# TECH TIPS
## TECHNOLOGY INSIGHT THAT BUILDS BUSINESS

**HODGSON**
CONSULTING & SOLUTIONS

**NEW Upcoming Webinars**
**SEE PAGE 2 FOR MORE DETAILS**

**IT MANAGERS**
FREE SUMMER WEBINAR SERIES
Securing YOUR IT Infrastructure From Risk To Recovery

**PROTECT YOUR BUSINESS ASSETS**
Incident Management & Response
· July 20 | 1:00pm CST

**PLAN AHEAD, PREPARE NOW**
How To Create An Effective IT Disaster Recovery Plan
· August 3 | 1:00pm CST

**HODGSON**
REGISTER NOW! Limited Space Available
www.HodgsonConsulting.com/summer

## July 2023

This monthly publication provided courtesy of Robert Zehnder President of Hodgson Consulting & Solutions.

### Our Mission:
To eliminate every technical frustration, obstacle and inefficiency for companies with multiple locations and/or a remote workforce.

# Don't Settle For Less
## 5 Questions Every IT Professional Should Say Yes To

Business owners have a wide variety of responsibilities. In many cases, they oversee the hiring process, ensure operations run smoothly, and find the best third-party vendors to help benefit their business for years to come. One problem many business owners face when hiring a third party is knowing whether they're the right fit for their business. Making the wrong choice can be detrimental to your business, so how can you ensure you make the right decision? You ask essential questions.

Knowing which questions to ask is easier said than done though. Most business owners are convinced to use a third party, thanks to the persuasive skills of an excellent salesperson or representative. Still, many of these salespeople hold their cards close to their chest. They only tell you what you want to hear, leaving out anything that might make you doubt their expertise or

abilities. We've seen this with many IT "experts," so we wanted to help you by providing you with some questions you should ask before they get anywhere near your network.

Here is what you should ask any IT professional before hiring them to oversee your network, IT, and cyber security practices. These are simple yes-or-no questions; if you get a no from the "*expert*" for any of them, you're probably better off finding a different option.

### Are They Monitoring Your Network At All Times To Ensure Security Settings And Security Patches Are Current?
For many businesses, the whole purpose of hiring an IT team or individual is to keep their cyber security protected. They might work with sensitive data that, if compromised, could harm their clients and the business's reputation.

You need to make sure any IT expert you hire is going to stay up-to-date with the current security patches so they can ensure all holes are covered to keep your business protected. There should not be gaps when they aren't monitoring your network.

### Do They Provide Detailed Invoices That Clearly Explain Everything You're Paying For?

Some IT "experts" believe the business owners they work with are clueless about the IT and cybersecurity industry. They'll try to overcharge for simple tasks without fully explaining what they did, and their invoices are as basic as it gets. This shouldn't fly with you. Every third party you work with should provide detailed invoices so you can see exactly what you're paying for. It's a huge red flag if they refuse to do this.

### Will They Be Proactive And Provide You With Regular Updates?

If you're hiring someone to oversee your IT needs, you don't want them to be another responsibility you must manage. You want to trust them and know they're doing everything possible to assist your business. If you have to constantly go to them to see

> **You need to make sure any IT expert you hire is going to stay up-to-date with the current security patches so they can ensure all holes are covered to keep your business protected.**

how they're doing on certain projects, you're better off with someone else.

### Do They Offer Any Guarantees On Their Service?

This is a big one many people don't think about, but it could make all the difference in your decision. A business or individual who does excellent work will stand behind their service no matter what, which means offering guarantees that they'll do what they say they'll do. Find out how they respond if your company's data is compromised or something goes wrong with a particular piece of software. Their response should tell you whether they're trustworthy or not.

### Do They Have Set Rates For Each Project?

Before hiring them to assist with your IT needs, you should know how much everything costs. You should be cautious if they say they won't know how much something will cost until they start working. There's no telling how much they'll try to charge you, and it could be difficult to know if you're getting bamboozled or not.

It's important to have IT assistance for your business, as it helps keep your company, employees, and customers protected. These are just a few questions you should ask before hiring an IT expert. If they answer no to any of the above questions, then continue your search and find someone who is a better fit and has your best interests in mind.

# Out Of Office:

## 6 Cybersecurity Best Practices For Business Travelers Going On Vacation

As we get into the summer, many business owners and employees look forward to a well-deserved break. However, high achievers are known to do a little work on vacation. Unfortunately, studies show that working outside the office, whether on vacation, from a local coffee shop, or even business travelers out on work trips, can lead to significant cyber security issues. If you or your employees plan on answering urgent emails or checking in on projects while on vacation this summer, it's essential to maintain strong cyber security best practices to avoid exposing the company network to hackers preying nearby. In this blog post, we'll cover what cyber security best practices for remote workers must be implemented so that you and your team can get your work done and enjoy your vacation without worrying about a data breach.

### Why Cybersecurity Matters While Travelling

For business travelers, the need to stay connected to the office is a reality of the digital age, and our handheld devices make it easy. But with this constant connectivity comes an increased risk of cyber threats. Whether you're using a public Wi-Fi network in the lobby or accessing sensitive files from your hotel room, you can expose your company to hackers, malware, and other cyber risks.

Cybercriminals know how this works! They understand that people are more likely to let their guard down while on vacation. They know

you're more focused on enjoying your time off than ensuring your devices are secure. This situation makes travelers an attractive target for cybercriminals, who can use a variety of tactics to compromise your data, such as phishing emails, fake websites, and man-in-the-middle attacks.

To minimize the risk of a cyberattack while traveling, here are a few best practices to cover with your team:

- **Use A Virtual Private Network (VPN):** A VPN encrypts your internet connection, ensuring your data is secure even when using public Wi-Fi networks. Before you leave, set up a VPN on your devices and use it whenever you're online.

- **Keep Your Devices Updated:** Before leaving for vacation, update your devices to the latest software and security patches. Outdated software can leave you vulnerable to cyberattacks, so staying current is essential.

- **Be Wary Of Public Wi-Fi:** Although convenient, public Wi-Fi networks can be a hotbed for cybercriminal activity. Avoid using these networks whenever possible. Yes, that means no checking your email poolside unless you have a VPN.

- **Enable Two-Factor Authentication (2FA):** Using 2FA adds an

extra layer of security to your accounts by requiring a second form of verification, such as a text message code or fingerprint scan. Make sure to enable 2FA for all of your critical accounts before you depart.

- **Beware Of Phishing Attempts:** Cybercriminals often target travelers with phishing emails, which are designed to trick you into revealing sensitive information. Be cautious of any emails you receive while on vacation, and never click on suspicious links or download unfamiliar attachments.

- **Secure Your Devices:** Physically secure your devices by always keeping them with you and never leaving them unattended in public places. Additionally, enable password protection, biometric authentication when applicable, and remote wiping capabilities in case your device is lost or stolen.

Traveling for business or pleasure doesn't mean you should compromise on cyber security. Following these best practices can reduce the risk of a data breach or other cyber security issue while away from the office. However, it's important to know that these steps aren't infallible. To truly ensure that your company's cyber security measures are up to par, you need to work with a qualified IT team that can monitor your network 24/7, patch any vulnerabilities that pop up (which happen regularly), and can alert you if something goes wrong.

# Create An Experience Your Customers Won't Forget



Businesses that create an exceptional customer experience will always hold a position within their industry. This is especially noticeable with companies like Apple or Disney. Around 58 million people travel to Orlando annually to visit Walt Disney World, and many who visit annually cite the customer experience as their primary reason for returning. Apple consistently goes above and beyond to help its customers with whatever they need, and because of this, it's rare to walk by an Apple Store that isn't full of customers.

So, how can you create a similar following for your business? It starts with creating a phenomenal customer experience for everyone walking through your doors. Here's how to do so:

- Ensure you and your team are knowledgeable about the products and services offered. You should never have to say, "Give me one second while I find out."

- Give your customer-facing employees the power and tools to rectify customer problems.

- Find ways to amaze your customers. Even something as simple as providing a discount on your customers' birthdays can make them loyal for life.

## The Secret To Hiring The Right Employees For Your Business

Hiring can be one of the most stressful situations a business leader can experience. Who you hire plays a role in every aspect of your business's success, from customer satisfaction to profitability. This leaves many wondering how to ensure they hire the right people.

Begin by carefully analyzing the potential hire's resumé and cover letter. Ensure their skills and experience are a good fit for the position while checking for grammar and spelling errors. When you bring them in for the interview, ask questions about how they handled difficult situations in the past, and don't be afraid to role-play. From there, you should have them take a skills test or participate in an exercise, if applicable, to ensure they can do the job well. If everything goes well, and you think they're a good fit for the position, call their references and run a background check. Performing these steps will help ensure you hire the right person for your open position.

## Get The Sleep You Deserve



Every day is important for an entrepreneur, so you have to stay at the top of your game. One of the best ways to ensure you perform at your best is to get enough sleep every night, but that isn't always easy. It's difficult to fall asleep when your mind is racing about the next day's meetings or an upcoming presentation. Thankfully, there are a few things you can do to help you get a good night's rest.

- Forgo alcohol and caffeine in favor of water, especially before bed.

- Get outside and exercise throughout the day.

- Use blackout curtains, remove nightlights, and don't leave the TV on while you sleep.

- Create a consistent sleep schedule and stick to it!



*"Cancel that call to tech-support. This may be beyond their capabilities."*