بد یو اس بی ها دقیقا مانند یک فلش مموری هستند که روزانه بارها و بارها آن ها را مشاهده می کنید ، اما با این تفاوت که توسط یک هکر دستکاری شده و فایل های مخربی در آن هست که منتظر شما اونو به سیستم خودتون وصل کنید

هکر با نوشتن کد هایی مخرب و جایگذاری آن ها در یک Bad USB ، به فلش مموری دستور می دهد که هنگامی که به سیستم قربانی متصل شد یک سری فرایند ها را به صورت خودکار اجرا کند.این فرایند ها می تواند از دستیابی به اطلاعات شخصی و ذخیره سازی آن ها در فلش مموری باشد تا از کار انداختن کلی یک سیستم عامل

**بد یو اس بی کلیر USB Killer**

این نوع از USB ها فقط با هدف تخریب ساخته میشوند و میتواند هدف تخریب به قسمت خاصی باشد. مثلا یک یو اس بی کیلر میتواند هارد را برای حذف اطلاعات با مشکلات جدی مواجه کند.یا انواع دیگر که میتوانند صدمات هزینه بر مانند اسیب رساندن به CPU را انجام دهند.لازم به ذکر است این USB ها مختص کامپیوتر ها نمی باشند و برای تمامی سیستم های موبایلی و کامپوتری وجود دارند.

### USB های جاسوسی

این USB ها برای نفوذ به سیستم و از بین بردن اطلاعات خاصی در نظر گرفته شده اند ، به عنوان مثال با قرار دادن keylogging USB در سیستم اجرا می شود.

بد یو اس بی (Bad Usb)  در همه بازارها برای فروش نیستند و مخصوصاً در ایران کمتر در دسترس هستند. اما به طور کلی ، آنها قیمت های نسبتاً بالایی دارند و سایت های فروش آنها برای کلاهبرداری بسیار زیاد است. و برای تهیه آنها باید مراقب باشید که از مکانی امن خرید کنید.

#### امنیت در برابر USB بد

از سیستم عامل های مورد اعتماد که کمتر استفاده میشوند استفاده کنید مانند انواع Linux و Mac

فراموش نکنید که ابزارهای امنیتی مانند آنتی ویروس های اصلی می توانند تا حد زیادی از این روش ها جلوگیری کنند. از USB Locker ها استفاده کنید تا بدون پسورد شما نتوانند USB را اجرا کنند. در صورتی که از پورت USB استفاده نمیکنید اتصالات آنرا به سخت افزار قطع کنید. قبل از اتصال USB آنرا در سیستمی دیگر تست نمایید. از اصالت برند و سریال USB مطمئن شوید.

## با وصل کردن یک USB سیستم قربانی هاتو هک کن

تو فیلم ها زیاد دیدید که هکر با اتصال یک فلش یک سیستم رو هک میکنه میخواهید یاد بگیرید که چطوری اینکار انجام میشه؟ پس این دوره رو از دست ندید

## **راه‌های پیشگیری از حملات Bad USB**

دستگاه‌های Bad USB با سرعتی عمل می‌کنند که برای یک کاربران عادی غیر ممکن است که از حضور آن با خبر شوند. اسکریپت‌های زیادی در حال حاضر جهت دانلود در اینترنت وجود دارند که حتی به کاربران عادی با کمترین دانش نیز این امکان را می‌دهد تا از این قابلیت مخرب استفاده کنند. در اینجا به معرفی مواردی می پردازیم که می‌توانند به جلوگیری از این حملات کمک کنند.

### مجوز اتصال کیبورد

به دلیل نوع حمله، راه‌های زیادی برای جلوگیری از آن وجود ندارد. برخی شرکت‌های سازنده آنتی ویروس در آنتی‌ویروس‌های خود قابلیت پیشگیری از حملات Bad USB را ایجاد کرده‌اند. آن‌ها برای جلوگیری از شناساندن USB به عنوان کیبورد به کامپیوتر از این روش استفاده می‌کنند. وقتی یک دستگاه USB به کامپیوتر متصل می‌شود و خود را به عنوان کیبورد معرفی می‌کند، آنتی‌ویروس با ارسال پیامی از کاربر می‌خواهد تا به منظور تایید هویت دستگاه، یک کد چند رقمی را بر روی کیبورد وارد کند. در این حالت، آنتی‌ویروس تنها به کیبوردهایی اجازه اتصال می‌دهد که تایید شده باشند و از اتصال کیبوردهای تایید نشده جلوگیری می‌کند.

### لیست سفید USB

این امکان وجود دارد که تنها به درایورهای خاصی با توجه به GUID آن‌ها امکان نصب داده شود. همچنین می‌توان از نصب دستگاه‌های USB خاصی مثل کیبورد و … جلوگیری کرد.

### دستگاه‌های فایروال USB

برخی از شرکت‌ها فایروال‌های سخت‌افزاری USB را تولید می‌کنند که به عنوان واسطی بین کامپیوتر و دستگاه USB قرار می‌گیرد و دستورات ارسال شده به کامپیوتر توسط دستگاه متصل شده را محدود می‌کنند.

### استفاده از برنامه‌های نظارت بر سرعت تایپ

برنامه‌هایی وجود دارند که در پس زمینه سیستم عامل به منظور نظارت بر سرعت تایپ، اجرا می‌شوند. از آنجایی که دستگاه‌های Bad USB با سرعتی تایپ می‌کنند که عملا برای انسان تایپ در این سرعت غیر ممکن است، این برنامه‌ها با شناسایی سرعت تایپ مشکوک، از عملکرد بدافزار جلوگیری می‌کنند.

### ایجاد پسورد برای CMD

از آنجایی که با دسترسی به CMD فعالیت‌های مخرب زیادی می‌تواند صورت بگیرد، بهتر است تا با ایجاد پسورد برای CMD دسترسی به آن محدود شود.