

## The Top 5 Questions For Hiring A Superstar



The whole interviewing process can be a long and gruesome task for both parties involved. On the other hand, having to fire an employee once you've invested energy and money, is even worse.

To waste less time on interviewing, and then potentially firing, lets get the interview process down so we can move along quickly and efficiently.

Here are the top 5 questions you'll want to ask in your preliminary 5 minute phone interview:

1. Tell me about your current job.
  - Are they a complainer?
2. What do you know about our organization?
  - Did they do their research?
3. Is it better to be perfect and late, or good and on time?
  - See where their values lie.
4. Tell me about a time you set difficult goals, and how did you achieve them?
  - Can they handle the audacious goals you have in store?
5. What are your salary requirements?
  - Be clear about what is offered.

Once you find the right fit, you can focus on cultivating good employees and in turn, growing your business.



This monthly publication provided courtesy of CTTS, Inc.



## The #1 Mistake Companies Make With Their IT

If you're like many businesses today, there's a good chance you've made this one mistake with your IT security: you don't budget for it.

Or if you do budget for it, it's not enough to really protect your business.

Time and time again, business owners decide NOT to invest in IT services. Instead, they go it alone or skip it completely.

Or they might approach an IT services company and ask, "What do you charge for your services?" They don't ask, "What will I get for my money?" or "How can you meet the needs of my company?" This is a backward approach to IT – and it's a big mistake.

The fact is that a lot of business owners don't take IT seriously. They think that because they haven't been hit by a data breach or a malware

attack that it will never happen to them. That's another big mistake. Just because a business hasn't fallen victim to a cyber-attack DOES NOT mean they're safe, just the opposite.

When you hire an IT services company, what do you get for your money? The honest answer is that it depends on your specific needs. Many IT services companies offer everything from basic to advanced network security. You can expect services like:

- Cloud backup
- Data protection
- Data monitoring
- Threat detection
- Technology maintenance
- And more!

Everything is designed to protect you, your network, your technology, your employees and your business as a whole. It's all about giving you the information and resources you need

so you can worry less about outside threats and focus on your customers and the success of your business.

When you're invested in good IT security, you shouldn't even know it's there. It runs in the background like a quiet but powerful electric motor. It's there when you need it, and it's there when you're not even thinking about it.

For some business owners, this is a tough pill to swallow. They don't have something tangible in front of them that they can see 24/7. A lot of business owners like to be more hands-on. They like to see what their money is buying.

The great thing is that a good IT services company will provide you with something tangible. If you want to see what is going on behind the scenes of your IT security, they will give you a complete report. Every day (or week or month), you can have an e-mail delivered to your in-box that breaks down exactly what your IT services firm is doing for you.

**“We can't wait to react until something happens. Because when something does happen, it's often too late.”**

You can see things like the threats they blocked from getting through. You can see when they performed system maintenance or when your data was backed up. You can customize these reports to your needs. Basically, you can see what you're paying for and how it's working. This is the very definition of “peace of mind.”



Today, none of us can afford to skip out on good IT security. We can't wait to react until something happens. Because when something does happen, it's often too late. The cybercriminals have done their damage and moved on. Meanwhile, your business comes to a screeching halt, and you have to pay the big bucks to get everything back on track – if you can get back on track.

Some businesses don't get back on track. They are forced to close after a cyber-attack because they don't have the money or resources to recover. The damage is simply too much and the cost too high. If they had invested in IT security upfront, it might be a different story.

Don't get caught off guard by a data breach, malware infection, hacker attack or data loss due to technology failure or natural causes like flood or fire. It's time to take your IT to the next level. Protect your business the right way and avoid the mistake so many others make when they avoid investing in good IT.

Work with an IT services firm that takes your business as seriously as you do, like CTTs.

## Our Top 10 Technology Tips to Help Your Business Thrive



Stop getting behind and start utilizing smart and strategic IT systems to PROTECT your business from cybercriminals, viruses, hackers, downtime, disgruntled employees and other threats. Threats that can shut down your business or cause major interruptions that cost you big bucks, not to mention a lot of aggravation you don't have time to deal with.

For the past 3 years, our Team of engineers has been combining their expertise for your weekly Tech Tip Tuesday article. We've scoured through all 180 tech tips to bring your our top 10 most useful and easy to implement technology tips. We believe you'll find this eBook to be an invaluable tool as your business grows and faces new challenges. At CTTs, we're here to face IT together as Your Business Partner.

**Download your FREE copy today at : [www.CTTOnline.com/Top-10](http://www.CTTOnline.com/Top-10)**

Get More Free Tips, Tools and Services At Our Web Site: [www.CTTOnline.com](http://www.CTTOnline.com)  
(512) 388-5559

## Will Your Password Win or Fail?



Over 80% of cybersecurity incidents are caused by bad passwords. Bad passwords are bad for business!

To keep your data safe and secure, start by avoiding the top 3 password fails and implementing these top 3 password wins:

**FAIL #1: Recycling the same password for multiple accounts.** While we do encourage recycling, we highly discourage recycling your password!

**WIN #1: Add multi-factor authentication (MFA) for every user.** Weak user-made passwords are strengthened with a second identifier.

**FAIL #2: Being Too Familiar.** Don't use: loved ones' names (pets included), maiden names, hometowns, birthdays, wedding dates or anything else that can be gleaned with Online research.

**WIN #2: Stay Educated.** Constantly train and educate your Team about good cybersecurity habits. At CTTS, we offer regular, automated, security awareness training for all employees.

**FAIL #3: Storing Password on device or in a "cheat sheet."** If hackers gain access to this list, you've just handed the keys to your company over to cybercriminals. Use a password manager to securely keep tabs on all your credentials.

**WIN #3: Watch the Dark Web.** Sensitive personal or company data may be circulating even if you haven't had a breach. At CTTS, we can keep an eye out for your company on the Dark Web, to make sure you haven't already been compromised and to alert you if a breach does happen. Call now for a free demonstration: (512) 388-5559.

## The Rest Is My Job

How would you like to be in the position to create the largest army that the world has ever seen (over 13 million soldiers) and do it mainly with people who have NEVER commanded troops in their life?

That was exactly the position General George C. Marshall found himself in during World War II. Not only did he have to assemble this incredible army, but he also had to do it in the shortest amount of time possible. He appointed over 600 people to positions of general officer or division commander, with few "slackers."

So, what was his secret to being so successful in putting the right people in the right positions? Smart leaders hire people based on their strengths – what the person can do, not what they can't do.

For example, General Marshall's aides were worried about him putting a certain colonel, who was known for not getting along with his superiors and being terribly rude, in charge of training. They told Marshall, "If things go wrong and he has to testify in front of Congress, he will be a disaster for you and your reputation."

General Marshall asked his aides, "What is his assignment... what do we need him for?"

They responded, "To train troops – an entire division."

Marshall then asked, "Is he a first-rate trainer?"

His aides responded, "Yes sir, General. He is the best we have."

He said, "Well, give him the assignment. The rest is my job."



*Geoff Smart is chairman and founder of ghSMART. Geoff is co-author, with his colleague Randy Street, of the New York Times best-selling book Who: A Method For Hiring and the author of the #1 Wall Street Journal best seller Leadocracy: Hiring More Great Leaders (Like You) Into Government. Geoff co-created the Top grading brand of talent management. He is the founder of two 501(c)(3) not-for-profit organizations. SMARTKids Leadership Program™ provides 10 years of leadership tutoring, and the Leaders Initiative™ seeks to deploy society's greatest leaders into government. Geoff earned a B.A. in economics with honors from Northwestern University and a master's and doctorate in psychology from Claremont Graduate University.*



**THE REST IS MY JOB.** What a great statement. Sometimes a good leader will have to protect, and even defend, some of their subordinates who may have some rough edges when it comes to diplomatically communicating with other bosses or departments. These leaders know they have a high achiever, a real winner when it comes to getting the job done, and they will do everything they can to protect their assets.

Who would you rather have in a position: 1) the most polite communicator who ruffles no feathers; challenges no person, policy or procedure and has an average performance rating, or 2) a highly focused, determined, loyal, "tells it like it is – good or bad" leader who occasionally upsets those who hindered their progress and is known for always getting the job done? Give me #2 any day – the rest is my job to keep the peace.

Leadership is not about authority. If you are taking the position because it gives you power, supremacy, or authority over people, please do not apply. It is a servant position. You are there to help others succeed. It isn't about you; it's about them. Hire others for their strengths and let them at it.

Learn about the man who created the largest army in the history of the world and who understood we are graded on the results... The rest was his job.

## The ‘Not Me!’ Problem ...

Remembering 24 different passwords, memorizing four PIN numbers, and installing updates all the time is frustrating enough. Many of us also have to remember the code for the door, the alarm code for the alarm panel next to the door, the secret password to tell the alarm company, the passcode to your phone, the garage code ...

You get the idea.

This logic is based on a time when threats were more “real,” like the idea of someone robbing our house. In 2020, these types of threats are statistically less likely to happen than virtual threats like fraudulent credit card charges, data loss, and identity theft. In fact, cyberattacks occur three times as often as home burglaries in the United States, according to a 2016 study by the University of Kentucky.

It’s important to avoid the “Not me!” approach to this shift.

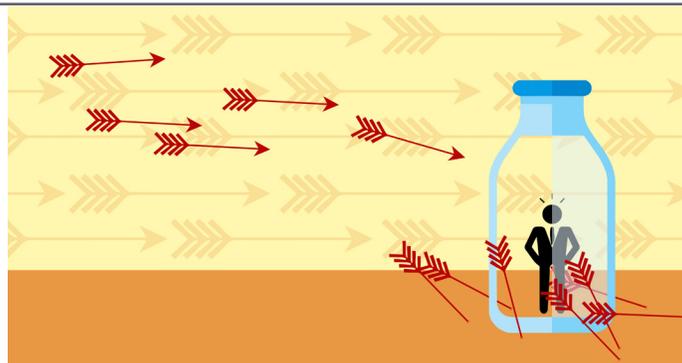
Businesses say this all the time: “I’m too small for anyone to want to steal my data. I have a good firewall,

hourly backups, and a great IT support partner – no one will steal my files.”

But the truth is that businesses with under 100 employees are low-hanging fruit for cybercriminals – yes, that’s a lot of you! It can happen to you, so you must approach all aspects of physical and electronic security with the attention they deserve in today’s business world.

## Do You Have The Right Business Insurance To Protect Your Company?

There are several types of business insurance on the market. Each one serves a different purpose, and getting the right insurance can save you the major headache that comes with not having insurance or having the wrong type of coverage. While we can’t list them all here (there are too many!), here are a few examples:



**Commercial Property Insurance** – This is one of the most important forms of insurance. It protects equipment in the business against damage or loss.

**General Liability Insurance** – This is another important one. It helps cover injury and legal expenses should someone get hurt on your business’s premises.

**Cyber-Insurance** – This offers protection should you fall victim to malware, cyberattacks and other digital threats. Basically, if your business is connected to the Internet, you need extra protection.

**Umbrella Insurance** – This is another layer of protection on top of existing insurance. Exact details vary by plan, but it can often protect you if you need to pay legal fees or costs related to building or equipment damage.

*Small Business Trends 2020*

Central Texas Technology Solutions  
Your Business Partner  
www.CTTSONline.com (512)388-5559

Tech Tip #183  
**Protect Your Data From the Dark Web**

### Tech Tip of the Month:

#### Protect Your Data From the Dark Web

There is a lucrative market on the dark web for more than just personal information and credentials. Here are 3 simple steps to better protecting your identity, your employee’s identities, and your customer’s private information from cybercriminals.



By Josh Wilmoth

Read it Here: <http://bit.ly/Tech-Tip-183>

Get More Free Tips, Tools and Services At Our Web Site: [www.CTTSONline.com](http://www.CTTSONline.com)  
(512) 388-5559