Project: Blog Post
Client: VTS
Writer: Debby Wadsworth, Freelancer
SME: Dylan Kerling, VTS Technician

GOALS: Build Awareness of VTS
Position VTS as an Expert
Solicit Used Equipment

DW-Writer.com
debby@DW-Writer.com

How to Fight Back Cybersecurity Attacks

An unparallel number of Cybersecurity threats are bombarding the U.S. government, American companies, and citizens. It is a security war exacerbated by a pandemic creating havoc in our everyday lives. Threat levels continue to intensify with more people working remotely from places other than their usual office.

Enemies like hackers are always ready, quick to take advantage of old technology. They are creating fake CDC and vaccine sign-up sites to steal data. Plus, launching ransomware attacks and holding data hostage. In 2021, an estimated at six trillion dollars was paid in ransom to get data back.

IT Departments are in overdrive working on overcoming a long list of challenges. They include passwords, unsecured personal devices, unencrypted file sharing, and insecure home Wi-Fi. It is a challenge that at times is overwhelming for it's hard to stay ahead of the attackers. Plus, it is very costly cutting into budgets and bottom lines.

Those fighting fail to see a light at the end of a tunnel. For factors like working from home is here to stay. A 2021 Gartner survey reported 80% of company leaders surveyed responded they plan to continue allowing people to work from home at least part-time.

But there are ways to effectively fight and win the war. It takes strategies to overcome cyber-bombs with key elements for creating a more robust cyber security strategy or improving your current one. They include the following:

#1 - It's Time to Technology-up

It is time to evaluate your IT infrastructure, including hardware, software, applications, subscription services, processes, etc. If you use PC or Apple older technology, it is time to replace it with newer models. The costs can be offset by selling your current equipment to companies like Velocity Tech Solutions (VTS). Plus, by considering newer hardware models from VTS or another resale vendor.

#2 - Data Isolation - Air Gap Protection

Another effective technique is creating an 'Air Gap' to isolate critical operational areas like accounting or your organization's data system. If one system becomes infected, the Air Gap can prevent further contamination.

#3 – Never Enough Education

Organizations are constantly changing as they evolve and grow. Keeping the entire organization in alignment, including every employee, requires regular communication and education. Failure to do so has affected organizations by unaware or informed employees who click to open a link that unintentionally introduces malware into the network.

#4 – Continuous Monitoring, Testing, Upgrading

Continuously monitoring and testing systems is mandatory to detect potential intrusions or vulnerabilities early. Also, making sure there are no open doors or exploits that can enable unauthorized entry.

#5 – Continuous Backup and Recovery

It is crucial to have backup and recovery plans in place and use them. Most backups are implemented as 2-1-1¾two copies, one media type, and one location. Better still is a 3-2-1 backup strategy¾3 copies, 2 media types, 1 media location, 1 air-gapped copy.

#6 – Improve Data Storage, Management & Security

Basic protection plans with data backups are not enough. A strategy is needed that detects potential failures and intrusions from inside and outside the company, including customer portals. Plus, move to a higher level of data security by upgrading or adding things like hybrid cloud storage that prevents ransomware attacks.

To sell your current hardware and learn other ways of protection, contact the experts at Velocity Tech Solutions by calling 888-784-2088 or 651-633-0095. Or visit www.velocitytechsolutions.com.