How to avoid malware

Written by GCF Global, Excerpted from https://bit.ly/3afAD98

Malware is one of the most common hazards to your computer when you're online, but it's easy to avoid. Developing safe and smart browsing habits can protect you from malware and other threats, like viruses. Securing your computer and learning how to identify and avoid suspicious links are the fundamentals of safe browsing habits.

Secure your computer

Limiting your computer's vulnerability to malware is a crucial safe browsing habit. You can protect your computer by running antivirus and antimalware software like Bitdefender or Norton. These programs can block malware from being installed and can remove it if it does get onto your computer. Even if you don't see signs of malware on your computer, running regular scans can catch any malware that has escaped notice.

Many malware programs take advantage of security flaws in Windows and other software. Keeping your OS, browser, and other programs updated is an important step in protecting your computer. The security patches in these updates make your computer immune to many threats.

Back up your files

Some malware can delete or corrupt data on your drives. Preparing for the possibility of data loss is much easier and cheaper than attempting to recover data after a malware attack. The two most common ways of doing this are copying your data to an external drive and using an online backup service.

Avoid suspicious links

Most malware requires you to click something to download and install it. These links are often disguised as something they are not. If you are aware of what suspicious links can look like, you can avoid them. Here are some examples of misleading links concealing malware downloads.

Ads on websites can look like system messages or diagnostics warning you that something is wrong with your computer, like the image below.

Ads can look like messages saying you have won a prize and instructing you to click to claim it.

Pop-up windows frequently contain malware or attempt to lead you to a less secure site. Most reputable sites don't use pop-up windows. Many browsers block pop-up windows by default.
If you are prompted to download something you weren't expecting—or if it seems to be unrelated to the page you were on—it's probably malware.

Headlines that are ambiguous and sensational that encourage you to click to read more are called clickbait. Sites that use lots of clickbait headlines are more likely to contain links to malware.

Identify suspicious sites
If you're ever unsure whether a website or download is safe, close it and investigate the site before returning to it. It's always a good idea to be cautious when browsing unfamiliar sites.

Ask your friends if the site is reputable or if they have any experiences with the site.
Search for information about the site. Use a search engine to find news about the organization that runs the site, or look for posts on forums about other people's experiences with that site.

Check the address bar in your browser. Some malicious websites are designed to look like other well-known sites, but your address bar will tell you which site you're actually on. If you are no
longer on the site you expected to be, it's suspicious.

Run a Google safe browsing diagnostic on the site. Copy and paste the URL of a site into the search box on the diagnostic page, then click the search button. This will display a site safety report.