How do I deal with cyber attacks?

Never open unexpected attachments, especially if they contain .pdf or .zip files, says Rick Maybury.

Cyber attacks can slip past security software Photo: ALAMY

By Rick Maybury

7:00AM GMT 02 Nov 2013

I have this been subjected to a vicious cyber attack and from nowhere ten or more years of saved documents have been encrypted. I have been offered a release Key in three days time provided I pay $300 or Euros 300. I refused to pay, and am now saddled with some quite important file losses of files. Is there any hope? Can anyone detect the source of such criminal tactics?

David Harris, by email

A Ransomware program called Cryptolocker has been doing the rounds since September and is arguably one of the nastiest pieces of malware, to date. It can get on to your PC through an email attachment, often purporting to come from someone you know or a company or organisation that you have had dealings with, or by visiting an infected website or by downloading pirated software. Once activated it swiftly encrypts all of your data files and you are given 96 hours to pay up, typically £100 to £300, before the decryption key is destroyed.

To date all attempts to track down the villains who created it, or break the encryption within the

time limit have failed. To make matters even worse it can slip past security software, or by the time it is detected, it is too late. The usual malware avoidance techniques can help protect your computer, so never open unexpected attachments, especially if they contain .pdf or .zip files and avoid pornographic and pirate software websites. However, in the end the best protection is make sure that all of your important data is frequently and securely backed up on protected drives or systems.

Security software should eventually catch up with Cryptolocker but there are steps you can take now to protect your files. If you know your way around the Windows Group Policy Editor you can create rules that stop the infection from working. There are instructions on how to do this, and a useful article on Cryptolocker on the **bleepingcomputer** website. Otherwise there is a simple freeware tool that does it for you on the Foolish It website, called **CryptoPrevent**. If you have inadvertently opened an attachment and think your PC may have become infected it is probably too late to stop the damage but if you are quick you might be able to stop it spreading to other drives and PCs on your network by immediately disconnecting from your WI-Fi or router.