

# IT<sup>2</sup> TECHNOLOGY TIMES

*"Insider Tips To Make Your Business Run Faster, Easier And More Profitably"*

## Spring Cleaning

Under quarantine, many people are using the extra time at home for spring cleaning. Reminder that computers need periodic cleaning too! Use a can of compressed air to blow out the dust from the case and a soft cleansing wipe & q-tips to clean off keyboards and mouse.

If you are getting rid of old PC's it is very important when decommissioning to: # 1. Capture any software licensing that you are going to reuse and # 2. Either pull the hard drive for storage/archive or wipe and destroy the hard drive before disposing machine at your local county e-recycling center.



## 3 Ways To Stop Cybercriminals Cold In Today's Crazy Times



### Spring 2020

**IT Squared Resource, Inc.**  
1201 Commerce Center Dr.  
Franklin, OH 45005



**IT Squared Resource, Inc.**  
Delivering Exceptional Results

**Your IT & Telecom Resource  
since 1999.**

**Our Philosophy:** TO ADD VALUE TO ALL THOSE WE SERVE. To our clients as a trusted advisor and resource delivering exceptional results. To our employees, through continuous growth, opportunity and flexibility. To our partners and community as active contributors and involved supporters.

You've seen it. You've probably even experienced it. For what feels like forever now, just about everyone has been forced to modify priorities. As a business owner, you've probably been focused on shifting your business to accommodate this world crisis. You may even be investing more of your time in retaining customers and generating new cash flow. If you're like most people out there, you've barely even had time to think about cyber security and protecting your important data.

Maybe you've heard the saying "Never let a crisis go to waste." It's as if cybercriminals wrote it because that's exactly what they're thinking right now. In fact, they're probably working overtime right now to craft new malware while our lives have been turned upside down. Yes, as

you're focused on your business, hackers are finding new ways into your IT network. Their objective is to steal data and passwords, compromise your clients' private information and even demand large ransoms.

Did you know that cybercrime is expected to cost \$6 trillion (that's a 6 followed by 12 zeroes!) by the year 2021? But, now is when hackers are expected to do their absolute most damage.

Here are three strategies you can use right now to help protect your business data, money and productivity during these unusual times.

**1. Guard Your Inbox.** People aren't paying as much attention as they usually do, which makes it the perfect

*Continued on pg.2*

*Continued from pg.1*

time for cyber-attackers to send e-mails with dangerous malware, worms and viruses. Always carefully inspect every e-mail received and make sure you know the sender.

Here's another tip: avoid clicking links in the e-mail unless it's abundantly clear where they go. Also, don't ever download an attachment unless you know who sent it and what it is. While it takes a few extra seconds, double check by calling the person who sent you the attachment. Better safe than sorry. Make sure you communicate these safeguards to everyone on your team, especially if they are working from home.

**2. Secure Your Company-Based Technologies.** During crises like this one, your passwords are a critical first line of defense. Don't wait for your company's finance data to be compromised. Make a point now to reevaluate your passwords and direct your team to create stronger passwords. Too many employees are guilty of using the same password across multiple applications. Use a unique password for every single application.

Your team may tend to save your passwords in their web browser. Don't do this. A skilled hacker can bypass the PIN required to access your saved passwords. Once they have the password or PIN to access your web browser, they can steal as much as they want – credit

**“Did you know that cybercrime is expected to cost \$6 trillion (that's a 6 followed by 12 zeroes!) by the year 2021?”**

card information, customers' private data and more!

We recommend our clients use a password manager. It's convenient, but more importantly, it's far more secure.

**3. Secure Your Home-Based Technologies.** With the coronavirus pandemic, far more businesses are encouraging their employees to work from home. That means a lot of people are working from the living room or kitchen without giving a second thought to security. This negligence is an invitation to new cybercrimes.

Here are a few tips to ensure your work-from-home employees are keeping your network and data secure: make sure your employees and contractors are not using their home computers or devices when they are working from home. Add a firewall to ALL computers and devices that will be utilized at home. Finally, your network and data are not truly secure unless your employees utilize a VPN (virtual private network).

There's no need to invite in more problems by letting your computer and network security slide during these times. We would be happy to help you create or even improve your work-from-home environment.

While this coronavirus scare has negatively affected countless businesses, we are proud to say we are open and continuously servicing our customers. If you need additional security advice or would like to have a consultation to discuss how to keep your data safe or how we can help you work more effectively, simply connect with us today.

## Free Report: The 7 Most Critical IT Security Protections Every Business Must Have In Place Now To Protect Themselves From CyberCrime, Data Breaches and Hacker Attacks



Cybercrime is at an all-time high, and hackers are setting their sights on small and medium businesses who are “low hanging fruit.” Don't be their next victim! This report will get you started in protecting everything you've worked so hard to build.

**Download your FREE copy today and be subscribed to our weekly IT Security Tips e-mail [www.it2resource.com/cybersecuritytips](http://www.it2resource.com/cybersecuritytips)**





## Should You Invest In A VPN?

Virtual private networks (VPNs) are safe and useful tools for connecting to the Internet. They offer protection against potential intruders on whatever network you may be connected to. But when do you really need a VPN?

There is one clear answer: whenever you need to connect to a public WiFi network. You should never connect to an unsecured public WiFi network. It puts your device and your personal data at serious risk. Even using a secured public WiFi network—like those often found at hotels—can be risky. You don't know who might be snooping on the network.

Don't take that chance. If, for whatever reason, you need to connect to a public network, do so through a VPN. A VPN gives you encrypted protection between your device and the Internet. Prying eyes can't see what you're doing, and no one else can access your device. If you don't already use one, consider investing in one today!



# How To Deal With Increasing Customer Expectations

The more you do for customers, the more they expect. That is the nature of customer service.

Excellent service providers scramble to meet the expectations of customers who have become accustomed to great service. Aggressive competitors continue to bump up their offerings in an attempt to take your customers from you. This has resulted in a perpetual desire by customers for more, better, different and/or improved.

In most cases, "good enough" isn't enough.

The great art and science of business is to improve product and/or service offerings without giving up margins or increasing prices beyond what customers are willing to pay. It really is about adding value without spending too much to do it.

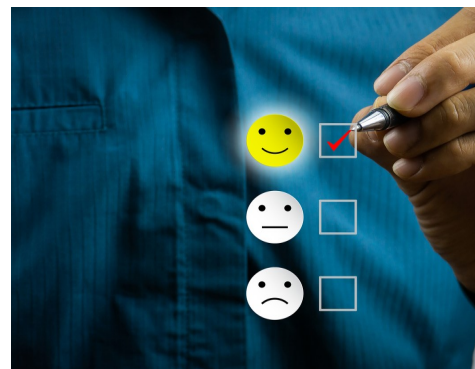
Any business that can't do this will be relegated to competing at the low end of the market on price alone, and that is a difficult place to be.

Rally your team, from engineering and manufacturing to sales and support, to regularly brainstorm how you can profitably grow your value proposition. Customers will increasingly demand it.

Here are eight things you can do about them.

**1.** Find out what is important to customers: what they require and what they desire. You're not clairvoyant, so routinely ask customers for input.

**2.** Explain your value proposition when you must say no. If you can't do something the customer wants, explain why. But see if there is something acceptable you can do instead.



**3.** Educate customers about the value you create for them. If they don't know about it or appreciate it, it isn't valuable.

**4.** Hold quarterly sessions with your team to brainstorm how to add value to the customer experience.

**5.** Evaluate the entire customer experience. Look for failure points and irritations that can be eliminated and improvements that can be made.

**6.** Pay more attention to your customers than to your competition. Know what your competitor is doing, but put your customer at the center of your focus.

**7.** Pleasantly surprise customers whenever you can. Work with your team to brainstorm ideas on how to do that.

**8.** Treat better customers better. Treat all customers well, but those who spend more should get preferential treatment.

Business goes to the bold and innovative. Creativity and imagination are the best tools for continually rethinking your value proposition. Good execution delivers and makes customers glad they keep coming back to you for more.



Mark Sanborn, CSP, CPAE, is the president of Sanborn & Associates, Inc., an "idea studio" that seeks to motivate and develop leaders in and outside of business. He's the best-selling author of books like *Fred Factor* and *The Potential Principle* and a noted expert on leadership, team building, customer service and company change. He holds the Certified Speaking Professional designation from the National Speakers Association and is a member of the Speaker Hall of Fame. Check out any of his excellent books, his video series "Team Building: How to Motivate and Manage People" or his website, [marksanborn.com](http://marksanborn.com), to learn more.

## ■ DO THESE 3 THINGS TO MAKE SURE YOU DON'T GET HACKED

**Train up.** Get your entire team trained on IT security fundamentals and best practices. They should know how to create strong passwords, how to safely access the web and how to securely use e-mail – including how to identify phishing scams. They should have a clear understanding of today's threats and how to be proactive in addressing those threats.

**Invest in good tech.** You should be invested in solid malware protection, including antivirus software and firewalls. All of your data should be backed up to the cloud and expertly secured using encryption

software. You should also be invested in threat monitoring.



**Establish relevant systems and processes.** Have standard operating procedures (SOP) in place to train employees, respond to threats and access networks. For example, are employees connecting with unverified devices from home? Establish rules on what can and cannot happen. Another example: are your cloud backups set up correctly? Is someone checking it? Again, have SOP in place to address these kinds of issues.  
*Small Business Trends, Feb. 13, 2020*

## ■ 3 WAYS TO GROW YOUR BUSINESS WITHOUT SPENDING A DIME

**Follow a thought leader in your industry.** Whether you follow them on social media or their blog, keep up-to-date with the issues they're talking about. Then do further research into those issues. This keeps you in the know and more likely to learn something you can easily apply to your own business.

**Use your best testimonials.** If someone posts a great review on Google, for example, reach out and ask about using it in your marketing. Or reach out to customers who you already have a good relationship with and ask if they're willing to give you a testimonial. It builds credibility.

**Partner up.** It pays to develop partnerships with existing vendors or other businesses that are adjacent to yours. That is to say, look for opportunities to share customers. If you have a customer who's looking for a specific service you don't offer, point them to someone who does (your partner). And your partner will do the same. Reach out into your business community and see what kind of relationships you can form.  
*Business Insider, Feb. 13, 2020*

### INFRASTRUCTURE » SUPPORT » STRATEGY

Not a client yet?

Contact us today to learn how our CompleteCare<sup>sm</sup> Managed Service can protect and help your business grow.

937.428.5880

[askIT2@it2resource.com](mailto:askIT2@it2resource.com)

