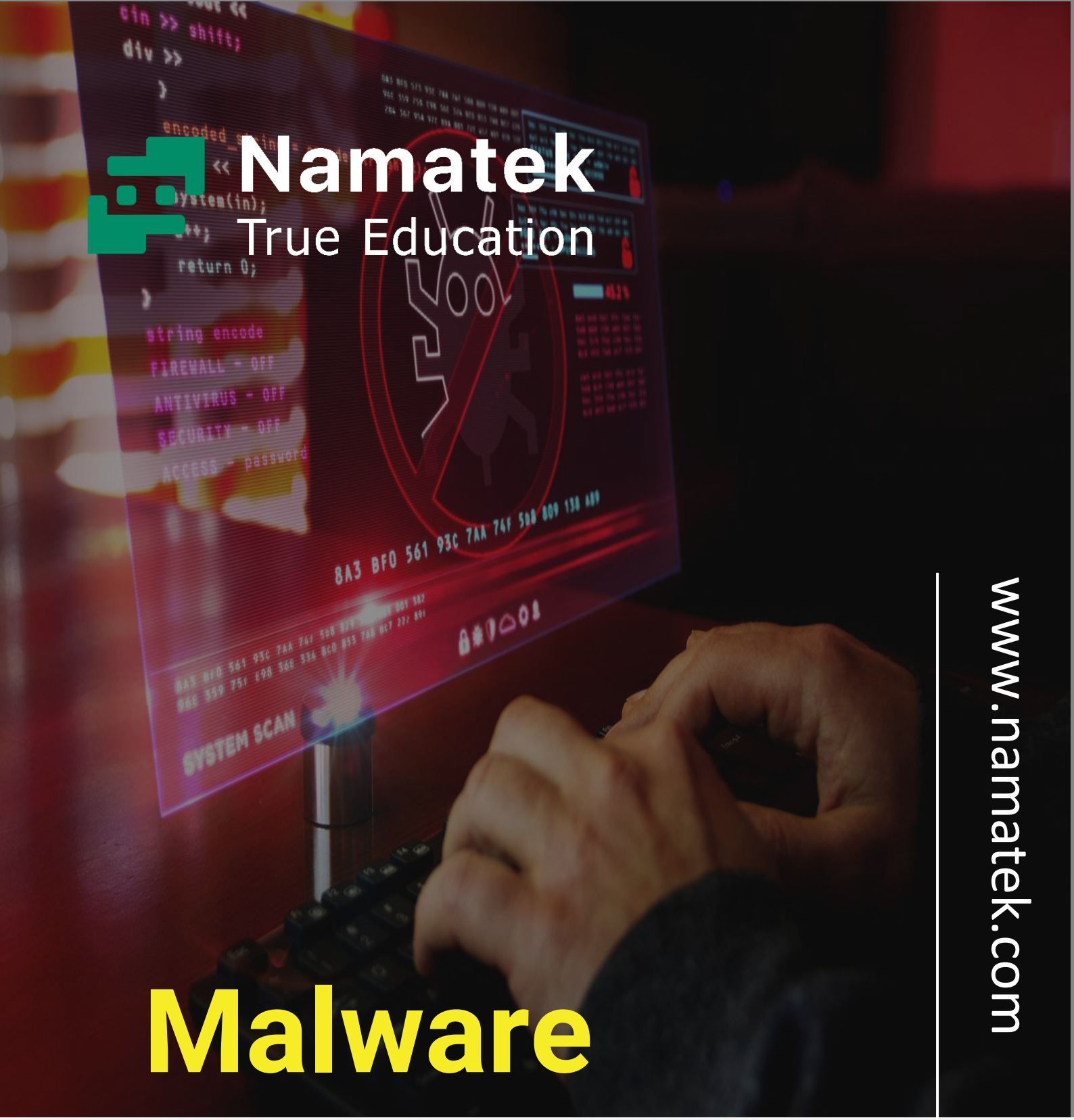


Malware

www.namatek.com

بدافزار چیست؟

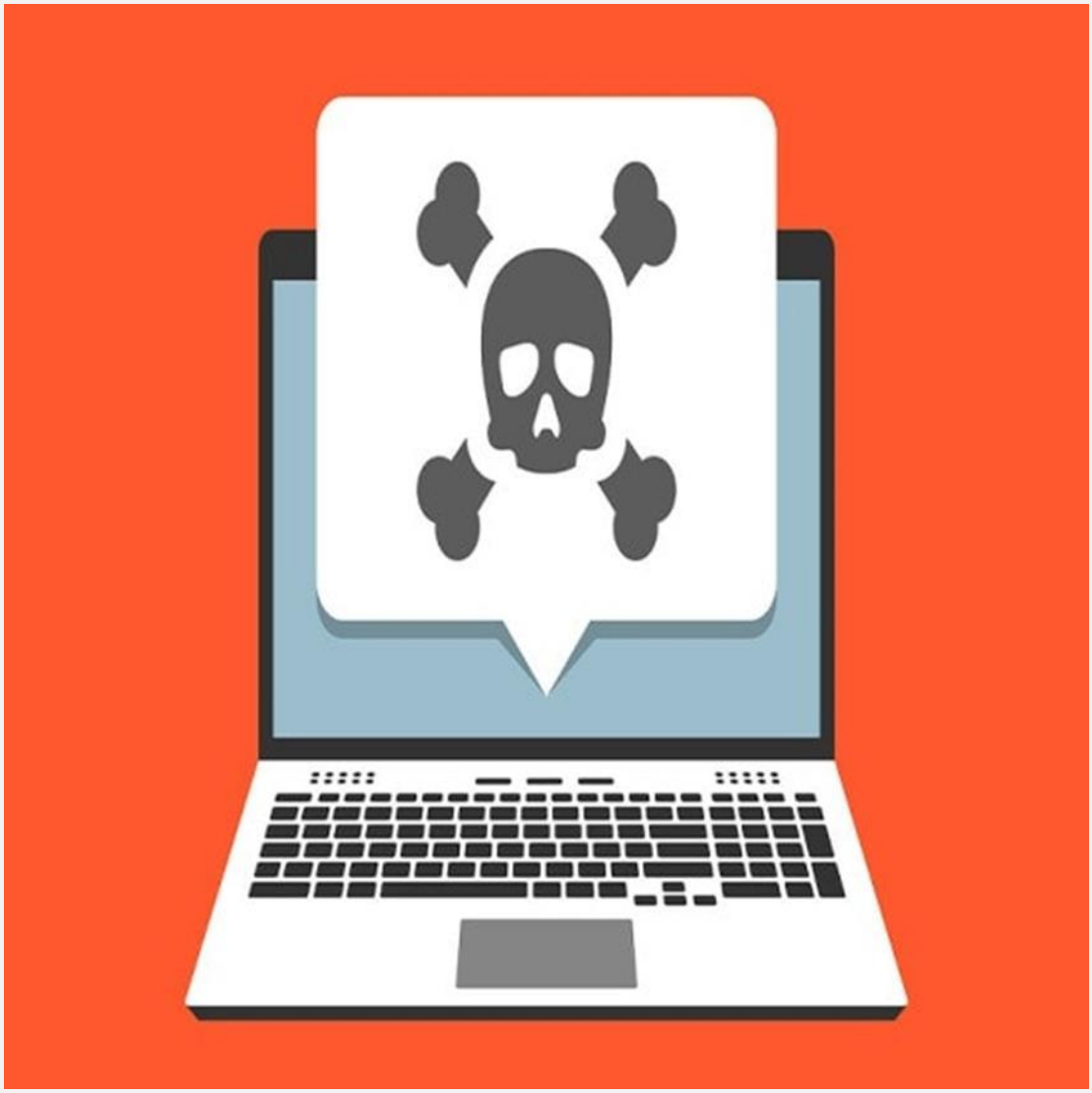
فهرست مطالب

اصولا زمانی که افراد مورد تهاجم نرم افزار های غیر ایمن قرار می گیرند و اطلاعات یا دستگاه های آن ها به خطر می افتد، با این سوال رو به رو می شوند که بدافزار چیست و چرا سیستم ها را تهدید می کند؟ حذف امنیت داده های یک سیستم شخصی قطعا برای تمامی کاربران این سیستم ها ضروری و مهم است و برای رسیدن به این هدف باید به خوبی با این مفهوم و راه های جلوگیری از ورود آن ها به سیستم آشنا بود.

در این مطلب قصد داریم علاوه بر ویروس ها، انواع بد افزار ها را نیز خدمت شما معرفی کنیم. با ما همراه باشید.

#۱ تعریف بدافزار چیست؟

بدافزار یا Malware که مخفف عبارت malicious software است به نرم افزار هایی نسبت داده می شود که مخرب هستند. در واقع این اصطلاح به طور کلی به ویروس ها، تروجان یا اسب تروآ، کرم های مجازی و دیگر برنامه های تخریب گر رایانه ای اشاره دارد. هکرها از چنین برنامه هایی برای تخریب و دستیابی به اطلاعات حساس استفاده می کنند.
مایکروسافت بیان می کند: «بدافزار به نرم افزار هایی گفته می شود که جهت آسیب به رایانه ها، سرور ها و یا شبکه های رایانه ای طراحی شده اند.»



#۲ انواع بدافزار

متاسفانه در دنیای امروزی انواع زیادی از بد افزار ها به وجود آمده اند. شناخت این نوع نرم افزار های مخرب می تواند یکی از راه های موثر در محافظت از داده ها و دستگاه های شما باشد. در ادامه این بخش می توانید نمونه هایی از انواع بدافزار ها را مشاهده نمایید.

۱-۲# ویروس (Virus)

ویروس ها معمولا به شکل فایلی که به ایمیل پیوست شده است به دستگاه های مختلف انتقال می یابند. این ایمیل ها دارای بار ویروسی بوده و یا یک بدافزار را شامل می شوند که عملکرد مخربی دارد. هنگامی که قربانی فایل ها را باز می کند، دستگاه آلوده می شود.

۲-۲# باج افزار (Ransomware)

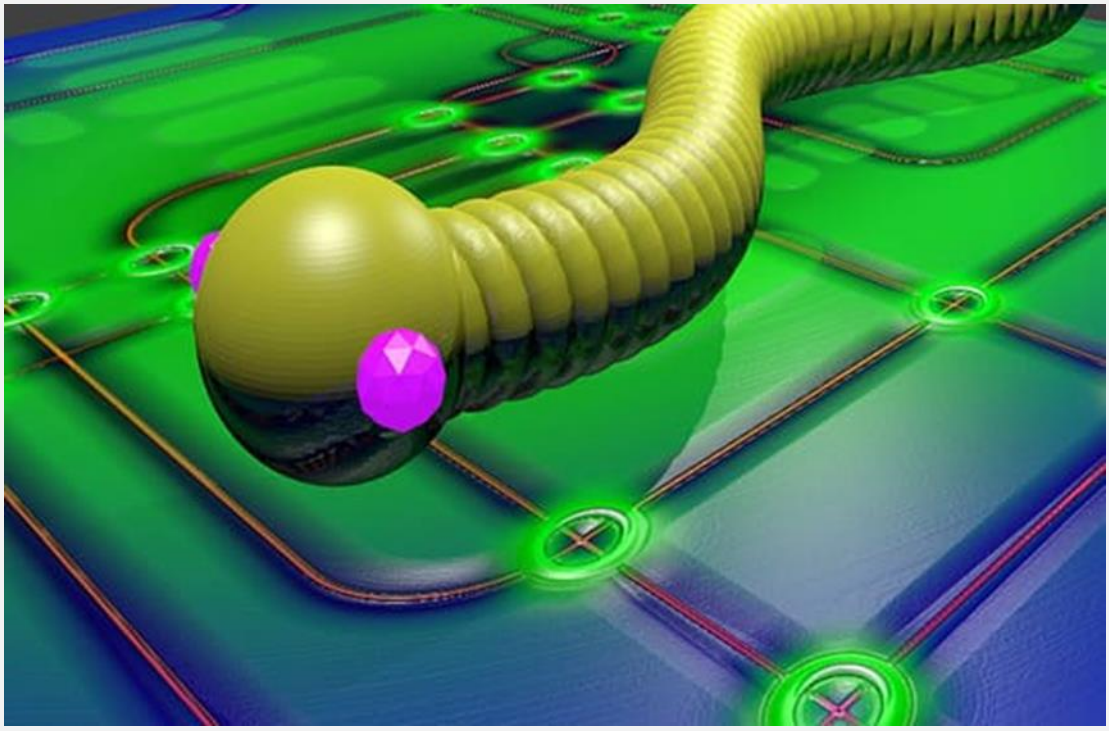
در پاسخ به سوال بدافزار چیست، لازم می دانیم یکی از سودآورترین و در نتیجه محبوب ترین انواع بد افزار ها در میان هکر ها را به شما معرفی نماییم. به این نوع بدافزار ها، باج افزار می گویند. این Malware خود را بر روی دستگاه های قربانیان نصب می کند. سپس داده ها و فایل ها را رمزگذاری می نمایند. پس از آن از کاربران باج می گیرد تا اطلاعات را بازگرداند. بیشترین کاربرد آن ها در بیت کوین است.

۳-۲# ترس افزار (Scareware)

در این بدافزار ها مجرمان با پیام هایی قربانیان را می ترسانند. به عنوان مثال زمانی که قربانی در حال کار با رایانه یا تلفن هوشمند خود است، برای او پیامی ارسال می شود که درباره آلوده شدن دستگاه هشدار می دهد. احتمالا با چنین پیام هایی رو به رو شده اید که می گویند: «هشدار، رایانه شما آلوده است.» بدین ترتیب هکرها با ایجاد ترس، قربانی را برای نصب برنامه های مخرب فریب می دهند.

۴-۲# کرم ها از انواع بدافزار (Worms)

در ادامه بررسی پاسخ بدافزار چیست، به معرفی کرم ها می پردازیم. این بدافزار ها می توانند از دستگاهی به دستگاه دیگر کپی شوند. کرم ها از ضعف های امنیتی یک نرم افزار یا سیستم عامل برای انتقال به دستگاه های مختلف استفاده می کنند.



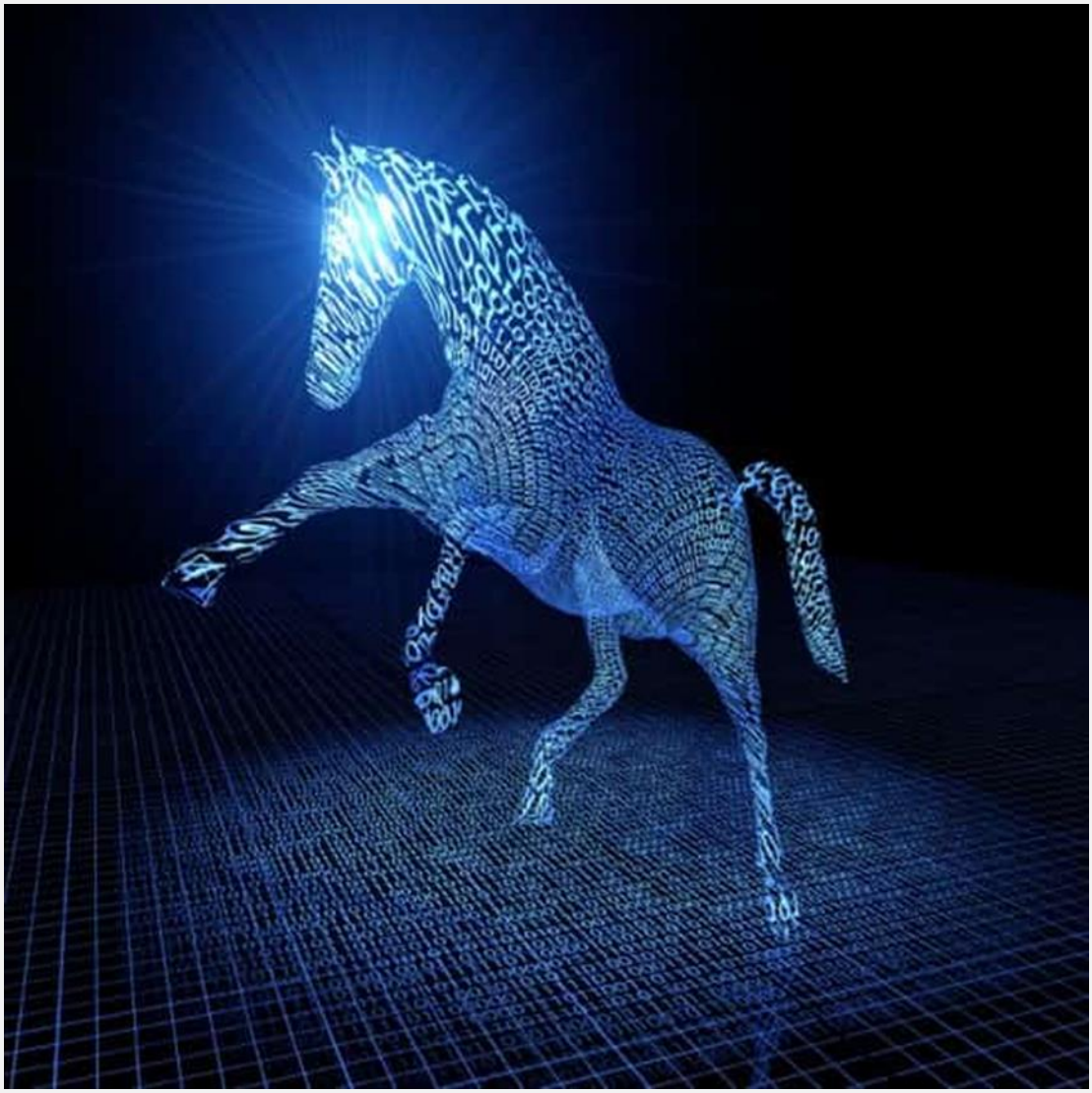
#۵-۲ نرم افزار های جاسوسی (Spyware)

این نرم افزار ها برنامه هایی هستند که بدون اطلاع به دارندگان تلفن های همراه، رایانه های شخصی و... بر روی سیستم آن ها نصب می شوند. به این ترتیب هکرها را قادر می سازند تا تمامی تماس ها، پیام ها و دیگر داده های موجود در دستگاه را کنترل کنند. چنین بدافزاهایی معمولا توسط مجریان قانون، سازمان های دولتی و امنیتی مورد استفاده قرار می گیرند تا محیطی حساس را نظارت کنند و یا تحقیقاتی را به انجام رسانند؛ اما امروزه نرم افزار های جاسوسی در اختیار هکرها نیز قرار گرفته و افراد برای کنترل همسر، فرزندان و... از آن بهره می گیرند.

#۲-۶ تروجان یکی از بدافزار ها (Trojan)

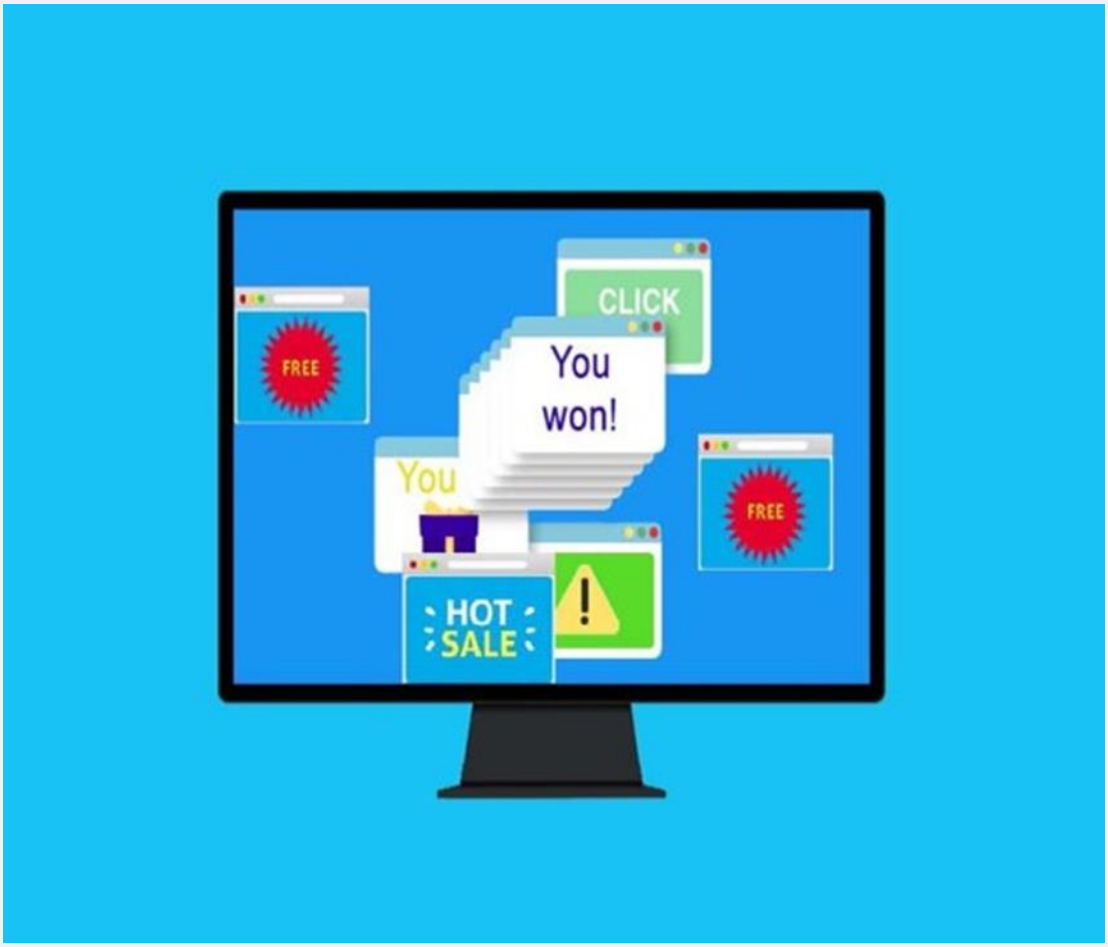
پرسش بدافزار چیست، می تواند برای قربانیان تروجان ها نیز ایجاد شود.

این نوع بدافزار ها خود را به گونه ای جلوه می دهند که کاربران گمان می کنند آن ها برنامه هایی بی خطر هستند و سپس به نصب این موارد می پردازند. بدین ترتیب تروجان اطلاعات شخصی آن ها را می دزدد و به جاسوسی می پردازد و یا خرابی هایی را در سیستم ایجاد می کند.



#۲-۷ تبلیغ افزار ها (Adware)

تبلیغ افزار ها معمولا با استفاده از ارسال تبلیغ های ناگهانی برای کاربران، آن ها را به سمت انجام کاری خاص سوق می دهند. بدین ترتیب وارد سیستم فرد شده و بر روی سرعت رایانه ها و گوشی ها آثار منفی بر جای می گذارند.



#۸-۲ بدافزار های بدون فایل (Fileless malware)

بد افزار بدون فایل از انواع نرم افزار های مخرب است که کامپیوترها، تلفن های همراه و... را آلوده می کند. این نوع بدافزار ها هیچ فایلی برای اسکن و شناسایی از خود به جا نمی گذارند. همین مسئله مبارزه با آن ها را دشوار ساخته است.

#۳ نشانه های آلودگی به بدافزار چیست؟

رایج ترین علامت آلودگی به بد افزار ها کاهش سرعت سیستم شما است. به طور کلی می توان نشانه هایی را برای آلوده شدن دستگاه ها بیان کرد که عبارتند از:

- کاهش سرعت: عملکرد کامپیوتر کند می شود.
- هدایت به سایت های مختلف: مرورگر شما را به وب سایت هایی می برد که قصد بازدید از آن ها را نداشته اید.
- هشدار ها: دائما هشدارهایی را در ارتباط با آلودگی سیستم مشاهده خواهید کرد که اغلب از شما می خواهد تا برای رفع این مسئله کاری انجام دهید.
- مشکل در خاموشی و راه اندازی دستگاه: ممکن است با مشکلاتی در خاموش کردن و یا روشن کردن دستگاه مواجه شوید.

- پاپ آپ (pop-up): این امکان وجود دارد که دائما تبلیغات pop-up برای شما نمایش داده شود.

هرچه بیشتر با موارد فوق رو به رو شوید، احتمال آلودگی دستگاه شما بالاتر است. هدایت به سایت های مختلف و نمایش هشدارهای دائمی از قطعی ترین نشانه های آلوده شدن دستگاه شما هستند.

حرف آخر

همان طور که با مطالعه این مطلب در ارتباط با پرسش بدافزار چیست، متوجه شده اید، گسترش فناوری های مختلف با تمام مزایای خود، بدی

هایی نیز دارد. امروزه اطلاعات شخصی افراد و امنیت دستگاه های آن ها در خطر است.

بنابراین کاربران باید آگاهانه در برابر اقدامات مجرمان مجازی عمل کنند تا هرگز از آن ها سوء استفاده ای نشود. امیدواریم توانسته باشیم با ارائه این مطلب شما را با بد افزار ها آشنا نماییم.