

**This Issue:**

Managed IT Services for Your Remote Workforce

Working at the Office Has Its Benefits, Too

Laptop Battery Best Practices

Train Your Staff to Protect Your Business

Smartphone Addiction and Its Effects

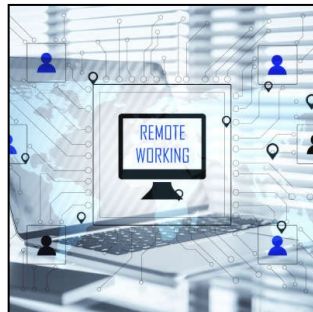
Working from Home Isn't Without Significant Cybersecurity Risks

Employee Spotlight - Kelly Hoyt



"Where liberty dwells, there is my country." -- Benjamin Franklin. **Happy Fourth of July!**

**Managed IT Services for Your Remote Workforce**



Whether your business is just starting to open up, or your staff is diligently working remotely, the effects of COVID-19 are going to be long lasting for most businesses. For those of us who were lucky enough to get our employees situated and productive without putting them at risk, we've started to see the value in having the infrastructure to allow for remote access.

**A Quick Recap for an Effective Remote Workforce**

In case you are still flying by the seat of your pants and managing to get by, there are some really important capabilities that your IT infrastructure needs to have to protect your users, your data, and your business in general.

*(Continued on page 2)*

**Laptop Battery Best Practices**



Nowadays, laptops are the weapon of choice for productivity. They function much like a desktop computer but are mobile enough to go anywhere with.

Unfortunately, most laptops chew through their batteries in only a few hours of work and need to be plugged in in order to function. With so many people working from home, many people are using their laptops more like a desktop and keeping them plugged in around the clock. For this week's tip, we'll discuss the best practices of a laptop battery...



Read the Rest Online!  
<https://dti.io/laptopbattery>

**Working at the Office Has Its Benefits, Too**



It's incredible how working from home has become the new normal. Just a short time ago most business owners wouldn't have batted an eye at shutting down the dreams of remote work, but because of the COVID-19 pandemic, they were forced to adjust the way they looked at the situation. Employees in several industries have been working from home ever since. Now that most places have begun to re-open, we thought we would remind you that there are actually some benefits to coming to the office.

**Back to Normal**

With much of the U.S. facing a phased reopening schedule, offices will be back in business. Many businesses will be recalling their employees, while many others will use the wait-and-see approach; especially if their workforce has proven to be productive during the pandemic. For business owners that plan on restoring their pre-pandemic employment strategies, they may be surprised to find that not all of their employees will have to be dragged back kicking and screaming. Many workers who have been working remotely love it, but many don't feel like they can be as productive as they need to be and find that by coming into the office they are able to focus on the task at hand a little better than they can from home.

Three benefits include:

**Collaboration**

Now, collaboration is more than working on a task or project with other people. It is

*(Continued on page 3)*



## Train Your Staff to Protect Your Business



In the course of doing business, sometimes the mundane and repetitive tasks, or the responsibilities that employees don't necessarily always consider to be part of their jobs, can be overlooked. Like any other business, yours needs people to be vigilant to ensure that it isn't the victim of a phishing attack. If your team isn't well-trained, or if it isn't engaged in the fight against cybercrime, you may find that your business is a sitting duck.

There's a pretty decent chance that your staff may not prioritize the security of your business' network. They are probably more focused on doing their job, after all. The easiest way to make them understand how important it is for them to know and follow the best practices of dealing with scams that come into their various work (and personal) inboxes is to make sure they get the applicable training. After all, 90 percent of all cyberattacks start from

someone mishandling a scammer's phishing message.

### Are Your Employees Prepared?

Have you made an effort to level with your people about their role in your organization's cybersecurity? Your efforts will definitely pay off if they work to protect your network. If you implement a comprehensive training program only to have your network breached, you're likely dealing with negligence and will have to respond accordingly.

The best way for your staff to understand how serious the issue is is to level with them. If they are negligent in their duties, there will be appropriate repercussions. You don't even have to mention what that means. They'll get it, and most of them will be more careful. In this case, the straightforward ultimatum is absolutely warranted.

### Here Are Some Best Practices

If you are going to put out the effort of developing a comprehensive cybersecurity procedure, and make the investment to ensure that your employees are on board, you will want them to

understand solid practices. Here are a few that you would find in any professional cybersecurity seminar.

- **Threats** - Making employees understand what threats that are actively working against them.
- **Password policies** - Passwords should be set individually and use NIST best practices.
- **Web practices and protection** - Educating employees about how their actions online make a difference.
- **Email practices and protection** - Phishing attacks are mostly found in email, so educating them about email best practices.
- **Preventative measures** - Educating your staff about all the things you do to protect company data, their PII, and the investment it takes to do so.

Once they are educated properly, they should be ready to help you secure your business. If you would like help developing a strategy to protect your network and educate your staff, reach out!



Share this Article!  
<https://dti.io/stafftraining>

## Managed IT Services for Your Remote Workforce

*(Continued from page 1)*

- Secure, encrypted access to your office network (via a VPN, or Virtual Private Network).
- Communication tools, such as Voice over IP, video conferencing, and instant messaging.
- Employees need devices at home that can reliably perform the tasks required of them.
- Security awareness is still a critical piece, even when working remotely.

### How Does IT Support Fit In?

If it works for them, most businesses decided to go remote. Even though some businesses were steadfastly against the whole work-from-home experience before the pandemic, we see that many feel fortunate due to the possibility of continuing operations while some other businesses weren't so

lucky. In order to accomplish this, most businesses had to significantly alter their operational strategies, and some, months into this thing, haven't successfully made it work for them yet.

In order to run a successful business of remote employees, you need to lean on your IT. Not only do you need to provide reliable and secure access to the resources you host internally, you also need to provide your remote workers with the software they need to do their jobs. Most businesses, instead of investing more capital into buying software licenses for home use will provide remote access to office computers, where they can utilize the software securely without any major expense.

These systems need to be sufficiently monitored and managed to avoid major

problems. It's true that the remote workforce is, by and large, using their own hardware and using some type of secure connection to get the resources they need. For those that don't have access to that type of hardware, they'll need to be outfitted with them.

If you rely on in-house IT support, you may not have the resources you need to sufficiently keep malware and other unwanted entities off of your business' computing network. At Directive, our professional technicians are well-versed in building and supporting the type of IT infrastructure that promotes remote workers and in-house workers, alike. How are we able to accomplish...



Read the Rest Online!  
<https://dti.io/managedremote>

## Working at the Office Has Its Benefits, Too

(Continued from page 1)

communicating the best way to get things done. When your team works remotely, they exclusively depend on collaboration software to get what needs to be done, done. While the collaboration tools help with efficiency and boost teamwork, some of the best collaboration is done by people having face-to-face conversations. Without the constant contact with colleagues, the intricacies that make your product or service special, won't be there.

### Work/Life Balance

Working at an office allows you to actually differentiate between work and home. This may not have been the biggest selling point three months ago, but today many people are getting stir crazy from working all day at their own PC and then trying to relax in the same

space. By working in the office, workers can separate their home life from their work life.



### Improved Engagement

It stands to reason that someone who goes into the office will be more engaged in the goings on there than someone that is working remotely. People will be more motivated to do their best if they are actively working alongside other people in a social setting. Whether it is the competition or the camaraderie, people that work in an

office are more apt to be motivated to achieve for your company.

### Other Considerations

For the workers, there is some debate on whether working remotely or in the office produces a better product or service, but there are some who suggest that, depending on the job, the office setting allows businesses to more succinctly track the productivity of their staff. If yours is like millions of other businesses that are working with small margins, getting the most out of your staff has to be a priority. Having them in one location can help you manage that...



Read the Rest Online!  
<https://dti.io/officebenefits>

## Smartphone Addiction and Its Effects



Nowadays, most of us use smartphones; and, yes, probably most of us use them more than is

healthy. There are those, however, that have come to depend on their mobile device so much that it completely dominates their lives. As people become even more attached to their phone, the impact this behavior has on their lives becomes more and more detrimental.

### The Skinny of It

"Everything in moderation" is a great piece of advice. If you drink too much water, your body's sodium levels become dangerously low and can make you sick. It can even put you in a coma. So then is drinking water good for you? Of course, but too much of a good thing is always going to have negative effects.

Smartphone use is the same. Sure, you can now handle multiple tasks in a short period of time via your smartphone. You

can keep conversations going with your friends, your family, your co-workers, and that special someone while walking down the street. You can play games, read a book, and scroll through social media to keep up on the world around you. You can work: write and send emails, update spreadsheets, use collaboration tools, and communicate through several methods. A wealth of knowledge is available in your pocket. Your smartphone can simultaneously be a home phone and a work phone.

Smartphone addiction is taking these benefits too far. It's finding more in the soft glow of a Retina or Super AMOLED display than the rest of us can see. It's ignoring the world around you to invest your time and energy into whatever is on the other side of the device. Young people tend to have the biggest problem. People between the ages of 15-to-24 check their phones an average of 150 times per day. In fact, 60 percent of surveyed college students said...



Read the Rest Online!  
<https://dti.io/phoneaddict>

## Cybersecurity Tips

### Tech Support Scams

Technical support companies can be critical in helping solve some complex issues with our digital devices. Unfortunately, scammers are using this dependence as a way to get their foot in the door and trick their victims into paying them money or installing a virus.

Learn some of the tactics scammers use in a tech support scam, and how to avoid becoming the next victim.

<https://dti.io/lc>

### Get our Cybersecurity Tips to your inbox weekly!

Each week we send an email with **FREE** cybersecurity tips to help you to avoid a data breach. These tips can be used to educate yourself and your employees on security best practices.

Sign up today!  
<https://dti.io/gettips>

## Working from Home Isn't Without Significant Cybersecurity Risks



The COVID-19 pandemic has greatly disrupted daily life, restricting people to their homes and preventing them from going into the office to work. In response, many companies are hurriedly changing over to a remote-capable workforce and having their employees work from home. This strategy can be highly effective, but if a company and its team isn't careful, it can also be risky.

### Why This Matters Now

Many businesses have had no choice but to shut down as "non-essential" businesses are closed. While the

definition of an "essential" business varies from place to place, the Department of Homeland Security and the Cybersecurity and Infrastructure Security Agency have provided some general guidelines describing what kind of services should be seen as essential.

This list includes many businesses who could conceivably operate on a remote basis, if they had the internal capabilities. Unfortunately, this often isn't the most secure option. Let's review why working from home can be less secure than working in the office, and what you can do to help minimize these effects.

### Security Threats for Remote Workers

As you would expect, there are a lot of factors that can serve as a detriment to remote work's inherent security. This is exacerbated by the fact that there is currently a global health disaster that cybercriminals can use to their advantage:

- The security implemented into the business' network is no longer protecting the employees and their devices.
- Employees may have more lax security habits when not in the workplace...



Read the Rest Online!  
<https://dti.io/remoterisks>

We partner with many types of businesses in the area, and strive to eliminate IT issues before they cause expensive downtime, so you can continue to drive your business forward. Our dedicated staff loves seeing our clients succeed. Your success is our success, and as you grow, we grow.

## Employee Spotlight - Kelly Hoyt



Every so often, we like to celebrate some of the people that we are fortunate to have as part of our team, putting one of them in the spotlight so you get to know them a little better. This month, we're highlighting Kelly Hoyt, a member of our outbound marketing department.

Raised outside Morris, NY, Kelly spent 16 years working

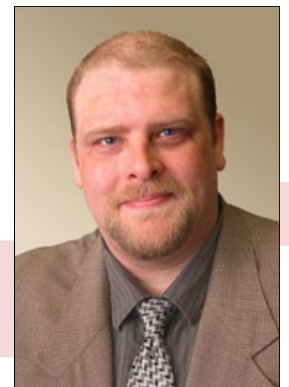
as a licensed practical nurse after graduating from trade school. After running into a friend from her high school days, Kelly joined our team (much to our delight).

When she isn't in the office building newsletters, writing social media posts, or completing the assorted other tasks she is responsible for, Kelly can often be found caring for her assorted animals. Her menagerie includes a dog, six cats, a rooster, and 19 chickens. An animal lover to

the core, she still finds the fact that Directive is a pet-friendly business cool.

In her spare time, Kelly enjoys attending concerts and music festivals, as well as kayaking and fishing. Someday, she hopes to travel, visiting all the places on her list of destinations. In the meantime, we are so happy to have her here with us as a part of our team!

Thank you so much, Kelly, for all that you do!



Chris Chase  
Solutions Integrator



Charlotte Chase  
Solutions Integrator

## Directive

330 Pony Farm Road  
 Suite #3  
 Oneonta, NY 13820  
 Toll-Free 888-546-4384  
 Voice: 607-433-2200

Visit us online at:  
[newsletter.directive.com](https://newsletter.directive.com)



[newsletter@directive.com](mailto:newsletter@directive.com)



[facebook.directive.com](https://facebook.directive.com)



[linkedin.directive.com](https://linkedin.directive.com)



[twitter.directive.com](https://twitter.directive.com)



[blog.directive.com](https://blog.directive.com)



[instagram.directive.com](https://instagram.directive.com)

