CARBONITE

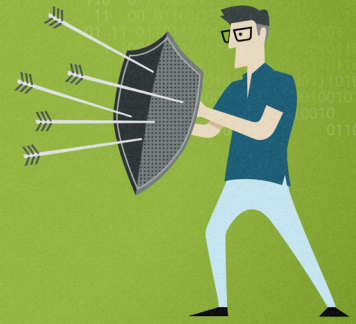# Fight back against a ransomware attack in four easy steps

Ransomware attacks are on the rise and they're a big problem for both businesses and households.

If you need proof, just ask the city of Durham, North Carolina. Some of the city's computers recently became infected with a ransomware virus that locked up their files and threatened to render them useless unless a ransom was paid.

But the city of Durham had the perfect weapon in the fight against ransomware: backup software.

When a ransomware virus attacks, people who use cloud backup software like Carbonite Safe™ Backup can retrieve their files quickly without paying the ransom. The key is to proactively make sure your files are protected with cloud backup software because that's the best insurance against ransomware.

If you're a cloud backup user that falls victim to a ransomware attack, getting your files back is a breeze. Just follow these four easy steps:

1. As soon as you're aware of a ransomware attack on your computer, file server or network, immediately shut down any file-sharing activity.

2. Assess the extent of the infection and the damage. If needed, your computer's antivirus software can help you locate any digital files that have been encrypted with ransomware.

3. Remove the virus by deleting all infected files.

4. Log into your cloud backup system and recover clean versions of the infected files.

See, when you have a backup plan, recovering from a ransomware attack is as easy as 1-2-3-(4).

Learn more about Carbonite data protection today.

Visit Carbonite.com.