



COMPUTER DEPOT INC.

BUSINESS SOLUTIONS

Tech Bits and Bytes to Help You with Your Business

Computer Depot Inc. Business Solutions Newsletter

February 2021



Thomas Hill, President & Founder

"Count-Upon Character is the foundation of our core values. It is doing what is right, doing our best, and doing what we say we will."



How To Enable Remote Work Without Exposing Your Entire Business To Cybercriminals

A record number of businesses said goodbye to the traditional in-office work model in 2020. They embraced the remote work model as they adapted to the new COVID-19 reality. It was a huge shift that came with many challenges, and some of those challenges are still felt today.

One of those challenges was - and is - cyber security. Businesses wanted to get their remote workforce up and running, but there were a lot of questions about how they would keep their newly remote employees secure.

So, how can you enable remote work while keeping your business and your employees secure? How do you keep cybercriminals out? The answer is multifaceted. There is no one-size-fits-all approach to cyber security - that would make things much easier! But there are several steps you can take to help your

remote team stay productive while keeping the cybercriminals out. Here are three things you need to do:

1. Skip the public WiFi. This is Cyber Security 101. Never use unsecured, public WiFi, especially when working. For remote employees who have the option to work from anywhere, using public WiFi is tempting. It's just so easy to access, but it comes with huge risks, including the potential to expose your device to intruders. Thankfully, there are plenty of options to help keep employees connected without having to worry about snoops. The most popular is the VPN, or virtual private network. VPNs allow remote workers to securely access the Internet, even through public WiFi. VPNs are ideal for remote workers who need to routinely access your network.



FEBRUARY IS HEALTHY HEART MONTH

TRIVIA

Congratulations

Melissa Flowers

from

Pratt Aycock

who knew that **THE BALD EAGLE** is an animal found in every US State except Hawaii.



TURN TO PAGE 3 FOR THIS MONTHS TRIVIA



Continued from page 1

Another option is the personal hotspot. This is a portable WiFi access point, usually paired with data service through a telecom like Verizon, AT&T or T-Mobile. It gives remote workers flexibility to work anywhere they can get high-speed data service. Because the remote worker is the only person on the hotspot (and should be the only person), there is less worry about hackers snooping for your data.

2. Have a strong device policy.

When it comes to cost-cutting, it can be appealing to let employees use their own devices while working remotely. Avoid this, if possible. The bring-your-own-device (BYOD) approach has its benefits, including keeping costs down, but the security costs could be massive, especially if an employee gets hacked or misplaces crucial data. In short, BYOD can get complicated fast, especially for businesses unfamiliar with the BYOD approach.

That said, many businesses work with an IT services company or managed services provider to create a list of approved devices (PCs, laptops, tablets, smartphones, etc.) that employees can use. Then those devices are loaded up with malware protection, a VPN, and other security solutions. So, while employees may be using a variety of devices, they all have the same security and other necessary software in order to perform their duties.

The best device policy, however, is to provide employees with work devices. This ensures that everyone is using the same hardware and software, and this makes it much easier to keep everyone up-to-date and secure. It takes a little more effort logistically, and it has a higher up-front cost,

but when it comes to keeping your business secure, it's worth it.

3. Don't forget about physical security.

While a lot of businesses are focusing on digital security right now, they're not putting a similar focus on physical security. They may have a team of people working remotely spread across different neighborhoods, towns, states or countries. This mobility comes with the risk of device theft or loss.

If employees will be carrying their work devices with them for any reason, those devices should be kept nearby at all times. That means never leaving work devices in vehicles or unattended at a café or airport (or any location). Never leave a device where it has the potential to be taken.

It's also important to remind employees to not only keep their doors locked but also keep work devices out of sight. You wouldn't want to set up a home office in a room facing the street outside while leaving the windows open and the door unlocked, because you never know who may walk or drive by. Just as cybercriminals are always looking for ways to break into your network, criminals are looking for opportunities to walk away with high-value items.

The way we work is changing, so we must be prepared for whatever happens next. Implementing these three steps will give you a starting point, but they aren't the end point. Work with an experienced MSP to get the most out of your remote work approach. Many businesses will not be returning to the traditional in-office model, so the more steps we take to secure our businesses and our remote teams, the better off we'll all be.

.....
"I would highly recommend anyone to use Computer Depot that has a business. You would not regret choosing them as your IT firm, they're amazing to work with."

**Shawna Bates,
City Diesel, Inc.**

.....



If your actions inspire others to dream more, learn more, do more and become more, you are a leader.

~John Quincy Adams

When you get to be President, there are all those things, the honors, the twenty-one gun salutes, all those things. You have to remember it isn't for you. It's for the Presidency.

~Harry S Truman

Anyone who is capable of getting themselves made President should on no account be allowed to do the job.

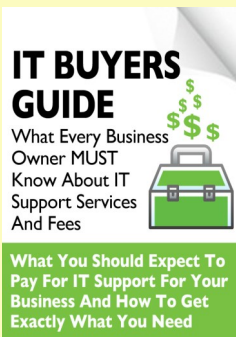
~Douglas Adams

I would rather belong to a poor nation that was free than to a rich nation that had ceased to be in love with liberty.

~ Woodrow Wilson

Free Report Download:

The Business Owner's Guide To IT Support Services And Fees



You'll learn:

- The three most common ways IT companies charge for their services and the pros and cons of each approach
- A common billing model that puts ALL THE RISK on you, the customer, when buying IT services; you'll learn what it is and why you need to avoid agreeing to it
- Exclusions, hidden fees and other "gotcha" clauses IT companies put in their contracts that you DON'T want to agree to
- How to make sure you know exactly what you're getting to avoid disappointment, frustration and added costs later on that you didn't anticipate

Claim your FREE copy today at www.ComputerDepotBusiness.com/17questions/

Get More Free Tips, Tools and Services At Our Website: www.ComputerDepotBusiness.com
 (865) 909-7606

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.

CALL 909-7606

TO SCHEDULE A FREE 10 MINUTE CONSULTATION

or learn more at

www.ComputerDepotBusiness.com

The Realities Of Burnout

We all feel burned out every now and again. It's the point when we feel completely exhausted with our work and need to step away. But here's a different way to think about burnout: we don't get burned out because we're working *too much*, we get burned out because we're doing *too little of what we love*.

When we do things that we're passionate about, that gives us energy and keeps us going. When our work becomes work for the sake of work, that's what drives us toward exhaustion. You may be productive, but does your productivity enrich your life in any meaningful way? To truly avoid burnout, engage in activities, projects and tasks that drive you forward and keep the passion alive. *Inc., Nov. 23, 2020*

4 Traits To Keep In Mind When Hiring

1. Value-minded. They're someone who fits in with your company culture and values. They're ready and willing to learn and grow within that culture.

2. Purpose-driven. They aren't in it just to collect a paycheck. Yes, being paid is important, but there must be drive beyond that. They have their purpose and they're working toward it.

3. Standout. There's something about them that strikes you – it could be anything from their credentials to their personality, but it's something that sticks with you in a positive way. They go the extra mile.

4. Open-minded. They're receptive to feedback and criticism and use it to grow. But more than that, they're willing to give feedback to others. They're comfortable with honesty. *Forbes, Nov. 23, 2020*

Who Is At Risk and Who's Watching the Watchers?

Nearly every week, you hear a news story about a cyber-attack or a rogue virus sweeping through the country or the world. Last month SolarWinds experienced a supply chain attack and it was a big deal and made big news. Maybe you're a little bit skeptical. Are these viruses really a problem for you? Are these cyber-attacks really aimed at a business like yours? So we thought it might be fun to share some statistics with you.

In just the last 12 months, we have done the following: stopped 4.3 million ransom attacks; kept 4682 computers and servers safe from those attacks; required our staff to undergo over 200 hours of continuing education to stay on top of current threats; replaced 73 old, outdated firewalls.

So, as you can see, this is a very present threat to your company, and we are always watching your back.

But who is watching the watchers?

This past year, to further verify and enhance our own security, we partnered with a cyber security firm out of Nashville to audit our network and to guide us in improving our processes and controls. After all, *your* network is only as secure as *our* network. They have assured us that all of our products and protocols are exactly as they should be. You can trust the products we use and trust that we are always working to keep your data and your business safe.

If you're not 100% sure you're protected, give us a call today at 909-7606 or go to www.ComputerDepotBusiness.com/DiscoveryCall and schedule a FREE 10 minute consultation.



This Month's TRIVIA

Here is your next chance to WIN!

According to billboard.com what is the number 1 love song of all time?

Correctly answer this month's trivia question and you may win the prize and all the glory!


Email your answer to RHill@ComputerDepotOnline.com



February 2021



Look What's Inside...

- **How To Enable Remote Work Without Exposing Your Entire Business To Cybercriminals**
- **Who Is At Risk and Who's Watching the Watchers?**
- Hurry-You could WIN this month's Trivia and this 
- **4 4 Traits To Keep In Mind When Hiring**
- The Realities Of Burnout. You're NOT alone.
- **Driving Business Success In The Age Of COVID-19**

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

Driving Business Success In The Age Of COVID-19

Countless businesses had to figure out how to navigate the last year. Some didn't make it, but at the same time, many thrived. Nearly a year after the pandemic began, many businesses are still trying to navigate COVID-19 repercussions. How do you drive success in 2021? Here's two suggestions.

Budget Wisely. Countless businesses had a knee-jerk reaction to the pandemic. They rapidly cut costs in an effort to survive. Cutting certain areas can work. But cut the wrong area of a business, and it may be hard to recover. Some companies that put off upgrading technology during the pandemic are now paying for this costly mistake with out-of-date hardware and software that created holes in their network that are open to cybercriminals. However, if your customers didn't stick around, cutting the marketing budget is disastrous.

Embrace New Ideas. COVID-19 isn't going anywhere soon. Businesses that decided not to adapt because they thought it would blow over were put into a tough spot. Meanwhile, businesses that planned and focused on innovation were in a much better spot. When your customers' habits change, your habits need to change as well. Forbes, Nov. 23, 2020

What do you call romance in a fish tank?

Guppy love.

Why do skunks celebrate Valentine's Day?

Because they're scent-imental.

What did one octopus say to the other octopus?

Can I hold your hand, hand, hand, hand, hand, hand, hand, hand?

What do you call two birds in love?

Tweethearts.



How did the phone propose?

He gave her a ring.

What kind of flower is the worst to get on Valentine's Day?

Cauliflower.

Why are artichokes so beloved? They're known for their hearts.

What does a caveman give his wife on Valentine's Day?

Ughs and kisses.

Contact Us

**Computer Depot
Business Solutions**

**For over two decades
Serving Knox and Sevier**

**5416 S Middlebrook Pike
Knoxville, TN 37921**

Phone: (865) 692-4247

or

**10721 Chapman Hwy
Seymour, TN 37865**

Phone: (865) 577-4775

Email:

thill@ComputerDepotOnline.com

Visit us on the web at

www.ComputerDepotBusiness.com