## مراقب ویروس‌ها و جاسوس افزارها باشید:

### ۱–مقدمه

بدافزار، اصطلاحی برای "نرم افزارهای مخرب" است. ویروس‌ها و جاسوس افزارها بعضی از بدافزارها هستند که در رایانه، تلفن یا دستگاه همراه و بدون اطلاع شما نصب می‌شوند. این برنامه‌ها می‌تواند منجر به کِرَش کردن ( crash ) دستگاه و برای مانیتور و کنترل فعالیت آنلاین شما استفاده شود. مجرمین از بدافزارها برای دزدیدن اطلاعات شخصی، ارسال هرزنامه و کلاهبرداری استفاده می‌کنند.

### ۲–توصیه‌هایی برای مقابله با بدافزارها:

کلاهبرداران امروزه تلاش می کنند تا کاربران روی لینک‌هایی که منجر به دانلود بدافزار و جاسوس افزار می‌شود کلیک کنند. برای کاهش مخاطره دانلود بدافزار و جاسوس افزارهای ناخواسته کارهای ذیل را انجام دهید:

- نرم افزارهای امنیتی خود را به روز نگهدارید. رایانه شما باید حداقل نرم افزارهای ضد بدافزار و ضد جاسوسی و یک دیوار آتش داشته باشد. نرم افزارهای امنیتی، مرورگر اینترنت و سیستم عامل را طوری تنظیم کنید که به صورت خودکار به روز رسانی شوند.
- به جای کلیک روی لینک در ایمیل، URL سایتی که قصد بازدید از آن را دارید مستقیماً در مرورگر وارد کنید. مجرمان ایمیل‌هایی را ارسال می‌کنند که به نظر از سمت شرکت‌های شناخته شده برای شما است اما در واقع اینگونه نیست. ایمیل ممکن است حاوی لینک‌هایی باشد که به نظر معتبر هستند اما کلیک روی آنها می تواند منجر به دانلود بدافزار یا باز شدن سایتی جعلی برای دزدیدن اطلاعات شخصی کاربر شود.
- ضمیمه‌های ایمیل را فقط در شرایطی باز کنید که ارسال کننده را می شناسید و آنچه را هم که ارسال کرده است می شناسید. باز کردن ضمیمه‌ها – حتی در ایمیل‌هایی که به نظر می‌رسد از سمت دوستان یا فامیل باشد– می‌تواند منجر به نصب بدافزار در رایانه شما شود.
- نرم افزار را فقط از وب سایت‌هایی که می شناسید و مورد اعتماد است دانلود و نصب کنید. دانلود بازی‌های جدید، برنامه‌های به اشتراک گذاری فایل، و نوار ابزارهای سفارشی شده ممکن است جذاب به نظر رسد، اما توجه داشته باشید نرم افزارهای رایگان می‌تواند حاوی بدافزار باشد.

- از مسدود کننده‌های پاپ آپ ( pop-up blocker ) استفاده کنید و روی هر لینکی در پاپ آپ‌ها کلیک نکنید. اگر از جنین مسدودکننده‌هایی استفاده نکنید، ممکن است بدافزاری روی رایانه شما نصب شود. پنجره های پاپ آپ را با کلیک روی علامت "X" در نوار عنوان ( title bar ) ببندید.
- تبلیغات خرید نرم افزارهایی که توسط پیام‌ها یا ایمیل‌های غیرمنتظره به شما پیشنهاد می شود را نادیده بگیرید. بویژه تبلیغاتی که هدفشان پایش رایانه شما و شناسایی بدافزار است- دانلود چنین نرم افزارهایی تاکتیکی برای پخش و گسترش بدافزارها است.
- درباره محاسبات ایمن با فرزندان خود صحبت کنید. به فرزندان خود گوش زد کنید که برخی فعالیت‌های آنلاین مانند کلیک روی پاپ آپ‌ها، دانلود بازی‌ها یا برنامه‌های رایگان، باز کردن ایمیل‌های زنجیره‌ای، یا ارسال اطلاعات شخصی می تواند رایانه را به مخاطره بیاندازد.

## شناسایی بدافزار:

رایانه خود را برای رفتارهای غیرمعمول مانیتور کنید. رایانه شما ممکن است در موارد ذیل تحت تاثیر بدافزاری قرار گرفته باشد:

- کند شدن، کِرَش کردن، یا نمایش پیام‌های خطای تکرار شونده
- عدم خاموش شدن یا راه اندازی مجدد رایانه
- باز شدن پی در پی تعداد زیادی پاپ آپ
- نمایش صفحاتی که قصد مشاهده آنرا نداشته‌اید و ارسال ایمیل‌هایی که شما ننوشته بودید

## رهایی از بدافزار:

اگر گمان می کنید که بدافزاری در رایانه شما وجود دارد، اقدامات زیر را انجام دهید:

- خرید اینترنتی، بانکداری الکترونیک و دیگر فعالیت‌های آنلاین را که نیازمند نام کاربری، کلمات عبور، یا دیگر اطلاعات حساس است متوقف کنید.

نرم افزار امنیتی خود را به روز کرده و سپس آنرا برای پایش رایانه در برابر ویروس‌ها و جاسوس افزارها اجرا کنید. هر آنچه که این نرم افزار به عنوان مشکل شناسایی می‌کند پاک ( حذف ) کنید. ممکن است برای اعمال تغییرات، مجبور به راه اندازی مجدد رایانه خود باشید.