COMPUTER DEPOT INC.
BUSINESS SOLUTIONS

Tech Bits and Bytes to Help You with Your Business

Computer Depot Inc. Business Solutions Newsletter — November 2020

Thomas Hill, President & Founder

*"To stay **focused** on what I **should** be doing, I continually ask myself two questions. What am I good at? and What is holding me back?"*

November 26th

TRIVIA

CONGRATULATIONS

WINNER

Derek Jarnigan

Manning Windows

Scientists looking for the Loch Ness Monster found 100,000 golf balls instead!

TURN TO PAGE 3 FOR THIS MONTHS TRIVIA

Making This One Mistake With Your Computer Network Could Put You Out Of Business

How do you handle network issues? If you're like most small businesses, you wait until something breaks or goes wrong before getting an IT services company on the phone. At a glance, it makes sense. Why pay to fix something if it isn't broken?

Sadly, this way of thinking can do more harm than good, and it has taken many businesses out of commission.

When you get right down to it, there are two primary ways to handle network security:

- **By being reactive**
- **By being proactive**

One of these costs *significantly* more than the other and can destroy a business. You can probably guess which one we're talking about.

When you're reactive with your IT services, which includes data security, it means something bad has already happened. There are many different things that can harm your data and your business, like an employee accidentally downloading malware onto their computer, you getting hit by a data breach or a power surge occurring late in the night after a thunderstorm hits.

However, being reactive basically opens the door to these threats. It's the one mistake that can put you out of business *for good*.

Hackers, for example, are a HUGE threat to small businesses. These cybercriminals will stop at nothing to break into your network to steal whatever they can get their hands on or do whatever damage they can.

Continued on pg.2

These people don't care if their actions put you out of business.

This is why you cannot rely on a reactive approach to your IT services. When you do, you're a step behind hackers, malware and even natural disasters and equipment failures.

In the past, IT services were very reactive. They were built on the break-fix model, which is exactly as it sounds. A business would wait for something to break or go wrong before calling an IT services company for help to fix it.

In the 1990s and even into the 2000s, the break-fix model had its place and it worked. But as technology improved and it became easier for even the smallest businesses to stay ahead of the curve, the break-fix model stopped making sense.

The number of external threats has increased *dramatically* over the last 10 years. There are countless malware programs floating around on the Internet, and hackers are working 24/7 to wreak havoc.

It's time to get proactive.

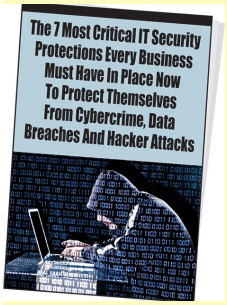
Today, IT services companies can predict threats. They can stop attacks in their tracks and protect your business and your data. This is called **managed services** — and it could save your business.

When you work with a managed services provider, you can state exactly how you want to be proactive. Do you want your network monitored for threats 24/7? Do you want them to have remote access to your networked devices so they can provide instant support to you and your team? They can do all of that!

A good IT services company can help you make sure all your data is backed up and secure. They can make sure external threats are spotted before they become a problem. They can make sure phishing e-mails don't expose you to harm. The list goes on!

If you're already working with an IT services company and they're only providing outdated break-fix support, it's time to say, "Enough!" Demand that they get proactive to manage your network. Don't wait until something breaks to make that phone call. Because, as many businesses have learned, waiting to make that call can be devastating!

FREE Report: The 7 Most Critical IT Security Protections Every Business Must Have In Place Now To Protect Themselves From Cybercrime, Data Breaches And Hacker Attacks



Eighty-two thousand NEW malware threats are being released every day, and businesses (and their bank accounts) are the No. 1 target. To make matters worse, a data breach exposing client or patient information can quickly escalate into serious damage to reputation, fines, civil lawsuits and costly litigation. If you want to have any hope of avoiding a cyber-attack, you MUST read this report and act on the information we're providing.

Claim your FREE copy today at

https://www.ComputerDepotBusiness.com/7security

"I can talk DIRECTLY to the techs at Computer Depot and explain what my problems are. I like that!"

Joel Owenby
Supervisor, CEMEX

Thank You!!!

Camp Wesley Woods

We want to say a huge thank you to everyone who donated to our Camp Wesley Woods campaign. CWW is located less than 10 minutes from the Great Smoky Mountains in Townsend, TN and the camp's 700 acres include mountains views with a forested valley with the Capshaw Branch flowing through the middle into the Little River. CWW offers a wide range of programming and mission includes inspiring youth to grow as disciples of Jesus Christ and experience adventure in the midst of God's wondrous creation. We were able to raise over $2500 and are blown away by all the support that poured in. Congratulations to Jim Glasscock of Locke Plumbing, the laptop winner!

Top 7 Reasons to Choose COMPUTER DEPOT Business Solutions

1. **Prompt Response Time** We begin working on your issue in 20 minutes or less during normal service hours.
2. **Phones Are Answered by Us.** Your call will never leave Big Orange country! Ever. Not to mention, when you have a problem WE ACTUALLY PICK UP THE PHONE!!!
3. **We Have Been Serving Knox and Sevier County for 20 years.** As a locally owned and operated business, you are our neighbor!
4. **We Are Your IT Service Department** WE take care of it. No blaming, no finger-pointing. We Focus on the Fix.
5. **Freedom of Choice** There are No Long-Term Contracts to sign.
6. **90-Day Test Drive** What is better than risk-free?!
7. **A Package Tailor-Made To Fit You** We address *your* unique technology needs.

HIPAA FACTS

Top 3 Causes of Data Breach

Employee Action

Third-Party Error

Lost or Stolen Devises

We can help you

Protect Your Practice from HIPAA Violations

865-909-7606

THANK YOU, VETERANS.

For your service and sacrifice

Become A Pro At Videoconferencing From Home

At the start of the year, most of us weren't prepared to take video calls at home. We just didn't have the right setup. Now we're practically at the end of the year, and we're out of excuses! Here are four quick tips to transform into a videoconferencing pro:

1. **Boost your sound.** A dedicated microphone is going to sound much better than the mic in your phone or laptop. Creating an optimal sound environment can make a difference, so turn off external speakers and hold the call in a quiet zone.

2. **Adjust the video.** Keep your camera at eye level with a simple background. This not only looks more natural, but it also minimizes visual distractions and instantly looks more professional.

3. **Light it up.** This can get complicated fast. You want a light source in front of you, but your computer monitors are not enough. However, you don't want harsh, direct lighting. Diffused lighting is best, but ring lights are popular among YouTubers and work great for video calls.

4. **Look good!** Keep simple button-down shirts, ties, blouses and other items near the computer so you can dress and look professional for a call. Keep it business casual and avoid complicated patterns and harsh colors that can look awkward on camera.

This Month's

TRIVIA

The winner is always randomly selected from ALL correct responses.

Here is your next chance to WIN Lunch on us with a question my teenagers say is waaaaay too easy!

The next upcoming Marvel Movie to be released is Black Widow. What is Black Widow's real name?

Email your answer to RHill@ComputerDepotOnline.com

Don't Leave This Backdoor Wide Open!

Most of your employees probably have wireless networks set up in their homes.

Unlike your business WiFi, many home wireless networks lack proper security, leaving a backdoor open to hackers. WiFi signals often broadcast far beyond your employees' homes and out into the streets. Drive-by hacking is popular among cybercriminals today.

Here are a few tips for securing your employees' WiFi access points:

- Use stronger encryption and a more complex password.
- Hide your wireless network name.
- Use a firewall.

These security measures are not difficult to set up. If you have any questions or need assistance, we will be happy to help get your employees set up remotely. Call us today at **865-909-7606**

"Nice try, but no, it's not like going to the Thanksgiving Parade."

Computer Depot
Business Solutions
10721 Chapman Hwy #30
Seymour, TN 37865

PLACE STAMP

November 2020

Look What's Inside...

- **Making This One Mistake With Your Computer Network Could Put You Out Of Business !**
- Hurry-You could WIN this month's Trivia and this
- 5 Tech Trends Heading into 2020!
- Become A Pro At Videoconferencing From Home!
- **The Biggest Cyber Security Risk Your Business Faces**
- **Don't Leave This Backdoor Wide Open**
- *Special Invitation to Medical Practices*

COMPUTER DEPOT BUSINESS SOLUTIONS - AFFORDABLE IT HELPDESK AND CYBER SECURITY SUPPORT IN 20 MINUTES OR LESS

ATTENTION Medical Practices with Remote Work Challenges

In March 2020, medical practices were forced to quickly deploy their support staff to remote working environments, usually the worker's home. Medical billers, coders and clinicians, were set up with remote access to protected health information without much time to assess the HIPAA privacy and security risks, let alone the impact on work performance.

Now is the time for medical practices to evaluate their compliance and business risks related to remote work environments and to put corrective action plans in place for any issues that may need attention. Join Jennie Hitchcock, President of Compass Healthcare Consulting, and Thomas Hill, President of Computer Depot Business Solutions, to learn:

- New ideas and best practices for increased security in the home office.
- Monitoring for remote workers to ensure protocols are followed.

COMPASS HEALTHCARE CONSULTING

- Potential administrative issues in the home office setting that can jeopardize HIPAA security and privacy.
- Home WiFi setup for best practices.
- Current pitfalls for medical practices.

A live Q&A session will also be hosted to discuss situations that you've experienced in the remote work environment.

Jennie and Thomas will be live on Thursday, November 12th at 11:30am EST for this free one hour webinar.

Registration is open now at CompassHealthcareConsulting.com.

Contact Us

Computer Depot Business Solutions

For over two decades
Serving Knox and Sevier Counties

5416 S Middlebrook Pike
Knoxville, TN 37921
Phone: (865) 909-7606

or

10721 Chapman Hwy
Seymour, TN 37865
Phone: (865) 577-4775

Email: thill@ComputerDepotOnline.com
Visit us on the web at www.ComputerDepotBusiness.com