



The Teck Report

What's New



Omega Tecks would like to wish everyone a Happy Fourth of July!

During this holiday, please remember to be vigilant as attackers will use the holiday to target business.

Three Email Security Tips

- ✓ If the email includes an attachment, double check who sent the email. Look closely at the email address.
- ✓ If the email has a link, hover over the link and see where it will take you.
- ✓ If in doubt, contact the sender!

July 2022



This monthly publication provided courtesy of Jason Mance, CEO of Omega Tecks.

Our Vision:

Is to be a great IT partner that helps small businesses grow, be more productive, excel, achieve great things all while being protected and secure.



Compliance And Cyber Security

Why Both Are Important

In the world of business, you'll inevitably hear about the many ways to beef up your cyber security to ensure your company's and clients' safety. However, another term is often heard when discussing cyber security: compliance. It's not talked about as often, but both cyber security and compliance are essential for any business to succeed.

Compliance helps businesses keep consumer information protected, and this compliance is fulfilled when businesses and organizations prove that their cyber security practices meet specific security regulations and standards set by third parties like government agencies. Compliance is not optional; businesses must meet these

requirements to protect sensitive information as well as their clients. Failure to meet compliance requirements results in fines, penalties and even legal ramifications.

If your business is compliant with its cyber security protocols, it'll also appear more trustworthy to the clients and other businesses that work with you. One cyber security breach can permanently damage your company's reputation. Customers will no longer want to do business with you for fear that their personal information could become compromised.

While cyber security and compliance sound fairly similar, there is a slight difference between them. Compliance is

Continued on pg.2

Continued from pg.1

often driven by business needs rather than technical needs, whereas security is driven by the need to protect against constant threats. If you want to maximize your company's cyber security practices, then you'll need to go further.

Overall, compliance and cyber security should work hand in hand. Your initial cyber security plan should be based on compliance. You must know the standard requirements to remain compliant and put the necessary practices in place to achieve that status. This comes down to knowing the exact details of what is necessary to stay protected. You should be specific so your team knows exactly what is needed to protect your business.

You also need to make an effort to document your practices as frequently as possible. You should create a paper trail of everything you have done to stay compliant as well as your added cyber security practices. It can help to add potential

"Compliance is fulfilled when businesses and organizations prove that their cyber security practices meet specific security regulations and standards set by third parties like government agencies."



audits and any frequency-bound events to your calendar so you don't get blindsided or miss something important.

After you've gathered all of your evidence and put your cyber security and compliance protocols to work, you can automate many of your reports. That way, you won't have to dig and pull data yourself in the future.

While it might seem like a lot of work to ensure your business remains compliant, companies out there can help. Managed IT services providers go above and beyond to ensure your cyber security is bulletproof. While they are taking care of all of your IT needs, they are also ensuring your business remains compliant with any third-party governing bodies. New cyber security threats are introduced every day, and only with strong cyber security and compliance practices can you ensure your business is protected for the foreseeable future.

Free Report: What Every Small-Business Owner Must Know About Protecting And Preserving Their Company's Critical Data And Computer Systems

PROTECT YOUR NETWORK

"What Every Business Owner Must Know About Protecting and Preserving Their Network"



Don't Trust Your Company's Critical Data And Operations To Just Anyone!

This report will outline in plain, nontechnical English the common mistakes that many small-business owners make with their computer networks that cost them thousands in lost sales, productivity and computer repair bills, and will provide an easy, proven way to reduce or completely eliminate the financial expense and frustration caused by these oversights.

Download your FREE copy today at

<https://otlnk.com/NLArticle0722>

or call our office at (913) 281-6457 .

The Difference Between a Reliable vs. Risky IT Service Provider

Reliable IT Service Provider:

- Centralizes your IT services
- Provides reliable and responsive customer service
- Proactively identifies tech risks

Risky IT Service Provider:

- Offers a standard package right away
- Speaks in tech jargon
- Takes a long time to get back to



IT SERVICE PROVIDERS
AREN'T EQUAL EITHER

The Secret to Getting Reliable IT Services for Your Small Business

If you are a small company trying to find its footing in today's competitive business landscape, getting reliable IT services can be particularly challenging. Luckily, you have the option of hiring an external IT service provider who can get you all the software solutions and technical support you need to run an effective

Contact Us to see how Omega Tecks can provide superior service while keeping your business secure and protected!
913-281-6457

The 3 Hardest Questions About Your Career

One of the best parts of my job is helping people strategize about their careers. Success at work plays a large role in how we view the successes in our lives. If someone doesn't feel like they're succeeding or fulfilled at work, they probably don't feel like they're living a very fulfilling life.

My team and I have advised many people from various backgrounds over the years. From billionaire entrepreneurs who are looking to brainstorm ideas for the next stage of their careers to private equity titans who are solely focused on dealmaking, I've learned that background doesn't always matter. People from nearly every background still have the same challenges when it comes to career management.

Luckily, there are three questions you can ask yourself to help decide the next steps you should take for your career.

First, ask yourself where your skills lie. You also need to gain an understanding of the work that you're willing to do. Once you've found the sweet spot between your skills and what you're willing to do, you're ready for the next step.

You should then ask yourself about potential career paths. It's best to come up with three career paths that you could realistically follow. While one could be a promotion or growing in your role, you should also consider working for other companies or even starting your own business.

The final question you should ask yourself relates to the people you know.



You need to think about 10 people who can help you get your dream job. It's not about putting out a blast message to all of your friends and followers on social media. Instead, you should focus on those who know your work ethic. Start with bosses who know of your work ethic and are well-respected. Any clients or customers who truly appreciate your work should also go on the list as well as well-connected friends and family – and even a recruiter or two. Once you've created a list of 10 people, send them all a message asking for ideas to help you land your dream job. Those brainstorming sessions could easily turn into referrals if done right.

Maybe one day, career management will be automated and our dream opportunities will approach us. But until then, it'll take hard work to reach your goals. If you don't know where to start, try asking yourself these three valuable questions.



Dr. Geoff Smart is chairman & founder of ghSMART, a leadership consulting firm that exists to help leaders amplify their positive impact on the world. Dr. Smart and his firm have published multiple New York Times best sellers. He stays active in his community and has advised many government officials.

3 Types Of Technology Every Business Needs

Over the past 20 years, technology has developed rapidly and advanced to levels that previously only existed within the confines of our imaginations. Whether you're an entrepreneur starting a new business or a seasoned business owner, there are many pieces of technology you can incorporate into your business to produce better results.

Digital marketing tools have seen some of the biggest advancements over the past decade. To stay ahead of the competition, you need to have an informative and useful social media presence that coincides with your website and other digital campaigns. You also need to invest in cloud technology since it will allow your company to revolutionize how you share information. If your business deals with customers, it can be incredibly beneficial to find customer relationship management software that works for you. Various studies have shown a direct correlation

between using CRMs and positive customer retention.

4 Ways Businesses Can Go Green

There's been a renewed focus on how businesses interact with the environment. There are many consumers who prefer to do business with companies that are more eco-friendly. While it's great for attracting new clientele, putting your business on the path to a greener and cleaner future is the best way to stay environmentally conscious. Don't know where to start? Try out these four easy methods for a greener workplace.

- Avoid using paper, and go digital where you can.
- Allow your employees to work remotely whenever possible to help eliminate carbon emissions.
- Analyze your company's current consumption and waste management practices and make adjustments where needed.

- Partner with environmentally conscious vendors and partners so all of your processes will be as green as possible.

Be Cautious Of These 3 Cyberthreats

If you own or operate a small business, you're probably aware of some of the different methods that cybercriminals will use to try to steal sensitive information from your business, but there are some new threats making headlines. A recent report from CyberCatch saw the cyber security platform provider review 20,000 randomly selected small businesses in the U.S. for vulnerabilities that can be exploited by cybercriminals. It found that "spoofing," "clickjacking" and "sniffing" are new methods they are exploiting, but what do these terms actually mean?

- Spoofing happens when a cybercriminal uses a fake IP address to pretend to be someone who has access to the company's private system.
- Clickjacking occurs when a user clicks on something on their computer that appears harmless but is actually malicious.
- Sniffing takes place when hackers intercept a network's traffic to access unencrypted data.

It's important to stay up-to-date on all the new methods used by cybercriminals in order to keep your business protected.



"Is that computer, down there, the one you were having problems with?"