Reduce the time to Remove Malware by Weeks with Expert Help

The cyber world is a hazardous place. Hacker attacks deliver a seemingly endless supply of malicious programs to steal or encrypt data, monitor user activity, or even hijack computers remotely. And once an infection occurs, it can prove both time-consuming and costly to remove malware.

For example, most companies take between two and four weeks to recover from a ransomware or other serious malware attack. To minimize damage, learn to recognize the signs of infection and know the proper remediation steps to take. Additionally, engaging the expertise of security professionals can cut the recovery time in half and reduce the impact on your business.

You Might Have Malware If…

The longer malware lives in your system, the more damage it will do. Consequently, a reminder about the signs of infection can prove essential in minimizing the effects of an attack. Make sure that everyone in your organization knows to look for these signs and report them to IT.

Early warning signs of malware include:

- Unusually slow or inconsistent performance
- Applications that freeze
- Frequent popups
- System crashes
- Unfamiliar toolbars in the browser or icons on the desktop

Additionally, watch for computers running out of hard drive space, batteries that drain quickly, and antivirus protections suddenly deactivated.

First Alert IT and Disconnect from the Internet

When a user suspects a possible malware infection, quick action can save headaches. First steps involve alerting IT and disconnecting from the internet. Staying offline helps prevent the infection from spreading to other areas of the network. It also ensures that bad actors cannot steal additional data or passwords.

Then, while diagnosing the infection, make sure your antivirus is up-to-date and boot the computer in Safe mode. This means that the system will perform additional checks and that only the bare minimum of programs will load.

Note that ransomware involves additional problems, including file encryption and ransom demands. A ransomware attack may also necessitate involving law enforcement.

Scan for and Remove Malicious Applications and Code

With the computer in Safe mode, scan for malicious applications and dangerous code. Look through the activity monitor to identify suspicious applications that are hogging resources. Most importantly, use a reputable anti-malware program to run a thorough scan.

Even if you run a good antivirus program and keep it up to date, no antivirus solution will catch 100 percent of problems. Malware removal tools take the process a step further to detect and remove infections that standard antivirus may miss. Using antivirus and anti-malware tools in conjunction will help maximize protection.

Once you have found and removed malicious code, address the entry points to help ensure against reinfection. Because web browsers provide a primary gateway for malware, begin by restoring the original browser settings. Also, verify your homepage and connection settings to make sure the malware has not modified them. Then delete your browser cache.

If Attempts to Remove Malware Prove Unsuccessful

Hopefully, system scans and anti-malware tools will do the trick. Unfortunately, some malware infections prove more difficult to remove. In some cases, you will need to wipe the device and reinstall the operating system and applications. Before doing so, perform a system backup and enlist the help of an expert.

Remove Malware Quickly with Expert Help

Organizations that have experienced a malware attack may find themselves blindsided by the time and frustration involved in the recovery process. Finding and removing the source of the infection can prove challenging and expensive. And an inexperienced user may inadvertently cause additional problems in the process.

Fortunately, security professionals can ease the pain. With the proper tools, in-depth knowledge, and close cooperation on the client side, they can greatly improve the prognosis. eMazzanti's Security and Operations Center and Recovery services protect clients with continuous monitoring and expert remediation services.