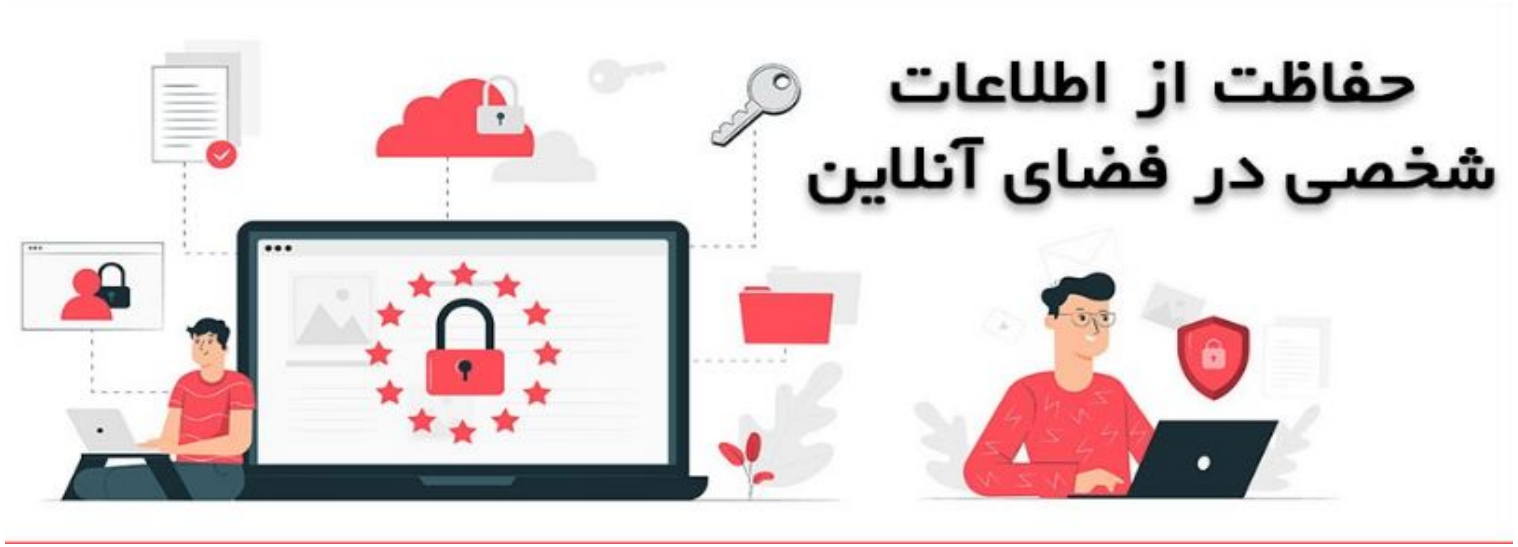
مهندسین مشاور سازه پردازی ایران (سهامی خاص)

SAZEH PARDAZI IRAN
Consulting Eng. Co

محافظت از اطلاعات در سامانه های اینترنتی

- **خطر در فضای آنلاین**
-
- جستجو در فضای وب و کفتگوی آنلاین در شبکه های مجازی به دلیل تنوع و پاسخگویی به نیازهای متنوع کاربران همواره جذاب و سرگرم کننده است. ما در دورانی زندگی می کنیم که بدون اینترنت بخشی از امورات زندگی مان فلج می شود و گویا نمی توانیم از زندگی لذت چندانی ببریم. امروز دیگر اینترنت فقط یک سرگرمی نیست بلکه قسمت مهمی از زندگی و کسب و کار ما است.
- وقتی یک پدیده تا این اندازه در زندگی اهمیت پیدا می کند تا جایی که به بخش تفکیک ناپذیر آن تبدیل می شود، پس نباید فقط توجه خود را معطوف جنبه های مثبت آن کنیم. این توجه یک جانبه موجب می شود از صدمات امنیتی و مخاطراتی که از رهگذر فعالیت در اینترنت متوجه ما می شود غفلت نماییم.



مهم ترین راههای مراقبت و ایمنی کاربران در اینترنت:

نسبت به لینک ها و فایل های مشکوک محتاط رفتار کنید

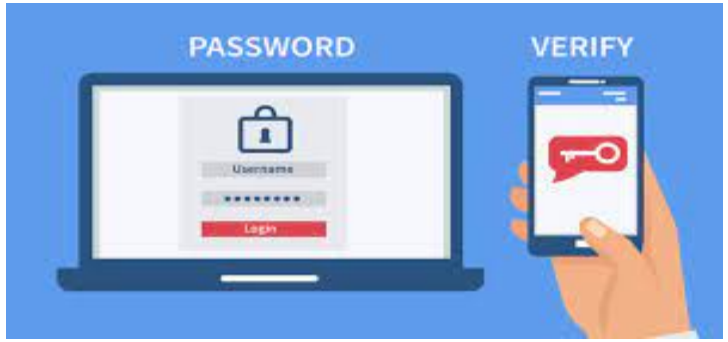
- برای جلوگیری از قربانی شدن در حملات فیشینگ، لینک ها یا فایل های ارسال شده از طریق ایمیل یا رسانه های اجتماعی را بدون فکر باز نکنید. آدرس لینک ها را بررسی کنید تا قبل از کلیک بر روی آنها از قانونی بودنشان اطمینان حاصل کنید. اگر یک پیشنهاد یا معامله بسیار عالی مطرح شده بود، محتاط تر عمل کنید. هرگز این ایمیل ها را با اطلاعات شخصی مانند رمزعبورها یا جزئیات حساب بانکی پاسخ ندهید.

از رمزعبور های قوی استفاده کنید

- رمز عبورهای قوی ترکیبی از حروف الفبای تصادفی و نمادهایی است که در مقابل حملات قوی مقاوم تر هستند. البته باید گفت که به خاطر سپردن چنین رمزهایی دشوار می باشد. به ویژه در صورتی که به توصیه های متخصصان عمل کنید و برای حساب های مختلف خود از یک رمز عبور مشابه استفاده نکنید. راه حل این مسئله استفاده از یک مدیر رمز عبور برای تولید و پر کردن خودکار رمزعبور حساب های شماست. تمام آنچه که شما نیاز دارید این است که فقط رمز عبور اصلی را به خاطر بسپارید.
- به عنوان مثال مرورگر گوگل کروم با یک مدیر رمز عبور داخلی ساخته شده است. حتی دارای ویژگی بررسی رمزعبور می باشد(این مدیر رمز عبور سال گذشته برای اندروید و وب راه اندازی شد) این مدیر می تواند رمزعبورهای ذخیره شده را بررسی کند تا ببیند تحت نقض های قبلی مورد نفوذ قرار گرفته یا به خطر افتاده اند یا خیر.
- یکی دیگر از روش ها، انتخاب روش های احراز هویت بیومتریک مانند تشخیص چهره یا اثر انگشت در صورت داشتن دسترسی به آنها می باشد.

احراز هویت دوعاملی را فعال کنید

- احراز هویت دو عاملی را به منظور تأمین امنیت حساب های آنلاین فعال کنید(احراز هویت دوگانه یک لایه اضافی برای تأیید هویت از طریق رمز عبور یک بار مصرف یا احراز هویت بیومتریک) است.
- به عنوان مثال، برای کسانی که بیشتر از سایرین در معرض خطر مجرمان سایبری قرار دارند(روزنامه نگاران ، فعالان اینترنتی و صاحبان کسب وکارهای آنلاین) گوگل دارای یک برنامه محافظتی پیشرفته می باشد که امنیت بالایی را در مورد حساب های شخصی ارائه می دهد .در این مورد کاربران باید برای ورود به سیستم حساب های گوگل خود از یک توکن امنیتی فیزیکی(علاوه بر یک رمز عبور) استفاده کنند.
- همچنین گوگل دسترسی به فایل های جیمیل و گوگل درایو را به برنامه های خود محدود کرده و برنامه های شخص ثالث را انتخاب می کند، در نتیجه احتمال دسترسی به یک برنامه مخرب را کاهش می دهد.

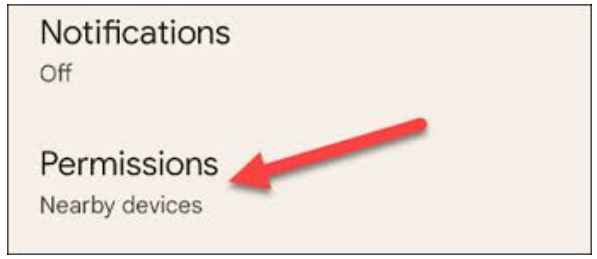


انجام به روز رسانی

- با استفاده از به روز رسانی کردن برنامه ها و نرم افزارهای خود، از وقوع حملات سایبری که از اشکالات نرم افزاری سوءاستفاده می کنند، جلوگیری کنید. بمنظور جلوگیری از اختلال، به روزرسانی های خودکار را که معمولاً در اواسط شب انجام می شود، روشن کنید.

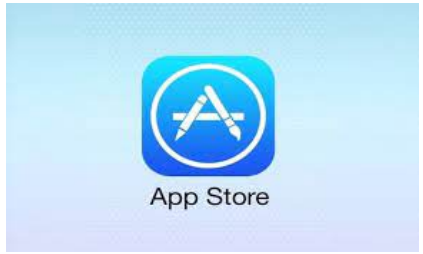
مجوز برنامه را به دقت بررسی کنید

- ممکن است بدافزارها برای عبور از دیوار دفاعی شما خود را به بصورت برنامه های قانونی نشان دهند. از این رو، از دانلود برنامه ها از طریق لینک هایی در ایمیل یا رسانه های اجتماعی جدا خودداری کنید.



همواره برای دانلود برنامه ها، از گوگل پلی . اپ استور و یا وب سایت های شخص ثالث استفاده کنید.

- با اینکه اکثر برنامه های فروشگاه های رسمی ایمن هستند، اما مواردی هم وجود داشته است که بدافزارها از بررسی های اپل و گوگل نیز عبور کرده اند .برای کاهش آسیب های احتمالی ناشی از چنین برنامه هایی، مجوزهای درخواست شده توسط یک برنامه جدید را بدقت بررسی کنید و موارد غیر ضروری را رد کنید. به عنوان مثال، یک برنامه هواشناسی نیاز به دسترسی به عکسها یا استفاده از تلفن شما ندارد .همچنین ممکن است بررسی تعداد دفعاتی که برنامه دانلود شده است، قبل از دریافت آن مفید باشد، به هرحال روشی برای سنجش می باشد.



از وی پی ان استفاده کنید

- یک شبکه خصوصی مجازی (VPN) یک اتصال امن و رمزگذاری شده از طریق اینترنت را ایجاد می کند. درصورتی که از اتصال به وای فای عمومی یا ناامن استفاده می کنید، این روش می تواند قابل استفاده و مفید باشد. در حالی که اکثر وی پی ان ها رایگان نیستند، اما نمونه های رایگان مناسبی همراه با محدودیت هایی مانند سهمیه داده ها وجود دارد. تعداد کاربران کمی که نیازی به داده های نامحدود ندارند، وی پی ان های رایگان مانند ProtonVPN ، hid.meو TunnelBear را بررسی کنند.

زمانی که از دوربین ها و میکروفن ها استفاده نمی کنید، آنها را غیر فعال کنید

- تعدادی از سازنده های رایانه شخصی محافظ های حریم خصوصی فیزیکی به دوربین جلوی لپ تاپ ها اضافه کرده اند تا در صورت بخطر افتادن سیستم توسط بدافزار نگاه های کنجکاوانه را بلاک نماید. یا اینکه می توانید یک نوار چسبی بر روی دوربین بچسبانید.
- برای غیرفعال کردن میکروفون در رایانه های شخصی ویندوز ۱۰ ، به قسمت Device Manager بروید، بخش ورودی ها و خروجی های صدا را انتخاب کنید، بر روی میکروفون راست کلیک کرده و آن غیرفعال کنید. در مورد رایانه های مک ، به تنظیمات سیستم مراجعه کنید، به قسمت امنیت و حفظ حریم خصوصی بروید، بر روی حریم خصوصی کلیک کنید. میکروفون را انتخاب کنید تا دسترسی برنامه به آن تغییر کند.

از داده های خود بکاپ بگیرید

- حتی اگر همه اقدامات احتیاطی موجود را انجام دهید، هنوز هم ممکن است دستگاه های شما از طریق حمله باج افزاری، تا زمان پرداخت مبلغی به عنوان باج، قفل شود .بنابراین، مهم است که از داده های خود به طور منظم در چندین مکان پشتیبان و بکاپ تهیه کنید تا امکان از دست دادن داده ها کاهش یابد. از یک فروشنده معتبر ذخیره سازی ابری، مانند Microsoft OneDriveیا Google Drive علاوه بر یک دستگاه ذخیره سازی خارجی استفاده کنید.