# The IT Insider

1

February 2019

## THE HIDDEN COSTS OF POOR IT SUPPORT

*In this industry, it's just as important to be wary of exceptionally cheap services as it is of exceptionally expensive ones. You pay for what you get, here, so be sure you know what you're getting.*

**Ask them "What will I get for my money?"**

### Look for these giant red flags when researching.

Unsurprisingly, one of the most common questions business owners ask us is "What do you charge for your services?". This question is always asked by someone who has never had to pay a professional for IT support - internal or external. They're also typically surprised by the answer. If they don't have a firm grasp on what their company needs in relation to IT support, it's hard to put a value on those needs. After all, when your technology works,  it's easy to believe it will continue working without issue. This isn't the case as systems require constant, behind the scenes monitoring and maintenance to ensure they stay up and running (and secure).

The better question is really "What will I get for my money?". The difference in cost is directly related to the quality of it. Businesses who are used to visiting the Geek Squad or Jim's Computer Repair for IT support may get their computer wiped of viruses at a low cost, but they are, frankly, unprepared to learn that these services are nothing but a bucket of water on a burning building: unsustainable and basically useless.

Reactive IT support (like what computer repair shops provide) is always going to be more unpredictable and nerve-wracking than proactive IT support. You can, and should, plan for disasters in your business instead of only reacting to them when they occur. IT support needs to be comprehensive and disaster preventing - not barely holding itself together.

Unfortunately, our industry is not well-moderated. Anyone can tell you that they provide outsourced IT services, and they can give you any level of service they see fit. In this industry, it's just as important to be wary of exceptionally cheap services as it is of exceptionally expensive ones. You pay for what you get, here, so be sure you know what you're getting.

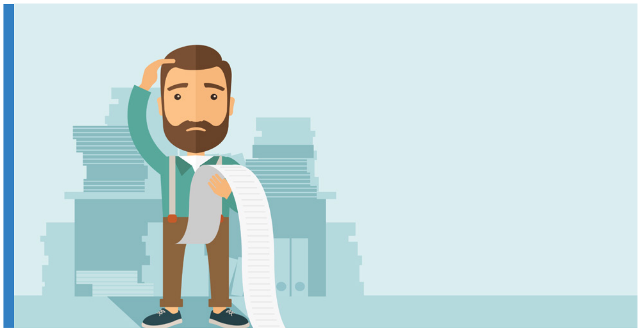
**Poor Customer Service**

One of the biggest complaints we hear from prospective clients about their IT support is poor customer service. They are unresponsive, never answer their phones, and don't follow up. The only way to be sure this isn't the case when researching your local IT support choices is to ask for testimonials and references.

**Nickel and Dime Hourly Work**

Pretty much every outsourced IT company has an hourly rate. This isn't inherently bad, but you should be sure

Clicking on a phishing link takes less than a second, and it can devastate any company - no matter its size.



They could be doing anything with this time, really - and it inherently provides the IT company a free-for-all with your cash. Instead, look for a managed service provider that uses the all-inclusive model. Pay one, unchanging monthly fee for any and all work done for your business.

**Band-Aid Solutions**

Patchwork solutions work great--until they don't and start costing you dozens of thousands. It's best to avoid the crises altogether, but cheap IT companies prefer to turn your network into an imitation of Frankenstein's monster instead of doing things the right way. It's easier and it's cheaper, but it's also dangerous and, frankly, stupid. With real IT experts looking over your technology needs, you won't have a mess of a network. You'll have finely tuned and fully functional systems that seldom need repairing.

**Natural and Human Disasters**

One thing you never want in your business is unpredictability. But, disasters happen and you need to be prepared to recover. While recovery for natural disasters like floods and fire comes with standard insurance, the same cannot be said for human disasters. Disgruntled employees, uneducated employees, or even straight-up hacking can all ruin the business you built. Viruses like Ransomware don't download themselves, after all. They must be facilitated by a human. Clicking on a phishing link takes less than a second, and it can devastate any company - no matter its size. This should be the most important topic of discussion when interviewing an IT support company. It's called Disaster Recovery, and if the IT company doesn't have a concise, understandable, easily implemented recovery plan? Run (don't walk) straight out of that meeting.

Today, business and technology are intertwined. You can't have one without the other, and those who cut corners on IT by hiring cheap and inexperienced professionals aren't protecting the most fundamental parts of their business. At the end of the day, it's cheaper to prevent than to replace. Even the smallest of IT problems can snowball into an expensive nightmare that threatens your company's very existence. So, next time you start looking for an outsourced IT company, ask the right questions and make a fully informed decision.

## Does Your Business Have a Disaster Recovery Plan?

What is your strategy for the aftermath of a terrible storm or aggressive ransomware attack? Likely, you have insurance on your building and your physical belongings like desks and computers and the coffee maker. But what about your data? What about the information stored on your server? Believe it or not, while the server itself may be covered by your insurance policy, everything it contains within its drives is not. For that, you need cyber insurance, which we do recommend, but even that won't help you recover lost data that you need to run your business. While a cyber insurance policy may provide a much-needed payout, it won't magically bring back all of those vital files, information, and software you need to run to your business every day.

For help crafting a disaster recovery plan within your business continuity plan, head over to preferreditgroup.com/thank-you-get-a-free-ebook/ and we'll give you our **Simplified Business Continuity Guide**.

# 9 Things Your Kid Can Teach You About Internet Security

**Don't give out personal information like a name, address, phone number, etc. on an online forum, discussion group, or social media site.** While you can use your name on social media sites like Facebook or LinkedIn, definitely use a pseudonym on other online forums where strangers abound. Never, ever put your phone number or home address here, though. It makes it much easier for people to use your PII (personally identifiable information) for identity theft.

**Never download a file from a site you don't trust.** You're inviting trouble this way. Viruses can be hidden in anything: cute desktop wallpapers, PDF cookbooks, and even those annoying Minion memes on Facebook.

**Don't allow a stranger to screen connect with you.** You'd be handing control over your computer to a random person, and potentially losing all of your data forever. Do not give a stranger over the phone or the Internet access to your computer for any reason.

**Don't use public wifi when banking**. Really, using public WiFi is never great, but we get it. But, don't use WiFi when banking or shopping. You could be broadcasting your checking account for the entire Starbucks to see.

**Keep your mobile device with you.** When you're outside of your home, keep your phone on your person. Don't lose it! If you're like most of the world, your phone knows your home address, your most used debit, and credit cards, and your bank account information.

**Don't open weird emails.** Go through your email with a finger on the delete button. Junk mail and spam are abundant in your inbox, and a lot of it could infect your computer. Never open an email unless you're expecting it.

**Save your files.** Computers are not always reliable, especially ones you've had for a while. Laptops over three years old start to deteriorate in speed and functionality. Therefore, save your work and your files often. Create backups, too. You never know when your old laptop will decide to kick the bucket.

**Email is not secure.** Really. Don't send anything private or sensitive through email. This mostly includes things like your credit card information or social security number. Honestly, you shouldn't even text this stuff. Phones are hackable, too.

**Don't use Internet Explorer.** It's outdated, it's slow, and it's much less secure. Unfortunately, some web applications only play nice with Internet Explorer  but avoid it whenever you can.

## PREFERRED IT SECURITY SPOTLIGHT

People never think it'll happen to them. Sure, they see the reports – 50 million-plus bundles of user data compromised by a Facebook breach; the billing information of more than 2 million T-Mobile users hacked by a mysterious malicious entity – but companies like those are massive, monolithic entities in American commerce. They're decidedly big fish, not like you and your small business. According to a recent JLT-Harvard Business Analytic Services survey, more than half of small business owners remain blissfully unaware of the threat cyber crime poses to the health of their organization.

We hate to burst the bubble of the happy majority, but the reality is that this optimistic attitude just does not square with the statistics. The incidents may not make the news, but small businesses are being targeted and breached by hackers at an astounding rate. In fact, the National Cyber Security Alliance reports that close to half of small businesses have experienced a cyberattack and that 60 percent of the companies that succumb to one of these attacks folds completely within 6 months. They state that instead of zeroing in on Fortune 500 corporations, hackers actually prefer to swoop in on the little guy, with 70 percent of cybercriminals specifically targeting small businesses.

Yet according to a Paychex survey, 68 percent of small business leaders aren't worried about cyber security despite data indicating that more than 7 out of 10 small businesses are woefully unprepared for a breach.

The first step to getting savvy in 2019 is to accept that cyber-attack isn't some unlikely crisis, but a virtual inevitability. It's a tough pill to swallow, but leaving it to chance is like flipping a coin where a "tails" outcome results in your business shuttering for good.

## Want To Know For Sure If Your Data Is Safe?

Thanks to our Done-For-You Disaster Recovery you can rest assured that your data is being backed up in a format that is not only secure, but also easily recovered when you need it.

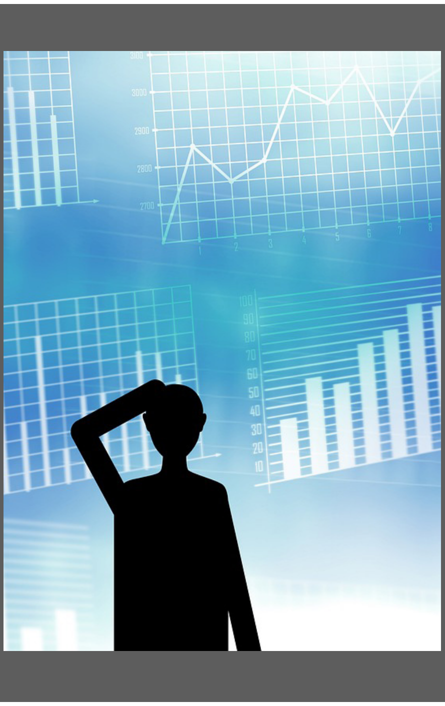
Your files are automatically backed up every hour locally and over the Internet.

Your data is safe from fire, floods, storms, viruses, hackers, hardware malfunctions, and human error! With image-based and file level backups, your data is immediately accessible even during a disaster.

Should a disaster occur, you can be back up and running the very same day…we **GUARANTEE** it.

Preferred IT Group will provide the hardware required, **absolutely free**.

Learn more at www.preferreditgroup.com/dfydr



## OUR COMMUNITY

The Fourth Annual Charity Event hosted by Preferred IT Group for the Children's Sanctuary is fast approaching and tickets are available now!

If you'd like to help local foster children have a fantastic year, join us for a round of golf and a poker game May 18-19! As always, our silent auction is held online and in-person at the event.

Tickets are available at preferreditgroup.com/charity.

We can't wait to see you there!

preferred IT group

## CONTACT US

| | |
|---|---|
| Fort Wayne | Warsaw |
| **260.440.7377** | **574.306.4288** |
| Columbia City | Indianapolis |
| **260.213.4266** | **317.426.8180** |

**www.preferreditgroup.com**

**6333 Constitution Drive
Fort Wayne, IN 46804**

**Subscribe to our blog and follow us on social media.**