New American

Written by **C. Mitchell Shaw** on May 15, 2017

How to Protect Yourself From a Ransomware Attack

With the recent ransomware attack taking its toll on nearly a quarter of a million computers and affecting millions of users and their customers around the world, the question in the minds of many right now is, "How do I protect myself from something like this?" Fortunately, the solutions are simple, even if some of the biggest names in business around the globe missed them or were unable to use them.

As *The New American* reported earlier today, ransomware has been around for almost 30 years, but has gained notoriety only in the past decade. In the past 10 years or so, ransomware has claimed millions of victims who have paid to regain access to the files on their computers. As this writer explained in that article:

> Ransomware works by encrypting all of the personal data files on a computer, making them inaccessible to the user unless he has the correct key to decrypt them. In a typical ransomware attack, the first indication the victim has of the attack is a warning that takes over his computer screen telling him that all of his files have been encrypted and that he must pay a ransom to the attacker to get the key. The ransom is only accepted in some type of untraceable currency — usually Bitcoin. It is also common for the attacker to give two deadlines. The first deadline is the day the demanded payment will go up — usually by at least 100 percent. The second deadline is the day the attacker will wipe all of his own files — including the keys to unlock the victim's files — and walk away. After that day, it would be impossible to recover the encrypted files.

When the victim is an individual user, the ransom is typically a few hundred dollars; for businesses, the ransom could be $10,000 or more. Since powerful encryption is — by design — uncrackable, a large percentage of victims simply pay the ransom and hope for the best. In most cases, the attacker provides the correct key and the victim — usually a few hundred (or thousand) dollars poorer — is able to unlock the encrypted files.

Since the most recent ransomware attack — like almost all others — relied on unpatched vulnerabilities in Microsoft Windows, the first thing to consider (regardless of your operating system) is whether your operating system is up to date with the most current security patches. If not, download and install them now. Of course, if you are among the millions who have resisted Microsoft's heavy-handed approach to force you to "upgrade" to Windows 10 in all of its spyware glory, you probably have most updates turned off. If that is the case, you may want to consider switching to a more liberty-friendly (and privacy-friendly) operating system, such as Linux. With a Linux distribution such as Ubuntu, you can take advantage of frequent security updates without sacrificing your privacy. As an added advantage, Linux is secure against viruses.

Besides keeping your operating system up to date with security patches, it is also important to keep all other software up to date. Remember, hackers rely on unpatched vulnerabilities. Keeping your software current means having the most recent security updates.

Underneath it all, though, is this: Every individual who ever paid a ransom to a hacker (or lost his data because he didn't) could have dodged the whole ordeal if he had kept a backup of his data. To keep it simple, remember ABC and 3-2-1.

ABC stands for Always Be Copying (your data). If it is important enough to have, it is probably important enough to have a copy of it.

And 3-2-1 stands for having three copies of all your important files in at least two formats with at least one of those stored off-site. Formats change over time. If you have all your wedding pictures backed up on a Zip drive from the early 2000s, you may find it difficult to restore that backup. If your data is in at least two different formats, the likelihood of recovery goes way up. If one of those backups is stored off-site and you are unfortunate enough to be the victim of fire or flood, you can still recover your important files.

A good example of applying ABC and 3-2-1 would be someone who has a regular schedule for backing up files to an external hard drive as well as using an online backup service. Such a person would have the copy on his computer, the copy on the external hard drive, and (in a different format) the copy stored off-site by the online backup service. Of course, if you are going to consider online backup, look for a service such as SpiderOak One, which offers end-to-end, Zero Knowledge encryption, so not even the people minding the servers can see your data or know your password.

In the event that you are hit with ransomware, do not attempt to restore from a backup until you have made sure your computer is free of the malware used to install the ransomware. If your computer is still infected and you plug in an external drive, it will likely be infected and encrypted, as well.

First, using a non-infected computer, make another copy of your backup. Then, make sure you have removed the malware from the infected computer. If you don't know how to do this, take your computer and one copy of your backup to a reputable computer repair shop and have it done. The techs there can also restore your data from the backup. Even if something should go wrong, you still have both the second backup at home and the backup in "the cloud." In a worst-case scenario, you could simply replace the hard drive and restore your backup.

This process allows you to securely restore your data without paying a ransom to criminals. If more people would do this, fewer would have to give in to the demands of these criminal hackers and the profit margin wouldn't be there to make the risk worth their while.

Written by **C. Mitchell Shaw** on May 15, 2017