون (فارسی)

نرم‌افزارهای مفید

- مرورگر فایرفاکس و افزونه‌های امنیتی مناسب برای آن.
- phishtank، ابزار اینترنتی برای بررسی و گزارش حمله های فیشینگ توسط دیگر وب‌سایت‌ها.
- onlinelinkscan، ابزاری برای بررسی امنیت وب‌سایت‌ها از نظر وجود بدافزار، جاسوس‌افزار یا فیشینگ در آن‌ها.
- K9 نرم‌افزار مجانی و کد-باز برای گوشی‌های اندروید. این نرم افزار امکان مرزگذاری، رمزگشائی و امضاء دیجیتالی پرونده‌ها، ایمیل‌ها و پیامک‌ها را فراهم می‌کند.
- OBSCURACAM نرم‌افزار مجانی و کد-باز برای گوشی‌های اندروید است که امکان شناسائی و حذف صورت افراد را در عکس فراهم می‌کند. این نرم‌افزار برای مواقعی مفید است که عده زیادی در تصاویر شما دیده می‌شوند که نمی‌خواهید شناسائی شوند.
- ORBOT نرم‌افزار مجانی و کد-باز برای گوشی‌های اندروید است که امکان انتصال امن و ناشناس به اینترنت را فراهم می‌کند. این نرم افزار را می‌توان نمونه موبایل TOR در نظر گرفت.
- ORWEB، مرورگر مجانی و کد-باز برای گوشی‌های اندروید است که با استفاده از ORBOT امکان مرور امن و ناشناس صفحات وب را فراهم می‌سازد.

درس پنج: شبکه‌های اجتماعی

فهرست عنواین

مقدمه

شبکه‌های اجتماعی در چندسال گذشته به مهم‌ترین وسیله ارتباطی میان افراد بشر بدل شده‌اند. صدها میلیون کاربر اینترنتی از طریق شبکه‌های اجتماعی با یکدیگر ارتباط برقرار کرده، از حال و روز هم با خبر می‌شوند. هم‌زمان که رسانه‌ها و کنشگران متوجه اهمیت این ابزار ارتباطی شده، شروع به استفاده از آن کردند، سازمان‌های امنیتی نیز به دنبال آن‌ها شروع کردند به پایش این شبکه‌ها. شبکه‌های اجتماعی راه سهل و آسانی برای ردیابی فعالیت‌های اینترنتی افراد به شمار می‌رود.

برای کنشگران اینترنتی، شبکه اجتماعی ابزاری است که از طریق آن خیل عظیمی از مخاطبان را می‌توان از مسائل باخبر کرده، آنان را خطاب کارزارهای آنلاین قرار داد. از سوی دیگر، استفاده بی‌ملاحظه از شبکه‌های اجتماعی ممکن است باعث علنی شدن نام، نشانی محل کار یا سکونت، آخرین فعالیت‌ها و تصاویر افراد شده، در مواردی جان و مال‌شان را به خطر بیاندازد. از این روی هنگام استفاده از شبکه‌های اجتماعی، رعایت نکات امنیتی از اهمیت بالائی برخوردار است.

بیشتر بخوانید:

- جزئیاتی از «پروژه عنکبوت» سپاه برای نظارت بر فعالیت کاربران ایرانی فیس‌بوک.
- ویکی‌پدیا: پروژه عنکبوت.

موارد کلی پیرامون امنیت در شبکه‌های اجتماعی

امنیت فردی یا امنیت گروه

هنگام فعالیت در شبکه‌های اجتماعی می‌بایست به‌طور مداوم از دو زاویه مراقب وضعیت امنیتی باشید. نخست امنیت فردی خودتان، این‌که تا حد امکان هویت واقعی‌تان، تصویر، روابط، نشانی منزل یا شماره تلفن‌تان محفوظ بماند و سپس امنیت جماعتی که با آن در ارتباط هستید یا شما را در شبکه اجتماعی پیگیری می‌کنند. برای این کار می‌بایست همیشه سطح دسترسی به اطلاعات شخصی و مطالبی که در شبکه‌های اجتماعی منتشر می‌کنید را به دقت تعیین کنید. همان‌طور که در دنیای واقعی همه مسائل خصوصی‌تان را با صدای بلند برای همسایه، فایل و همکاران شرح نمی‌دهید، در دنیای مجازی نیز می‌بایست مراقب باشید که چه کسی به چه اطلاعاتی در مورد شما دسترسی دارد. در مواردی شاید بهتر باشد حساب کاربری با یک نام مستعار ایجاد کنید که از آن برای کنشگری اینترنتی استفاده شود.

صفحه شخصی یا صفحه کارزار

اگر در موقعیتی نیستید که شهرت شخصی‌تان در کارزار اینترنتی نقش اساسی داشته باشد؛ یعنی مثلا رهبر جنبش خاصی نیستید که نام‌تان به آن جنبش اعتبار دهد یا دیگران را تشویق به پیوستن به آن کند، بهتر است از حساب کاربری شخصی‌تان برای راه‌اندازی کارزارهای اینترنتی استفاده نکنید. شبکه‌هایی مانند فیس‌بوک به کاربران امکان ایجاد صفحات خاص می‌دهد که جدا از حساب کاربری است. در غیر این صورت شاید بهترین روش استفاده از نام مستعار و ایجاد حساب کاربری جایگزین باشد.

گپ اینترنتی (چت)

برخی شبکه‌های اجتماعی مانند فیس‌بوک امکان گپ اینترنتی یا چت کردن را نیز به کاربران‌شان می‌دهند. معمولا این ابزارهای ارتباطی از امنیت کافی برخوردار نیستند. به طور کلی، سرویس‌های گپ ارائه شده توسط شبکه‌های اجتماعی از کمترین سطح امنیتی برخوردارند. حتی شبکه‌ای مانند فیس‌بوک که صفحه اصلی‌اش از ارتباط رمزگذاری شده HTTPS استفاده می‌کند، برای سرویس گپ اینترنتی از کانال‌های دیگر بهره می‌برد که امنیت پایین‌تری دارند. در ضمن، گاه پاک کردن تاریخچه چنین گپ‌هایی نیز دشوار است یا اصلا امکان‌پذیر نیست.

حساب‌های کاربری مرتبط

برخی شبکه‌های اجتماعی امکان ارسال همزمان مطالب پست شده را به شبکه‌های اجتماعی دیگر فراهم می‌کنند. به‌طور مثال، می‌توان فیس‌بوک و تویتر را به یکدیگر ارتباط داد تا هرچه در فیس‌بوک منتشر می‌کنید به‌طور همزمان در تویتر نیز منتشر شود. اگر از چنین امکانی استفاده می‌کنید می‌بایست به شدت مراقب سطح دسترسی دیگران به آن باشید، زیرا مطلبی که در یکی از آن‌ها ممکن است به صورت خصوصی منتشر شود در دیگری در اختیار همگان خواهد بود. توصیه ما این است که تا حد مقدور از چنین امکانی استفاده نکنید.

سطح دسترسی دیگران به مطالب شما

شبکه‌های اجتماعی مختلف امکان تعیین سطوح دسترسی گوناگونی را برای کاربران‌شان فراهم می‌کنند. البته همیشه باید در نظر داشته باشید که این سطوح دسترسی فقط مربوط به دیگر کاربران آن شبکه‌ها است، و مشمول صاحبان شبکه اجتماعی و در مواردی دولت‌ها نمی‌شود. صاحبان شبکه اجتماعی (چه ایرانی و چه غیر ایرانی) بدون محدودیت به همه اطلاعاتی که کاربران در آن قرار می‌دهند دسترسی دارند و گاه این اطلاعات را در دسترس مقامات دولتی یا شرکت‌های دیگر قرار می‌دهند.

در مورد سطح دسترسی دیگران به مطالب و اطلاعات‌تان می‌بایست به چند نکته خاص دقت کنید:

- **موقعیت مکانی**: بیشتر شبکه‌های اجتماعی، به خصوص از طریق نرم‌افزار تلفن هوشمندشان، مکان شما را به‌طور خودکار به مطالبی که ارسال می‌کنید اضافه می‌کنند. هدف آن است که دوستان‌تان بدانند شما این مطلب را از کجا ارسال کرده‌اید. گاه این مکان با دقت محل ارسال مطلب را نشان می‌دهد. این امکان از جنبه‌های مختلف ممکن است امنیت شخصی یا شغلی شما را به خطر بیاندازد. تصور کنید که رئیس‌تان در فیس‌بوک ببیند که شما مطلبی را در ساعت کاری از مکانی غیر از اداره یا شرکت ارسال کرده‌اید. برخی شبکه‌های اجتماعی حتی بدون استفاده از سیستم‌های موقعیت‌یاب تلفن هوشمند، و تنها با کمک نشانی IP رایانه مکان تقریبی‌تان را حدس زده آن را به مطلب ارسالی‌تان اضافه می‌کنند. معمولا در بخش تنظیمات می‌توانید این امکان را غیرفعال سازید.
- **اطلاعات شخصی**: شبکه‌های اجتماعی به‌طور معمول حجم زیادی از اطلاعات خصوصی‌تان را جمع‌آوری می‌کنند. آنان از این کار دو هدف را دنبال می‌کنند: یک آن‌که تا حد امکان ارتباط با دیگران و روند دوست‌یابی را ساده‌تر کنند و دیگر این‌که با شناخت بهتر شما و سلیقه‌های‌تان، تبلیغات مرتبط با آن را به شما نمایش دهند. برخی شبکه‌های اجتماعی حتی اطلاعاتی را از شماا فاش می‌کنند که ممکن است از آن خبر نداشته باشید. برای مثال، دوربین‌های عکاسی دیجیتال اطلاعات مربوط به زمان، مکان و تنظیمات دوربین هنگام گرفتن عکس را درون تصویر ذخیره می‌کنند. برخی شبکه‌های اجتماعی، هنگام انتشار تصاویرتان این اطلاعات را نیز به صورت عمومی منتشر می‌کنند.
  هر گاه اطلاعاتی از خودتان را در یک شبکه اجتماعی قرار می‌دهید می‌بایست از خود سؤال کنید:
  - اضافه کردن این اطلاعات به پروفایل من چه سودی در حال و آینده خواهد داشت.
  - چه کسی به آن دسترسی پیدا می‌کند.
  - اگر این اطلاعات به نحوی آشکار شود چه زیانی ممکن است متوجه من یا اطرافیان‌ام گردد.

- **ارتباطات**: نوع ارتباطات شما جزئیات مهمی از شخصیت، روابط و فعالیت‌های‌تان را بر ملا می‌کند. برخی شبکه‌های اجتماعی همچون فیس‌بوک امکان مخفی ساختن فهرست دوستان را ارائه می‌دهند. برخی همچون تویتر چنین امکانی ندارند و همه فهرست‌ها عمومی است. به این فکر کنید که آیا دم در خانه‌تان، فهرست همه دوستان و آشنایان‌تان را قرار می‌دهید؟ آیا با هر فرد غریبه‌ای که برخورد کردید به او می‌گویید چه کسانی را می‌شناسید؟

گروه‌ها و انجمن‌ها

گروه‌هایی که عضوشان می‌شوید

گروه‌ها و انجمن‌های بسیاری در اینترنت و در شبکه‌های اجتماعی وجود دارد که ممکن است به مسائل مورد علاقه شما بپردازند و شما بخواهید در آن عضو شوید. همیشه در این موارد باید به خاطر داشته باشید که تنظیمات مربوط به حریم خصوصی‌تان شامل فعالیت در گروه‌ها و انجمن‌ها نمی‌شود و گاه این فضاهای مجازی قوانین خاص خود را دارند. گاه نیز فعالیت در آن‌ها به‌طور کامل علنی است. پس بهتر است قبل از عضویت در هر گروهی تنظیمات مربوط به حریم خصوصی آن را به دقت بررسی کنید. به‌طور مثال، ممکن است بخواهید از نشانی ایمیل دیگری به جز ایمیل شخصی یا کاری برای عضویت استفاده کنید.

گروه‌هایی که خودتان ایجاد می‌کنید

ممکن است خود شما بخواهید گروه یا انجمن اینترنتی را به راه بیاندازید. پیش از شروع کار می‌بایست به پرسش‌های امنیتی فکر کنید:

- ✓ آیا نام و مشخصات گروه باید علنی باشد یا فقط افراد خاصی از وجود آن آگاه باشند؟
- ✓ چه کسی عضو گروه خواهد شد؟
- ✓ چه کسی به مطالب گروه دسترسی خواهد داشت؟
- ✓ آیا فهرست اعضای گروه باید علنی باشد، محدود به خود اعضای گروه یا به‌طور کامل مخفی؟

نبض ایران
تقویت صدای ایرانیان

دوست‌یابی در اینترنت

مهم‌ترین جنبه هر شبکه اجتماعی ایجاد ارتباطات مجازی است. هنگام این‌کار با خود فکر کنید اگر از هویت واقعی فرد پشت این پروفایل آگاهی کافی ندارید، چه اطلاعاتی از خودتان را می‌خواهید با او به اشتراک بگذارید. اگر او را می‌شناسید، تا چه حد می‌خواهید از هویت و فعالیت‌های مجازی‌تان سر در بیاورد.

فعالیت و رفتار شما در دنیای مجازی نیز همچون دنیای واقعی پیامدها و عواقب خود را دارد. همان‌طور که در دنیای واقعی مراقب رفتار و گفتارتان هستید، در دنیای مجازی نیز می‌بایست این موضوع را در نظر داشته باشید. فراتر این‌که اگر در دنیای حقیقی عده کمی از یک رفتار مشخص‌تان آگاه شوند یا به آن واکنش نشان دهند، در دنیای مجازی همه می‌توانند آن را مشاهده کرده و برای ابد به آن دسترسی داشته باشند.

برگرفته از مقاله: از خود و داده‌های‌تان در شبکه‌های اجتماعی مراقبت کنید.

امروزه شبکه‌های اجتماعی متنوعی برای کاربران خاص و عام موجود است. هرچند منطق اصلی همه آن‌ها مشابه به نظر می‌رسد؛ هم‌رسانی لینک‌های اینترنتی، پرونده‌های چندرسانه‌ای و ...اما نحوه به اشتراک‌گذاری و کارکرد آن‌ها متفاوت است. وب‌سایت امنیت در یک جعبه، توصیه‌هایی را فراهم آورده برای هر یک از چند شبکه اجتماعی مشهور از جمله، فیس‌بوک، تویتر، فلیکرز و یوتیوب. ما مطالعه این صفحه را به شما پیشنهاد می‌کنیم.
تنظیمات امنیتی در شبکه‌های اجتماعی مختلف.

(در صورتی که در فهم مطالب به زبان انگلیسی مشکل دارید یا هر گونه پرسشی در این زمینه را می‌توانید با ایمیل info@nabz-iran.com در میان بگذارید.)