CS CYBER SECURITY & YOU

OCTOBER 2019

WHAT IS RANSOMWARE?

Recently, there have been several news stories reporting that businesses and school systems throughout Louisiana have experienced a Ransomware attack. This Ransomware problem has been so pervasive that Governor John Bel Edwards issued a statewide emergency declaration in July making available state cyber security resources to help fight this problem.

Ransomware is software that is installed on a computer without the owner's consent or knowledge, allowing the hacker to lock up valuable data files and hold them for ransom. Ransomware attacks are a lucrative business for hackers in America as many small businesses and local governments do not have the financial resources to hire and maintain professional Information Technology (IT) staff. Many victims find it is easier to just pay the ransom than to incur the costs of fighting the problem.

So what can you do to make sure you do not become the next victim? There are steps you can take to combat this threat, but keep in mind these hackers are smart and resourceful, and are constantly finding new ways to breach security efforts. Here are the things you should absolutely do to greatly diminish your chances of becoming a victim of Ransomware:

1. **Use a newer operating system on your computer.** Microsoft and other operating system makers release security patches for operating systems, but not forever. Microsoft will announce the "end of life" of operating systems and no longer release any security updates. If you still run one of the older operating systems, you risk being hacked.
2. **Turn on automatic updating.** Operating systems, such as Microsoft, release security patches weekly to defend against known threats. Make sure your operating system is set to automatically download and install these updates.
3. **Backup important data.** If you have important data that you cannot lose, make sure you backup that data to an external hard drive or to a secure cloud backup service.
4. **Install an anti-virus software.** Installing Anti-Virus software is essential to good cyber security safety, but make sure you have it set to automatically update itself or you will become vulnerable.
5. **Beware of suspicious emails.** Never click on a link in an email. If you want to go to that website, open an Internet browser, and manually type in the link. This is the number one cause of malware and ransomware.

SAFE COMPUTING!

LASERS IT
Making Digital Retirement a Reality