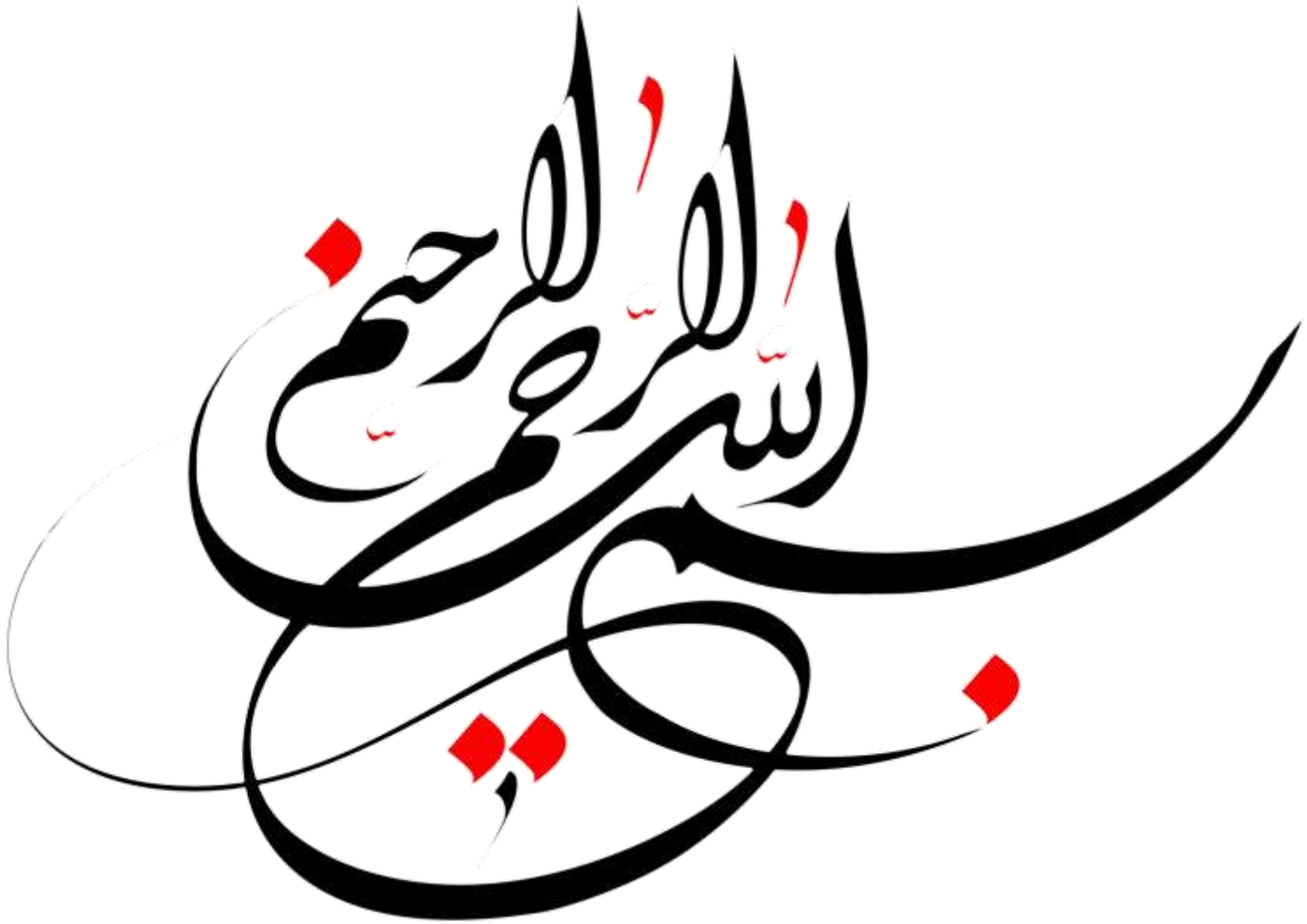

بسم الله الرحمن الرحيم

دانشگاه علوم پزشکی و خدمات بهداشتی، درمانی کرمانشاه

مدیریت اطلاع رسانی پزشکی و مرکز اسناد

مفاهیم حفاظت دیجیتالی

امنیت اطلاعات

- امنیت اطلاعات (Information Security) یعنی حفاظت اطلاعات و سیستم‌های اطلاعاتی از فعالیت‌های غیرمجاز.
- این فعالیت‌ها عبارتند از دسترسی، استفاده، افشاء، خواندن، نسخه برداری یا ضبط، خراب کردن، تغییر، دستکاری.
- اطلاعات در تعریف علمی آن به مجموعه ای از داده ها که دارای معنی و هدف باشند اتلاق می شود.

اطلاعات چاپی، کاغذی، الکترونیکی، صوتی و تصویری گفته شود و حتی گفته های شفاهی

تعاریف و مفاهیم اولیه امنیت اطلاعات

- دارایی Asset
  - هر چیزی که مخاطره در مورد آن دارای معنا دارد.هر چیزی که ارزش حفاظت دارد.
- تصدیق اصالت Authentication
  - اطمینان از این که کاربر، همانی است که ادعا میکند.(یوزر و پسورد–کارت مغناطیسی–اثر انگشت و...)
- مجاز(اجازه داشتن) Authorization
  - کاربر همان میزان حق دسترسی دارد که به او اعطا شده است.

تعاریف و مفاهیم اولیه امنیت اطلاعات

- حفظ حریم خصوصی Privacy
  - مقاومت در مقابل افشای اطلاعاتی (فرد یا گروه بتواند خود یا اطلاعات مربوط به خود را مجزا کند و در نتیجه بتواند خود یا اطلاعاتش را با انتخاب خویش در برابر دیگران آشکار کند)
- خط مشی امنیتی Security Policy
  - بیان رسمی قواعد و باید و نبایدهایی که باعث می شود تا دارایی های اطلاعاتی یک سازمان به طور امن باقی بمانند
- راهکار امنیتی: Security Mechanism
  - راهکاری که برای تشخیص، جلوگیری یا ترمیم از حمله امنیتی طراحی شده است.

تعاریف و مفاهیم اولیه امنیت اطلاعات

- آسیب پذیری Vulnerability
  - هر گونه نقطه ضعف در توصیف، طراحی، پیاده سازی، پیکربندی، اجرا که بتوان از آن سوءاستفاده کرده و سیاستهای امنیتی سیستم را نقض کرد.
- مخاطره یا تهدید Threat
  - احتمال سوء استفاده کردن از یک یا چند آسیب پذیری
- حمله Attack
  - هر فعالیتی که امنیت اطلاعات مربوط به یک سازمان را به خطر می اندازد.
    - محقق کردن یک Threat از طریق یک یا چند Vulnerability بر روی یک Asset

جنبه های اصلی امنیت اطلاعات

- محرمانگی Confidentiality
  - محرمانگی یعنی جلوگیری از افشای اطلاعات به افراد غیر مجاز.
- جامعیت Integrity
  - جامعیت یعنی جلوگیری از تغییر داده‌ها بطور غیرمجاز و تشخیص تغییر در صورت دستکاری غیر مجاز اطلاعات.(رمزنگاری پیام ها)
- در دسترس بودن Availability
  - اطلاعات باید زمانی که مورد نیاز توسط افراد مجاز هستند در دسترس باشند.(نسخه پشتیبان، سرور جایگزین و...)

انواع حملات

- حمله غیر فعال
  - حمله ای که در آن مهاجم اطلاعاتی تولید نمی کند
  - از اطلاعات سیستم استفاده می کند اما تاثیری بر منابع سیستم ندارد
  - ترافیکی در شبکه ایجاد نمی کند
  - سعی دارد اطلاعاتی از سیستم یا سازمان را کشف کند

مثلا: استراق سمع

انواع حملات

- حمله فعال

- مهاجم سعی می کند منابع سیستم را تغییر دهد یا بر عملیات آنها اثر بگذارد
- مهاجم خودش اطلاعات جدیدی تولید می کند
- یا اطلاعات موجود را تغییر می دهد یا اطلاعات موجود را از بین می برد

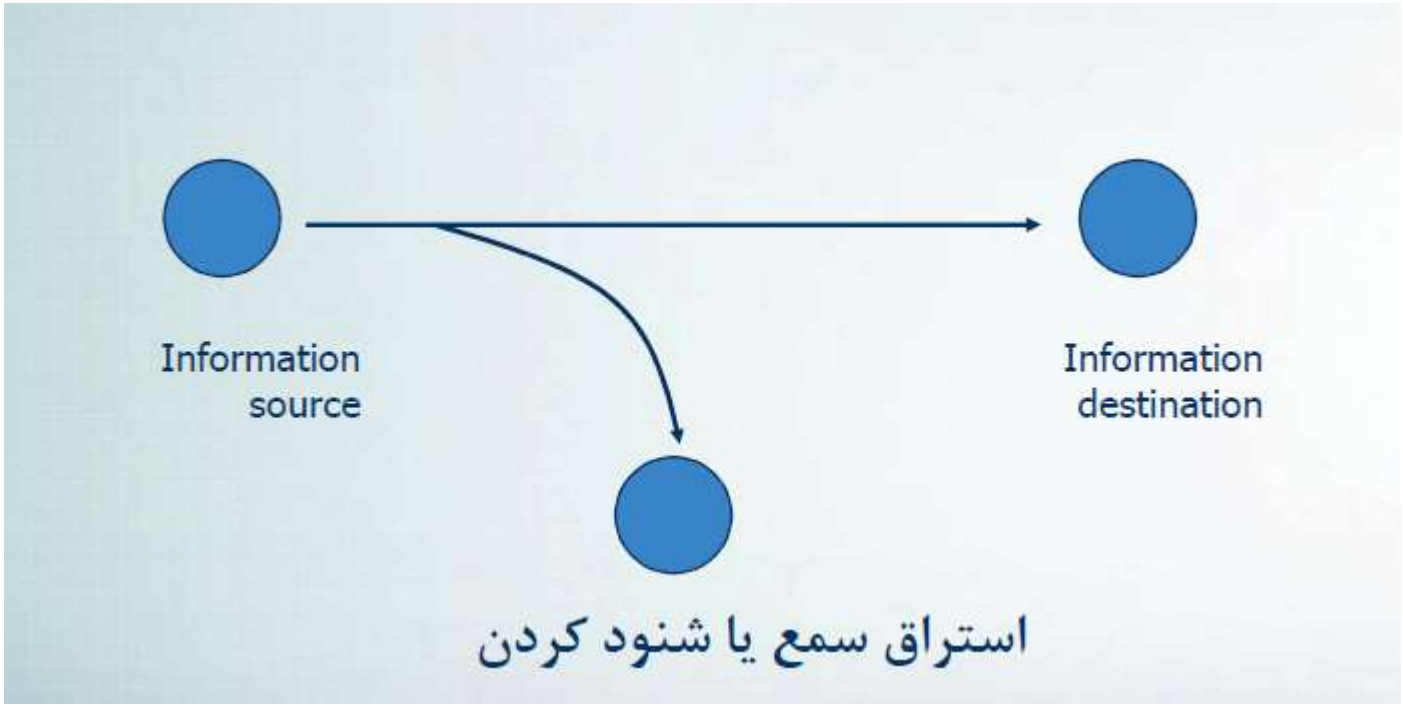
مثلا: جعل هویت، تغییر اطلاعات، قطع ارتباط و ...

تهدیدات امنیتی

تهدیدات امنیتی

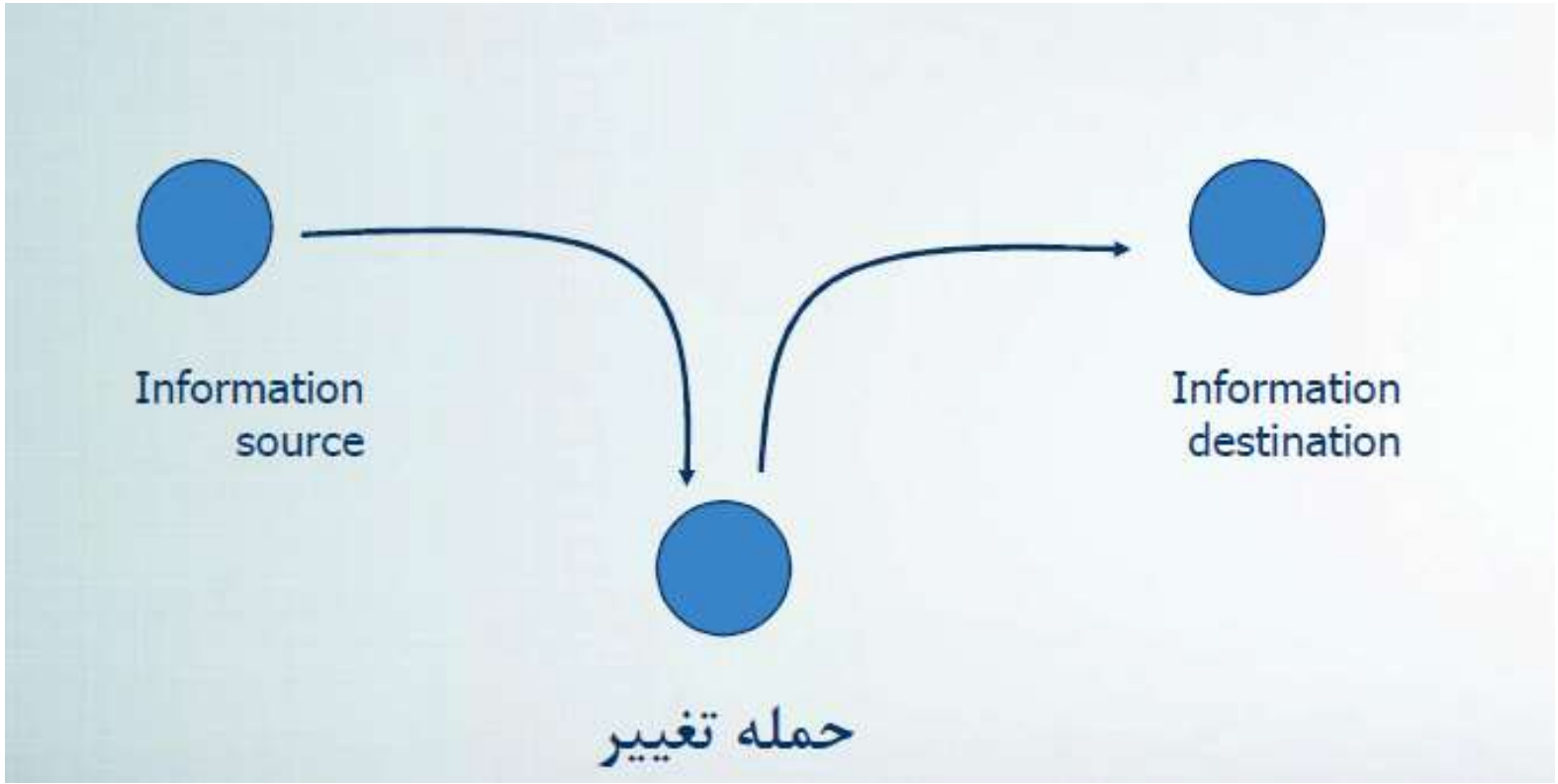
- حمله به در دسترس پذیری (Availability)
- فعال

تهدیدات امنیتی



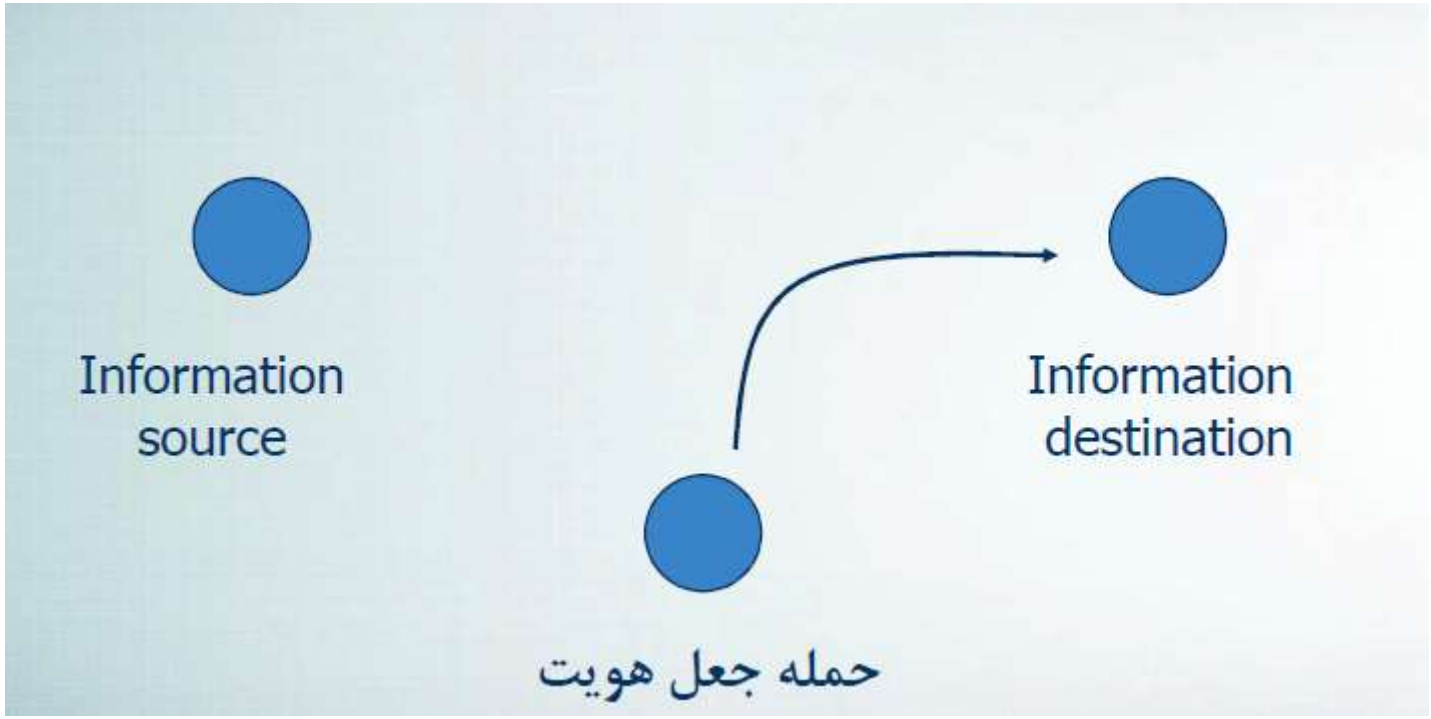
- حمله به در محرمانگی (Confidentiality)
- غیر فعال

تهدیدات امنیتی



- حمله به جامعیت (Data Integrity)
- فعال

تهدیدات امنیتی



- حمله به جامعیت (Data Integrity)
- فعال

تهدیدات امنیتی

- سرقت آنلاین (Phishing)

بدافزارها و نرم افزارهای مخرب

- **بدافزار (Malware)**

واژه بدافزار به ویروس، کرم، تروجان و هر برنامه دیگری که با نیت اعمال خرابکارانه ایجاد شود، اطلاق می شود.

بدافزارها و نرم افزارهای مخرب

- **ویروس کامپیوتری (Virus)**

ویروس، یک نوع بدافزار است که در اغلب مواقع بدون اطلاع کاربر اجرا شده و تلاش می کند خودش را در یک کد اجرایی دیگر کپی کند. وقتی موفق به انجام این کار شد، کد جدید، آلوده نامیده می شود.

به عبارت دیگر، ویروس به برنامه ای اطلاق می شود که نرم افزار قابل اجرایی، را آلوده می کند و هنگامی که آن نرم افزار اجرا می شود سبب شود که ویروس به فایل های قابل اجرای دیگر نیز منتقل شود.

بدافزارها و نرم افزارهای مخرب

- **کرم اینترنتی (Worm)**

به برنامه ای گفته می شود که توانایی بازتولید خود را داراست، و با استفاده از شبکه، کپی های خود را به دیگر رایانه های موجود در شبکه می فرستد.

کرم در برخی از خصوصیات با ویروس مشترک است. مهمترین ویژگی مشترک آن ها این است که کرم ها نیز خود – همانندساز هستند، اما تولید مثل آن ها از دو جهت متفاوت است.

اول اینکه، کرم ها مستقل و متکی به خود هستند، و محتاج به کد اجرایی دیگری نیستند.

دوم، کرم ها از طریق شبکه ها، از ماشینی به ماشین دیگر منتقل و توزیع می شوند. برخلاف ویروس،کرم ها خود را به برنامه های دیگر نمی چسباند .

بدافزارها و نرم افزارهای مخرب

- **اسب تروآ (Trojan Horse)**

یک اسب تروآ برنامه ای است که کاربر را ترغیب می کند تا اجرایش کند در حالی که قابلیت خرابکاریش را مخفی می کند. آثار منفی ممکن است بلافاصله آغاز شوند و حتی می توانند منجر به آثار نامطلوب فراوانی گردند.

به عبارت دیگر، نرم افزاری است که برای کاربر هم اثر مفید دارد و هم اثر مخرب. کاربر به واسطه اثر مفید ترغیب می شود تا از آن استفاده نماید ولی اثر مخرب نیز برای کاربر برجای می گذارد

بدافزارها و نرم افزارهای مخرب

- درب پشتی (Back Door)

هر کد یا رشته کدی که منجر به دور زدن پروسه امنیتی سیستم مقصد شود و از این طریق موجب دسترسی نفوذگر به منابع سیستم گردد، درب پشتی گویند.

به عبارت دیگر، به راهی گفته می شود که بتوان از آن بدون اجازه به قسمت/قسمت های مشخصی از یک سامانه مانند رایانه، دیواره آتش و. .. دسترسی پیدا کرد.

بدافزارها و نرم افزارهای مخرب

- **درب پشتی (Back Door)**

درهای پشتی معمولا به صورت محرمانه و عمدی توسط سازنده محصول یا اشخاص ثالث طراحی می‌شوند. البته برخی از آن‌ها نیز به صورت گسترده شناخته شده هستند. به علاوه ممکن است یک در پشتی به صورت غیرعمدی (برای مثال در اثر یک باگ یا خطای برنامه نویسی) در محصول به وجود آمده باشد.

برخی از توسعه دهندگان برای انجام امور مدیریتی به صورت از راه دور (نظیر عیب یابی و نگه داری سیستم) از بک درها در محصولات خود استفاده می‌کنند. در عین حال ممکن است بدافزارها (تروجان های دسترسی از راه دور) نیز با ایجاد یک Backdoorامکان دسترسی هکرهای متجاوز را به یک سیستم رایانه ای فراهم کنند.

بدافزارها و نرم افزارهای مخرب

- باج افزارها (Ransomware)
- WannaCrypt-CryptoMix-Locky-SynAck-Cerber
- WannaCrypt در سال ۲۰۱۷ بیش از ۲۳۰ هزار رایانه را در بیش از ۱۵۰ کشور جهان آلوده ساخت و به ۲۸ زبان از قربانیان باج طلب می کند.
- Cerber در سال ۲۰۱۶– تغییر حالت هر ۱۵ ثانیه–حمله به آفیس
- Locky آلوده نمودن بیمارستان هالییوود و مبلغ ۲,۴ میلیون یورو باج بگیرد.

بدافزارها و نرم افزارهای مخرب

- ردگم کن ها (Rootkits)
- جاسوس افزار ها (Spyware)
- آگهی‌افزار (Adware)
- کی‌لاگر (Keylogger)
- ...

بدافزارها و نرم افزارهای مخرب

- **نمونه هایی از تاثیرات بدافزارها بر روی رایانه ها**
- کندی سیستم کاربر
- ایجاد پیام های خطا بطور مستمر
- راه اندازی مجدد سیستم
- ارسال هرزنامه هایی به پست الکترونیکی دیگر از پست الکترونیکی شما
- نصب نوارابزارهای جدید و ناخواسته
- نمایش آیکون های جدید و ناخواسته

بدافزارها و نرم افزارهای مخرب

- **نمونه هایی از رو شهای مقابله با بدافزارها**
- فعال کردن تنظیمات فایروال
- نصب و به روز رسانی آنتی ویروس
- استفاده از مرورگرهای امن
- مدیریت نمودن رایانه
- اسکن نرم افزار جدید(پس از نصب یک برنامه جدید)
- تهیه نسخه پشتیبان از داده ها
- نصب نرم افزارها از منابع معتبر

این حمله ها به چه صورتی انجام می شود؟

- بدافزار میتواند شکل های متفاوتی به خود بگیرد؛ ممکن است از راه برنامه هایی با منابع نامطمئن ،همچون نرم افزارهای قفل شکسته، به رایانه تان منتقل شود. در ضمن این امکان وجود دارد که بدافزار از راه های زیرکانه ای به رایانه تان نفوذ کند؛ برای مثال، صفحه ای که همچون یک اخطار امنیتی طراحی شده باشد. علاوه بر این، بدافزارها میتوانند از راه ابزارهای ذخیره سازی مثل یو.اس.بی درایو یا انتقال فایل از طریق شبکه منتقل شوند. برخی وبسایت های دانلود رایگان توسط هکرها مدیریت میشوند. این وبسایت ها (که در ایران نیز بسیار پرطرفدار هستند) به کاربر امکان دانلود مجانی نرم افزارها رامیدهند، اما به طور پنهانی بدافزار روی رایانه نصب میکنند.

- **آنتی ویروس**

- به برنامه یا مجموعه ای از برنامه ها اطلاق می شود که برای محافظت از کامپیوتر ها در برابر ویروس ها استفاده می شوند. مهم ترین قسمت هر برنامه ضد ویروس موتور اسکن آن است

- جزئیات عملکرد هر موتور متفاوت است ولی همه آنها، وظیفه اصلی شناسایی فایل های آلوده به ویروس را بر عهده دارند .

- آنتی ویروسها دارای یک بانک اطلاعاتی هستند که شامل امضای ویروس Virus signature هاست. یک رشته بایتی است که با استفاده از آن می توان یک ویروس را به صورت کد یکتا مورد شناسایی قرار داد.

- آنتی ویروس، به محض این که کدی را ملاحظه کرد که معادل یکی از امضای ویروس ها باشد آن را به عنوان ویروس شناسایی می کند.

- **آنتی ویروس**

- در بیشتر موارد در صورتی که فایل آلوده باشد برنامه آنتی ویروس قادر به پاکسازی آن و از بین بردن ویروس است .

- در مواردی که این عمل ممکن نیست مکانیزمی برای قرنطینه کردن فایل آلوده وجود دارد.

- حتی می توان تنظیمات آنتی ویروس ها را به گونه ای انجام داد که فایل آلوده حذف شود.

رتبه بندی آنتی ویروس ها

در زیر می توانید لیستی از اول تا دهم را مشاهده نمایید

رتبه	نام آنتی ویروس	امتیاز آنتی ویروس	قیمت آنتی ویروس	تعداد دستگاه ها
۱	BitDefender Plus 2017	۹/۹	$۳۹/۹۹	۳
۲	Kaspersky 2017	۹/۸	$۴۹/۹۹	۳
۳	Norton Security 2017	۹/۷	$۳۴/۹۹	۱
۴	Avast Antivirus 2017	۹/۶	$۴۹/۹۹	۱
۵	McAfee	۹/۵	$۵۴/۹۹	۱
۶	MalwareByte	۹/۴	$۳۹/۹۹	۱
۷	AVG Anti-Virus	۹/۳	$۵۹/۹۰	۱
۸	Avira	۹/۲	$۲۹/۹۰	۱
۹	ESET Node 32	۹/۱	$۳۹/۹۹	۱

کنترل امنیت اطلاعات

- به اقداماتی گفته می‌شود که منجر به حفاظت ، پیشگیری ، مقابله/واکنش، و به حداقل رساندن دامنه تهدیدات امنیتی در صورت بروز می شود.
- مدیریتی
  - کنترل مدیریتی عبارتند از سیاست‌ها، رویه‌ها، استانداردها و رهنمودهای مکتوب که توسط مراجع مسئول تأیید شده است.
- فنی
  - کنترل فنی استفاده از نرم‌افزار، سخت‌افزار است برای نظارت و کنترل دسترسی به اطلاعات و سیستم‌های کامپیوتری.
- فیزیکی
  - کنترل فیزیکی برای حفاظت و کنترل محیط کار و تجهیزات کامپیوتری و نحوه دسترسی به آنها است که جنبه فیزیکی دارند

درب، قفل، گرمایش و تهویه مطبوع، آژیر دود و آتش، سیستم دفع آتش‌سوزی، دوربین‌ها مداربسته، موانع، حصارکشی، نیروی‌های محافظ

خط مشی امنیت اطلاعات Information Security Policy

- حفاظت از کدام دسته از اطلاعات سازمان برای ما مهم تر است؟
- ما باید خود را برای چه نوع ریسکهایی آماده کنیم؟
- چه خطراتی درستی، محرمانگی و در دسترس بودن اطلاعات سازمان ما را تهدید می کند؟
- پیشنهادهای ما برای پیشگیری یا واکنش در برابر این خطرات کدامند؟

موضوعات امنیتی مرتبط با نیروی انسانی

- یکی از چالش های بزرگ امنیت اطلاعات نیروی انسانی در هر شرکت یا سازمانی هستند، در این زمینه باید موارد زیر را کنترل کنیم.
  - آیا افراد سازمان کارهای مجاز و غیرمجاز امنیتی را می شناسند و از تبعات آنها آگاهند؟
  - آیا آنها از گزارش دهی در مورد وقایع امنیتی اطلاعات (نظیر خطاهای نرم افزاری، نقص‌های امنیتی، ویروس‌ها و ...) را یاد گرفته‌اند؟
  - چه سطحی از گزینش برای هر شغل لازم است؟
  - آیا برای کارکنان تازه و کم تجربه، آموزش‌های خاص در ارتباط با امنیت اطلاعات در نظر گرفته می‌شود؟

امنیت فیزیکی و محیطی

- آیا به مسائل زیر در سازمان توجه شده است؟
  - تعریف سطوح امنیت فیزیکی در سازمان
  - توجه به فضاها، دیوارها، مکانیزم‌های کنترلی، نگهبانی، نرده و حفاظ، سیستم‌های هشداردهنده، قفل‌ها و ...
  - توجه به حفاظت در برابر حوادث طبیعی نظیر سیل و زلزله و ...
  - توجه به سایر حوادث نظیر آتش‌سوزی، ترکیدگی لوله و ...
  - کنترل‌های ورود و خروج و عبور و مرور در سازمان
  - تعریف مسیرها و مکانهای ایزوله برای حمل و بارگیری
  - نصب و حفاظت از تجهیزات مهم

امنیت فیزیکی و محیطی

- آیا به مسائل زیر در سازمان توجه شده است؟
  - منابع تغذیه و منابع انرژی، برق اضطراری
  - امنیت کابل کشی‌ها (شبکه کامپیوتری، تلفن، دوربین مدار بسته، سیستم اعلام حریق، دزدگیر و ...)
  - تعمیرات و نگهداری تجهیزات
  - امنیت تجهیزات قابل حمل (مثل لپ تاپ) در خارج از سازمان
  - شیوه خروج اموال از شرکت و ورود مجدد اموال به شرکت

کنترل دسترسی ها

- دسترسی به اطلاعات همواره می تواند موجب بروز مشکلات امنیتی شود بنابراین موارد زیر باید به روشنی تعریف شده باشد:
  - مدیریت سطوح دسترسی کاربران
  - مدیریت و کاربرد اسامی رمز
  - امنیت تجهیزات کاربر در غیاب کاربر
  - کنترل مسیرهای شبکه ای
  - اعتبارسنجی کاربران در اتصال از خارج از شبکه
  - حفاظت درگاه های دسترسی از راه دور

چکار کنیم؟؟؟

تهیه نسخه پشتیبان

- یکی از راهکارهای پاسخگویی به حوادث و رخدادهای رایانه ای نظیر خرابی یا عملکرد نادرست سخت افزار یا نرم افزار، اشتباه کاربران، حملات عمدی یا غیر عمدی رایانه ای، هر حادثه ای که منجر به تخریب داده می شود، تهیه نسخه پشتیبان قابل اعتماد است.
- در یک سازمان لازم است از کلیه داده های الکترونیکی اعم از بانک داده ها و اطلاعات ، نرم افزارهای کاربردی، فایلهای پیکربندی، سیستم عاملها، فایلهای داده ای، ابزارهای سیستمی، و ... نسخه پشتیبان قابل اعتماد تهیه گردد و در محل امنی نگهداری شود و بطور مستمر بروز رسانی گردد

- استفاده از کلمه عبور مناسب
- تغییر کلمه عبور
- نصب و بروزرسانی آنتی ویروس
- عدم دانلود فایل از سایت های ناشناس
- بازنکردن ایمیل های ناشناس
- بروزرسانی سیستم عامل
- دریافت فیلترشکن از منابع مطمئن

مفاهیم حفاظت دیجیتالی در کتابخانه ها

تاریخچه اینترنت

- Arpanet
- 1967

مفهوم شبکه

- انواع شبکه به لحاظ گستردگی جغرافیای
- Lan,man wan
- internet

پروتکل

- Tcp/ip
- Pop3
- Smtp
- http

کلاس های مختلف ip

- Class a(1-126)
- Class b(128-191)
- Class c(192-223)

دستورات تست شبکه

- Ipconfig/all
- Ping ip address

فضای مجازی فرصت ها و تهدیدها

- فضای مجازی با هر تعریف و تعبیری، قلمروی وسیع و رو به رشد است. هر روز در آن شاهد نوآوری و ورود نرم افزارهای جدید هستیم که با توجه به نیازهای کاربران طراحی و ساخته می شود، این فضا به محل و محملی برای پاسخگویی به نیازهای ارتباطی و عرضه تولیدات تبدیل شده است.

عموماً وقتی که صحبت از فضای سایبری و مجازی می‌شود، قریب به اتفاق ما متوجه سایت‌ها و صفحات وب می شویم حال آنکه این فضا بسیار گسترده و وسیع است که مهمترین ابعاد آن عبارتند از شبکه‌های خبری و اجتماعی مجازی چند لایه، بازی های آنلاین، آموزشگاه های الکترونیک، اتاق های گفتگو، بانک های اطلاعاتی دیجیتال و ... که در کنار سایر تولیدات فرهنگی مثل فیلم ها و انیمیشن ها که با کمک ابزارهای رایانه ای، سطح و فرآیندهای جدیدی پیدا کرده اند.

در چنین شرایطی بهترین گزینه برای مواجهه با آن، شناخت دقیق این پدیده با همه ابعاد به خصوص فرصت ها و تهدیدات است تا بتوانیم آگاهانه به سراغ آن برویم.. همچنین لازم است مسئولان امر به جای رها کردن این محیط بسیار مهم و تأثیرگذار در زندگی فردی و اجتماعی افراد جامعه، نسبت به هدایت و فرصت‌سازی از آن اندیشه‌ای جدی و راهبردی داشته باشند

- واقعیت این است که امکان انسداد مسیر توسعه فضای مجازی در زندگی انسان امروز بسیار سخت و شاید غیر ممکن است و اساساً چنین اندیشه‌ای، با توجه به اینکه این ابزارها غالباً برای کمک به انسان ها و پیشبرد اهداف و پاسخگویی به نیازهای او ساخته می شوند، امری غیر عقلایی به نظر می‌رسد

بهترین راه برای بهره مندی از فضای مجازی و رسانه های دیجیتال شناخت ابعاد مختلف آن به خصوص فرصت ها و تهدیدات و لایه بندی کردن این فضا براساس مخاطبین و مصونیت بخشی راهبردی در برابر تهدیدات و بهره مندی از فرصت های پیش روی است

الف- فرصت ها

- گسترش جهان پیرامونی انسان ها؛
- سرعت در انتقال و دسترسی به اطلاعات و دانش
- تنوع و جذابیت؛
- ارتباطات دوسویه و چند سویه
- برچیده شدن انحصار رسانه ای و گسترش عدالت در این حوزه؛
- کاهش هزینه‌های اقتصادی زندگی؛
- کمک به حفظ محیط زیست؛
- گسترش و سرعت تعاملات و تبادل نظر؛
- کمک به کاهش ترافیک در شهرهای بزرگ؛

ب- تهدیدات؛

- ایجاد تغییر در حوزه فرهنگی و سبک زندگی؛
- تخریب چهره و شخصیت های معروف و تاثیرگذار
- مسایل و مخاطرات امنیتی؛
- به خطر افتادن حریم خصوصی و حقوق افراد جامعه؛
- جابجایی واقعیت ها،
- آسیب های اجتماعی؛

چرا حفاظت اطلاعات

- هنگامی که اطلاعات در قالب های دیجیتالی قرار می گیرند،ماهیت،ارزش،اهداف و ساختار متفاوتی را پذیرفته اند.ماهیت محیط کاملا" متفاوت دیجیتالی بر چالش های موجود در حفاظت منابع افزوده است.حفاظت از منابع دیجیتال به واسطه طبیعت پویا ومتغییری که دارند بسیار متفاوت از منابع آنالوگ است. و این تفاوت ها است که ضرورت مطالعه ماهیت متفاوت اطلاعات دیجیتال را نمایان می سازد.از طرفی دموکراسی سرمایه گذاری در دنیای فناوری اطلاعات ،عامل دیگری است که ماهیت به سرعت رشد کننده انواع نرم افراها و سخت افزارها را سبب گشته است.سرعت تغییرات به حدی است که اگر امروز به تبیین راهبردهای حفاظتی نپردازیم فردا بسیاری از اطلاعات دیجیتالی را از دست خواهیم داد.

چرا باید از داده ها حفاظت کرد

- ماهیت داده ها:داده ها در خطر هستند،چرا که در غالب مشخص پرونده ای برروی رسانه ای موقت و گذرا ظبط شده اند و به یک الگوی رمز گذاری(زبان برنامه نویسی) نیز نیاز دارند.رمز گشایی منابع آنالوگ تنها به توانایی های بشری نیاز دارد ،اما مدارک دیجیتال از آن جهت که ماهیتا" به "ابزارهای ذخیره ای"خود محدود نشده اند،با منابع آنالوگ متفاوت اند.
- ناپایداری داده ها:داده های دیجیتالی در خطرند،نه به این خاطر که ذاتا"آسیب پذیر یا ناقص هستند ، بلکه به این دلیل که شتاب پیوسته آهنگ همانند سازی،انطباق و افزونگی سخت افزار،نرم افزار،و قالب بندی داده ها،و استاندارد های تسهیل شده که ممکن است به معنای نا خوانایی،تفسیرناپذیری یا بی استفاده بودن جریان بیتی در آینده باشد،در جریان است.داده ها به صورت"رمز"ذخیره می شوند،در نتیجه پیش از تشخیص و استفاده از آن ها در محیط رایانه ای-حتی اگر از استانداردهای آزادی نیز بهره گرفته باشند-به عنصری رمزگشا نیاز دارند و این عناصر رمزگشا روز به روز تغییر می کنند.

- پیچیدگی داده ها:اگر تولید کنندگان کنونی،داده های دیجیتالی را صریح و روشن ارائه ننمایند،خوانندگان و بهره گیران آینده با مشکل روبرو می شوندو پیچیدگی داده ها برای آن ها رمزگشایی نخواهد شد. یک دیسک نوری چند رسانه ای و ابتکاری،بسیاری از ارزش های خود را ازارتباطات بین اشیای دیجیتالی کسب می کند نه ازمحتوای اطلاعاتی خود اشیا.
- سه دلیل بیان شد تا دریابیم که اطلاعات دیجیتال برای بقا نیازمند حفاظت هستند و این،موضوع کم اهمیتی نیست.چرخه زندگی داده های دیجیتال آنقدر طولانی نیست که منتظر ظهور رسانه ای بهتر بمانیم .ذخیره سازی داده ای تا کنون نتوانسته است همانند کاغذ یا ریز فیلم ،دوام و پایداری خود را اثبات کند،اما تحولات فناورانه در سوی دیگر این فرایند قرار دارند.ذخیره سازی داده ها فقط ۵۰ سال پیش و با کارت پانچ شروع شد و به نوارهای کاغذی،نوارهای مغناطیسی،دیسک مغناطیسی،دیسک نوری

نرم افزارهای تحت وب

- این نرم افزار نوع خاصی از نرم افزارهای کلاینت و سرور هستند که روش طراحی و توسعه آنها نسبت به نرم افزارهای ویندوزی مدرن تر و توانا تر است، نرم افزار تحت وب روی کامپیوتر کلاینت نصب نمی شود و کاربر با استفاده از Browserهای مرسوم مانند (گوگل کروم، فایرفاکس، اپرا، اکسپلورر) به آن دسترسی پیدا می کنند و از یک هسته پایدار بهره می برند و با تغییر در عملکرد یا آپدیت برای همه کاربران در سطح شبکه جهانی اینترنت تغییر می کند.

- سرعت دسترسی به نرم افزار تحت وب یا web basedاز سرعت و عملکرد بسیار بهتر و مطلوب تری برخوردار است و میتواند با استفاده از موبایل، تبلت و لپ تاپ و هر دستگاهی که اجازه باز کردن صفحات اینترنتی را می دهند مانند تلویزیون های هوشمند از قابلیت های آن بهرمند شد.
- یک پایگاه داده برای همه کاربران از دیگر ویژگی های تحت وب بودن است همه عملیات از قبیل عضویت، تراکنش های مالی، سفارشات، رزرو ها در یکجا قرار می گیرند و این مهم موجب حذف پراکندگی و تکرار اطلاعات می شود، از سویی پشتیبان گیری از این پایگاه داده به سادگی قابل انجام خواهد بود.

تهدید ها در فضای مجازی کدامند

تهدیدها در فضای مجازی دو گروه هستند

گروه اول

- تهدید هایی که فعالیت هایتان را تحت تاثیر قرار میدهند.اگر امنیت سیستم تان به خطر بیافتد،داده و اطلاعات تان آسیب دیده ،به دست افراد ناشایست افتاده و یا در اطلاعات ار سالی/دریافتی تان و وب سایت هایی که بازدید می کنیددست برده می شود

گروه دوم

- تهدید هایی هستند که به شخص شما آسیب می رسانند.بدون رعایت احتیاط،امکان دارد هویت،محل کار و یا دیگر اطلاعات شخصی تان افشا شده،امنیت تان به طور جدی به خطر بیافتد

تهدید ها چگونه عمل می کنند

- روشهای حمله به کنشگران و خبرنگاران در محیط های آنلاین بسیار است، هرچند برخی از همه مشهورتر هستند.سه نوع معمول این حمله ها:
- جعل اینترنتی
- بد افزار
- حملات با واسطه

تهدید شماره ۱ :جعل اینترنتی(فیشینگ)

- در این نوع حمله اینترنتی حمله کننده وانمود می کند که شخص یا وب سایتی است که شما به آن اعتماد دارید.هدف از این کار دریافت پسورد شما یا نصب بد افزاری برروی سیستم شماست


facebook
Dear Facebook user,
In an effort to make your online experience safer and more enjoyable, Facebook will be implementing a new login system that will affect all Facebook users. These changes will offer new features and increased account security.
Before you are able to use the new login system, you will be required to update your account.
Click here to update your account online now.
If you have any questions, reference our New User Guide.
Thanks,
The Facebook Team
Update your Facebook account
Update
This link goes to http://facebooki.ir - NOT the real Facebook!


aparat.com/cyberpolice.ir

چرا اگاهی از این نوع حمله اهمیت دا رد

- نفوذ گران با استفاده از پسورد شما به محتوای ایمیل،حساب بانکی،یا هر حساب کاربری دیگری که در اینترنت دارید دسترسی پیدا می کنند.با داشتن پسوردایمیل می توانندایمیل های شما را بخوانند نام افرادی که با آنها در ارتباط هستید ببینند،به حساب بانکی تان دسترسی پیدا کنندو حتی خودشان را به جای شما جا بزنند بطور کلی هر کس که در اینترنت از پسورد استفاده می کند در معرض این نوع حمله است.

این نوع حمله چگونه انجام می شود.

- نفوذ گران اینترنتی اغلب با آدرسهای ایمیل مشابه یا نشانی وب سایت هایی شبیه اسامی آشنا،خودشان را به جای اشخاص معتبر جا می زنند.برای مثال ممکن است ایمیلی با شناسه کاربری دوستان یا همکاران تان ارسال کنند که از سرویس ایمیل دیگری فرستاده شده باشد،یعنی به جایjlxxxx@gmail.com آدرس ایمیل xxxx@yahoo.comاستفاده کنند. یا لینکی برای تان ارسال کنندکه شما را به صفحه ای هدایت می کند که نشانی اش بسیار شبیه آدرس وبسایت های مورد اطمینان تان است.برای مثال،آدرس سایت هایی مانند facebookیا gmailاما با اندکی تفاوت در طرز قرار گرفتن حروف(faceboook.com به جای facebook.com).حتی همانطور که در تصویر بالا دیده می شود،متن نمایش داده شده ممکن است کاملا" درست باشد،حال آنکه آدرس پشت لینک شما را به جای دیگری هدایت می کند.این تفاوت ها آنقدر ظریفند که افراد کمی ممکن است متوجه آن شوند و این نقطه قوت نفوذگران است

رعایت نکات زیر را به همه کاربران توصیه می کنیم:

- همیشه نشانی ایمیل فرستنده را چک کنید
- محتوای ایمیل های دریافتی را با دقت بررسی کنید،ممکن است بی ربط یا غلط باشد.ایمیل های فیشینگ معمولا"از شما می خواهند که هر چه زودتر کاری را انجام دهید یا روی لینکی کلیک کنید.ایمیل ممکن است دقیقا"نام و نام خانوادگی شما را ذکر نکرده باشد.
- نشانی لینک های 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 بوده اید؟

تهدید شماره ۲: بدافزار

- **بدافزار چیست؟**

- بدافزار اصطلاحی کلی است برای برنامه های کامپیوتری مخرب نظیر انواع ویروسها، کرمها، و برنامه های مشابه آن. بدافزار میتواندبه چند روش به شما ضربه بزند؛ ممکن است با ربودن گذرواژه هایتان - یا هر چیز دیگری که تایپ میکنید - به حسابهای کاربریتان دسترسی پیدا کند یا از کامپیوترتان به اینترنت وصل شده و به دیگر کامپیوترها حمله کند. بدافزار حتی میتواند فایل هایتان را بازرسی کرده یا اطلاعاتی که روی کامپیوتر ذخیره کرده اید را به جای دیگری ارسال کند.

- برخی گونه های 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 نظرفنی، یک ویروس برای انتقال از رایانه ای به رایانه دیگر نیازمند اقدام کاربر است؛ مثلا، ارسال مجدد ایمیل، اما کِرم به طورخودبه خودی گسترش مییابد. با این حال، همه انواع بدافزار به طور بالقوه از امکان انتشار و تخریب مؤثر برخوردارند.
- • **اسب تروِیا**. این گونه بد افزار برنامه مخربی است که خود را درون نرم افزارهای به ظاهر بی خطر پنهان میکند؛ همانطور که درافسانه اسب تروِیا اشاره شده. این نوع بدافزار در آغاز به نظر بی خطر میآید یا اصلا تشخیص داده نمیشود. او منتظر میماند
- و در موقع مناسب با آغاز حمله تهدیدش را عملی میسازد


aparat.com/ashnasecure

چرا باید درباره این نوع حمله هوشیار باشم؟

- بدافزار راه مناسبی برای رخنه گران است تا برنامه های نظارتی شان را به منظور
- جمع آوری اطلاعات درباره شما یا شناسائی فعالیتهایتان اجرا کنند. هر
- کاربر اینترنتی در معرض آسیب دیدن از سوی بدافزار است.

این حمله به چه صورتی انجام می شود؟

- بدافزار میتواند شکل های متفاوتی به خود بگیرد؛ ممکن است از راه برنامه هایی با منابع نامطمئن ،همچون نرم افزارهای قفل شکسته، به رایانه تان منتقل شود. در ضمن این امکان وجود دارد که بدافزار از راه های زیرکانه ای به رایانه تان نفوذ کند؛ برای مثال، صفحه ای که همچون یک اخطار امنیتی طراحی شده باشد. علاوه بر این، بدافزارها میتوانند از راه ابزارهای ذخیره سازی مثل یو.اس.بی درایو یا انتقال فایل از طریق شبکه منتقل شوند. برخی وبسایت های دانلود رایگان توسط هکرها مدیریت میشوند. این وبسایتها (که در ایران نیز بسیار پرطرفدار هستند) به کاربر امکان دانلود مجانی نرمافزارها رامیدهند، اما به طور 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 دیگرمنتقل 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 برنامه ها ارائه میکنند، همواره میبایست در برابر تهدیدهای امنیتی بالقوه گوش به زنگ ماند

نمونه های دیگری از بد افزارها

ردگم‌کن‌ها:به انگلیسی: (Rootkits)

- رد گم کن واژه مصوب فرهنگستان زبان و ادب فارسی برای (به انگلیسی: (Rootkits است. هنگامی که یک برنامهٔ خرابکار روی یک سیستم نصب می‌شود بسیار مهم است که مخفی باقی بماند تا از تشخیص و نابودی در امان باشد. همین وضعیت دربارهٔ یک مهاجم انسانی که به‌طور مستقیم وارد یک رایانه می‌شود برقرار است. ترفندهایی که به عنوان روتکیت‌ها شناخته می‌شوند اجازه این مخفی کاری را می‌دهند. آن‌ها این کار را با اصلاح سیستم عامل میزبان انجام می‌دهند به نحوی که بدافزار از دید کاربر مخفی بماند. روتکیت‌ها می‌توانند از این که یک پروسهٔ خرابکارانه در لیست پروسه‌های سیستم دیده شود ممانعت کنند، یا مانع خوانده شدن فایل‌های آن شوند. در ابتدا یک روتکیت مجموعه‌ای از ابزارها بود که توسط یک مهاجم انسانی بر روی یک سیستم یونیکس نصب می‌شد که به مهاجم اجازه می‌داد تا دسترسی مدیریتی داشته باشد. امروزه این عبارت به‌طور عمومی تر برای فرایندهای مخفی‌سازی در یک برنامهٔ خرابکار استفاده می‌شود.

درهای پشتی:(به انگلیسی: Backdoors)

- درِ پشتی روشی است برای خنثی‌سازی رویه‌های معمول تأیید اعتبار. وقتی یک سیستم دارای چنین رویه‌هایی باشد یک یا چند درِ پشتی ممکن است نصب شوند تا دسترسی‌های آتی را آسان‌تر سازد. درهای پشتی ممکن است حتی پیش از یک نرم‌افزار خرابکار نصب شوند تا به مهاجمان اجازهٔ ورود دهند.

جاسوس‌افزارها

- جاسوس‌افزارها (Spyware،) اطلاعات مختلف در مورد او را جمع‌آوری می‌کنند. اکثر جاسوس‌افزارها از دید کاربرها مخفی می‌مانند و تشخیص و پیدا کردن آن‌ها در اغلب موارد مشکل است. برخی از جاسوس‌افزارها مانند کی‌لاگرها ممکن است توسط مسئول یک سازمان یا شرکت بر روی رایانه‌ها نصب شوند تا رفتار کاربران قابل ارزیابی و بررسی باشد. جاسوس‌افزارها هر گونه اطلاعاتی را می‌توانند جمع‌آوری کنند. این اطلاعات می‌تواند اطلاعات شخصی یک کاربر مانند گشت و گذارهای وی بر روی اینترنت یا مشخصات حساب‌های مختلف وی مانند رمز عبور پست الکترونیکی و... باشد. علاوه بر این، جاسوس‌افزارهای می‌توانند در کنترل رایانه توسط کاربر اختلال ایجاد کنند. به عنوان مثال، جاسوس‌افزارهای می‌توانند کاربر را به بازدید از یک صفحهٔ خاص اینترنتی مجبور کنند یا اینکه با تغییر تنظیمات رایانهٔ وی، باعث کاهش سرعت اینترنت و دسترسی غیرمجاز به رایانهٔ وی شوند.

آگهی‌افزار

- آگهی‌افزار یا برنامه‌های تبلیغاتی (Adware): این‌گونه برنامه‌ها همانند جاسوس‌افزارها دارای اثر تخریبی نمی‌باشند و وظیفه آن‌ها باز کردن صفحات خاص اینترنتی جهت اهداف تجاری و تبلیغی است

جوک‌ها

- جوک‌ها (Joke)برنامه‌هایی هستند که ادعا می‌کنند در حال انجام عملیاتی تخریبی بر روی سیستم شما می‌باشند ولی در واقع این‌گونه نبوده و کار آن‌ها چیزی جز یک شوخی ساده نمی‌باشد. متأسفانه برخی کاربران به سادگی تحت تأثیر جک‌ها قرار گرفته و با تلاش برای از بین بردن چیزی که مخرب نیست باعث ایجاد تخریب بیشتری می‌شوند.

کلک

- کلک (Hoax)این برنامه‌ها با سوء استفاده از کم بودن اطلاعات تخصصی کاربران، آن‌ها را فریب داده و با دستورات و توصیه‌های اشتباه باعث می‌شوند که کاربر شخصاً کاری تخریبی بر روی سیستم خود انجام دهد. به عنوان مثال وانمود می‌کنند که فایلی خاص در مسیر سیستم‌عامل یک برنامه خطرناک است و باید توسط کاربر حذف شود. غافل از اینکه این فایل سیستمی بوده و برای عملکرد درست سیستم‌عامل، وجود آن لازم است.

شماره‌گیرها

- شماره‌گیر (Dialer): این‌گونه برنامه‌ها وظیفه‌شان ارتباط دادن کاربر از طریق خط تلفن به سرورهایی در دیگر کشورها برای دسترسی مستقیم به اطلاعات آن‌ها می‌باشد. این سرورها معمولاً مربوط به سایت‌های غیراخلاقی بوده و برقراری ارتباط با آن‌ها از طریق خط تلفن باعث هزینه بسیار زیاد مالی می‌گردد.

بارگیرها

- بارگیر (Downloader): کار این‌گونه برنامه‌ها Downloadکردن بدافزارها و اجرای آن‌ها است.

کلیک‌کننده‌ها

- کلیک‌کننده (:(Adclicker)این‌گونه برنامه‌ها لینک صفحات تبلیغاتی را دنبال نموده و به این طریق حالت کلیک شدن بر روی آن صفحه تبلیغاتی خاص را شبیه‌سازی می‌کنند و باعث بالا رفتن hitآن می‌شوند.

درهای پشتی

- درهای پشتی (Backdoors)ابزاری برای نفوذگرها هستند که به وسیله آن‌ها می‌توانند سیستم‌های دیگر را در کنترل خود درآورند. درهای پشتی درون شبکه، پورت‌های TCP یا UDP را باز می‌کنند و شروع به گوش کردن نموده تا دستورات نفوذگرها را اجرا کنند. درهای پشتی از جهت نداشتن قابلیت تکثیر شبیه ترویاها هستند.

گذرواژه‌دزدها

- گذرواژه‌دزد (:(Password-Stealer)این‌گونه برنامه‌ها که نوعی ترویا هستند کارشان دزدی پسورد از روی سیستم‌ها و ارسال آن‌ها برای نفوذگرها است.

بهره‌کش‌ها

- بهره‌کش‌ها ((Exploits)کدهای مخربی هستند که با استفاده از آسیب‌پذیری‌های یک سیستم امکان دسترسی از راه دور به آن سیستم را فراهم می‌کنند.

کی‌لاگر

- کلیدنگار یا کی‌لاگر ((Keylogger)برنامه‌هایی هستند که با قرار گرفتن در حافظه از کلیدهای زده شده توسط کاربر گزارش گرفته و در قالب یک فایل برای نفوذگر می‌فرستند. البته باید بدانیم که کی‌لاگرها به صورت سخت‌افزاری نیز وجود دارند.

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

- حمله فرد میانی به حمله ای گفته میشود که شخص ثالثی اطلاعات رسالی/دریافتی تان از طریق اینترنت را برباید. هنگام اتصال به اینترنت، در تک تک گره های ارتباطی مسیر انتقال اطلاعات، ممکن است چنین حمله ای 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 گره های طول مسیر، با هدف جاسوسی، اقدام به جمع آوری اطلاعات کرده، اطلاعات عبوری را تغییر داده یا به شما اطلاعات دروغین تحویل دهد.

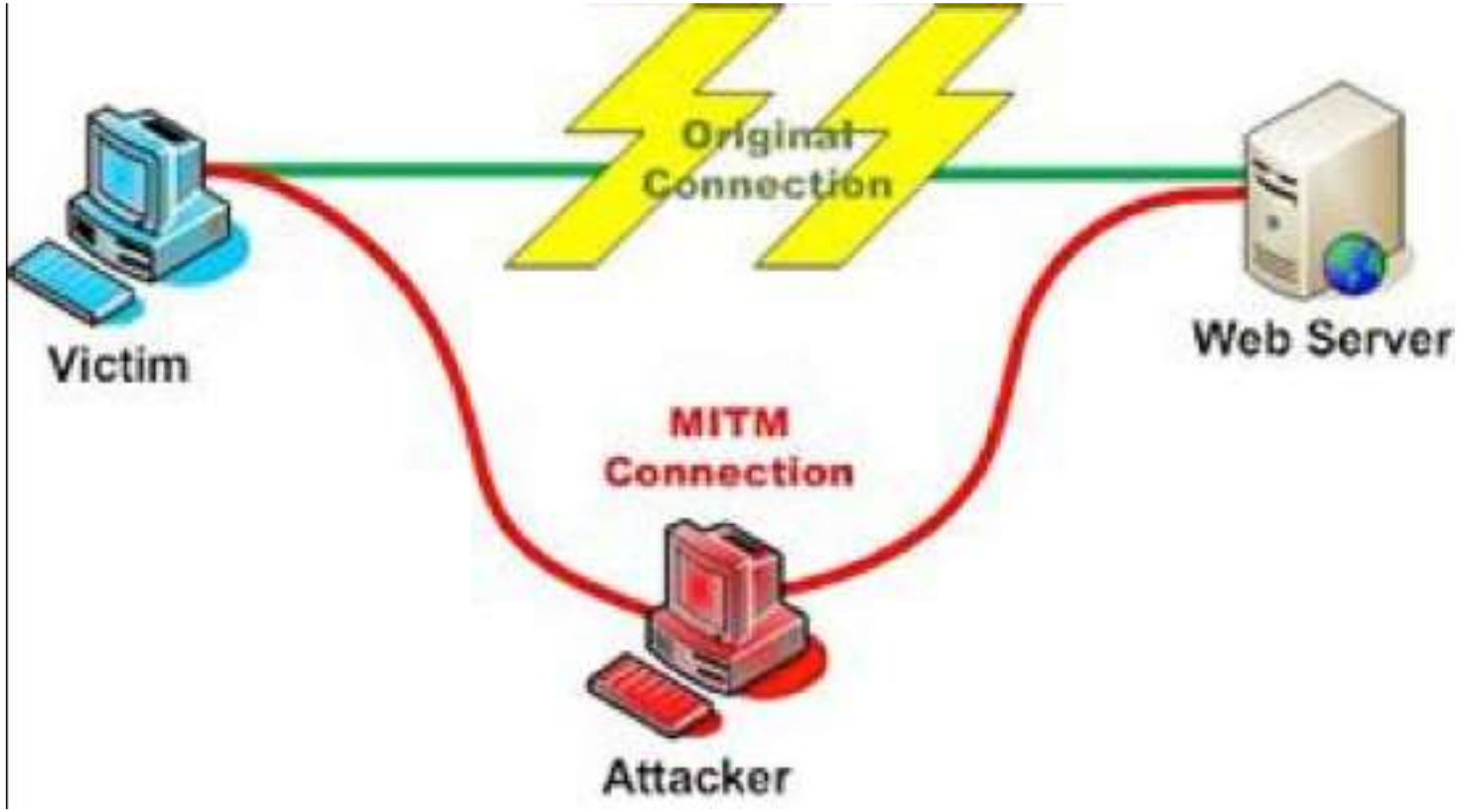
حمله مرد میانی (man-in-the-middle) چیست؟

- در حمله مرد میانی هکر میاد و خودش رو بین دو دستگاهی قرار میده که دارن با هم دیگه تبادل اطلاعات میکنن و از این طریق به راحتی میتونه اطلاعات رو شنود کنه و از طریق شنود میتونه به اطلاعات حساسی دست پیدا کنه بدون اینکه سیستم قربانی متوجه بشه. فرض کنید میخواهید از سیستم Aبه سیستم Bیک پیغام ارسال کنید هکر میخواد اطلاعات بین سیستم Aو Bرو شنود کنه پس میاد به سیستم Aمیگه که من سیستم Bهستم و به سیستم Bمیگه که من سیستم Aهستم و هر دو سیستم اطلاعاتشون رو میدن به هکر و تمامی اطلاعات از سیستم هکر عبور میکنه و توسط هکر قابل رویت و تغییر است.

چگونه میتوانیم جلوی حملات مرد میانی (man-in-the-middle)رو در شبکه خودمون بگیریم؟

- یکی از راه های جلوگیری از این حمله رمزنگاری اطلاعات است, پروتکل هایی مثل telnet , ftp , httpو... اطلاعات رو به صورت clear textارسال میکنند و در نتیجه اگر شخصی در شبکه ما حمله مرد میانی (man-in-the-middle)رو اجرا کند به راحتی به اطلاعاتی که توسط ما انتقال پیدا میکند دسترسی دارد و ما میتوانیم با استفاده از مکانیزم های رمزنگاری مثل ipsec , httpsو... جلوی لو رفتن اطلاعات رو در شبکه مون بگیریم.

- در نوع دیگری از حمله فرد میانی، تمرکز بر نظارت برکلمات کلیدی است. در این نوع حمله، به جای بررسی همه اطلاعات رد و بدل شده، گره ارتباطی حمله کننده، یاتنها بر کلمات کلیدی از پیش تعریف شدهای تمرکزمیکند 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


Original
Connection
Victim
Web Server
MITM
Connection
Attacker

چرا باید نسبت به این نوع حمله هشیار باشیم؟

- حمله فرد میانی بیشتر در شبکه های بی سیم عمومی(public wifi) رخ می دهد جایی که کاربران می توانند ارتباطات دیگر کاربران را رصد کرده یا مختل سازند.هرچند در دیگر گره های ارتباطی نیز ممکن است رخ دهد.

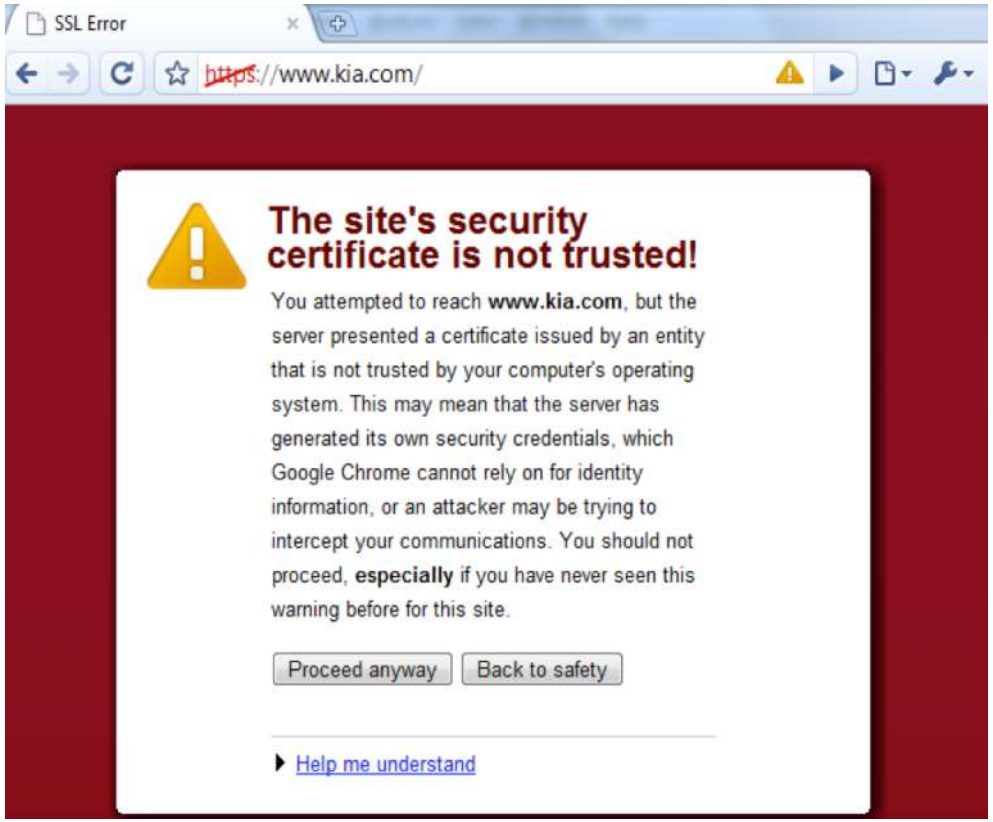
- علاوه بر خواندن و رصد اطلاعاتی که رد و بدل میشود، صاحبان کا فی نت ها یا ارائه دهندگان خدمات اینترنتی نیز میتوانند دسترسی به سایت های مورد نظر را محدود سازند. فیلترینگ ممکن است براین اساس انجام شود که شما چه کسی هستید، به چه سایتی قصد دارید مراجعه کنید، یا به دنبال چه محتوایی میگردید. فیلترینگ ممکن است همه دامنه وب را از کار بیاندازد، یا تنهاصفحات 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 وب سایت 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 سرمیزنید که حاوی اطلاعات حساس است، رایانه شما مجوزسایت را به طور خودکار، مرور و تأیید میکند. کسی که جریان اطلاعات را دستکاری کرده باشد نمیتواند از آن مجوزاستفاده کرده، شما اخطاری شبیه این دریافت خواهید کرد:(توجه داشته باشید که سایت های بدون گواهینامه امنیتی چنین اخطاری نشان نمیدهند و شما هنگام بازدید از آن وب سایت ها احتمالا متوجه نخواهید شد که تحت نظر قرارگرفته اید)

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 جستجوی های اینترنتی کاربران ایرانی که ازمرورگرهائی غیر از گوگل کروم استفاده کرده بودند، دسترسی پیدا کنند.


SSL Error
https://www.kia.com/
The site's security certificate is not trusted!
You attempted to reach www.kia.com, but the server presented a certificate issued by an entity that is not trusted by your computer's operating system. This may mean that the server has generated its own security credentials, which Google Chrome cannot rely on for identity information, or an attacker may be trying to intercept your communications. You should not proceed, especially if you have never seen this warning before for this site.
Proceed anyway
Back to safety
Help me understand

ارزیابی میزان خطر: قسمت

- 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
- ضعف های 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 نشسته اند. 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 شبکه ها: ترسیم تهدیدهای پیش روی**

موارد ایمنی زیر رعایت گردد

- فهرست رایانه ها، تبلت ها و موبایل هایی که با آن کار میکنید را درنظر بگیرید. آیا **سیستم عامل های** این رایانه ها ثبت شده وقانونی اند؟ یا از سیستم عامل های قفل شکسته استفاده میکنید؟برای هر دستگاه، پاسخ به این پرسش را جلوی نام آن یادداشت کنیداگر از سیستم عامل های قفل شکسته استفاده می کنیدباید در نظر داشته باشید که این نسخه ها، احتمالا حامل ویروس های از پیش جاسازی شده هستند. سیستم عامل و دیگرنرم افزارها را تا حد امکان از وب سایت رسمی یا توزیع کنندگان معتبر تهیه کنید. در ایران فروشگاه های لوازم رایانه ای به صورت گسترده نرم افزارهای قفل شکسته عرضه میکنند. این نرم افزارها غالبا آلوده به انواع بدافزارهایی اند که برخی از آنها برای جاسوسی از رایانه ها طراحی شده اند. 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 مرورگرهانسبت به حملات اینترنتی آسیب پذیری بیشتری دارند. هر دو مرورگر فایرفاکس و گوگل کروم از از این نظر امن تر از بقیه اند.
- برای مثال، مرورگر کروم راه یک سری حملات به خدمات gmail را سد میکند. در نتیجه این مرورگر برای کسانی که ازgmail زیاد استفاده میکنند مناسب تر است. اگر از رایانه های موجود در مکانهای عمومی (مانند کافی نت) استفاده میکنید و در آن امکان استفاده از گوگل کروم یا فایرفاکس وجود ندارد، تا حد امکان از وبسایت های حاوی اطلاعات حساس پرهیز کنید. با این حال، بدون رعایت نکات ایمنی دیگر، مرورگرها به تنهایی قادر به تضمین امنیت شما نیستند

- آیا از **افزایه ها (پلاگین)** در مرورگرتان استفاده میکنید؟ برخی افزایه ها ممکن است ناقل بدافزار باشند. همیشه سعی کنیدافزایه ها را از منابع قابل اطمینان، همچون وبسایت رسمی شان بگیرید.
- - آیا در وبسایت ها و برنامه های مختلف از **گذرواژه های متفاوت** استفاده میکنید؟ بکارگیری یک گذرواژه برای حسابهای کاربری متفاوت ممکن است به خاطر سپردنش را ساده تر کند، اما بسیار خطرناک است. اگر فردی گذرواژه تان را به دست آورد میتواند به دیگر حساب هایتان نیز دسترسی بیابد.

- آیا **passwordهااز ترکیب حروف و اعداد و علائم نوشتاری** ساخته شده اند؟ حدس زدن پسوردی که شامل ترکیب حروف، اعداد و علائم نوشتاری باشد دشوارتر است. سعی کنید پسوردهای یکتا و منحصربفردی بسازید که به سادگی قابل حدس زدن نباشند

- آیا با کمک **رمزگذاری از حریم ارتباطاتیتان** محافظت میکنید؟ رمزگذاری یکی از بهترین راهها برای محافظت از مکالمات درمحیط اینترنت است. در این باره در درسهای بعد بیشتر توضیح داده خواهد شد. آیا برای **دسترسی به ایمیل هایتان** از وبسایت استفاده میکنید یا از نرم افزار ایمیل؟ شبکه های اجتماعی چطور؟ آیادسترسی به آنها نیز با واسطه است؟
- - آیا از **ضد بدافزار و فایروال (دیوار آتش)** استفاده میکنید؟ و آیا این نرم افزارها به روز هستند؟بسیار مهم است که از آخرین ترتیبات امنیتی برای حسابهای کاربری و ابزارهای واسطه ای که استفاده کنید. به این موضوع بیشتر خواهیم پرداخت

آیا از فیلترشکنvpn یا دیگر انواع ابزارها برای دور زدن فیلترینگ استفاده میکنید؟ از کجا آنها را به دست آورده اید؟

- فیلترشکن ها و vpn ها خود میتوانند عامل توزیع بدافزار باشند شما میبایست از اعتبار منبع تأمین کننده فیلترشکن ها ی VPNآگاه باشید. به خاطر داشته باشید که تنها وبسایت رسمی تولیدکنندگان چنین ابزارهایی قابل اطمینان است.
- آیا **دیگران** نیز از رایانه تان استفاده کنند؟ اگر پاسخ مثبت است، این افراد چه کسانی هستند؟ آیا به حساب های کاربریتان نیز
- دسترسی دارند؟ برای حفظ امنیت خود و آنان، میبایست از محرمانه بودن اطلاعات دسترسی به حسابهای کاربری اطمینان
- حاصل کنید. این موضوع به خصوص وقتی اهمیت پیدا میکند که افراد مختلفی از یک رایانه استفاده کنند.

اقدامات عملی

- ✓ میزان امنیت و قابل اطمینان بودن شبکه هایی که از آن استفاده می کنم را بررسی
- کرده ام.
- ✓ به منظور افزایش سطح امنیت، گذرواژه ها را تغییر داده ام.
- ✓ سیستم عامل رایانه ام را به نوع رسمی و گواهینامه دار تغییر داده ام.
- ✓ دسترسی افراد به رایانه و حسابهای کاربری ام را محدود ساخته ام.
- ✓ مطمئن هستم همه برنامه های واسطه ای 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 ایمن تری استفاده میکنم. ✓
- همه افزایه ها (پلاگین ها)ی نصب شده روی مرورگرم را غیرفعال ساخته ام. ✓
- ضدبدافزار و فایروال مناسب نصب کرده و آنها را به روز نگه دارید.