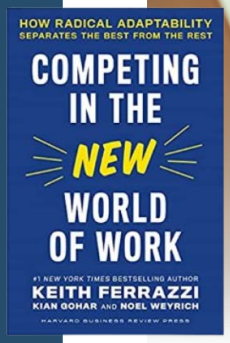
WCI Technology Insider
Insider Tech Tips - Written for Humans, Not Geeks

Competing in the New World of Work

by Keith Ferrazzi



Businesses should be adaptable so they can remain competitive with others in their industry. This is something that became painfully clear for thousands of companies throughout the pandemic. Some needed to stay ahead of trends to even keep in business - and Keith Ferrazzi's newest book, *Competing in the New World of Work*, provides the perfect guide for those who may be struggling to keep up. Ferrazzi details the changes that occurred during the pandemic, while also unveiling new visions for the future and new leadership models that will help bring success to any business. With this road map in hand, your business will be well on its way to a successful future, no matter what changes are thrown your way.

October 2022

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.

Keep Your Information Secure

by using strong passwords

We use passwords for just about everything. Most of us have to enter a password to get into our computers, then enter more passwords to access our email, social media profiles, databases and other accounts. Even our cell phones and tablets can and should be password-protected. In fact, if you aren't securing all of your devices and accounts with passwords, you should definitely start. it could help prevent your business and personal information from becoming compromised.

Why Passwords?

We use passwords to ensure that those who don't have access to our accounts can't get access. Most of our devices hold large amounts of personal information. Think about the potential harm someone could do if they gained access to your personal cell phone. They would immediately be able to see all of your contacts, pictures and applications. They might even be able to log in to your email, where they could obtain your banking information. If this type of access falls into the wrong hands, it could be detrimental to your life. Passwords offer the first line of defense to prevent others from obtaining sensitive information.

This becomes even more important if you own a business. Each of your employees should be utilizing strong passwords to access company information. If your business is not using passwords - or is using simple passwords - you could be opening yourself up to hackers and cybercriminals. If a cybercriminal gains access to your company's private information through a weak password, they will gain access to customer information, which could damage your reputation and open you up to lawsuits.

Continued on Page 2 ...

... Continued from Cover

That being said, everyone within your business needs to utilize complex and unique passwords.

Making a Strong Password

Not all passwords are created equal. When it comes to making a strong password, you must think about it. If you use a password that you can't remember, then it's essentially useless. And if you use a password that's too easy to remember, your password won't be strong enough to keep cybercriminals out. Your password should be long, have a mix of lowercase and uppercase letters, utilize numbers and special characters, have no ties to personal information, and should not be a word from the dictionary.

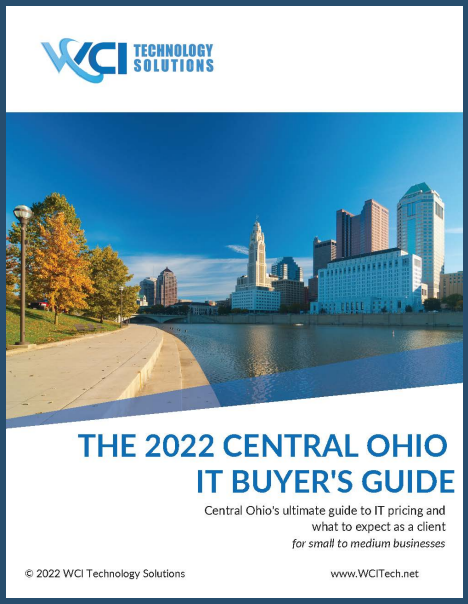
In the grand scheme of things, it's not enough to just create complex passwords. They also need to be unique. In addition to this, you should use a different password for each and every one of your accounts to help maximize their effectiveness. Think about it this way: let's say you use the same password across your business email accounts, social media accounts and bank accounts. If someone decrypts the password for your Facebook page, they now have the password for more valuable accounts. It's a dangerous game that can be avoided by using unique and complex passwords for every account you use.

Remembering All of These Passwords

You may be worried about remembering all of your passwords if you have to create a unique one for each of your accounts. Your first thought may be to write them down, but that might not be the most secure option. If someone gets their hands on your little black book of passwords, they'll immediately gain access to all of your accounts with a handy directory showing them exactly where to go. Instead, you should utilize a password manager to help keep track of all of this sensitive information.

With a password manager, you only have to worry about remembering the master password for your password manager. All of your other passwords will be securely hidden. Password managers also give you the option to create random passwords for your accounts to bolster their security. That way, you can have the most complex password possible without worrying about forgetting it. Additionally, password managers can also help you remember the answers to security questions and more so that you never get accidentally locked out of one of your accounts. They're easy to use, convenient, and secure.

Passwords are an important part of your cybersecurity plan. Make sure you and your employees are using complex and unique passwords. It can also help to implement some training so your employees understand the importance of secure passwords. When use correctly, passwords will help deter any would-be cybercriminals from accessing your sensitive information.



The 2022 Central Ohio IT Buyer's Guide

If you're actively looking for new IT support options, or know that you will be soon, head over to our website and check out this year's edition of the IT Buyer's Guide. As a trusted MSSP and IT expert in Central Ohio, you can rest assured that this eBook is packed full of all the information that you need to make the right decision for your company's IT needs. Check it out today at

www.WCITech.net/2022ITBuyersGuide

#1

Two years after its launch, Microsoft Teams generated $800 million in revenue

#3

on average, there are 500,000 new internet users every day

#2

The most expensive domain name (CarInsurance.com) cost $49.7 million

TECH FACTS

Bill's Favorite Business Gadget of the Month

Need a new wireless mouse? Microsoft has a really sleek-looking, minimalist one for you.

The Microsoft Modern Mobile Mouse (try saying that 5 times fast, huh?) is nice to look at, affordable and comes in a range of different colors too.

Inspirational Quote of the Month:

"The first rule of any technology used in a business is that automation applied to an efficient operation will magnify the efficiency. The second is that automation applied to an inefficient operation will magnify the inefficiency.""

- Bill Gates, Co-founder of Microsoft

October's Featured Everyday Gadget:

Bril

It might be surprising to hear, but our toothbrushes are some of the dirtiest items in our households. There's a good chance that there are more than a million kinds of bacteria living on your toothbrush right now. Unfortunately, rinsing your toothbrush after brushing is only so effective. That's why Bril was invented.

Bril is a portable toothbrush case that sterilizes your toothbrush after every use. It contains an all-natural ultraviolet light that kills 99.9% of germs on contact. It's simple to use, as all you have to do is place your toothbrush inside and close the lid. Bril does the rest. It's the quickest, most effective and easiest way to ensure your toothbrush head stays clean.

The Secret to Job Happiness Might be Who You Work With

If I were to ask you where job happiness comes from, how would you respond? Conventional wisdom says that your happiness at work comes from one of these four sources:

- "Follow your passion" (what)
- "Play to your strengths" (what again)
- "Do something with purpose" (why)
- "Live your values" (how)

It's also true that 95% of career-success books follow one of these lines of advice, but what if they're wrong?

What if your job happiness comes not from ***what*** you do, ***why*** you do it, or ***how*** you do it... but instead comes from the people around you? Your bosses, peers and subordinates all can play a huge role in your job happiness. Let me give you a few examples that support this idea.

I know a talented MBA who works for a public-private partnership with a mission that would make any do-gooder proud. He is planning to quit that job because he feels the firm's leadership disregards the human element of their work, bickers internally and lacks integrity. I'm reminded of a well-researched fact I learned during graduate school: employees don't quit jobs, they quit supervisors.

My firm once did a pro bono project for the US Navy where I observed a grueling exercise routine. I asked one of the instructors why anyone would sign up for that - and honestly, I think I expected a response about patriotism. Instead, he explained that they join to be part of a camaraderie. It was a community where they had each other's backs.

If the secret to job happiness is who you work with, then that means you should plan your career differently. Rather than meditate for too long on your passion and purpose, you could think about the kinds of people you really want to be around. Who do you want to be your customers? Who do you want to be your colleagues? What sorts of personalities?

Rather than sourcing job titles, you could sourcing bosses and colleagues you want to work with. I recently told a young job-seeker, "Don't just go find any old job in your industry. The most important thing you can do right now is to find the right boss - to hire your boss. Hire the best boss in your industry - someone who will teach invest in you, tell you the truth, give you real feedback, put energy into helping you discover your ideal path and then help you achieve it."

Once you land your new dream job, be mindful of the time you are spending with the people you want to work with. Don't just track your goals and results, track the time you are spending working with the specific people in your company you want to work with.

Dr. Geoff Smart is the chairman and founder of ghSMART, a leadership consulting firm that exists to help leaders amplify their positive impact on the world. Dr. Smart and his firm have published multiple *New York Times* best sellers. He stays active in his community and has advised many government officials.

Do you know exactly what services your staff are signing up for?

Whatever problem, need or want you have... there's a cloud application out there that can help you.

We've never lived in such a rich time for problem solving. Every day, hundreds of new services launch to make our lives easier and help us be more productive.

These applications all live in the cloud. They're known as Software as a Service - or SaaS - because you don't load any software onto your device. You use them in your browser.

We would argue this SaaS revolution over the last 15 to 20 years has played a critical part in shaping the way we work today.

However, there's an issue. Many businesses aren't 100% aware what new services their staff have signed up to. And this problem isn't a financial one, it's a security one.

Let's give you a scenario. Suppose a member of your team, Shanice, is trying to do something creative, but just can't with her existing software. She Googles it, and finds a cool application. Shanice signs up for an account, and as she's in a rush, uses the same email address and password as her Microsoft 365 account. Yes, reusing passwords is a very bad practice. But, this gets worse.

She uses the application for half an hour to achieve what she needs to do... and then forgets it. She's got no intention of upgrading to a premium subscription, so just abandons her account.

That's not an issue... until 6 years later. When that SaaS application is hacked by cybercriminals, and all its login credentials are stolen.

It's well-known that cybercriminals will try stolen details in other sites, especially big wins like Microsoft 365.

Can you see the issue here? Shanice's 365 account would be compromised, and she'd have no idea how it happened. She won't remember an app she used for half an hour years before.

The answer is to have a solid policy in place about who can sign up for what kind of service. Also ask your technology partner if they have any way to track what apps are being used across your business.

And definitely get a password manager for your staff... this will generate a new long, random password for each application, remember it, and autofill login boxes.

Password managers encourage good password practice because they make it easy.

Did You Know

you can change your mouse cursor color in Windows 11?

It probably won't make you any more productive, but it might be a good mood-booster!

- Open settings and choose: Accessibility > Mouse Pointer and touch the web
- Select Custom. Choose the pointer style and color you want.
- Close settings.

Ta da! A cursor that matches your mood/coffee mug.

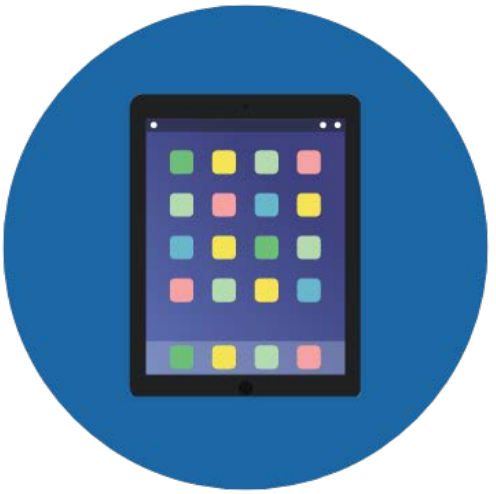
New to Windows 365

Word & Excel are getting an iPad redesign

Do you ever get a bit of work done at home using your iPad?

Microsoft's giving the standard Office Tools (Word, Excel, and PowerPoint) a bit of a redesign on the iPad, to make them look more like they do on your computer.

The preview is available now and we reckon it could go into general availability in the next few months.



Would you pay if your business was crippled by ransomware?

Ransomware is scary. It's where cybercriminals lock your data and charge you a ransom fee to get it back.

If it happened to you, would you pay the fee?

Despite what the criminals promise, they don't always unlock data when the ransom fee is paid. or they ask for a second fee. Or they unlock it and then sell it on the dark web anyway.

Many large companies are now refusing to pay, finding other ways to get their data back. And ransomware groups are looking for different opportunities.

Small, financially stable businesses are the new targets. And the size of payments demanded has increased.

This means you and your team need to be vigilant about cybersecurity. Continue to take the necessary precautions such as using a password manager, checking emails are from who they say they are from, and making sure your network is being monitored and protected.

It's also vital that you have a working backup of all data. Check it regularly.

Even without paying the ransom demand, your business stands to lose a lot of money if hit by ransomware. It takes ages and can cost a ton to get back on your feet.

If you want us to audit your business and check its ransomware resilience, get in touch!

Technology Update

If you use Microsoft Teams on desktop, you'll be able to use a Bluetooth enabled headset to control your calls.

An update means you can use the buttons on your headset (or a speaker phone) to answer and end calls, rather than fumbling about for the on-screen button.

An end to awkward pauses?

Sign us up!

Gather round for this month's tech quiz!

Who has the most random technology knowledge in your office?

1. **What shape was the original design for the first Apple phone?**
2. **True or False: 50% of the world has never made a phone call?**
3. **What is nomophobia a fear of?**
4. **How do you pronounce "PNG" file?**
5. **What was the first home computer to have a color display?**

The answers are on page 8.

Question

Should I let my team have work apps on their personal phones?

ANSWER

It's personal preference. But if you do, make sure their phones are protected by the same security measures they'd have on work devices.

Question

I've received an email that looks genuine, but hasn't addressed me by name. Should I click the link?

ANSWER

If you ever have cause for doubt, don't click links of download files. Phone the sender to check if they really send the email.

Question

Should I be monitoring my remote staff?

ANSWER

Software exists to do this, but what message does it send to your team? It can be highly counterproductive in many cases. Take the time for regular catchups over Teams instead, or try a productivity tracker if you have concerns.

QUIZ Answers

1. APPLE WAS DEVELOPING AN APPLE-SHAPED FLIP PHONE BEFORE THE IPHONE. WOULDN'T YOU LOVE TO SEE THAT ONE?
2. FALSE. IT'S A STAT STILL USED TODAY, BUT DATES BACK TO THE MID 90'S
3. NOT HAVING A WORKING MOBILE PHONE
4. PING
5. THE APPLE II IN 1979

WCI TECHNOLOGY SOLUTIONS

81 Mill Street, Suite 300
Gahanna, OH 43230

@WCITech

WCI Technology Solutions

@WCITech

Take Advantage of Google Reviews

When you are deciding on a restaurant to dine at, you might check the Google reviews to help with your decision. The same thing goes for your business. Before people come in to buy your product or services, they might check your Google reviews, so it's important that your reviews positively reflect your business. If you own a company, you should understand how Google reviews work and do everything you can to encourage customers to leave positive ratings and comments.

If you haven't already claimed your Google business profile, you should do so immediately. It will allow you to add pictures and a description so customers know what to expect from your business. When customers have complete a purchase with you, encourage them to leave a review if they had a positive experience. Some customers may need help with the review process, so teach them how to leave a review if they have never done it before. Make sure you thank customers who leave positive reviews and try to fix the issues explained in your negative reviews. Being a responsive owner will reflect positively on your business. When you use Google reviews to your advantage, you will see a boost in clientele.