

۱۰ روش هکرها که امنیت دیجیتالی تان را به خطر می اندازند!

مردمیانی (Man-in-the-Middle Attack)

در این حمله، هکریه طور مخفیانه ارتباط دو طرف را رصد یا تغییر می دهد بدون اینکه متوجه شوند.

هک هایی که در شبکه های وای فای عمومی انجام می شوند، که در آنها هکرها به اطلاعات ارسال شده بین کاربر و سرور دسترسی پیدا می کنند.

حملات بدافزار (Malware Attacks):

بدافزارها نرم افزارهایی هستند که برای آسیب رساندن به سیستم های کامپیوتری طراحی شده اند. این شامل ویروس ها، کرم ها، تروجان ها و رنسومورها می شود. حمله بدافزار WannaCry در سال ۲۰۱۷ که به سیستم های ویندوز نفوذ کرد و اطلاعات کاربران را گروگان گرفت و برای بازگرداندن از آنها درخواست پول کرد.



حمله دیداس (DDoS Attack):

در حملات دیداس، هکرها حجم زیادی از ترافیک غیر واقعی را به یک سرور ارسال می کنند تا سیستم دچار اختلال یا خاموشی شود. در سال ۲۰۱۶، حمله DDoS به سرورهای Dyn باعث شد وبسایت هایی مثل توئیتر و اسپاتیفای برای ساعت ها از دسترس خارج شوند.



حمله رمز عبور (Password Attacks):

این حملات شامل حدس زدن یا استفاده از تکنیک های دیگر برای به دست آوردن رمز عبور کاربران می شود. حمله Brute Force که در آن هزاران ترکیب از رمز عبور امتحان می شود تا رمز صحیح پیدا شود.

