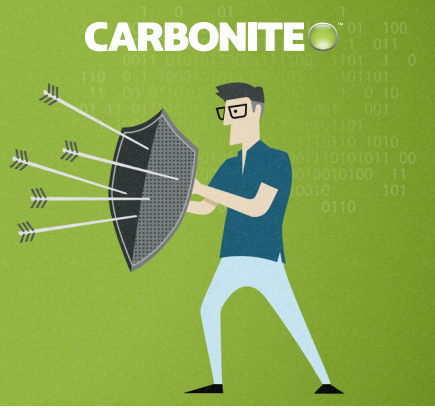
Your ransomware response: Prepare for the worst

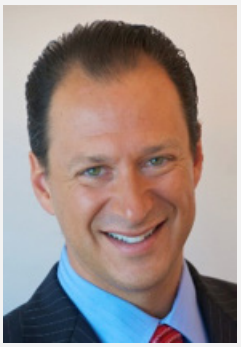


A ransomware attack is when your computer gets locked down or your files become inaccessible, and you are informed that in order to regain use of your computer or to receive a decryption key to unlock your files, you must pay a ransom. Typically, cybercriminals request you pay them in bitcoins.

The attack begins when you're lured, by a cybercriminal, into clicking a malicious link that downloads malware, such as CDT-Locker. Hackers are skilled at getting potential victims to click on these links, such as a phony email, apparently from a company you do business with, luring you into clicking on a link or opening its attachment.

And if you find your computer is being held hostage:

- Report it to law enforcement, although it's unlikely they can provide help. It's just good to have it recorded.
- Disconnect your computer from its network to prevent the infection from spreading to other shared networks.
- You need to remove the ransomware from your computer. Remember, removal of the ransomware won't restore access to your files; they will still be encrypted.
- If you already had your data backed up offline, there's no need to even consider paying the ransom. Still, you will want to remove the ransomware and make sure your backup solution was working.
- But what if very important files were not backed up? Prepare to pay in bitcoins. The first step is to find out what the experts say about making payments in bitcoin.
- The crook will be essentially impossible to trace. You'll be required to make the payment over the Tor network (anonymous browsing).
- Finally, don't be shocked if the crook actually provides you the decryption key—essentially a password; ransomware thieves often follow through to maintain being taken seriously. Otherwise, nobody would ever pay them. But it would not be unprecedented to not receive the key. It's a gamble.



Robert Siciliano

Robert is a security analyst, author and media personality who specializes in personal security and identity theft and appears regularly on Good Morning America, ABC News and The TODAY Show.

Your ransomware response: Prepare for the worst

The best course of action is to prevent a ransomware attack, and that means looking for all the clues to malware and phishing scams. Don't let threatening emails, saying you owe back taxes or bank fees, jolt you into hastily clicking a suspicious link or attachment. If you regularly back up your data online and to an external drive, then you'll never feel you must pay the ransom.

Learn about Carbonite data protection today.

Visit Carbonite.com.