# **What is Malware and How to Detect it**

We all have been a victim of malware one way or another at some point. The term malware indicates a broad category of malicious software that is created to damage, infect or disrupt a system. Malware refers to virus, spyware, ransomware, trojan horses or any other form of dangerous software. It is installed into the victim's system without consent and may cause the device to crash. Even if malicious software is not designed to crash the victim's system, it can be used to monitor the victim's online activity or gain access to confidential data.

A malware attack can have disastrous consequences on the system. It may even destroy the system from its core along with the additional blow of losing precious data. Therefore, it is extremely important to have in place certain security measures that can make early detection possible and somehow limit the impact of a potential malware attack.

Let’s look at some common types of malware that can damage a system and how they can be detected.

## **Common Types of Malware**

There are six categories of malware that are most common and dangerous.

**Virus**

There is a common misconception that all malware programs are viruses. This is not true. In fact a virus becomes part of the victim's system – which means that when other legitimate files are running, the virus file is also executed. Today, viruses form a small portion of the malware that is infecting systems. During the execution process, viruses tend to infect other files too which makes the system extremely hard to clean-up after a virus infection.

**Worm**

Worms are malicious software that spread into the system. Unlike viruses, worms don't need a user-action to spread. They can clone themselves and destroy systems. A single worm in a system can cause the entire organization to suffer.

**Ransomware**

Ransomware requires the victim to pay a certain "ransom" if they want the malicious software to leave the system. Ransomware is one of the most dangerous forms of malware as they spread very fast and encrypt all the files that come in their way while making them inaccessible to the system owners. To decrypt the files, the hackers require a certain ransom to be paid.

**Spyware**

Spyware is a type of malware that makes it possible for hackers to spy on systems. By doing so, hackers can get their hands on private information such as log-in credentials and financial information. Fortunately, spyware does not spread like viruses and worms and is comparatively easier to remove.

**Trojan**

Trojan is a type of malware that is usually spread either through infected websites or via links in emails. Hackers trick users into downloading Trojan viruses through pop-ups on websites or through other sources. Once the Trojan has downloaded, the system becomes infected and security is compromised.

**Hybrid Attack**

A Hybrid attack is one of the most dangerous forms of attacks. What makes them hazardous is the fact that they are a combination of two malware programs. In other words, they have combined features of two malicious software programs. For example, a virus that is initially behaving like Spyware may replicate itself like a Worm malware and cause irreversible damage to the system under attack.

## **How to Detect Malware?**

Detecting malware at an early stage can save a company from massive amounts of data loss. A free cybersecurity assessment can also help you understand the status of your system’s health and whether or not it is affected by any kind of malware. Early detection can also reduce the amount of money and resources being spent. Your system may be infected with a type of malware if it is displaying some or all of the characteristics below:

* Your system is displaying error messages repeatedly, is slower than usual, or crashes without any warning messages
* Your system is not shutting down, or restarting as usual
* You are receiving pop-up messages of irrelevant or inappropriate content
* Inappropriate ads are appearing on your screen and interrupting your activity
* You are unable to remove unwanted software
* You are shown webpages that you did not visit or emails are being sent under your name without your knowledge.

Some other less common signs of a malware attack include:

* Your system battery is draining quicker than usual.
* Some icons appear on your toolbar that you did not opt for or other changes made to your browser.
* Your browser's homepage changes repeatedly without warning.

For detecting the presence of malware in your system, use a reliable anti-malware program and run periodic scans for their timely removal.

## **How to Prevent a Malware Attack?**

There are several preventive measures to avoid a malware attack. Let’s have a closer look below.

* Make backups for all important files on your system so that you don’t have to worry about losing precious data when you’re fighting a virus
* Make sure that all the software on your system is up to date. A cybersecurity assessment can help you get this information
* You should have a powerful anti-virus program installed into your system which is updated to the latest version.
* You and your team (if you are working as part of a company) should be trained to not open any emails or click on any pop-up messages that randomly appear on your browser
* Use two-factor authentication to enable high-grade protection. Two-factor authentication helps gain protection from hackers gaining confidential information.
* Use strong password combinations and update them regularly
* Educate yourself on safe browsing practices

**Staying Protected**

Having strong protection against malware is extremely important for the safety of your system. However sometimes, no matter how well-guarded your system is, the hackers might still be able to gain entry and infect your system's health in some way. Using strong anti-virus programs and firewalls is one way to protect yourself, but one should always have a strong plan of action in case your system is infected.

Consulting with a team of experts in this regard can help to improve the security of your system and prepare you in case of an attack. Depending on the magnitude of the attack, it can be derived whether or not it is possible to recover from the damage or not. KMTech’s Cyber Security Vulnerability Assessment solution can help you determine the presence or likelihood of a potential malware attack on your system. To get to know more about our solution, book a [free assessment](https://kmtech.com.au/book-a-cyber-assessment/) with us today.