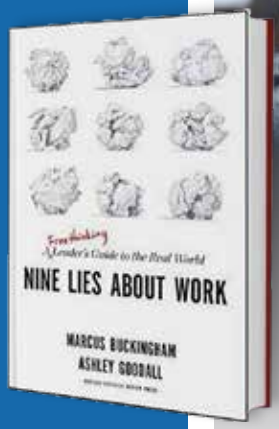
WCI Technology Insider
Insider Tech Tips - Written for Humans, Not Geeks

Nine Lies About Work

by Marcus Buckingham and Ashley Goodall



We all believe certain things about work and the way we run our businesses. But as authors Marcus Buckingham and Ashley Goodall point out, not everything is as it seems. In *Nine Lies About Work: A Freethinking Leader's Guide To The Real World*, they break down nine lies we tell ourselves or have been told. One example: *the best plan wins.* Good plans can get good results, but the best plans can still fail. In the real world, there are countless obstacles or variables that can derail our best-laid plans. The authors discuss how to overcome this "lie" and others. Change your perspective with *Nine Lies About Work.*

October 2020

Bill Wright
Founder & CEO

Our Mission:
Technology systems that anchor your business and protect what you have built, from a company inspired to make the world better.

Employees Are Letting Hackers Into Your Network ...

What You Can Do To Stop It

Cyberthreats are everywhere these days. Hackers, scammers and cybercriminals are working overtime to break into your network – and the network of just about every business out there. They have a huge arsenal of tools at their disposal, from automated bots to malicious advertising networks, to make it possible.

But there is one "tool" that *you* may be putting directly into their hands: your employees. Specifically, **your employees' lack of IT security training**.

While most of us expect hackers to attack from the outside using malware or brute-force attacks (hacking, in a more traditional sense), the truth is that most hackers love it when they can get others to do their work for them.

In other words, if they can fool your employees into clicking on a link in an e-mail or downloading unapproved software onto a company device, all the hackers have to do is sit back while your employees wreak havoc. The worst part is that your employees may not even realize that their actions are compromising your network. And that's a problem.

Even if you have other forms of network security in place – malware protection, firewalls, secure cloud backup, etc. – it won't be enough if your employees lack good IT security training. In fact, a lack of training is the single biggest threat to your network!

It's time to do something about it. Comprehensive network security training accomplishes several things, including:

1. **Identifying Phishing E-Mails** Phishing e-mails are constantly evolving. It used to be that the average phishing e-mail included a message littered with bad grammar and misspelled words. Plus, it was generally from someone you'd never heard of.

Continued on Page 2 ...

... continued from Cover

These days, phishing e-mails are a lot more clever. Hackers can spoof legitimate e-mail addresses and websites and make their e-mails look like they're coming from a sender you actually know. They can disguise these e-mails as messages from your bank or other employees within your business.

You can still identify these fake e-mails by paying attention to little details that give them away, such as inconsistencies in URLs in the body of the e-mail. Inconsistencies can include odd strings of numbers in the web address or links to YourBank.**net** instead of YourBank.**com**. Good training can help your employees recognize these types of red flags.

2. Avoiding Malware Or Ransomware Attacks One reason why malware attacks work is because an employee clicks a link or downloads a program they shouldn't. They might think they're about to download a useful new program to their company computer, but the reality is very different.

> **"Every device on your network should be firewalled and have updated malware and ransomware protection in place."**

Malware comes from many different sources. It can come from phishing e-mails, but it also comes from malicious ads on the Internet or by connecting an infected device to your network. For example, an employee might be using their USB thumb drive from home to transfer files (don't let this happen!), and that thumb drive happens to be carrying a virus. The next thing you know, it's on your network and spreading.

This is why endpoint protection across the board is so important. Every device on your network should be firewalled and have updated malware and ransomware protection in place. If you have remote employees, they should only use verified and protected devices to connect to your network. (They should also be using a VPN, or virtual private network, for even more security.) But more importantly, your employees should be trained on this security. They should understand why it's in place and why they should only connect to your network using secured devices.

3. Updating Poor Or Outdated Passwords If you want to make a hacker's job easier than ever, all you have to do is never change your password. Or use a weak password, like "QWERTY" or "PASSWORD." Even in enterprise, people still use bad passwords that never get changed. Don't let this be you!

A good IT security training program stresses the importance of updating passwords regularly. Even better, it shows employees the best practices in updating the passwords and in choosing secure passwords that will offer an extra layer of protection between your business and the outside world.

If you or your employees haven't updated their passwords recently, a good rule of thumb is to consider all current passwords compromised. When hackers attack your network, two of the big things they look for are usernames and passwords. It doesn't matter what they're for – hackers just want this information. Why? Because most people do not change their passwords regularly, and because many people are in the habit of reusing passwords for multiple applications, hackers will try to use these passwords in other places, including bank accounts.

Don't let your employees become your biggest liability. These are just a few examples of how comprehensive IT and network security training can give your employees the knowledge and resources they need to help protect themselves and your business. **Just remember, you do not have to do this by yourself! Good IT training programs are hard to find, and we are here to help.**

October is Cybersecurity Awareness Month

Do you know what virtual monsters could be threatening your business?

It's easy to get lost down the dark and twisted path of the Dark Web and Cyber Attacks, where an infinite number of scary threats live. The biggest problem, though, is that too many of us don't even realize that they're there. This month, we want to help you understand what threats exist out there, and get you on the much sunnier path of Cybersecurity.

Are you ready for Cybersecurity to shine a light into the darkness?

Check out our free action pack, Cybersecurity, at **www.WCITech.net/cybersecurity-guide** to find out what you didn't even know you didn't know.

www.WCITech.net/cybersecurity-guide

SHINY NEW GADGET OF THE MONTH

Ovo Portable Steam Iron And Garment Steamer

The Ovo Portable Steam Iron And Garment Steamer is much smaller than your average iron and yet capable of so much more. It's an iron and a steamer and the perfect companion for when you're traveling and want to look sharp. Or keep the Ovo at home to save space!

The Ovo fits easily in your hand. It's lightweight and won't take up much space in your luggage. Plus, it holds enough water to create up to 10 minutes of steam. You can quickly switch from the metal ironing plate to the brush attachment to add finishing touches to delicate fabrics (and remove any lint or pet hair). It even comes with a heat-resistant travel case.

Do Smartphone Apps Listen To Your Conversations?

We've all seen this: you scroll down Facebook or Google search results and see an ad for a restaurant or product you were just talking about the other day. How can this be? Was your phone "spying" on you? According to *Consumer Reports*, not exactly.

Instead, what you're seeing is a personalized ad created by your search habits. Google, Facebook and others collect data as you enter search terms and click on various results or other ads. They know you, and as a result, you are likely to see ads regarding things you just talked about last week. The best way to around this is to turn off app permission, browse in "incognito mode" or uninstall intrusive apps.

The Leader's Most Important Job

Can you guess what the most important trait is for effective leaders? You can probably guess all sorts of things: relationship building, communication, awareness, positivity, innovation … The list goes on. And you probably do a lot of those things too.

When I speak with leaders, I emphasize that a person's success as a leader doesn't come from what they do or how they do it — it's about *how often they do these important things*.

The Most Important Thing For Leaders: Focus Your Team

A leader's most important job is taking the time and effort to focus their team. Leaders must help their team members focus their time and expertise to complete the organization's most important work.

The most successful businesses are driven by **profit, innovation, efficiency and effectiveness.**

Your team's revenue and results are all driven by how people spend their time (effort) and expertise (knowledge and skills), and these are the keys to elevating your team's success. By doing these things and being a role model for your team, you can experience amazing results.

How To Elevate Your Team

1. Passion Creating a vision requires passion. This passion elevates your own commitment and helps both you and your team be productive. It's unlikely that a leader will be fully immersed in their role, their organization or their team if they are not passionate about what they are doing.

2. Time, Expertise And Motivation Everything is the by-product of time and expertise. When a leader invests both time

and expertise into their team, the team grows. When time and expertise are invested wisely, the organization also achieves great success. By putting the time and expertise into your team members, you can motivate them to improve in their roles.

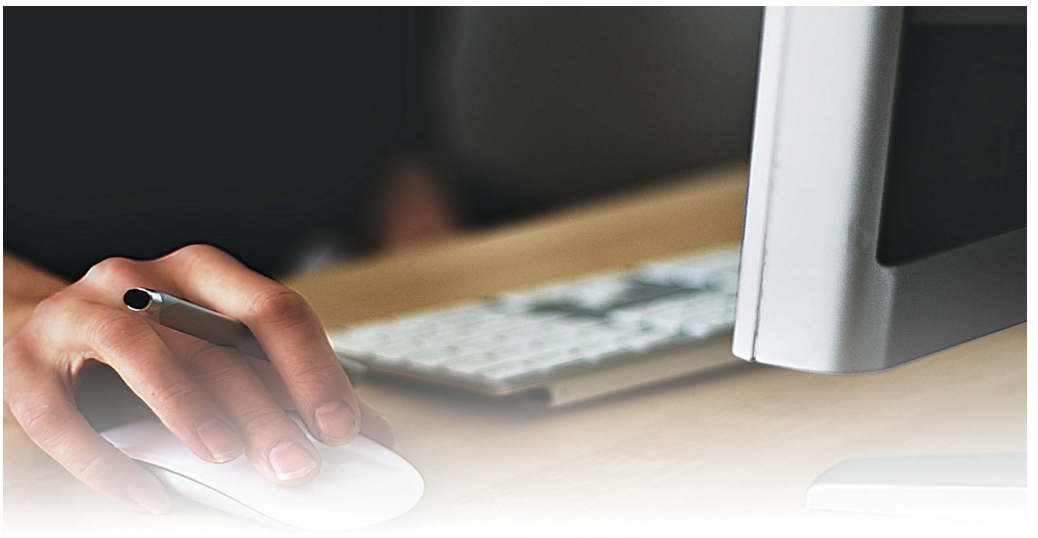
3. Focus This goes hand in hand with time and expertise. By focusing on the strengths (and weaknesses) of a team and learning how to constantly improve and grow, an organization can produce positive results. When a leader doesn't have this focus, the organization suffers. Mediocrity becomes the norm.

A great deal of time and expertise is wasted in companies where employees are doing low-priority work or work that shouldn't be done at all. When a team lacks an effective leader, it is difficult for them to know what they should be doing instead.

When a leader takes the time to show their team the importance of their work and how their work will achieve success, the whole organization grows. This commitment is what creates remarkable performances. You can learn more about this in my book *The Encore Effect: How To Achieve Remarkable Performance In Anything You Do*.

At the end of the day, it's most important for leaders to regularly take the time to focus on and elevate their team. Just as a conductor makes sure members of an orchestra are all playing the right music to the best of their ability, so does an effective leader do their job.

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, to learn more.*



What is National Cybersecurity Awareness Month, and *Why Is It Important?*

Simply put, National Cybersecurity Awareness Month (NCSAM) is a focused effort to raise awareness about the need for Cybersecurity in the US.

The number of Internet and electronic users has grown exponentially (there are currently an estimated 4.8 billion - that's over 62% of the world's population! - Internet users) since the birth of technology. Unfortunately, though, our ability - and even our awareness of the need - to stay safe while on our devices, has not grown at that same rate.

The problem is that this lag in awareness, education, and action in keeping ourselves and others safe on the Internet, has left many doors open for threats to sneak in.

You've more than likely heard, if not experienced for yourself, some of the most common types of Cybercrime: Phishing, Ransomware, Bots, Malware, Spam, and others. But, the reality is that there are an infinite number of ways that cyber criminals can access and attack your business, personal electronics, data, and so much more.

To get a little better of an idea of what it is that we're talking about, let's take a moment to review what Cybercrime in general can mean.

Cybercrime is any crime that is committed electronically. Really narrows it down for us, huh? To be a little more specific, Cybercrime can include things like we've already mentioned, but it can also include fraud, theft, malicious social engineering, intellectual property violations, the use and spread of child sexual abuse materials, and so much more. Some forms of Cybercrime can even lead to physical endangerment or even death. The most important thing to remember about Cybercrime, however, is that it's not just adults who are risk of becoming victims of it. Young adults just learning how to manage their finances, new graduates entering into the workforce for the first time - even grade school children and younger - all can become victims of Cybercrime, and they are often victims of the most heinous of Cybercrime events.

It may seem silly and even obvious to some of us, but just looking at this brief explanation shows us just how much is actually at risk if we do not stay proactive, protected, and aware of the dangers that exist on the Internet. The whole point of Cybersecurity Awareness Month isn't to get people to understand what's at stake solely for their business if they do not have proper security measures and training in place, but is to get people to understand what's at stake in every single facet of their lives, and the lives of those around them, if they do not take the necessary measures to keep their electronics protected, and stay educated on the growing industry of Cybercrime.

This is why this month is so important.

National Cybersecurity Awareness Month (NCSAM) 2020

This month, we're celebrating the 17th year of raising awareness around the need for cybersecurity across the country, and the world. Won't you join us?

The Cybersecurity & Infrastructure Security Agency (CISA) and the National Cyber Security Alliance (NCSA) have announced the theme for this year:

"Do Your Part. #BeCyberSmart"

Throughout each week of October, you'll find these organizations (and WCI!) focusing on the following areas:

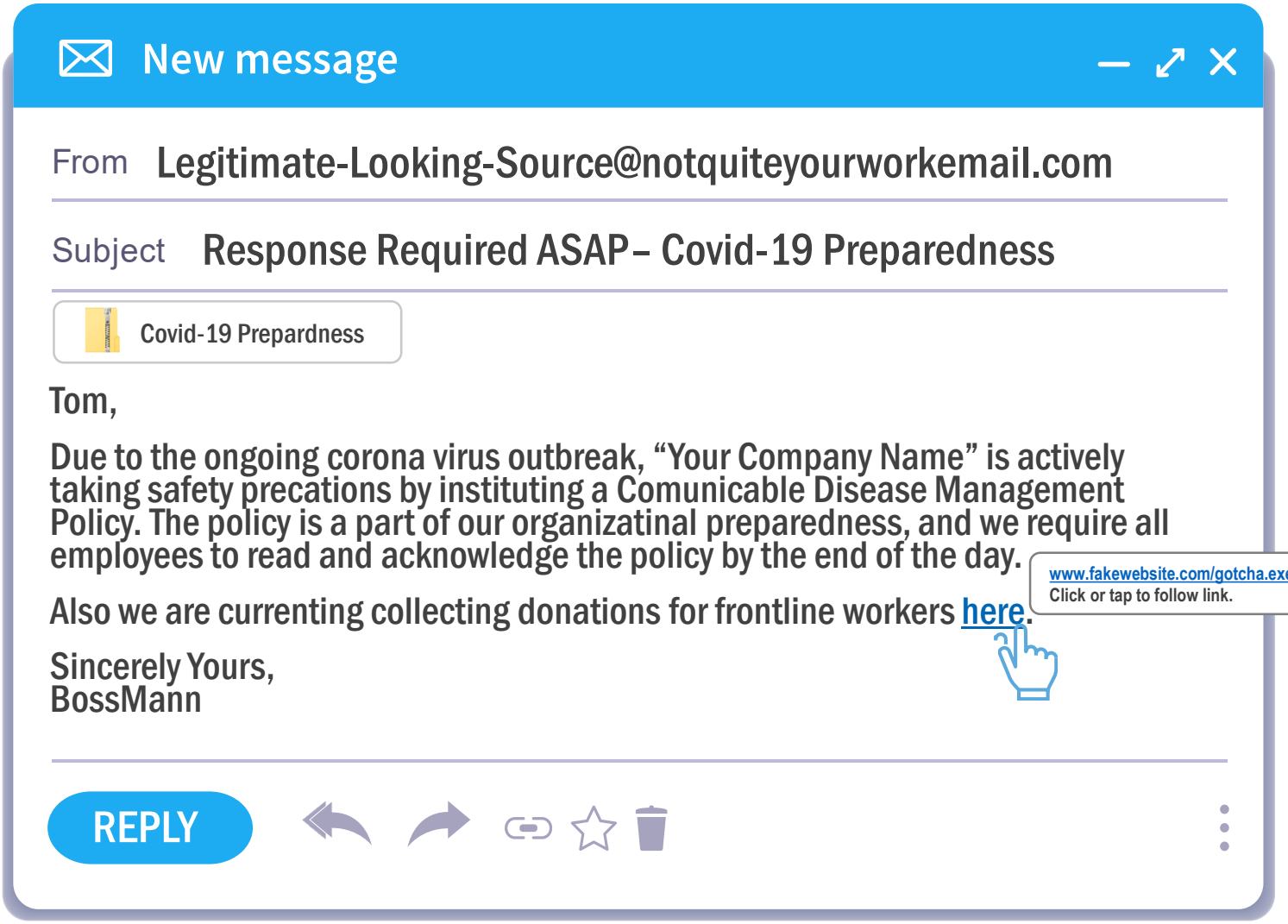
Week 1: If You Connect It, Protect It
Week 2: Securing Devices at Home and Work
Week 3: Securing Internet-Connected Devices in Healthcare
Week 4: The Future of Connected Devices

Follow the hashtag #BeCyberSmart on social media to follow along with updates and resources, and use it to show your own involvement!

If you see or fall victim to any form of Cybercrime, report it at us-cert.cisa.gov/report.

Final Thoughts

Would This Email Fool You?



If this email arrived in your inbox, addressed to you, with almost your company's name (or some other trusted source's name) in the "From" section, it would be reasonable to think that this was an email that was safe to open and follow through. If something like this could even have the chance of fooling you, it's time to take action in becoming more aware of what's going on in the Cyber world.

We can help you with this. Start with our free guide on Cybersecurity, found at www.WCITech.net/cybersecurity-guide.

We've created this introductory guide with our partners at The 20 to help you learn about this global concern, and fill in any gaps that you may have. Once you've taken this step, sign up for our weekly email tips, and follow us on our social media accounts to get even more info on how to stay protected, in bite-sized portions.

And when you're ready to talk about what you could be doing to keep your business and your family safe, give us a call at 614.76.2911, or visit us at www.WCITech.net/cybersecurity-schedule, to pick a time to discuss your options.

You can see my live calendar and choose a time that works best for you to discuss your security needs and options at www.WCITech.net/cyberseurity-schedule

Bill Wright, Founder & Chief Visionary Officer

1989

IT'S FUN TO DRESS UP AS GOBLINS, GHOULS AND OTHER MAKE-BELIEVE THINGS FOR HALLOWEEN, BUT IT'S NEVER FUN TO HAVE VIRTUAL MONSTERS ATTACKING YOUR NETWORK. THE FIRST STEP IN COMBATING THESE THREATS, IS UNDERSTANDING THEM; THERE'S NO HOPE IN PROPERLY PROTECTING OUR SYSTEMS IF WE DON'T KNOW WHAT IT IS THAT WE'RE UP AGAINST. WE'VE ALWAYS BELIEVED HERE AT WCI TECH THAT EDUCATION HAS TO BE JUST AS VITAL TO WHAT WE OFFER, AS THE TECHNICAL WORK WE PERFORM IS. THAT'S WHY WE'RE TAKING OCTOBER TO TEACH YOU ALL ABOUT CYBERSECURITY.

2020

WCI TECHNOLOGY SOLUTIONS

81 Mill Street, Suite 300
Gahanna, OH 43230

@WCITech

WCI Technology Solutions

@WCITech

Do These Things To Protect Your Business From Getting Hacked

1. **Train Employees.** Your team needs to know how to identify and handle today's IT security threats. Cybercriminals often rely on your employees' lack of training to break into your network. Ongoing training gives employees tools and resources to overcome this and many other IT security challenges. Make training a top priority!

2. **Hold Employees (And Yourself) Accountable.** Training and company guidelines don't mean much without accountability. When you set rules, follow them, just as you follow industry and government rules and regulations when operating your business. Be willing to hold anyone who does not accountable.

3. **Have A Disaster Recovery Plan.** Things happen. When you store sensitive data, you need to have a plan in place to recover and restore that data should anything happen. This doesn't just include data loss from malicious attacks but other types of disasters, including hardware failure, fire and flood. How is your data being backed up and saved? Who do you notify in the event of a breach? Who do your employees call in the event of disaster? *SmallBiz Technology, Dec. 26, 2019*

4 TIPS TO GET PROJECTS DONE ON TIME WITH A SMALL TEAM

Give Them The Tools And Resources They Need — We all need tools to get things done – project management software, content creation tools, messaging apps, virtual private network access and more. Have a conversation about what each team member needs to maximize productivity and work closely with them to meet that need.

Set Aside Time For Proper Research
Don't jump headfirst into a project without jumping into research first. Information is a powerful tool to get things done efficiently and effectively.

Assign Accordingly —Before the team goes to work, make sure assignments or responsibilities are delegated properly and check in with everyone on a regular basis to make sure things are going smoothly (or to see if they need help).

Plan And Plan Again —Plan out the project before you set to work. Give yourself and your team a map to follow as you work through the project. As with any project, expect obstacles along the way and be willing to update your map accordingly. *Small Business Trends, July 4, 2020*