Ransomware

Three things converged at once to prompt me to write about Ransomware. Thing #1: news items in the popular press. Thing #2: a happenstance conversation with one of my dedicated newsletter readers. Thing #3: an article about the evolution of Ransomware. All this on the same day…!

The short definition of ransomware is a sophisticated software program that activates when clicking on an email link or attachment, or installing a downloaded program, or clicking on an infected ad within a website. The ransomware immediately begins encrypting all your data files, scrambling and "locking" them from use. After that, a warning screen pops up saying that your files are encrypted, and a note about how to pay the ransom to get the "unlock" key.

Important Note: if you think you are immune because you have anti-virus installed on your PC, the short answer is you are not. Anti-Virus will not stop a ransomware program from encrypting your files. Anti-Virus programs also cannot keep up with the volume of new ransomware versions that are released daily. At the rate of 3,500 per day or more, it's just impossible.

If you are unlucky enough to be affected by ransomware, here is my advice: **don't pay the ransom.** Two reasons: #1: It only encourages more of this activity. #2: sometimes the unlock key does not work, and then you are totally out of luck **and** your money is gone... Ransomware perpetrators don't offer refunds. So the best defense is a good offense.

A Good Offense: the usual list of things to avoid: Don't...

1. Surf to sketchy websites or click on sketchy ads
2. Click links or open email attachments
3. Download files or programs, unless you absolutely verify they are safe

Ransomware is not hacking: the perpetrators do not get "on your machine" and plant it. To date, it only arrives on a computer because the users themselves did one of the "no-no's" above.

The answer to all this is an oldie, but seldom used goodie: **application whitelisting**. In short, application whitelists are the opposite of what anti-virus programs do. Instead of a "blacklist" of dis-allowed known ransomware programs, a Whitelist blocks all programs except those in the known "good" list. This solves the basic problem inherent in blacklisting:iIf new ransomware (or any other type of virus) comes out faster than your anti-virus can be updated, you are essentially unprotected from anything but old versions.

Why isn't Whitelisting more popular? **Because it's not easy to set up**, **and people don't like it.** Creating the whitelist involves some trial and error, and once it is set, every new program requires another addition to the whitelist. People don't like it because it removes the freedom to install programs. But it's the only way to insure 99.9% safety, and I recommend it, especially if you have kids at home. Here's a how-to article on Whitelisting.
-John Becker