پایه‌های امنیت رقمی

موضوع درس‌نامه: آموختن بنیادهای حفظ امنیت داده‌ها و حساب‌های کاربری آنلاین و ابزارکارها

تلاش همیشگی و در همه جا، برای حفاظت از داده‌های خود، خسته کننده و کمترعملی است.
امنیت یک فرآیند است و تنها در بکارگیری ابزارها و نرم‌افزارهای باری‌گذاری شده، خلاصه نمی‌شود.
فرایند با ریشهٔ لاتین به معنیِ «پیش رفتن» به معنای پیشرفت گام به گام به سوی هدف است

چه باید کرد؟

تهدیدها را باید شناخت !

شناخت تهدیدها

ایمن بودن، نخست با شناختن تهدیدهایی آغاز می‌شود که با آن روبرو می‌شویم .

سپس روش‌هایی که برای مقابله با تهدیدها انتخاب می‌کنیم.

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 و داده‌هایی را باید حفاظت کنم؟

ایمیل‌ها، پیام‌ها، مکالمات تلفنی، عکس‌ها، فیلم‌ها، آدرس‌ها و هویت و مشخصات ارتباط‌ها و غیره.

۲- 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.

۳- برای دسترسی 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)
- به شکل فیزیکی: دزدیدن، نصب بدافزارها

۴- پیامد دسترسی آن‌ها به این اطلاعات چیست؟

- افشا شدن موضوع / سوختن اطلاعات برای انتشار
- مشکلات حقوقی/ عدلی برای یک منبع یا خبرنگار
- تهدیدهای فیزیکی

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

- تکنیکی : همه‌ی راه‌کارهایی نرم‌افزاری و سخت‌افزاری
- حقوقی و عدلی : مطلع کردن مراجع 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 خود را به اشتراک بگذارند.

حفاظت از فیشینگ

اگر نصب یک نرم‌افزار **ضد ویروس** بر روی کامپیوتر یا گوشی هوشمند یک اقدام مهم است، اما هوشیاری لازم به هنگام دریافت لینک یا فایل‌های ضمیمه از طریق ایمیل، مسنجر، پیامک، واتساپ، اسکایپ و سایر ابزارهای ارتباطی بسیار **مهمتر** است.

فراموش نکنیم : **شبکه‌های اجتماعی و ابزارهای ارتباطی یکی از عوامل اصلی انتقال ویروس‌ها هستند.**

مقابله با فیشینگ

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 از سلامت آن 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.

مقابله با فیشینگ

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

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 است**

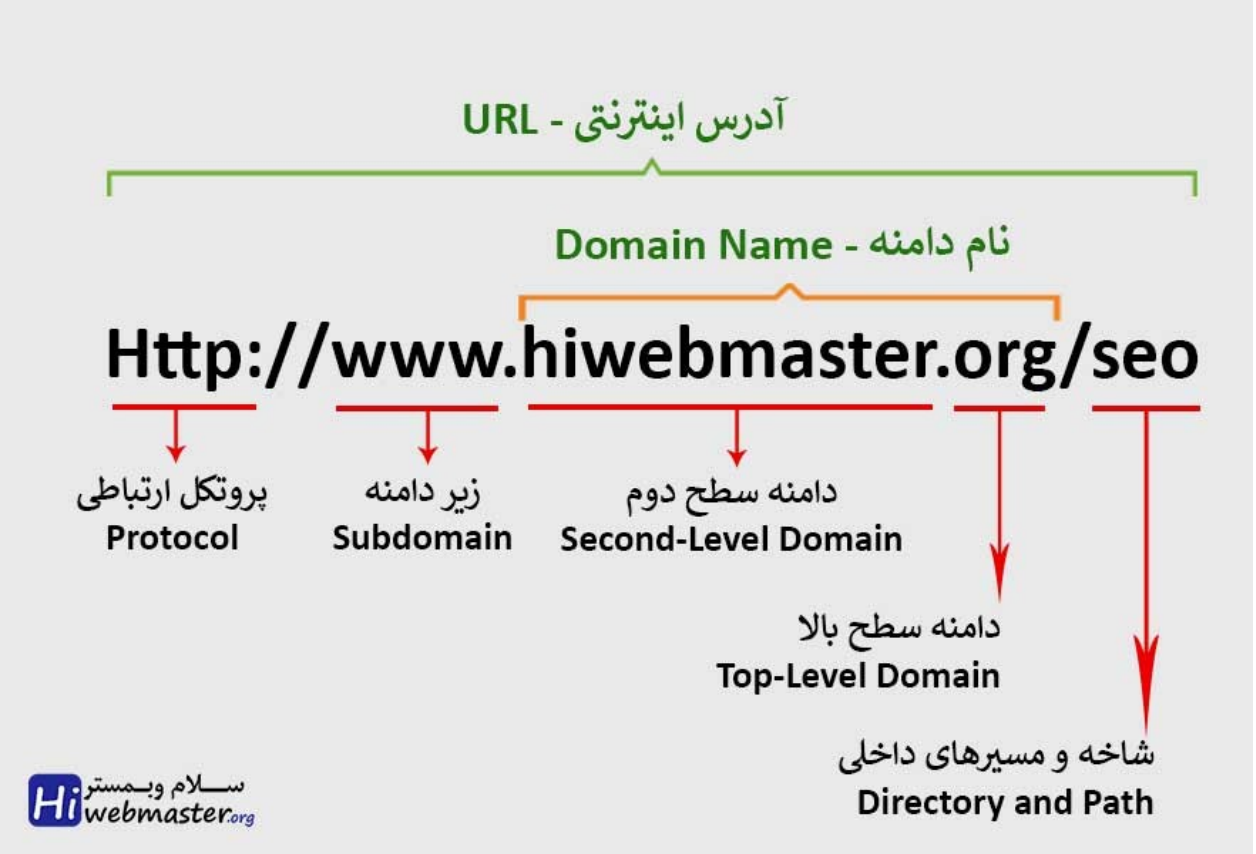
مثلا:

http://www.google.com

یا آدرس همین صفحه URL است :

https://hiwebmaster.org/urls

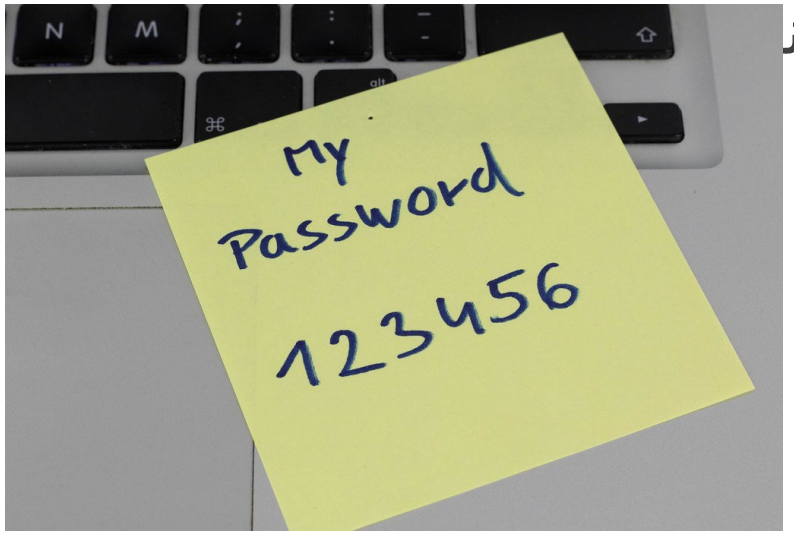
URL یا آدرس اینترنتی



حفاظت از حساب‌های کاربری آنلاین (برخط) خود

بیشترین خدمات آنلاینی که ما استفاده می‌کنیم، مانند ایمیل، شبکه‌های اجتماعی و غیره، با **گذرواژه‌ها** محافظت می‌شوند.

بسیار مهم است که گذرواژه‌های قوی و دشواری درست کنیم که در برابر حدس زدن یا پیدا کردن آن مقام باشند



گذرواژه‌ها = passwords

می‌توانید گذرواژه‌های خود را با استفاده از بررسی‌کننده گذرواژه در سایت nothing2hide آامتحان کنید.

توصیه‌های بنیادی : برای گذرواژه‌ی قوی

چه راهبردهایی برای گذرواژه داشته باشیم

شما **دو گزینه کلان** دارید که بستگی به میزان امنیتی دارد 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 بیش از ده گذرجمله را به خاطر بسپارید.

•آن‌ها را بر روی یک کاغذ یادداشت کنید، بدون اینکه آن‌ها را به سرویس مرتبط متصل کنید. این کاغذ را در خانه‌تان و در مکانی امن نگه دارید.

گذرواژه یا گذرجمله ؟

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

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

۳- از اسم‌های فیلم یا داستان و اطلاعات شخصی که آسان‌تر شناسایی می‌شو

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

ایجاد یک گذرواژه قوی

درازای یک گذرواژه، عامل اصلی برای ایجاد یک گذرواژه قوی است که قابلیت مقاومت در برابر یک حمله جستجوی فراگیررا دارد. افزودن اعداد، نویسه‌های خاص، حروف کوچک و بزرگ، اغلب منجر به ساختن گذرواژه ضعیف یا یادگیری آن را سخت می‌کند. 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 آن 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

,,,,,,BENAMKHODAVANDJAN!BAKSHNDEH

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

گذرواژه‌ی قوی: نرم‌افزارهای امن

داشتن یک گذارواژه 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.

گزینه ۲: ابزارهای مدیریت گذرواژه

ابزارهای مدیریت گذرواژه

به شکل آنلاین

Bitwarden، 1password 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

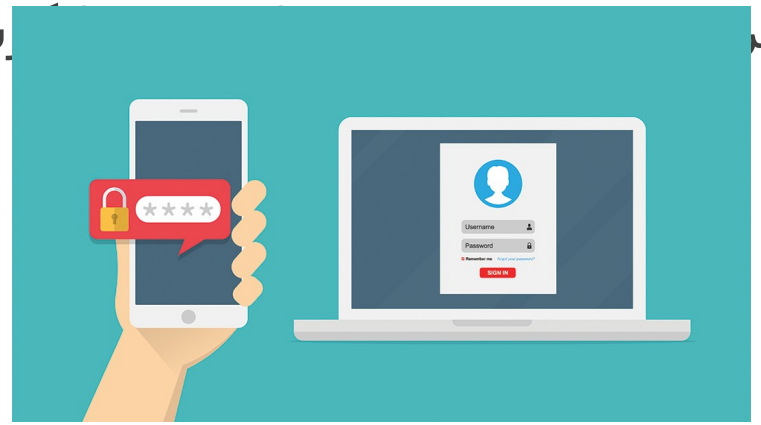
آفلاین و بر روی دستگاه‌ها

در دیگر سوی طیف، **KeePass** یک مدیر عبور محلی و آف‌لاین است. به عکس از سرویس‌های گفته شده، KeePass کلمات عبور را در یک پایگاه داده آنلاین نگه نمی‌دارد، بلکه تنها آن‌ها را بر روی کامپیوتر یا گوشی هوشمند شما ذخیره می‌کند.

تایید هویت دو مرحله‌ای یا دوگانه

بیشتر سرویس‌های آنلاین امکان اجرای یک اقدام ایمن سازی حساب‌های کاربری 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 کلمه عبور 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 یا گذرجمله

۳.کدی که از طریق پیامک یا از طر ی گوشی هوشمند شما دریافت می‌شود، هر بار که از یک دستگاه



بهداشت رقمی

اهمیت به رزو رسانی ویندوز

آیا ویندوزهای شما دارای شماره است و رسما ثبت شده است.

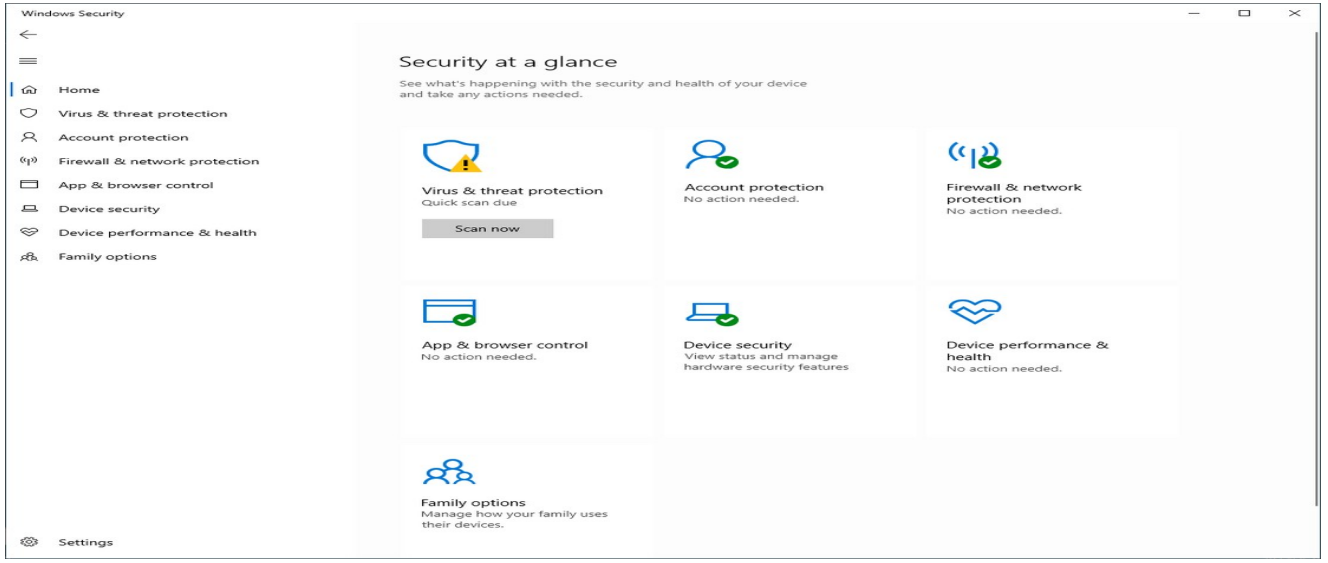
اهمیت دارد چرا که هرچند هوشیار باشید و از همه‌ی ابزارها برای حفاظت از داده‌های خود استفاده کنید، اما چون سیستم مدیریت محتوای شما به روز نیست، خطر هک و

بدون به‌روز رسانی سیستم شما آسیب‌پذیر هستید

آنتی ویروس - ضد بدافزار

ویندوز

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



آنتی ویروس - ضد بدافزار

برای رایانه‌های 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 به‌تازه‌گی تعداد نرم‌افزارهای مخرب 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.

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.

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.

۱-آیفون به دلیل کنترل‌ها و اعتبارات خود درعرضه عمومی شناخته شده است.

۲-.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.

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

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