چگونه با
تهدیدات اینترنتی
مقابله کنیم

راهنمای آموزشی ویژه جامعه دگرباشان جنسی ایران

زمستان ۱۳۹۳

فهرست مندرجات:

توجه به امنیت در استفاده از کامپیوتر

نخستین گام برای تأمین امنیت، نصب یک سیستم عامل (به عنوان مثال سیستم عامل Windows) مطمئن بر روی کامپیوتر است. در بازار ایران نسخه‌های مختلف سیستم عامل ویندوز با قیمت ارزان و مارک‌های مختلف به فروش می‌رسد. باید توجه داشته باشید که ممکن است این سیستم عامل‌ها به صورت عمدی یا غیر عمدی دارای مشکلات امنیتی باشند. برای مثال، ممکن است بخش‌هایی از سیستم عامل که باید امنیت کامپیوتر شما را حفظ کند، دست‌کاری یا حذف شده باشد یا ویروس‌هایی بر روی این سیستم عامل نصب شده باشد. بر فرض ممکن است در این سیستم عامل حفره امنیتی ایجاد شده باشد یا آلوده به انواع ویروس و بدافزار شده باشد. در این

صورت، بلافاصله پس از نصب چنین سیستم عاملی در معرض خطر قرار خواهید گرفت.

برای مقابله با چنین احتمالاتی، در صورت امکان از سیستم‌های عامل اصل و با بسته‌بندی باز نشده استفاده کنید. بسیاری از کامپیوترهای قابل حمل یک CD سیستم عامل هم دارند. باید مطمئن شوید که CD سیستم عامل اصل است و برچسب (هالوگرام) خورده است. اگر سیستم عامل اصل در دسترس ندارید، از یک فرد خبره در امر کامپیوتر که به او اعتماد دارید، درخواست کنید تا یک نسخه CD سیستم عامل مطمئن که خود از آن استفاده کرده باشد و از سلامت آن اطمینان دارد، در اختیار شما قرار دهد. توجه داشته باشید که فریب مارک‌های شرکت‌های معروف ایرانی را نخورید؛ زیرا احتمال دارد این شرکت‌ها نرم‌افزارهای جاسوسی را روی CDهایی که در بازار می‌فروشند، نصب کرده باشند.

به نرم‌افزارهایی که در بازار ایران به فروش می‌رسد، اعتماد نکنید. این نرم‌افزارها ممکن است آلوده به بدافزارهای مختلف و متعدد مانند انواع ویروس‌ها یا نرم‌افزارهای جاسوسی‌ای باشند که امنیت شما را

به‌خطر می‌اندازند. به‌خصوص برنامه‌های ضد ویروس و امنیتی که قاعدتاً قرار است از کامپیوتر شما محافظت کنند، ولی در صورتی که عمداً دست‌کاری شده باشند، می‌توانند خود تبدیل به یک مشکل امنیتی شود. همچنین، به وب‌سایت‌های ایرانی هم برای دانلود نرم‌افزار اعتماد نکنید. در صورت امکان، سعی کنید نرم‌افزارهای مورد نیاز خود را از وب‌سایت‌های غیر ایرانی یا از افراد مورد اعتماد و خبره در زمینه کامپیوتر بگیرید که چنین نرم‌افزارهایی را خود دانلود کرده‌اند و از سلامت آن اطمینان دارند.

نصب ضد ویروس و فایروال

بسیاری از برنامه‌هایی که به صورت قفل‌شکسته (کرک شده) مورد استفاده قرار می‌گیرند، آلوده به بدافزار هستند. زمانی که این نرم‌افزارها را روی کامپیوتر خود نصب می‌کنید، گاهی حتی ضد ویروس‌ها هم نمی‌توانند جلوی آلوده شدن کامپیوتر شما را بگیرند. بنابراین، تا جایی که امکان دارد، این نرم‌افزارها را بر روی کامپیوتری که ایمنی‌اش برای شما مهم است، نصب نکنید و از نرم‌افزارهای اصل یا رایگانی استفاده کنید که قابل دانلود از سایت اصلی هستند.

اطمینان از سلامت نرم‌افزارهایی که نصب می‌کنید

ویروس‌های کامپیوتری برنامه‌هایی هستند که می‌توانند به کامپیوتر شما و اطلاعات داخل آن صدمه بزنند یا آن‌ها را از بین ببرند. همچنین ویروس‌ها قابلیت انتقال از یک کامپیوتر به کامپیوتر دیگر از طریق DVD ،CD، هارد دیسک‌های قابل حمل، فلش و هرگونه وسیله انتقال داده‌ی دیگر و نیز شبکه‌های کامپیوتری و تلفن‌های همراه را دارند.

برای در امان ماندن از خطر ویروس‌ها:

سعی کنید برای انتقال اطلاعات کمتر از فلش درایو و هارد دیسک‌های قابل حمل استفاده کنید؛ در صورت امکان، بهتر است کامپیوتری را که بر روی آن اطلاعات حساس دارید، به صورت مجزا و ایزوله

نگه دارید و برای تفریحات و کارهای روزمره، از یک کامپیوتر دیگر استفاده کنید.

یک ضد ویروس مطمئن و کارآمد بر روی کامپیوتر خود نصب کنید. مراقب باشید که این نرم‌افزار ضد ویروس خود آلوده به ویروس نباشد؛ ضد ویروس را هم مانند سایر نرم‌افزارها از یک منبع مورد اعتماد دریافت کنید.

بعضی از بدافزارها به اطلاعات شما صدمه نمی‌زنند، ولی بر روی کامپیوتر شما جاسوسی می‌کنند و اطلاعات ذخیره شده بر روی آن یا هرگونه اطلاعات دیگری را که بتوانند جمع آوری کنند، برای یک منبع دیگر ارسال می‌کنند. این بدافزارها حتی ممکن است میکروفون یا وب‌کم کامپیوتر شما را روشن کنند و صدا و تصویر شما را به منبع دیگری بفرستند. برخلاف ویروس‌ها که به اطلاعات شما صدمه می‌زنند و ممکن است کامپیوتر شما را از کار بیاندازند، این بدافزارها معمولاً هیچ اشکالی در استفاده شما از کامپیوتر ایجاد نمی‌کنند و ممکن است بدون آن‌که متوجه شوید، کامپیوتر شما مدت‌ها به یک بدافزار آلوده باشد. معمولاً برنامه‌های ضد ویروس این بدافزارها را

هم شناسایی می‌کنند. برای امنیت بیشتر، می‌توانید از برنامه‌های «فایروال» استفاده کنید، فایروال‌ها تماس‌های کامپیوتر شما را بر روی شبکه و اینترنت نظارت می‌کنند و اگر از کامپیوتر شما ارتباط ناخواسته‌ای با یک منبع مشکوک برقرار شود، به شما هشدار می‌دهند و جلوی آن ارتباط و ارسال اطلاعات را می‌گیرند.

پیوندهایی که می‌توانید از طریق آن نرم‌افزارهای امنیتی ضد ویروس و فایروال دریافت کنید:

ضد ویروس AVG : http://free.avg.com

فایروال COMODO : http://personalfirewall.comodo.com

استفاده از Microsoft Security Essentials

استفاده از Microsoft Security Essentials (البته فقط هنگامی که از نسخه قانونی ویندوز استفاده می‌کنید) می‌تواند برای اطمینان از امنیت در پیوند با سیستم عامل ویندوز مفید باشد. این نرم‌افزار یک امکان مجانی است که می‌توانید با مراجعه به پیوند زیر آن را به سیستم عامل ویندوز اضافه کنید:

http://windows.microsoft.com/en-US/windows/security-essentials-download

نصب این نرم‌افزار تا حدی می‌تواند در مقابل ویروس‌ها و بدافزارها به شما کمک کند؛ اما باید توجه داشته باشید که چون یک سرویس مرتبط با «ویندوز» است، اگر ویندوز شما نسخه اصل و قانونی نباشد،

شما را دچار مشکل جدی می‌کند و نه تنها امنیت شما را افزایش نخواهد داد، بلکه می‌تواند موجب از میان رفتن تمام امکانات امنیتی ویندوز و حتی از کار افتادن کل این سیستم عامل شود.

پس از نصب این برنامه، یک آیکن در قسمت نوار پایین ویندوز در سمت راست اضافه می‌شود. روی آن دو بار کلیک کنید تا پنجره نرم‌افزار باز شود. در این پنجره با کلیک بر روی دکمه Scan می‌توانید کامپیوتر خود را در مورد ویروس‌ها جست‌وجو کنید. این نرم‌افزار همچنین به صورت خودکار از زمانی که شروع به استفاده از ویندوز می‌کنید، کامپیوتر شما را در برابر ویروس‌ها و بدافزارهای جدید حفاظت می‌کند.

نگه‌داری از اطلاعات و فایل‌های مهم

نگه‌داری اطلاعات بر روی CD و DVD این مزیت را دارد که اطلاعات شما پس از ذخیره نمی‌تواند پاک شود یا آلوده به ویروس شود؛ ولی اگر اطلاعات شما قبل از ذخیره بر روی CD و DVD به ویروس یا بدافزار آلوده شده باشد، این بدافزارها به CD و DVD هم منتقل می‌شود و برای همیشه باقی می‌ماند و حتی برنامه‌های ضد ویروس هم نمی‌تواند آن‌ها را پاک‌سازی کند.

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

فایل‌ها و اطلاعات شما پاک نمی‌شود

برخلاف تصور رایج، هنگامی که شما برای مثال یک فایل را از روی کامپیوتر خود پاک می‌کنید و Recycle Bin را هم خالی می‌کنید، هنوز امکان بازیابی آن فایل وجود خواهد داشت. زمانی که شما یک فایل را پاک می‌کنید، سیستم عامل شما، آن قسمت از حافظه داخلی خود را که برای نگه‌داری آن فایل اشغال شده بوده است، آزاد می‌کند و به این ترتیب شما دیگر آن را نخواهید دید و با روش‌های معمول، به اطلاعات آن فایل دسترسی نخواهید داشت. هرچند تا زمانی که اطلاعات جدیدی بر روی این حافظه آزاد شده ذخیره نشود، اطلاعات قدیمی همچنین در جای خود باقی خواهد ماند و با استفاده از نرم‌افزارهای خاصی می‌توان آن را بازیابی کرد. برای جلوگیری از

بازیابی اطلاعات پاک شده، می‌توانید از نرم‌افزارهایی که اطلاعات فایل را پس از پاک شدن به صورت کامل از بین می‌برند – برای مثال «File Shredder» یا «Eraser» – استفاده کنید. بااین‌حال، این نرم‌افزارها هم نمی‌توانند از بین رفتن فایل‌ها را کاملاً تضمین کنند. اگر نگرانی جدی دارید، حافظه کامپیوتر را کامل تخریب کنید یا از افراد معتمد متخصص در این زمینه کمک بگیرید.

استفاده از حساب کاربری مخصوص به خود در ویندوز

بهتر است یک حساب کاربری مخصوص خودتان روی سیستم عامل داشته باشید؛ به‌ویژه اگر افراد دیگری هم از کامپیوتر شما استفاده می‌کنند. حتی برای استفاده‌های مختلف خود هم می‌توانید حساب‌های جداگانه درست کنید. برای مثال، کارهای حساس را با یک حساب کاربری انجام دهید و سایر فعالیت‌ها را با شناسه‌ای دیگر به انجام برسانید. برای این کار، به بخش Control Panel ویندوز بروید سپس گزینه User Accounts را انتخاب کنید، سپس در پنجره‌ای که باز می‌شود، می‌توانید برای «اکانت» خود «گذرواژه» انتخاب کنید یا گذرواژه را تغییر دهید. همچنین، می‌توانید روی گزینه Manage

Accounts کلیک کنید و در صفحه‌ای که باز می‌شود، حساب‌های کاربری جدید اضافه کنید. در نسخه‌های مختلف ویندوز این کار را می‌توانید کم‌وبیش به‌همین ترتیب انجام دهید.

خطر استفاده از تلفن همراه هوشمند و وسایل تصویر و صدابرداری

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

در صورتی که تلفن همراه شما دزدیده یا گم شد، گذرواژه تمام سرویس‌هایی را که از طریق آن تلفن از آن‌ها استفاده می‌کردید (برای مثال گذرواژه ایمیل و فیس‌بوک) تغییر دهید.

توجه داشته باشید که سرویس‌های GPS (مکان‌یاب) نصب شده روی این تلفن‌ها، می‌تواند موقعیت شما را لو بدهد و بدون آن‌که متوجه باشید، موقعیت مکانی شما را بر روی سرویس‌های مختلف اینترنتی و شبکه‌های اجتماعی منتشر کند. قطع کردن امکان GPS تلفن همراه می‌تواند جلوی بعضی از این موارد را بگیرد.

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

اگر فرد متخصصی در این زمینه نیستید، در مورد تلفن‌ها برای این‌که مطمئن شوید اطلاعات مورد نظرتان کاملاً از بین رفته و به هیچ طریقی قابل بازیابی نخواهد بود، احتمالاً چاره‌ای نخواهید داشت جز تخریب کامل دستگاه – و در مورد دوربین‌ها و وسایل ضبط صدا،

تخریب کامل حافظه (در صورتی که تنها حافظه دستگاه، حافظه قابل تعویض باشد) – یا کمک گرفتن از فردی متخصص. در صورتی که از آتش برای تخریب وسایل الکترونیکی استفاده می‌کنید، مراقب گازهای بسیار سمی حاصل از سوختن این ابزارها باشید.

اگر امکان تخریب برای شما وجود ندارد، پس از پاک کردن حافظه سعی کنید تمام ظرفیت حافظه را با فایل‌های غیر مهم پر کنید؛ این کار احتمال امکان بازیابی فایل‌های پاک شده شما را کاهش می‌دهد.

امنیت در استفاده از اینترنت

۱. لازم است بدانید IP چیست و چطور کار می‌کند

هنگام اتصال به شبکه، به هر کاربر اینترنت یک شناسه اینترنتی (IP) تعلق می‌گیرد. هنگامی که در اینترنت به یک آدرس مراجعه می‌کنید، IP شما به آن آدرس متصل می‌شود. مقصد شما در اینترنت می‌تواند یک وب‌سایت یا یک نرم‌افزار مانند Yahoo Messenger باشد. درهرصورت، هنگام هرگونه استفاده از اینترنت، مقصد شما از IP شما آگاه خواهد شد. با دسترسی به امکانات دولتی و شرکت‌هایی که به شما اتصال اینترنت می‌فروشند و همچنین دسترسی به اطلاعات سایت یا سرویسی که شما به آن متصل شده‌اید، می‌توان متوجه شد که این شناسه اینترنتی یا IP متعلق به چه شخص و محلی است و به‌این‌ترتیب، هویت شما می‌تواند آشکار شود. بنابراین، هنگامی که

به صورت مستقیم به یک آدرس اینترنتی مراجعه می‌کنید، باید متوجه باشید که از خود رد پا به جا می‌گذارید. به یاد داشته باشید که ممکن است برخلاف تصورتان، در اینترنت و هنگام استفاده از سرویس‌های اینترنتی ناشناس باقی نمانید.

برای حل این مشکل، باید به‌جای آن‌که به صورت مستقیم به مقصدی در اینترنت متصل شوید، از یک واسطه یا «Proxy» کمک بگیرید. هنگامی که از واسطه برای ارتباط اینترنتی استفاده می‌کنید، این IP شما نخواهد بود که به مقصد متصل می‌شود، بلکه IP واسطه شما برای مقصد آشکار خواهد شد. برای مثال، هنگامی که شما در یک سایت یا وبلاگ نظر می‌نویسید، مدیر آن سایت می‌تواند IP شما را ببیند و از این طریق در مورد شما اطلاعاتی به‌دست آورد و یا مراجع دولتی می‌توانند به مشخصات کامل شما دسترسی پیدا کنند؛ ولی اگر از یک برنامه واسط استفاده کنید، هویت شما محفوظ خواهد ماند. معمولاً برنامه‌هایی که برای عبور از فیلتر استفاده می‌شوند، برای مثال نرم‌افزار «Tor»، این کار را برای شما انجام می‌دهند. توجه داشته باشید که هنگامی که از واسطه‌ها استفاده می‌کنید، IP شما و

همچنین مقاصدی که به آن‌ها دسترسی پیدا می‌کنید و اطلاعات رد و بدل شده، برای واسطه آشکار خواهد بود؛ بنابراین باید از واسطه‌ای استفاده کنید که به آن کاملاً اطمینان دارید.

برای پیدا کردن واسطه مطمئن، از افراد متخصص مورد اعتماد خود کمک بگیرید یا از نرم‌افزارهایی که مورد اطمینان عمومی است، مانند Psiphon (سایفون) و Tor استفاده کنید.

http://psiphon.ca/index.php

https://www.torproject.org

برای مثال، لینک زیر طریقه وبلاگ‌نویسی به کمک تُر و وردپرس را نشان می‌دهد:

به کمک تُر و وردپرس، ناشناس وبلاگ بنویسید

http://advocacy.globalvoicesonline.org/projects/guide

۲. به سایت‌های ایرانی فروشنده راهکارهای عبور از فیلتر اعتماد نکنید

بسیاری از راهکارهای عبور از فیلتر ممکن است شما را از فیلتر عبور دهد، ولی نه تنها امنیت شما را تأمین نکند، بلکه سبب آسیب‌پذیری بیشتر شما شود. بعضی از سایت‌هایی که راهکار عبور از فیلتر مانند وی.پی.ان یا انواع دیگر Proxy را به کاربران ایرانی می‌فروشند، تمام اطلاعات رد و بدل شما را کنترل و ثبت می‌کنند؛ پس باید از سرویس‌هایی استفاده کنید که به آن اطمینان کامل دارید.

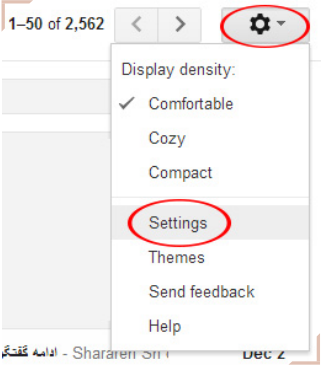
۳. از HTTPS استفاده کنید

بیشتر آدرس‌های اینترنتی با http شروع می‌شوند؛ برای مثال http://www.youtube.com ولی بعضی از آدرس‌ها با https شروع می‌شوند، مانند https://mail.google.com. https یک راهکار با امنیت بسیار بالاتر برای ارتباطات اینترنتی است. زمانی که شما از این راهکار استفاده می‌کنید، می‌توانید اطمینان بسیار بیشتری داشته باشید که آدرسی که قصد بازدید از آن را دارید از سوی دولت به یک سایت دیگر هدایت نشده یا اطلاعات شما هنگام کار با آن سایت قابل مشاهده

نیست. بیشتر بانک‌ها برای امنیت بالا از این راهکار استفاده می‌کنند. اگر سایتی که قصد بازدید از آن را دارید امکان دسترسی با https را دارد، حتماً از آدرسی که با https شروع می‌شود وارد آن سایت شوید.

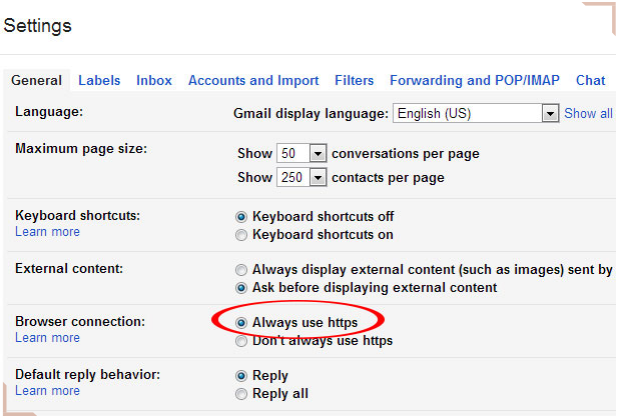
٤. امنیت email

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



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

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



- گذرواژه (password) ایمیل خود را فقط برای ایمیل استفاده کنید. برای مثال، اگر می‌خواهید در سایت دیگری ثبت‌نام کنید، دقت کنید که گذرواژه‌ای که در نظر می‌گیرید با گذرواژه ایمیل شما یکی نباشد.
- هرگز گذرواژه ایمیل خود را در اختیار سایت‌های دیگر قرار ندهید. بسیاری از سایت‌ها، حتی سایت‌های معتبری

مانند Facebook از شما می‌خواهند که گذرواژه ایمیل خود را وارد کنید تا دوستان شما را پیدا کنند. هرگز نباید چنین درخواست‌هایی را – به‌خصوص در مورد سایت‌هایی که شناخته شده و معتبر نیستند – بپذیرید.

- هنگامی که ایمیلی را باز می‌کنید، حتی اگر ایمیل را از طرف یک فرد آشنا دریافت کرده باشید، روی پیوندهایی که داخل ایمیل به سایت‌های دیگر وجود دارد تا حد امکان کلیک نکنید. اگر فایلی به ایمیل ضمیمه شده و نمی‌دانید چیست، آن را باز نکنید.

- فریب کلاه‌برداری‌های ایمیلی را نخورید، به ایمیل‌هایی که به شما می‌گویند برنده جایزه شده‌اید، توجهی نکنید و به ایمیل‌هایی که از شما نظرخواهی می‌کنند، به‌خصوص اگر فرستنده را نمی‌شناسید، پاسخ ندهید.

- حتماً چند ایمیل برای کارهای مختلف داشته باشید. برای مثال، می‌توانید یک ایمیل با اسم واقعی خود برای کارها و

مکاتبات رسمی درست کنید، یک ایمیل برای فعالیت‌هایی که حس می‌کنید، ممکن است برای شما خطرآفرین باشد و یک ایمیل جداگانه هم برای کارهای تفریحی مانند ثبت‌نام کردن در سایت‌های مختلف.

- دیدن تصاویر و دسترسی به فایل‌ها و پیوندهایی که در داخل متن ایمیل (نه قسمت پیوست‌ها یا Attachments) است، می‌تواند IP شما را برای منابع دیگر لو بدهد. نخست دقت کنید که در این‌جا از فایل‌ها و تصاویری که به ایمیل شما پیوست (Attach) شده‌اند صحبت نمی‌کنیم؛ فایل‌ها و عکس‌های پیوست شده این مشکل را ندارد، ولی این امکان وجود دارد که از طریق تصاویر احتمالی در داخل متن ایمیل شما که قابل دیدن باشند یا با کلیک کردن بر روی پیوندهایی که در داخل ایمیل وجود دارند، شناسایی شوید. سرویس Gmail به صورت پیش‌فرض این مشکل را حل کرده و شما تصاویر را در داخل متن ایمیل نمی‌بینید، مگر آن‌که در متن ارسال شده روی گزینه «Display

images below» کلیک کنید؛ در این صورت، به راحتی می‌توان «آی‌پی» شما (دارنده ایمیل) و از آن طریق، شما را شناسایی کرد.

چت کردن و استفاده از Messengerها

در بیشتر نرم‌افزارهایی که برای گفت‌وگوی اینترنتی یا «چت» کردن مورد استفاده قرار می‌گیرند، IP شما برای شخصی که با او چت می‌کنید، قابل دیدن خواهد بود و به این ترتیب، این امکان وجود دارد که هویت شما به‌راحتی شناسایی شود. به‌خصوص باید توجه داشته باشید که بسیاری از راهکارهای امنیتی که هویت شما را مخفی می‌کنند و راهکارهای فیلترشکن در مورد نرم‌افزارهایی که برای چت کردن استفاده می‌شود، بی‌تأثیر خواهند بود، زیرا بسیاری از راهکارهای امنیتی فقط در مورد «مرورگر وب» کارایی دارند. برای مثال، نرم‌افزار Tor Browser نمی‌تواند امنیت شما را هنگام استفاده از Yahoo Messenger یا Skype تامین کند. تشخیص آن‌که آیا هنگام استفاده از نرم‌افزارهای

گفت‌وگوی متنی، صوتی و تصویری اینترنتی امنیت دارید یا نه، برای افراد غیر متخصص کار دشواری است و بهتر است در این مورد از یک فرد متخصص کمک بگیرید. ولی در مجموع، پروکسی‌ها و VPNهایی که تمام ارتباطات اینترنتی شما را پوشش می‌دهند (نه فقط مرورگر وب را) این امکان را دارند که امنیت شما را هنگام چت کردن بالا ببرند. همچنین، مراقب فایل‌هایی باشید که از طریق نرم‌افزارهای چت برای شما فرستاده می‌شود. ممکن است یک فایل در ظاهر شبیه به یک عکس باشد، ولی در واقع یک ویروس یا بدافزار جاسوسی باشد.

در مورد پیوندهایی که هنگام چک کردن برای شما فرستاده می‌شود و نوشته‌هایی که در ظاهر مربوط به خود نرم‌افزار به نظر می‌رسند، دقت کنید و ندانسته روی چیزی کلیک نکنید. در صورتی که معنی و مفهوم یک پیام یا پیام خطا را درست متوجه نمی‌شوید، روی هیچ یک از گزینه‌ها کلیک نکنید و سعی کنید نرم‌افزار را ببندید.

از اطلاعات شخصی خود محافظت کنید

هنگام وارد کردن نام کاربری و گذرواژه خود، حتماً اطمینان حاصل کنید که آدرس صفحه‌ای که نام کاربری و گذرواژه خود را در آن وارد می‌کنید، مربوط به سایتی باشد که مورد نظر شما است. مثلاً اگر قصد دارید وارد فیس‌بوک شوید، دقت کنید که آدرس صفحه یکی از زیردامنه‌های فیس‌بوک باشد. اگر برای مثال آدرسی مانند www.abcd.com/login را در نوار آدرس مرور اینترنت خود می‌بینید، از وارد کردن گذرواژه و مشخصات خوداری کنید و صفحه را ببندید. به‌خصوص در شبکه‌های اجتماعی و در ایمیل‌ها، گاه به پیوندهایی برخورد می‌کنید که پس از کلیک بر روی آن، وارد صفحه‌ای مانند صفحه ورود سایت اصلی که مشغول کار با آن بودید می‌شوید و باید

مشخصات یا گذرواژه خود را وارد کنید؛ در صورتی که آن صفحه هیچ ربطی به سایت اصلی ندارد و برای فریب دادن و دزدیدن گذرواژه شما ساخته شده است. همچنین، برخی از سایت‌ها از شما می‌خواهند تا گذرواژه ایمیل خودتان را وارد کنید تا دوستان شما را دعوت کنند. اگر به سایت اعتماد کامل ندارید، هرگز این کار را نکنید. همچنین هنگام عضویت در سایت‌ها دقت کنید گذرواژه‌ای که برای سایت می‌سازید، با گذرواژه ایمیلی که برای عضویت در سایت وارد کرده‌اید، یکسان نباشد.

سایت‌هایی که مشخصات و گذرواژه شما را می‌دزدند

همیشه در نظر داشته باشید که می‌توان با تحقیقات و بررسی‌هایی، رد پای شما در اینترنت و اطلاعات پراکنده‌ای را که این‌سو و آن‌سو بر جای گذاشته‌اید، به هم متصل کرد و هویت شما را شناسایی کرد. برای مثال، ممکن است با یک ایمیل در یک سایت ثبت نام کنید و اسم حقیقی خود را وارد کنید و چند سال بعد با همان ایمیل، فعالیتی را با یک اسم مستعار آغاز کنید؛ اما باید توجه داشته باشید که حافظه اینترنت ممکن است قوی‌تر از حافظه شما باشد. در چنین وضعیتی، ممکن است کسی بتواند به‌راحتی رد پای شما را در آن سایت قدیمی پیدا کند و متوجه شود که هویت واقعی کسی که در حال حاضر با این ایمیل کار می‌کند، چیست. در ساختن ایمیل جدید هیچ گاه خست به خرج ندهید.

اطلاعات غیر لازم از خود را در سایت‌ها وارد نکنید و به اشخاص ندهید. برای مثال، اگر مشخص کردن این‌که در چه دانشگاه یا مدرسه‌ای درس خوانده‌اید یا شهر محل زندگی شما کجاست، الزامی برای‌تان ندارد تا این کار را نکنید.

سایت‌های اجتماعی

سایت‌های اجتماعی مانند Facebook و Google Plus و Manjam، می‌توانند در صورت سهل‌انگاری شما تبدیل به یک خطر جدی امنیتی شوند. درست است که این سایت‌ها از نظر فنی امنیت بالایی دارند، ولی معمولاً خطاهای انسانی کاربران این سایت‌ها می‌تواند نتایج فاجعه‌آمیزی حتی در کشورهای آزاد داشته باشد. برای پیش‌گیری از چنین خطرها و نتایجی، به موارد زیر توجه کافی مبذول دارید:

ایجاد شناسه‌های مجزا

بهتر است در این سایت‌ها یک شناسه جداگانه برای فعالیت‌هایی که می‌تواند برای شما خطرآفرین باشد داشته باشید و سپس با شناسه دیگری مثلاً با اعضای خانواده در ارتباط قرار بگیرید.

پرهیز از نشر اطلاعات شخصی

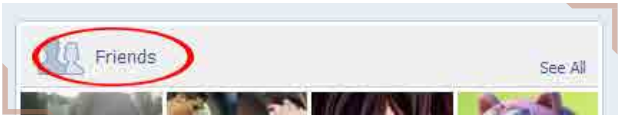
تا جایی که ممکن است اطلاعات شخصی خود را روی این سایت‌ها قرار ندهید. برای مثال، در شناسه‌ای که با آن فعالیت‌هایی که ممکن است خطرآفرین باشد انجام می‌دهید، نباید تصویری قابل شناسایی از خودتان را قرار دهید. همچنین، مراقب تصاویر دیگری هم که می‌تواند منجر به شناسایی شما شود (مانند تصویر خانه، ماشین، محله، دست‌خط و سایر چیزهایی که می‌تواند هویت شما را آشکار کند) باشید و آن‌ها را روی این سایت‌ها نگه ندارید. نوشتن نام و مشخصات محلی که در آن تحصیل کرده‌اید، آدرس دقیق محل سکونت، نام واقعی و شماره تلفن، می‌تواند بسیار خطرآفرین باشد.

توجه به ارتباطات و تماس‌های دوستانه

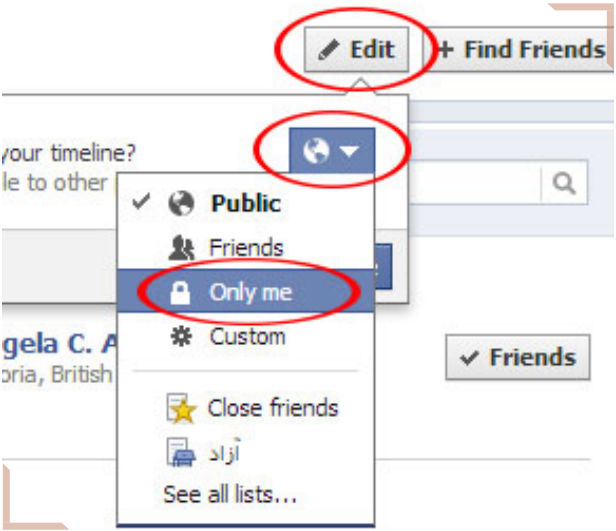
توجه داشته باشید که با وجود تمام رعایت‌های ممکن در صفحه و شناسه‌ی شخصی‌تان، می‌توان شما را از طریق دوستان‌تان و کسانی که به شناسه شما در این سایت‌ها متصل هستند، شناسایی کرد. این امر، یکی از مشکل‌ترین و پیچیده‌ترین مسائل امنیتی در سایت‌های

اجتماعی است. ممکن است شما هیچ رد پایی در شناسه‌های خود به جا نگذارید، ولی در لیست دوستان‌تان کسی باشد که می‌توان با بررسی شناسه‌اش او را شناسایی کرد و سپس از طریق او به شما دسترسی یافت. این مسأله حتی می‌تواند در مورد نظرهایی که زیر نوشته اشخاص دیگر می‌نویسید، نیز صدق کند. مثلاً مشخص شود که شما این فرد را می‌شناسید و او هم شما را می‌شناسد، پس از طریق شناسایی او می‌توان به شما دسترسی پیدا کرد یا اطلاعات بیشتری درباره شما به‌دست آورد.

- در فیس‌بوک برای پنهان کردن لیست دوستان می‌توانید در صفحه دیوار خود روی پیوند Friends (دوستان) مانند تصویر زیر کلیک کنید:



- در صفحه‌ای که باز می‌شود، با استفاده از دکمه Edit (ویرایش) گزینه‌ای را که در عکس زیر مشخص شده انتخاب کنید:



از شبکه‌هایی که کاربران زیاد دارند به اینترنت متصل شوید

اگر از اداره یا دانشگاه یا هر اتصال دیگری به اینترنت که کاربران کمی دارد استفاده می‌کنید، بیشتر در معرض خطر شناسایی خواهید بود؛ به‌خصوص اگر اطلاعاتی را روی اینترنت منتشر کنید که نشان دهد شما عضو این شبکه کوچک (برای مثال، اداره یا دانشگاه) هستید. در چنین صورتی، حتی از روی تاریخ انتشار مطالب شما بر روی اینترنت هم ممکن است بتوان شما را شناسایی کرد.

خلاصه مطالب

- از پاکیزه و سالم بودن نرم‌افزارهای خود، به‌خصوص سیستم عامل و ضد ویروس، اطمینان حاصل کنید و نرم‌افزارهای خود را از طریق منابع معتبر یا افراد معتمد تهیه کنید.
- سعی کنید اطلاعات مهم خود را روی یک حافظه خارجی (مثلاً فلش درایو) نگه‌داری کنید.
- توجه داشته باشید که هنگام استفاده از اینترنت IP شما مخفی بماند. برای حصول اطمینان در این زمینه، از نرم‌افزارها و خدماتی که IP را تغییر می‌دهند استفاده کنید.
- در مورد اطلاعاتی که از خود روی اینترنت قرار می‌دهید و پیوندی که میان شما و اطلاعات دوستان‌تان وجود دارد، دقت زیادی به خرج دهید.
- برای فعالیت‌ها و کارهای مختلف، ایمیل و هویت جداگانه ایجاد کنید.

پیوندهای مفید

نرم‌افزار Tor برای مخفی نگه داشتن IP و عبور از فیلتر:

https://www.torproject.org

ضد ویروس مجانی AVG:

http://free.avg.com

فایروال مجانی COMODO:

http://personalfirewall.comodo.com

مرورگر گوگل کروم:

www.google.com/chrome

سایر منابع آموزش امنیت:

https://securityinabox.org/fa

https://onorobot.org

https://protect.tacticaltech.org/content/flash-training-materials

How to Protect Your Online Security

Internet Security Manual for the Iranian LGBT Community

2015

آثار دیگر

چگونه مسائل دگرباشان جنسی را پوشش دهیم

راهنمای آموزشی ویژه روزنامه‌نگاران و رسانه‌های فارسی

چگونه در ایران از حقوق قانونی خود در جایگاه یک متهم همجنس‌گرا دفاع کنیم

راهنمای آموزشی ویژه دگرباشان جنسی در ایران

آموزش حقوقی در جمع‌آوری دلایل و شواهد نقض حقوق اقلیت‌های جنسی در ایران

آموزش مستندسازی و پیگیری نقض حقوق دگرباشان جنسی

راهبردهای مؤثر حقوقی در دفاع از دگرباشان جنسی

راهنمای آموزشی ویژه کارشناسان حقوقی، وکلای دادگستری و فعالان حقوق بشر