

Questions & Answers about Malware

1. What is malware?

Malware – formed from the words **malicious** and **software** – is a general term used by computer professionals to refer to many different kinds of computer software designed to infiltrate or damage a computer system without the owner's knowledge or consent. Malware includes computer viruses, worms, trojan horses, spyware and many other malicious and unwanted software types.

2. How can a malware infection occur?

Malware can infect a user's computer through many paths, including pop-up messages that ask users to download things, links in web pages or e-mails, infected websites and many other methods that can sometimes even be invisible to the user. Malware is often used in conjunction with phishing scams.

3. What are the consequences of malware?

At a minimum, malware is a nuisance, sometimes displaying unwanted advertising or using a user's computer to send spam. At its worst, malware has the potential to steal personal and financial information ranging from browsing habits to e-mail address lists to online banking passwords and even identity theft.

4. How can I protect myself from malware?

While there is no single fool-proof method, users should keep their anti-virus software up to date and running and keep their operating systems and applications updated with the latest patches from the manufacturers.

Other common suggestions include exercising extreme caution with e-mail links and attachments and using firewalls to protect information on personal computers. End users should also be warned to look for login windows or messages that appear strange or different, which could be signs that a user's computer has been affected with malware.
