5 Steps to Take If You're a Ransomware Victim

Spoiler alert: It still might end badly

by Randy Lilleston, **AARP**, May 16, 2017|Comments: 0

GETTY IMAGES

Imagine this scenario: You're at home, answering email or working on a presentation for your job. Suddenly, a screen flashes up on your computer, demanding you turn over money if you want to see your files again.

Your keyboard is locked. Rebooting the computer brings the screen right back. If you try to grab your files through another computer on your network, you find that everything has been encrypted. Your work is dead in the water.

That's the reality of a ransomware attack, as many people worldwide are learning in the wake of the WannaCry outbreak.

Still, there is a (possibly slim) chance you can solve the problem — and if nothing else, an attack can serve as a lesson learned to help protect you in the future. Here are five steps you can take now if you are a victim.

- **Don't pay the ransom.** Security experts emphasize this again and again: *Don't pay it.* Payment implies that you trust the attacker to resolve the situation. Why would an attacker risk exposing himself or herself by making good on a promise to unlock your computer or files? Better still, why wouldn't an attacker just install a new file on your computer to launch a fresh attack a few weeks later?

  "Remember, you're dealing with criminals," Christopher Budd, a global threat communications manager with the digital security firm Trend Micro, wrote in a company blog post last July. "There's no guarantee you'll actually get all your files back. Even if you do, you're only helping ransomware continue to be a problem by rewarding the criminals."

- **Reinstall your files from a backup.** Many people think the reason to back up files is to be able to replace them if computer hardware breaks. Here's a prime example of how backing up your files solves multiple woes. You can set up your computer to do this automatically to another drive or the cloud — and once you've set it up, you can forget it unless something goes wrong.

- **Make sure your operating system and antivirus are up to date.** Microsoft is aggressive about releasing updates to address potential security issues. A fully up-to-date Windows 10 system is protected against the current attack, but many companies use older versions of Windows or restrict automatic updates. They are the ones vulnerable to attack.

- **Contact your IT department or antivirus company.** If you're on a corporate machine, it's essential that your IT department be told of the attack right away. It may have tools to help you recover your files. There are also some antivirus tools that may help with certain kinds of ransomware attacks — but again, don't hold out too much hope.

If none of that works, consider the worst "solution":

- **Accept that your files are lost and gone forever.** Reformat your hard drive, reinstall your operating system and learn a hard lesson. Most of us have been there at some point. Just remember: Backups are your computer's best friend, so when you've finished reinstalling your operating system, make sure to set up an automatic backup.