October 2021

TechTidbit.com

brought to you by Tech Experts

Is A VoIP Phone System Good For A Small Business?

Thomas Fox is president of Tech Experts, southeast Michigan's leading small business computer support company.

Is VoIP worth it for a small business? The short answer is 100% Yes! In fact, VoIP makes the perfect communication solution for all-sized businesses, big or small. Let's look at the reasons why VoIP phone systems make sense for your business:

Pay less, save more!

You will be able to reduce your communication expenses by handling all your communication needs for offices, mobile and data services with one single provider. This not only saves you money, but also saves your precious time!

No management or maintenance needed

For a hosted VoIP service, your provider will manage and maintain the network, hardware and all for you. Let the experts do the job for you so you can focus on your core business!

Increase business efficiency

By taking advantage of the VoIP features such as automated attendant/customer service, voicemail to email, remote or virtual extensions and more, you will be able to increase your work efficiency and productivity.

Here are some more basic features of a VoIP phone system:

Direct inward dialing (DID): Employees can have a phone number that rings directly to them.

Caller ID routing: Calls can be routed to specific employees or departments based on the person calling.

Conference calling: Set up conference calls quickly and easily. Most VoIP systems include web conferencing, too.

Call monitoring and reccording: Calls can be monitored by supervisory staff or recorded for customer service or compliance purposes.

Call queues: If your company receives a lot of calls, you can use call queuing to "stack" callers until an employee is available. Some systems allow call-backs, so your customers aren't waiting on hold.

Analytics and monitoring tools: Nearly all VoIP platforms include robust reporting features to give you a handle on call volume, your busiest time of day, and when callers are waiting too long on hold.

Scale up or down easily

A VoIP phone system grows with your business! Whether you are dealing with a seasonal demand spike or adding a new branch office, a VoIP system can get you up and running quickly without having to invest in additional lines or hardware.

What are the disadvantages of VoIP?

The key to a successful VoIP deployment is to have a stable internet connection! Since VoIP relies 100% on your network bandwidth, if you don't have sufficient bandwidth, your VoIP service won't be good either.

Depending on the number of concurrent calls your business requires, you may need to increase the bandwidth for a better communication experience.

Is VoIP reliable?

As long as you have sufficient network bandwidth, an up-to-date network router, and a backup Ethernet cable, your VoIP service can be just as reliable as your traditional landline!

Give us a call at (734) 457-5000 if you'd like more information about how a VoIP phone system can reduce costs and improve business efficiency.

As long as you have sufficient network bandwidth, an up-to-date network router, and a backup Ethernet cable, your VoIP service can be just as reliable as your traditional landline!

Work-From-Home Precautions For Your Network

"This means you may need to provide anti-virus to your users. Yes, it's an expense, but it's much cheaper than recovering from a ransomware attack because an employee's 12-year-old downloaded a Fortnite 'hack' to get more V-Bucks."

Mark Funchion is a network technician at Tech Experts.

As our world has shifted to a heavy work-from-home environment, it is important that you do what you can to make sure your business's network is secure, whether your employees are working from home or in the office.

Working from home can pose many challenges. The first involves the device the employee uses. If they have a company-issued laptop and you implemented a VPN, then great, you're fairly secure.

What do you do if they are using their own home PC? Do they have anti-virus? Are they accessing documents through a common cloud storage location, such as OneDrive or Dropbox?

If so, that can cause issues because that home PC may have other users who are not careful about what they download or what emails they open. If that PC is infected and your employee connects to shared storage, your business may become infected.

For these reasons, you should really consider only allowing access to your data over a VPN that your employees must log into. Do not share files through cloud storage unless you are sure the devices connecting are secure.

This means you may need to provide anti-virus to your users. Yes, it's an expense, but it's much cheaper than recovering from a ransomware attack because an employee's 12-year-old downloaded a Fortnite "hack" to get more V-Bucks.

Next, push the use of two-factor authentication (2FA) and password managers. Having a simple password like "CompanyVPN1!" won't cut it.

Force your users to use strong and varied passwords. Now, those can be difficult to remember, so it may be a good investment to look into a corporate password manager. This will securely store passwords and make it easier for employees to use stronger credentials.

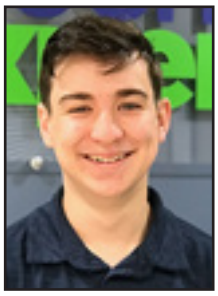
In addition to better passwords, use 2FA. This security measure sends a verification code to your employee via email or text when they log into secure apps or websites. It's another extra step, but again, the more precautions you take, the better off your security will be. Just because your employee logged in from home with a strong password doesn't mean it's actually your employee. That second authentication makes it much more difficult for the end user's information to be gained by cybercriminals.

Educate your employees about using public Wi-Fi as well. It's nice to sit in a comfy chair at Panera and enjoy a bagel and coffee while responding to emails, but who else is on that network? If they must do this, then using a VPN and 2FA are a must.

These are a lot of scary things, but don't lose sleep. Be diligent in securing your network. If you allow work-from-home, be prepared to invest in setting up VPNs, 2FA, password managers, and anti-virus software for your employees. This time and due diligence will greatly help you prevent your data and network from becoming compromised.

Also, remember you are not in this alone: Tech Experts is here to help. If you want to secure your network for remote work, reach out to us at (734) 457-5000. We secured our own network so we can work remotely and have the expertise to help you do the same.

Modern Utilization Of Tech In Schools & Workplaces



Wyatt Funchion is a tech support intern at Tech Experts.

Everywhere you look now, there is some type of technology in use and nearly every industry takes advantage of it. Between food delivery apps, the capability to review your accounts online, or the self-scan check-out lanes at the grocery store, we use technology every day and it's all part of our common experience.

While we may overlook a lot of it in our daily lives, the right tech can make your professional life much easier and efficient. Convenience is one of the main reasons we innovate, right?

One way you can bring helpful tech into the work setting is by using a company-wide chat. You can have a group messaging system like Discord or Slack, but even a group chat over text messages can be a helpful addition in the right workplace.

A company-wide chat allows you to have conversations as needed and communicate with minimal interruptions. Questions, updates, and requests can be reviewed, then responded to a timely matter or addressed right away. It creates a "paper trail" as well, so past messages can be referenced easily.

With chat, you are able to touch base with your peers, employees, or bosses anywhere and anytime. Instead of having ten people trying to reach the same person all at once, they can send them a message and have a reply almost instantly. Unlike email, chat is less likely to be buried in conversation chains, coupons, and other mail.

Another good way to use modern technology is by utilizing remote access. Being able to work remotely is a huge time-saver and a great help for online collaboration, in both schools and the workplace. It allows us to work from anywhere with an Internet connection.

Remote learning is also a very good use of new technology because it allows students to work from home and have all of the same access to resources as if they were sitting in the classroom in front of a teacher. For working professionals, it's the same – they can complete their work from anywhere as if they were sitting at their desk in the office.

Another great way that technology has influenced the workplace for the better is automation in repetitive tasks. Some examples are network monitoring, notifications, emails, file-sharing, and time management.

Automation allows employees to focus on critical tasks instead of repetitive, time-consuming ones that aren't necessarily as important. It also prevents some things from falling through the cracks by sending reminders or by entirely handling a task without human intervention.

Automation can also take on many forms, and you may already be benefiting from it. One example of automation that we use at Tech Experts is that our incoming service tickets, sent via email, are automatically disseminated to the right team. If this was not set-up, someone would have to manually sort every ticket that came in. The programs and apps that you already use in your business may have options to make your life easier through automation, such as email rules in Outlook.

Current technology has come a long way. Copiers, calculators, and faxes used to be amazing, and now, some of us can work entirely off of the phone in our pocket. Sometimes, it may seem overwhelming, but even small tweaks – like email rules – can have a big impact. Embracing the efficiency of tech can give you freedom and time back so you can make the most of your work hours.

"One way you can bring helpful tech into the work setting is by using a company-wide chat. You can have a group messaging system like Discord or Slack, but even a group chat over text messages can be a helpful addition in the right workplace."

Using Public Wi-Fi? Consider A VPN

With more of us working remotely now, coffee shops are getting busier again as we look for somewhere other than home to work. But while it can be great for getting rid of distractions, it's not so good for security.

That's because public Wi-Fi is a hotspot for data theft. Any data sent over public Wi-Fi that doesn't need a password to access is vulnerable to theft or manipulation from someone else using that network.

And it's not just other Wi-Fi traffic you need to consider. There are also fake networks to be wary of. You think you're connecting to the coffee shop's Wi-Fi… but how do you know it isn't a fake version with the same name?

As soon as you log on, they can suck up all of your credentials and any other personal data on your device.

If your team is using public Wi-Fi regularly, best practice is to use a VPN (Virtual Private Network) to keep your data safe. This acts as a private tunnel for your device to connect to a private network, keeping your info safe.

Contact Information

24 Hour Computer Emergency Hotline
(734) 240-0200

General Support
(734) 457-5000
(888) 457-5001
support@MyTechExperts.com

Sales Inquiries
(734) 457-5000
(888) 457-5001
sales@MyTechExperts.com

Take advantage of our client portal!
Log on at:
www.TechSupportRequest.com

TECH EXPERTS

15347 South Dixie Highway
Monroe, MI 48161
Tel (734) 457-5000
Fax (734) 457-4332
info@MyTechExperts.com

Three Steps To Improve Your Ransomware Resilience

This is a cold hard fact: Ransomware is on the rise.

What is ransomware?

It's where hackers break into your network, encrypt your data so you can't access it, and then charge you a large ransom fee to unlock it. It's the most disruptive and costly kind of attack you can imagine. And very hard to undo.

Why is it a big deal?

Ransomware attacks are dramatically up thanks to the pandemic. All the urgent changes that businesses went through last year created a perfect storm with plenty of new opportunities for cyber criminals.

Is my business really at risk?

Thanks to automated tools used by hackers, all businesses are being targeted all the time. In fact, hackers prefer to target small businesses as they typically invest less time and money into preventive security measures compared to large companies. It's estimated a business is infected with ransomware every 14 seconds.

How can my business get infected with ransomware?

42% of ransomware comes from phishing emails. This is where you get a legitimate-looking email asking you to take a specific action. You only need to click a bad link once to let attackers quietly into your system. And it doesn't have to be you who clicks… it could be any member of your team.

Why is it so hard to undo?

A ransomware attack takes weeks for the hackers to set up. Once inside a network, they stay hidden and take their time to make lots of changes. Essentially, they're making it virtually impossible for an IT security company such as ours to undo the damage and kick them out once the attack has started. If you haven't thoroughly prepared for a ransomware attack before it happens, you are much more likely to have to pay the fee.

How much is the typical ransom?

The hackers aren't stupid. They know trying to get $150,000 out of a small business simply won't happen. But you might stump up $10,000 just to end the hell of a ransomware attack. They will change their ransom demand based on how much money they believe a business has.

Of course, the ransom isn't the only cost associated with an attack. There are countless indirect costs. Such as being unable to access your data or systems for a week or longer. How horrendous would it be if noone could do any work on their computer for a week? How would your customers react to that?

What can I do now to protect my business?

This is the most important question to ask. It's virtually impossible to stop a ransomware attack from happening. But you can do an enormous amount of preparation, so if an attack does happen, it's an inconvenience, not a catastrophe.

Here are the three steps we recommend for maximising your ransomware resilience.

Act as if there's no software protecting you

Software is essential to keep your business safe from all the cyber security threats. But there's a downside of using this software – it can make you and your team complacent.

Actually, humans are the first defense against cyber-attacks. For example, if your team doesn't click on a bad link in a phishing email in the first place, then you're not relying on software to detect an attack and try to stop it.

This means basic training for everyone in the business, and then keeping them up-to-date with the latest threats.

Invest in the best data backup and recovery you can

Automatic off-site data backup is a business basic. When you have a working backup in place, it can be tempting not to give it a second thought.

But it's worth remembering that cyber criminals will take any means necessary to get you to pay their ransom. That means they'll target your backup files too. Including cloud-based data.

It's critical that you create and implement a comprehensive back-up and recovery approach to all of your business data. The National Institute of Standards and Technology sets out a cyber security framework which includes best practices such as:

• Constant backups: Separate from the computers and ideally in the cloud
• Immutable storage: This means once created, backups can't be changed
• Firewalls: To restrict what data gets in and out

Create a plan for cyber-attacks

When a cyber-attack happens, every second is crucial. The earlier you act, the less damage is caused.

So, prepare a detailed plan of action and make sure everyone knows what's in it, where to find it, and how to trigger it.

Test your plan regularly to make sure of its effectiveness and remove any risk of failure by keeping at least three copies of it in different places. One should be a printout kept at someone's home… just in case you have zero access to data storage.