پایه‌های امنیت رقمی

موضوع درس‌نامه : یادگیری پایه‌های ایمنی حساب‌های کاربری آنلاین وداده‌ها

شناخت تهدیدها

تلاش برای حفاظت از داده‌های خود به گونه‌ای همیشگی و در همه جا، خسته کننده و کمترعملی است. امنیت یک فرآیند است و تنها در بکارگیری ابزارها و نرم‌افزارهای باری‌گذاری شده، خلاصه نمی‌شود.

امنیت نخست با شناختن تهدیدهایی آغاز می‌شود که با آن‌ها روبرو می‌شویم و سپس انتخاب روش‌هایی که برای مقابله با این تهدیدها برمی‌گزینیم.

انواع تهدیدها

برای دیدآمد کردن تهدیدها بهتر است ۵ پرسش را از خود بپرسیم :

۱- چه اطلاعاتی و داده‌هایی را باید حفاظت کنم؟

۲- این اطلاعات و داده‌ها برای چه کسانی مهم هستند؟

۳- برای دسترسی به این اطلاعات آنها می‌توانند از چه ابزارهایی استفاده کنند؟

۴- پیامد دسترسی آن‌ها به این اطلاعات و داده‌ها برای ما چیست؟

۵- در برابر این تهدیدها، ما چه وسایل و ابزاری را می‌توانم بکار گیرم؟

چه اطلاعاتی را باید محافظت کنم.

ایمیل‌ها، پیام‌ها، مکالمات تلفنی، عکس‌ها، ویدیو، آدرس‌ها و هویت و مشخصات روابط و مخاطبان و غیره.

این اطلاعات برای چه کسانی مهم هستند؟

- **سازمان‌ها یا افرادی که موضوع مطلب هستند و یا مقاله آن‌ها را مورد پرسش قرار داده است.**
- **یک دولت خارجی و یا گروه‌های مخالف.**
- **یک قاضی یا پلیس خودسر که به شکل غیرقانونی قصد سواستفاده دارد.**
- **یک شرکت خصوصی و یک رسانه‌ی رقیب.**

برای دست‌یافتن به این اطلاعات، از چه ابزاری می‌توانند استفاده کنند؟

- **به شکل فنی: رصدکردن، هک**
- **به شکل قانونی: شنود، احضار**
- **به شکل اجتماعی: مهندسی اجتماعی (یعنی طراحی نقشه‌ای تا شما را به دام بیندازند)**
- **فیزیکی: دزدیدن، نصب بدافزارها**

پیامدهای دسترسی به این اطلاعات کدامند؟

- **افشا شدن موضوع / سوختن اطلاعات برای انتشار.**
- **مشکلات حقوقی/ عدلی برای یک منبع، برای خبرنگار و یا رسانه.**
- **تهدیدهای فیزیکی**

در برابر این تهدیدها، ما چه وسایل و ابزاری را می‌توانم بکار گیرم؟

- **تکنیکی ، نرم‌افزار و سخت‌افزارهای و مراقبت از داده‌ها**
- **حقوقی عدلی، مراجعه به پلیس و مراجع عدلی و شکایت**

حفاظت از فیشینگ

Phishing چیست؟ راهزن یا مهاجم ، طعمه‌ای را ارسال می کند ، پیام و اغلب به صورت ایمیل. این طعمه فرد را تشویق می‌کند تا داده‌های محرمانه خود را با او یا آن‌ها به اشتراک بگذارد.

اگر نصب یک نرم‌افزار ضد ویروس بر روی کامپیوتر یک اقدام مهم است، اما همچنین مهم است که هوشیاری لازم را به هنگام دریافت لینک یا فایل‌های پیوست از طریق ایمیل، مسنجر، پیامک، واتساپ، اسکایپ و سایر ابزارهای ارتباطی از خود نشان دهیم. **شبکه‌های اجتماعی و ابزارهای ارتباطی یکی از عوامل اصلی انتقال ویروس‌ها هستند.**

چند توصیه اساسی برای رعایت برای مقابله با پیام‌های آلوده:

- **فایل‌ها یا لینک‌هایی که از فرستندگان ناشناس دریافت می‌کنید، دانلود نکنید یا بر روی آن‌ها کلیک نکنید.**
- **آدرس ایمیل یا حساب شبکه اجتماعی فرستنده‌ی لینک را به دقت بررسی کنید.**
- **در صورت شک، از هویت فرستنده از طریق مخاطبان دیگر یا از طریق موتورهای جستجوگر اطمینان حاصل کنید.**
- **همچنین می‌توانید یک فایل یا آدرس اینترنتی دریافتی را با استفاده از خدمات آنلاینی مانند** Virustotal **بررسی کنید تا ببینید آیا مخرب است یا خیر.**
- **اگر فایل یا فرستنده به نظر شما مشکوک به نظر می‌رسد، به‌راحتی می‌توانید با تماس با متخصصان در این زمینه، راهنمایی و کمک بگیرید.**

چگونه یک لینک بدافزار را بشناسیم؟

تمرین : این لینک متعلق به چه کسی است

`https://www.facebook.secure.com/friends/`

پاسخ : این لینک ما را به فیس‌بوک نمی‌برد که به نزد secure.com **می‌برد!**

خواندن یک نام دامنه URL **برای پیشگیری از یک حمله فیشینگ بسیار اهمیت دارد.** (
(/https://freedom.press/training/email-security-tips

https://fa.wikipedia.org/wiki/%D9%81%DB%8C%D8%B4%DB%8C%D9%86%DA%AF

(https://webcade.ir/view/articleid/474)

URL یا آدرس اینترنتی

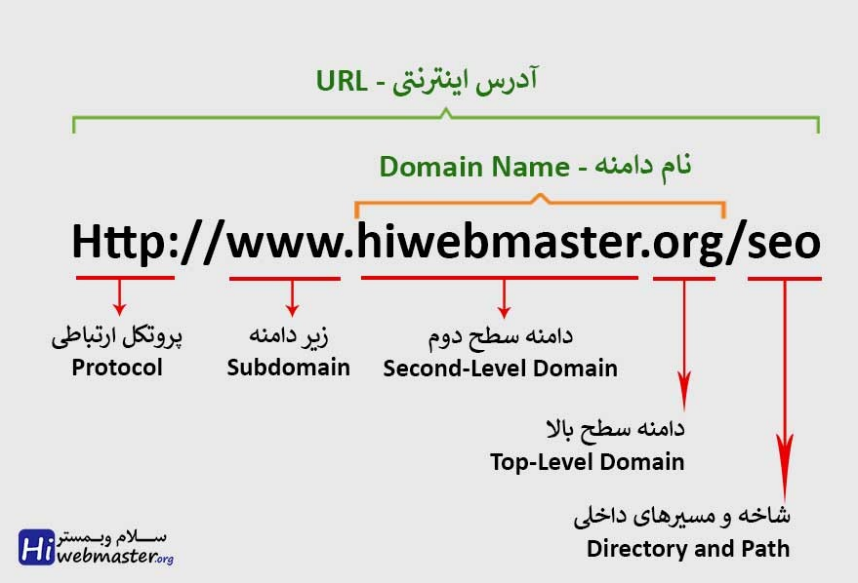
URL مخفف **Universal Resource Locator** است.
یک روش استاندارد جهانی برای مشخص کردن محل منابع در فضای جهانی اینترنت.

هر آدرسی که شما در نوار آدرس مرورگرتان وارد می کنید، یک URL یا ادرس اینترنتی است و **دامنه نیز بخشی از URL می باشد.** مثلا:

```
http://www.google.com
```

یا آدرس همین صفحه URL است :

```
https://hiwebmaster.org/urls
```



اولین جزء آدرس اینترنتی پروتکل آن است، پروتکل، استاندارد و قوانینی است که مشخص می کند چگونه کامپیوترهای درون یک شبکه با یکدگیر و با کامپیوتر های خارج از شبکه ارتباط برقرار کنند.

پروتکل انواع زیادی دارد که مهم ترین آنها پروتکل های http و https می باشد و این پروتکل ها در آدرس **برای ایجاد ارتباط، دریافت و ارسال داده ها** به کار می رود.

تمیرین :

این آدرس متعلق به کجاست؟
`https://drive.google.com.downlaod-photo.sytez.net`
و این؟

https://ajmfederation.com

برای دانسته‌های بیشتر می‌توانید به این آدرس‌ها بروید

https://learn.totem-project.org/courses/course-v1:Totem+TP_PM_FA+001/about

https://hiwebmaster.org/urls

حفاظت از حساب‌های کاربری آنلاین (برخط) خود

بیشترین خدمات آنلاینی که ما استفاده می‌کنیم، مانند ایمیل، شبکه‌های اجتماعی و غیره، با گذرواژه‌ها (Password) محافظت می‌شوند. بسیار مهم است که گذرواژه‌های قوی و دشواری درست کنیم، که در برابر حدس زدن یا پیدا کردن آن مقام باشند.

گذرواژه‌های خود را با استفاده از بررسی‌کننده گذرواژه در سایت nothing2hide آمتحان کنید!

درازای یک گذرواژه، عامل اصلی برای ایجاد یک گذرواژه قوی است، که قابلیت مقاومت در برابر یک حمله جستجوی فراگیر را دارد. افزودن اعداد، نویسه‌های خاص، حروف کوچک و بزرگ، اغلب منجر به ایجاد گذرواژه ضعیف یا یادگیری آن سخت می‌شود. اگر به جای استفاده از "گذرواژه"، از " گذرجمله " استفاده کنید، یک رشته کلمه آسان برای یادگیری و با درازای بسیار بیشتر نسبت به گذرواژه‌های قبلی‌تان به دست خواهید آورد.

Th$jHTo%46 : این گذرواژ کوتاه و یادآوردن آنهم دشوار است

اما این گذرواژه به آسانی در ذهن می‌ماند و دست‌یابی آن دشوار است.

به نام خداوند جان! بخشنده برای ما مردم کوشا و رستگار

(برخی از این کلمه‌ها را می توانید به زبان دیگری بنویسید! پشتو یا انگلیسی و....)

توصیه‌های بنیادی :

۱- گذرواژه‌های عادی را فراموش کنید و گذرجمله استفاد کنید.

۲- هر چه بیشتر جمله شما حرف و علامت داشته باشد، کمتر امکان شناسایی آن وجود دارد.

۳- از نام فیلم یا داستان و اطلاعات شخصی که آسان‌تر شناسایی می‌شوند، استفاده نکنید.

۴- برای هر حساب خود یک جمله متفاوت استفاده کنید.

چه راهبردهایی برای گذرواژه داشته باشیم

شما دو گزینه کلان دارید که بستگی دارد به میزان امنیتی که می‌خواهید دست یابید.

گزینه ۱: کاهش شمارعبارات جمله که باید به خاطر بسپارید :

- **حساب کاربری حساس و مهم خود مانند ایمیل، شبکه‌های اجتماعی و غیره را مشخص کنید. برای آن‌ها از گذرجمله استفاده کنید. شما نباید بیشتر از ده عبارت را به خاطر بسپارید.**
- **آن‌ها را بر روی یک کاغذ یادداشت کنید، بدون اینکه آن‌ها را به سرویس مرتبط پیوند دهید. این کاغذ را در خانه‌تان و در مکانی امن نگه دارید.**

- هرگز آن‌ها را در یک سند رقمی ذخیره نکنید. هر چیزی که دیجیتال است ممکن است هک شود. در اکثر مواقع، احتمال هک شدن شما بیشتر از دزدیده شدن است.

گزینه ۲: ابزارهای مدیریت گذرواژه

داشتن یک واژه‌گذار یا جمله‌گذار متفاوت برای هر حساب کاربری ممکن است برای کسانی که کم حافظه هستند، مشکل ایجاد کند. نگران نباشید، ابزارهای قابل اعتماد و امن برای ذخیره کلمات عبور شما وجود دارند.

به شکل آنلاین

1password، Bitwarden یا DashLane از جمله ابزارهای مدیریت گذرواژه آنلاین هستند. این ابزارها به صورت افزونه برای مرورگرهای Chrome، Firefox و Safari ، دردسترسی هستند و به شما این امکان را می‌دهند که تمام گذرجمله‌های خود را در یک پایگاه داده رمزنگاری شده ذخیره کنید و از چندین دستگاه به آن دسترسی پیدا کنید. دسترسی به این صندوق امانت آنلاین توسط یک عبارت عبوریگانه حفاظت می‌شود. اگر از این نوع ابزار استفاده می‌کنید، به شدت توصیه می‌شود که یک عبارت عبور بلند انتخاب کنید و تایید هویت دو مرحله‌ای را تنظیم کنید.

آفلاین و بر روی دستگاه‌ها

KeePass یک ابزار مدیریت آف‌لاین است. به خلاف نرم‌افزارهای پیش گفته . آنلاین، **KeePass** کلمات عبور را در یک پایگاه داده آنلاین نگه نمی‌دارد، بلکه تنها آن‌ها را بر روی کامپیوتر یا گوشی هوشمند شما ذخیره می‌کند.

	Keepass	Dashlane	Bitwarden
متن باز	بله	خیر	بله
هماهنگ‌سازی بین چندین دستگاه	بله	بله	خیر
تولیدکننده عبارات عبور	بله	بله	بله
رایگان	خیر	خیر	بله

تایید هویت دو مرحله‌ای یا دوگانه

بیشتر سرویس‌های آنلاین امکان اجرای یک اقدام ایمن‌سازی افزون‌تر را فراهم می‌کنند: "**تایید هویت دوگانه**". احراز هویت دوگانه یا احراز هویت دو مرحله‌ای بر اساس استفاده از دو عامل استوار است: چیزی که شما **می‌دانید** (مثل گذرواژّ شما) و چیزی که شما **دارید** (مثل گوشی هوشمند شما). بنابراین، برای ورود به یک سرویس که این سیستم را فعال کرده‌اید، شما نیاز به موارد زیر دارید:

۱. نام کاربری

۲. گذرواژه

۳. کدی که از طریق پیامک یا از طریق نرم‌افزار کاربردی (اپلیکیشن) که هر بار یا هر چند زمان که با یک دستگاه جدید وارد می‌شوید، گوشی هوشمند شما دریافت می‌شود،

اینگونه، بدون گوشی هوشمند شما، دسترسی به حساب‌های آنلاین شما ناممکن است. برای افزایش امنیت، کد دریافتی در گوشی هوشمند همچنین می‌تواند با یک دستگاه احراز هویت فیزیکی مانند یک کلید یوبی (YubiKey) جایگزین شود.

در ادامه، لینک‌های مستقیم به خدمات معروف جهت فعال‌سازی احراز هویت دوگانه آورده شده‌اند:

- Google
- Microsoft
- Twitter
- Facebook
- Instagram

بهداشت رقمی

به روزرسانی سیستم عامل نرم‌افزارها

برای کامپیوتر یا گوشی هوشمند شما، بسیار مهم است که سیستم‌عامل و نرم‌افزارهای کاربردی خود را به‌طور منظم به‌روزرسانی کنید. این اقدام باعث پیشگیری از حملات بدفزارهای و تقویت ایمنی دستگاه شما می‌شود. به‌روزرسانی‌ها همیشه شامل رفع نقایص‌های امنیتی نرم‌افزارها پیشین می‌شوند که به تازه‌گی کشف‌شده‌اند. بنابراین، مهم است که به‌صورت منظم آن‌ها را روزآمد کنید.

راهنمای به روزرسانی برای

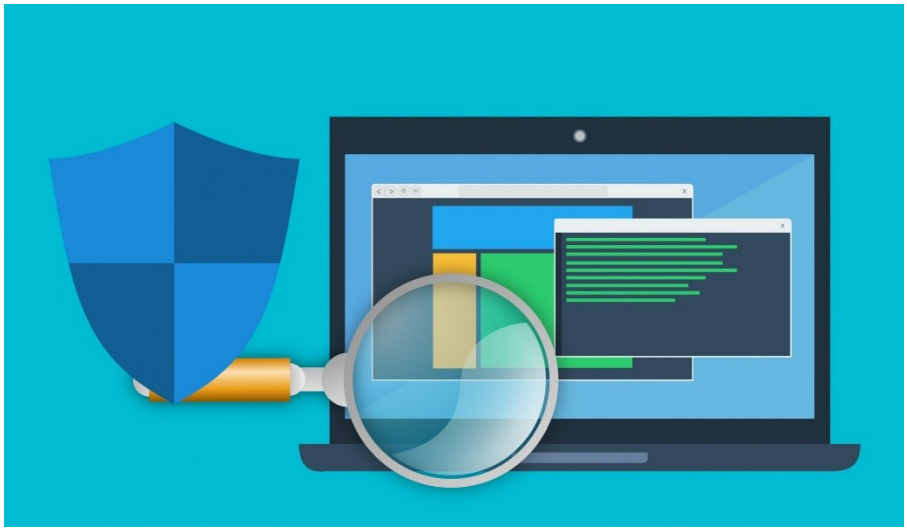
- Windows
- Mac
- iPhone

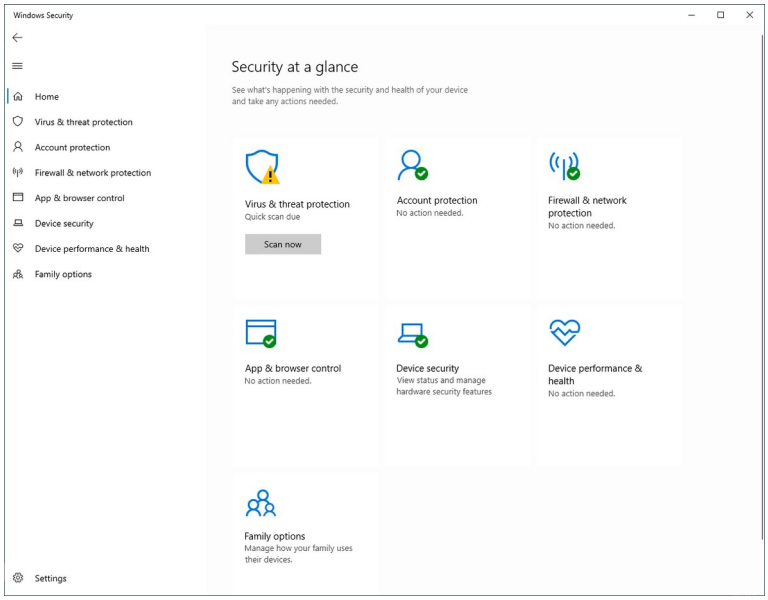
- Android

آنتی‌ویروس

ویندوز

برای کاربران ویندوز، آنتی‌ویروس بکار گرفته شده شرکت مایکروسافت به نام ویندوز دیفندر (Windows Defender) برای بیشتر کاربران کفایت می‌کند.





مک

کاربران مک به شکل سنتی کمتر از کاربران ویندوز به آلودگی نرم‌افزار مخرب حساس هستند، به دلیل کنترل‌های امنیتی سختگیرانه‌تر در دستگاه‌های اپل. اما اخیرا به شمار بدافزارهای که مک را هدف قرار می‌دهند، افزایش یافته‌اند. یک عادت خوب این است که تنها برنامه‌ها را از فروشگاه رسمی **اپ استور** مک نصب کنید. اگر فکر می‌کنید به آنتی‌ویروس نیاز دارید، Malwarebytes را نصب کنید. نسخه رایگان برای اکثر افراد کافی خواهد بود.

گوشی هوشمند

در مورد استفاده یا عدم استفاده از برنامه‌های ضد بدافزار بر روی گوشی هوشمند نظرهای متفاوت وجود دارد. این برنامه‌ها هرچند ازآلودگی‌های در برابر نرم‌افزارهای مخرب حفاظت می‌کنند، اما خود این برنامه‌ها نیز درسیستم نفوذ می‌کنند و علاوه بر آن نیاز به مجوز دارند. اگر واقعاً می‌خواهید یک برنامه ضدبدافزار را بر روی گوشی‌تان نصب کنید، از Malwarebytes یا Avira استفاده کنید.

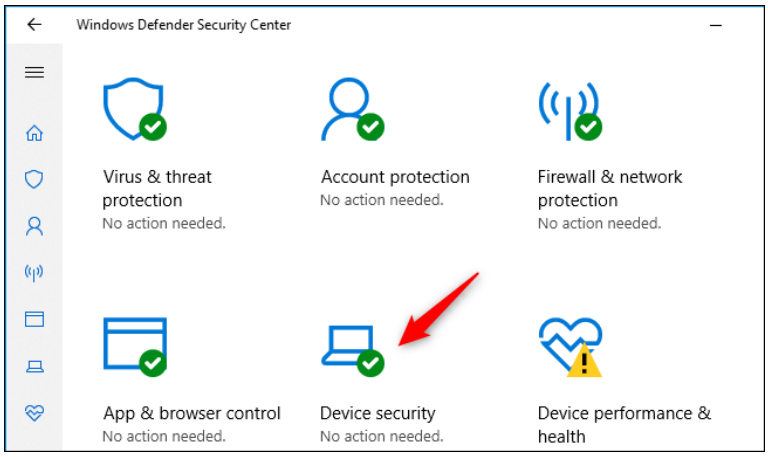
فایروال دیوار آتش

فایروال یک نرم‌افزار یا سخت‌افزار است که با استفاده از مجموعه‌ای از قوانین امنیتی، ارتباطات ورودی و خروجی را در رایانه‌تان (یا در یک شبکه) کنترل می‌کند.

فعال‌سازی فایروال بر روی ویندوز و مک

ویندوز

برای بررسی یا فعال‌سازی آنتی‌ویروس و همچنین فایروال، کلمه "Windows Defender" را در منوی جستجو تایپ کنید:



راهنمای بنیادین برای گوشی‌های هوشمند

مجوزها و دسترسی‌های به نرم‌افزارهای کاربردی

مانند کامپیوتر شخصی، بر روی گوشی‌هوشمند نیز هر برنامه‌ای را به سادگی نصب نمی‌کنیم. باید درخواست دسترسی‌ها را که یک برنامه از گوشی هوشمند شما می‌خواهد هم بررسی کنید. برای مثال، آیا معقول است که یک برنامه چراغ قوه از شما دسترسی به مخاطبینتان را بخواهد؟

دو اکوسیستم اصلی برنامه‌ها در حال حاضر، اندروید و آیفون هستند.

1. آیفون به دلیل کنترل‌ها و اعتبارات خود در عرضه عمومی شناخته‌شده است.
2. اندروید (گوگل) متاسفانه کمتر از این مسائل مراقبت می‌کند.

برنامه اندروید حاوی بدافزار

بسته به نسخه اندروید شما (از ۶ به بالا)، بیشترین مواقع باید در مسیر تنظیمات > برنامه‌ها > (گاهی اوقات در تنظیمات پیشرفته) > اجازه برنامه‌ها جستجو کنید.

برای بررسی دسترسی‌هایی که یک برنامه اندروید به گوشی شما اختصاص داده‌است، به پروژه Exodus Privacy **سر بزنید.**

در مورد استفاده یا عدم استفاده از برنامه‌های ضد بدافزار بر روی گوشی هوشمند نظرهای متفاوت وجود دارد. این برنامه‌ها هرچند ازآلودگی‌های در برابر نرم‌افزارهای مخرب حفاظت می‌کنند، اما خود این برنامه‌ها نیز به نوعی در مدیریت سیستم گوشی دخالت‌گر هستند و افزون بر این نیاز به مجوز دارند. اگر واقعاً می‌خواهید یک برنامه ضدبدافزار را بر روی گوشی‌تان نصب کنید، از Malwarebytes **یا Avira استفاده کنید.**

- برای دانستن بیشتر دوره Totem آنلاین (به زبان فارسی) را دنبال کنید.