What is MALWARE?

Malware, short for malicious software, is typically installed on a website by cybercriminals. Malware is a broad term that refers to a variety of malicious programs. It can spread viruses, steal personal or financial data and even hijack computers.
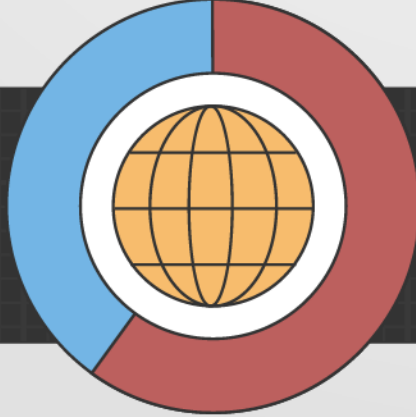
Exploring Malware

In 2015, **five out of six companies were targeted** by cybercriminals in some way.[1]

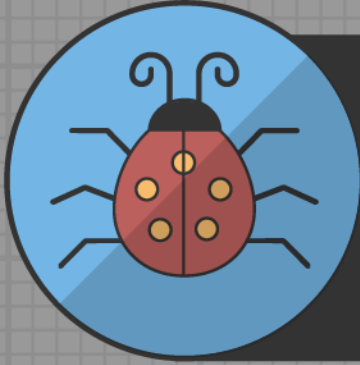Every day, over **ONE MILLION** malware threats are released.[2]

When hackers send malware-laced spam emails, it only takes **82 seconds** for someone to become the first victim.[3]
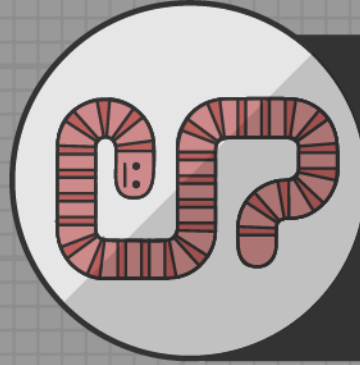
Over 60% of the websites that expose computers to malware are legitimate sites that have been compromised.[4]

Types of Malware

BUGS
A type of error, flaw or failure that produces an undesirable or unexpected result. Bugs typically exist in a website's source code and can cause a wide range of damage.

WORMS
A worm relies on security failures to replicate and spread itself to other computers. They are often hidden in attachments and will consume bandwidth and overload a web server.
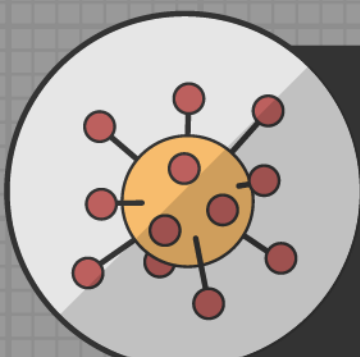
VIRUS
A piece of code that is loaded onto your website or computer without your knowledge. It can easily multiply and be transmitted as an attachment or file.
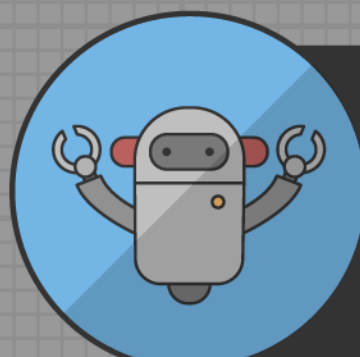
BOTS
A software program created to perform specific tasks. Bots can send spam or be used in a DDoS attack to bring down an entire website.
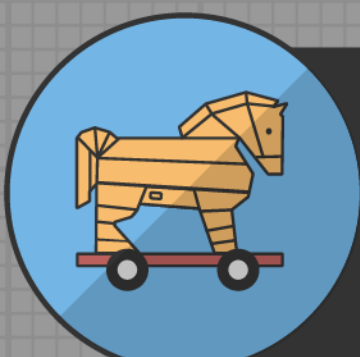
TROJAN HORSES
Much like the myth, a Trojan disguises itself as a normal file and tricks users into downloading it, consequently installing malware.
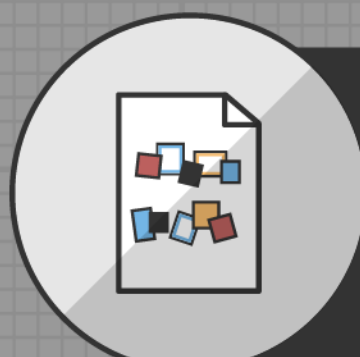
RANSOMWARE
Ransomware denies access to your files and demands payment through Bitcoin in order for access to be granted again.
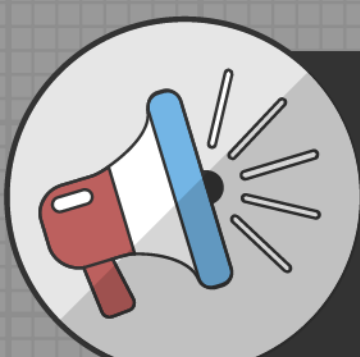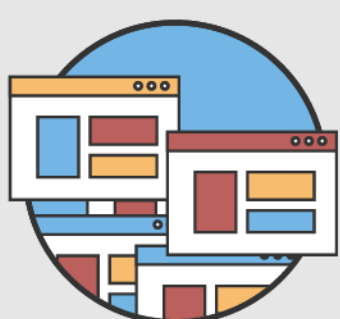
ADWARE
A type of malware that automatically displays unwanted advertisements. Clicking on one of these ads could redirect you to a malicious site.
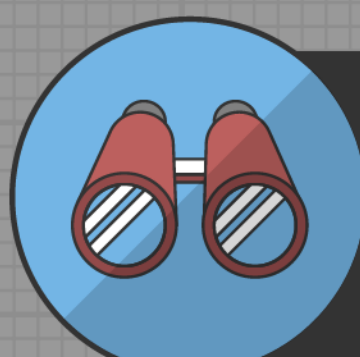
SPYWARE
A type of malware that functions by spying on a user's activity. This type of spying includes monitoring a user's activity, keystrokes and more.
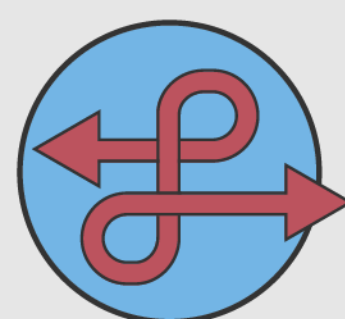
Signs You May Have Malware

Increased pop-up ads

Website or computer freezing or crashing

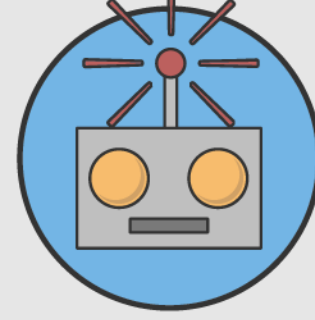Redirected browser navigation

Files being modified or deleted without your knowledge
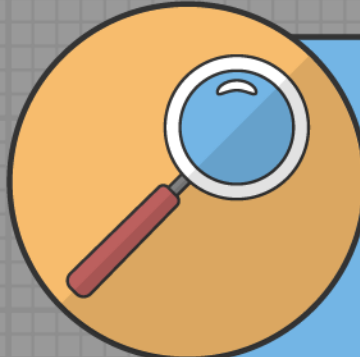
Emails and messages being sent without your prompting

Programs running, turning off or altering themselves

Putting a Stop to Malware

Have you scanned your website today?
Scan your website daily for malware and vulnerabilities. Make sure your service will automatically scan and remove malware found on your site.

Are you sure you want to download that?
Do not click or download an attachment from any unknown source. Files ending in, .jpg, .png, .pdf, .docx, .xlsx, and .pptx can be harmful, but are typically safer than other file extensions.[5]

Is this cruise to the Bahamas *really* free?
If an ad seems too good to be true, it probably is. Avoid clicking on pop-up ads, especially from brands you don't recognize.