HOW TO

PREVENT THE MOST COMMON MALWARE ATTACKS



COUNTYMICRO
YOUR TRUSTED IT SOLUTIONS PARTNER



TROJANS

WHAT ARE THEY?

A Trojan horse, or Trojan, is a type of malicious code or software that looks legitimate but can take control of your computer. A Trojan is designed to damage, disrupt, steal, or inflict some other harmful action on your data or network.

HOW TO PREVENT THEM

Trojans are usually sent via email attachments in spam emails or transmitted through fake software. Training your staff to recognize malicious emails and links and prohibiting downloads of software unless approved by your IT partner is a good place to start.

COUNTYMICRO
YOUR TRUSTED IT SOLUTIONS PARTNER



Viruses

WHAT ARE THEY?

A computer virus, is a type of malicious code or program written to alter the way a computer operates and is designed to spread from one computer to another. Because viruses can't hide behind the guise of a useful program, they are usually distributed as e-mail attachments.

HOW TO PREVENT THEM

Training your employees to recognize malicious emails as well as integrating a high-end spam filter and email-based antimalware software will do the trick. You IT partner can audit this software regularly to make sure everything is up-to-date.

COUNTYMICRO
YOUR TRUSTED IT SOLUTIONS PARTNER



Worms

WHAT ARE THEY?

A worm is a form of malware that operates as a self-contained application and can transfer and copy itself from computer to computer. They generally target pre-existing vulnerabilities in the operating system of the computers they attempt to infect.

HOW TO PREVENT THEM

By allowing your IT partner to install patch management tools for apps, operating systems, and firmware, you avoid a potentially huge and damaging attack on your operating system.

COUNTYMICRO
YOUR TRUSTED IT SOLUTIONS PARTNER



Ransomware

WHAT IS IT?

Ransomware is set apart by its use of extortion and encryption. When a computer or server is infected, all its files are rendered unreadable until victims pay a fee to return everything back to normal.

HOW TO PREVENT IT

Make sure that you have a tested, reliable off-site backup of your critical files, and that those backups are protected from being infected. Your IT partner can ensure that you have proper, secure backups and a layered security defense to prevent ransomware and set up an effective disaster recovery plan.

COUNTYMICRO
YOUR TRUSTED IT SOLUTIONS PARTNER