the NetWork

LeadingIT

Chicagoland CybersecurITy Support

July 2021

Six Tips to Reduce Cyber Risks With a Remote Workforce

Is Your Trusted IT Services Company Really Doing Its Job?

Don't Use Public Wifi, Here's Why

Are You Looking for New Internet Service and Phone System Providers?

Six Tips to Reduce Cyber Risks With a Remote Workforce

The major shift from the traditional working environment to remote working found many companies unprepared and lacking the digital capacity to support their employees. As companies focus on adopting new tools and systems to connect their employees and facilitate seamless collaboration, cybersecurity is often overlooked. This unpreparedness and ignorance expose vulnerabilities and makes the organization highly susceptible to various cybersecurity risks.

What can you do to prevent cybercriminals from having access to private and sensitive organizational data?
Here is a cybersecurity survival guide to help your businesses remain secure during this indefinite period of remote working.

1. Educate Your Employees on Cyber Threats

Cybersecurity training is crucial so that employees can understand the cybersecurity risk landscape. The training should cover various aspects of cybersecurity including, the different forms of cyber threats, how they present themselves, how they can be identified and how they can be prevented. Training should also be continuous as cyber threats tend to evolve and new threats prove to be more sophisticated and cause more damage.

2. Adopt the Trust No One Approach

As an organization, you need to adopt the mindset that everyone is after your data, and your data is never safe enough. While you may trust yourself and other employees in the office to keep company data safe while online, it's important to remember that while working from home, company computers are likely to be exposed to other members of the family who aren't as safe online. It's, therefore, crucial to remind your staff to keep company devices safe and restrict other members of their households from accessing their work mobiles, laptops, or any other form of company resource.

3. Install Internet Security and Antivirus Software

One of the most effective cybersecurity tips while working from home is investing in comprehensive, effective, and reliable internet security software for you and your staff. Antivirus software is designed to protect against threats such as ransomware, spyware, trojans, worms, viruses, and phishing scams sent via email. Internet software also takes all the work off your hands by providing automatic remote work security against these threats. The effectiveness of any antivirus software is dependent on how frequently it is updated.

4. Adopt Cloud Computing Services

If your employees are still storing company files locally, it's time to switch to the cloud. The cloud not only offers a centralized storage system where your employees can share and get access to company data, but it also offers an additional layer of security for your data. Various technologies and tools in cloud-based solutions allow you to insert restrictions between access and your company data.

The cloud also provides a backup solution for your data. This means that when your company gets compromised, and locally stored files are destroyed or lost, you can still access the data you stored on the cloud.

5. Implement a Strong User Authentication Processes

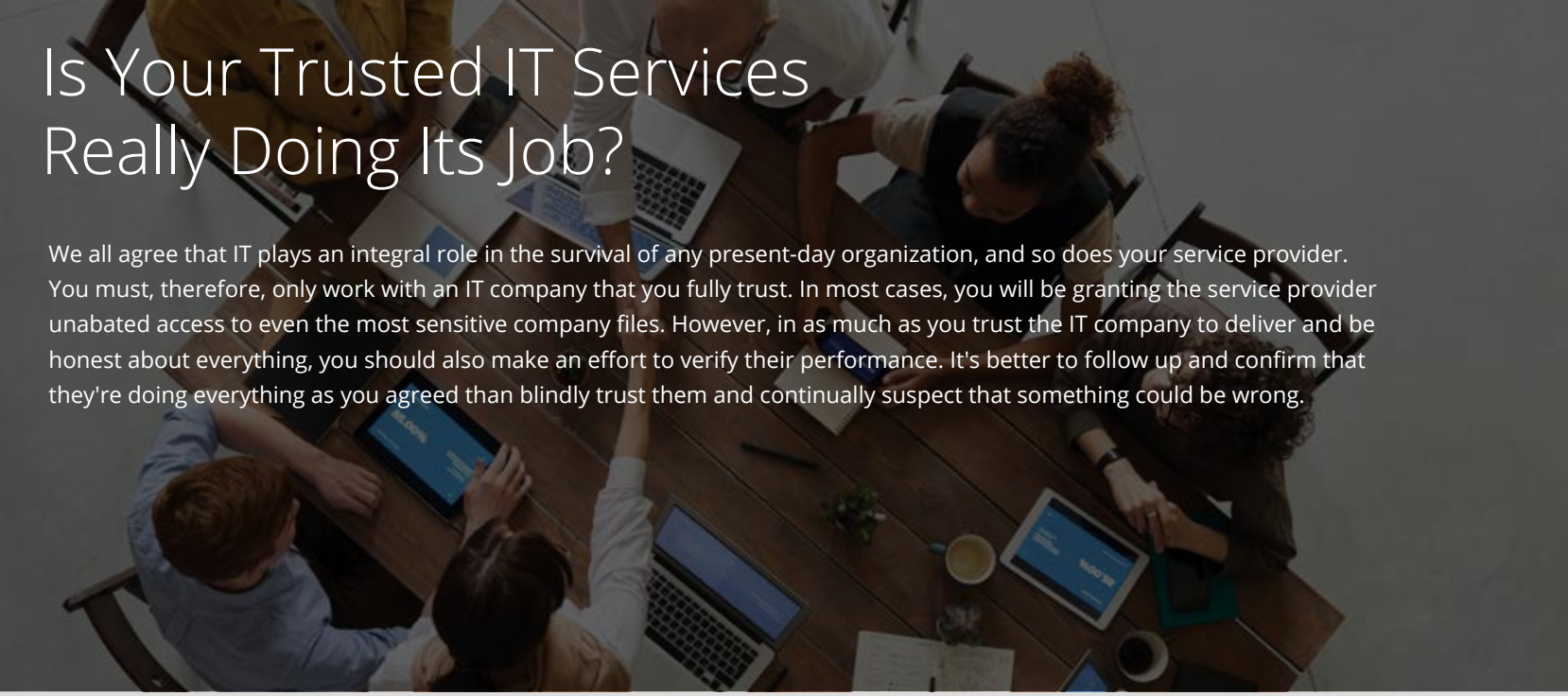
Poor user authentication processes are a source of various cybersecurity vulnerabilities. Ensure both you and your employees use complex passwords for all your devices, including your Wi-Fi routers. All passwords should include letters, numbers, symbols, and special characters.

You can also implement multi-factor authentication to add a security layer to the login process and lock out external parties from accessing your data and networks.

6. Keep Your Operating System and All Your Software Updated

Malware attacks often penetrate software loopholes in browsers and operating systems. It's, therefore, crucial to ensure that your operating system and all your software are up to date. Updates often include critical patches to security loopholes that were present in previous versions of the application.

Is Your Trusted IT Services Really Doing Its Job?



We all agree that IT plays an integral role in the survival of any present-day organization, and so does your service provider. You must, therefore, only work with an IT company that you fully trust. In most cases, you will be granting the service provider unabated access to even the most sensitive company files. However, in as much as you trust the IT company to deliver and be honest about everything, you should also make an effort to verify their performance. It's better to follow up and confirm that they're doing everything as you agreed than blindly trust them and continually suspect that something could be wrong.

What Should Your IT Service Provider Provide Your Company?

1. Proactive Management

Proactive management involves monitoring your systems for outages, taking time to learn your environment, deploying and maintaining the necessary tools, and regularly consulting with you to align their programs with your business goals. With this approach, the IT company will minimize unnecessary downtime and increase your overall productivity.

2. Cybersecurity

According to Purplesec, cyberattacks have increased by over 600% since the pandemic began.

Does the service provider have an elaborate data security plan that fits your needs and budget? Do they help you with industry compliance issues? Which security protocols do they have in place, and how often do they revise them? And most importantly, how often do they train their staff to keep them abreast with emerging threat patterns?

3. Proper Backup And Recovery

As we said, even with the best cybersecurity measures in place, there's always the threat of losing or misplacing your data. That's why data backup is very crucial. Does the service provider maintain in-the-cloud and offline duplicates of your files and credentials? If so, how often and is there any proof? In case of an incident, how easy will it be to retrieve these backups? The IT company should back up your files in easy-to-retrieve formats at least twice a day.

4. Data Storage and Management

Data is arguably one of the most valuable assets in any organization, regardless of the industry or scope. You rely on data to formulate policies, make decisions, and plan your growth. Without proper data management, storage, and backup, your operations are as good as stalled. Depending on your SLA's, you expect the IT company to set up and maintain the servers and databases that host your data. It should also design and implement strategies and techniques to ensure that these servers function seamlessly for fast and efficient access to the data they hold. By handling data storage and management, the service provider frees your staff to concentrate on more business-centric tasks.

5. IT Consulting and Help Desk Support

The service provider should be readily available for consultations just as they were when they were wooing you to engage their services. How long do they take to respond to your help desk support requests? And if they do, how long does it take them to resolve your issues. You can know how good an IT company is by the quality of help desk support they give. A service provider that takes too long to respond to your issues is probably overwhelmed or lacks the requisite skills.

At Leading IT, we personally make efforts to inform you about the measures we're deploying, your cybersecurity posture, and areas that need adjustments. For instance, we send our clients weekly reports about their systems and what we've done, e.g., proof of backup or are planning to do. Even then, you should still follow up and verify.

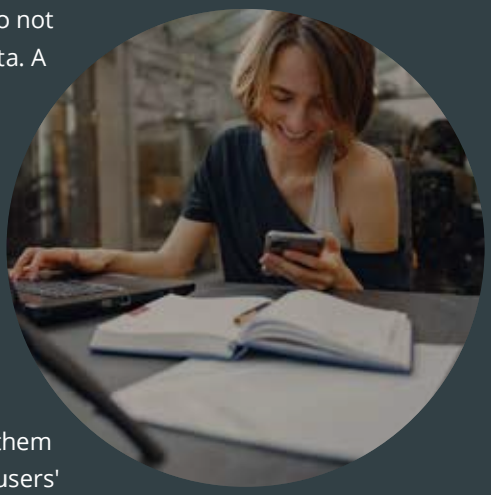
> “...cyberattacks have increased by over 600% since the pandemic began.”

Don’t Use Public Wifi, Here’s Why

Who doesn't love restaurants or hotel rooms with free Wifi? We all understand how intense the lure of surfing the internet and checking your social media networks for FREE can be. However, before you connect to that public hotspot, you should understand the dangers that come with it.

1. Most Free Wifi Hotspots Are Not Encrypted

When you use a private office or phone Wifi network, every data you generate or transmit between the connected gadgets and the router is automatically encrypted. So, anybody who's within the Wifi's range cannot snoop and view your browsing history. That's not the case with open public hotspots—most of them do not encrypt user traffic and data. A cyberattacker within the hotspot's range can easily see your browsing activity and even view what you post on social forums.



2. Rogue Hotspots

There's an emerging trend of cyber actors creating rogue hotspots and using them to peer into unsuspecting users' credentials. Sometimes, the hackers use names of popular hotspots such as local restaurants or public parks. As soon as you connect to the internet through these illegitimate hotspots, the cyber actors monitor and intercept your traffic and may even introduce malicious software into the gadgets you're using.

3. Man-in-the-Middle Attacks

Cyber attackers position themselves between your gadget and the Wifi router. They "eavesdrop" on your traffic, communication patterns, and sensitive credentials, which they can mine to sell or use to launch attacks on the connected gadget.

How To Stay Safe When Using Public Wifi

1. Encrypt your traffic with a VPN connection
2. Don't use public Wifi to access sensitive information
3. Stick to "HTTPS"
4. Turn off "Connect Automatically”

Our advice remains that your phone's hotspot should be your first option; it's safer than free Wifi. If you must connect to a public hotspot, ensure that it is legitimate first, then implement the above safety protocols.

Your phone's 4G network is encrypted, and so is the data you send through it. You can also set personalized solid access codes to keep off snoopers. Unless you share the hotspot's password with others, there are minimal chances that it will land in the wrong hands.

Are You Looking for New Internet Service and Phone System Providers?

LeadingIT can help! We work with providers that we trust and would be happy to help your business find the best fit. We can save you the hassle of paying for speeds that cannot be utilized, avoid common vendor issues, and ensure your current system is compatible.

Contact us today and let our knowledgeable staff take the task off your hands!

WE ARE CELEBRATING!

Anniversaries

Dave Gregory- July 22, 2013

Birthdays

Andy Latos - July 19th

Peter Apostle- July 23rd

Read Our Blog For More
https://www.goleadingit.com/blog