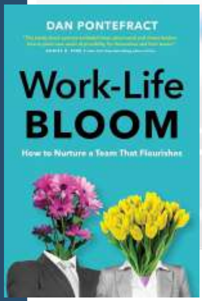
WCI Technology Insider

Insider Tech Tips - Written for Humans, Not Geeks

Work-Life Bloom: How to Nurture a Team That Flourishes

by Dan Pontefract

With the holidays already upon us, we here at WCI have been thinking more and more about the work-life balance we practice and encourage for our team. That's why this book has made its way onto our shelf for this month.

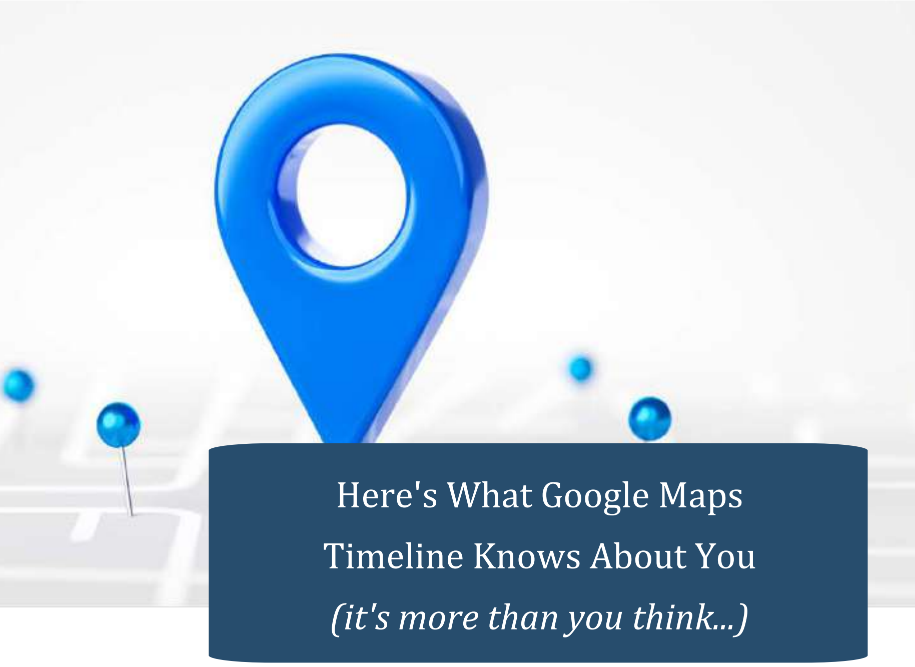


Just as a flower needs all the right conditions to thrive, we as people need the right combination of work and personal life factors to really be at our best. That's award-winning author, Dan Pontefract's, message in this book. To reach this right combination, Pontefract offers up 12 different factors - 6 for work and 6 for personal life - that, in combination, create the perfect 'ecosystem' we need to nurture a healthy Work-Life balance in ourselves, and in our teams.

November 2023

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.



Here's What Google Maps Timeline Knows About You *(it's more than you think...)*

It's 10 pm - do you know where your children are? Google probably does. Thanks to Google Maps' Timeline feature, the tech company probably knows where your whole family has been - down to the GPS coordinates. The feature was first rolled out in 2015 on Android devices and two years later on Apple, but many people still don't know how much information the app actually collects. Before you hit the road this holiday season, take a minute to review your privacy settings to see if the risk is worth the benefits.

What Google Maps Timeline Sees
With Google Maps Timeline, you can go back to any day and see in detail where you were, when and for how long. For example, the map will show you when you left work, got home and any pit stops you made. It can also tell if you traveled by bike, car, train or bus. If you haven't changed the settings, this information may have been stored for YEARS. This kind of tracking is helpful if you forget the name of a lunch place you visited last month. However, if you care about your privacy and prefer not to have your home address or daily jogging routine under Google's watchful eye, you need to turn this feature off.

Pros and Cons
Under the guise of being a digital assistant, Google collects information to make your life easier. At the same time, it's creating detailed profiles of all of us. In some ways, this makes our lives easier. In other ways, it invites severe risks.

Continued on Page 2 ...

... Continued from Cover

Upsides:

- Find what's lost: Has your kid ever lost their phone during an errand spree and is not sure if they left it in the cart at Target or the bathroom at The Cheesecake Factory? Yeah, it's not a great feeling. If your phone is connected to the Internet, Google Maps Timeline can retrace your steps.

- Peace of Mind: Many parents gain peace of mind about their children's safety by knowing where they are and where they've been.

- In business: It can be a good idea to activate this feature on devices that you provide to your employees. While we don't advise you keep tabs on their location, it could be useful to know where your devices are in cases of loss, theft or even hacking incidents.

- Tailored ads: Because Google apps speak to each other, your ads and recommendations.

Downsides:

- Peeping Toms: Anyone who gets hold of your account can build a profile of you - or worse, your kids and family. They know where you live, work, go to school, hang out, all of it. Threat actors weaponize profiles in extortion schemes or impersonate people to commit other heinous crimes.

- Not 100% accurate: You must be connected to the Internet and logged into Google for the feature to work properly.

- A lot less privacy: For as much as we love tech here, we have to say - it's pretty creepy when an app tracks and stores personal information!

How to Turn Off Tracking

If you don't like having Google's eyes on your every move, follow these steps on one of your devices to update the settings. here's how to do it from your computer:

- Log in to your Google account

- Tap your profile icon or initials and select "Manage Your Google Account"

- Click on "Data & Privacy"

- Scroll to "History Settings" and select "Location History"

- Pause your history

- Bonus Tip: Delete your timeline history by going to Maps Timeline, "Manage Location History", and selecting an auto-delete option.

Tips for Using Google Maps Timeline

If the benefits outweigh the negatives for you or your family, do two things. First, define a timeline to delete stored data. You can delete your location history after 3, 18, or 36 months - or keep it forever (which we don't recommend). Once your pick an option to remove the data, Google is legally obligated to delete it.

Second, use multifactor authentication on your devices and accounts so that even if someone finds your phone or hacks your account, they can't get in. Take control of your privacy and review this buried feature in Google's Maps app!

Byte-Sized Brain Challenge

What's the vertical three-line menu icon called?

A. Kebab

B. Hamburger

C. Meatball

Answer: B. Hamburger

What We've Been Chatting About This Month

Don't forget home office security: A guide to keeping remote workers safe and secure
WCI TECHNOLOGY SOLUTIONS

Home Office Security

Want to join the conversation? Our new guide is up on our website resource page now!

TECH FACTS

#1

The LG KE850 was the first phone to introduce a complete touchscreen to the mobile phone market, debuting in December 2006 - a whole month ahead of the Apple iPhone

#2

The record of the largest data breach involved Yahoo. Back in 2013, the birth dates, phones numbers and security questions of approximately 3 billion Yahoo account holder were hacked

#3

The "save" icon in most software applications, which looks like a floppy disk, is a totally outdated symbol. Most people today have never even seen, let alone used, a physical floppy

Bill's Favorite Business Gadget of the Month

Full HD Laptop Screen Extender

Work on a laptop, but love the functionality of multiple monitors? Here's a handy portable solution that will keep you productive wherever you choose to work.

This KEFEYA laptop screen extender just plugs and plays, leaving you free from fiddling with cables or stressing over setting up complicated software. It means you can work across a range of apps at the same time, or even share your screen with customers more easily.

Check it out on Amazon where it's currently selling for $389.99

Inspirational Quote of the Month:

"You don't have to be a genius or a visionary or even a college graduate to be successful. You just need a framework, and a dream."

- Michael Dell, founder and CEO of Dell Technologies

The WCI Team's Favorite Everyday Gadget of the Month:

The holidays are here, and that can only mean one thing: lots and lots of cleaning.

Whether you're traveling this holiday season to spend your time with loved ones, or having them travel to you, getting your abode in tip-top shape always seems to be at the top of the to-do list this time of year. Sometimes it can be difficult to get that cleaning done, though, especially when it's busy like this, or cleaning just isn't your thing.

Enter the Roborock S7 Ultra robot vacuum and mop combo. This nifty gadget can take care of two time-consuming chores for you while you're out getting holiday groceries, those last couple of gifts, wrapping the presents, or just simply taking a much deserved break to enjoy the season. Plus, it's self-emptying and refilling, and the mop feature has auto dry and wash functions, which will save you even more time when you go to clean out the canisters.

It's a bit pricey, we won't lie, but for some of us, the price is well worth it. Check it out on Amazon today.

WFH Strategies
that actually work

We all value a healthy work and family balance. There's no denying, though, that during the holidays, that scale tends to weigh more towards family - and rightfully so. That's what holidays are all about, right?

No one ever wants to be the office jerk who tells their employees "No" to flexible schedules, but with end-of-year deadlines hanging over our heads, it's sometimes hard to see any other option. That's where working remotely could really be a useful tool for your business. Working remotely is like having your cake and eating it, too; you as the leader are ensuring your company remains productive and that deadlines are met, while also giving your people some wiggle room as to where and what time of day they may be working so that they can still enjoy being with their families. Still, it's entirely appropriate to ask your employees (and yourself) to not eat the cake off the floor or in bed. What we mean is that to support your employees' productivity and the company's security, make sure you're implementing some Work From Anywhere (WFA) best practices. Just as they should eat their real cake at a table, if your employees are going to work from home, their vacation rental, or even Grandma's basement, they need to check that their setup meets simple expectations before taking their work out of the office.

WFH/A Best Practices:

Have a Decent Internet Connection
Most video calls require at least 5 Mbps, but 50-100 Mbps ensure multiple people can stream at once without issues.

Access Shared Company Resources
Make sure employees have tested their connection off your company's network BEFORE they leave, most ideally from the location they are planning to be working from. Can they access the VPN? Are their login credentials stored safely in a password manager? Make sure everything they need to do their job is still accessible to them.

Have a Place to Work
Preferably a room with a door (that closes... and locks). As adorable as Grandma is, no one wants her crashing a Teams meeting to bring you Christmas cookies and a sweater. They need to have a space where they can actually focus and get their work done. Noise-cancelling headphones are also an excellent suggestion for them to take along. You may even consider adding these as part of the equipment you provide your employees to work remotely if you offer that benefit frequently.

Agree on Core Working Hours
If your employees are working remotely (not taking vacation), make sure they've agreed to be available at certain times, including team meetings. Yes, this may mean they can't watch their kids and should have child care set up.

Have a Project
Especially for short-term WFH situations, having a clearly outlined deliverable is an easily tracked productivity metric. They either got it done, or they didn't.

Have a Cyber Security Policy According to Tenable's survey, 98% of remote workers use a personal device for work every single day. A cyber secuirty policy includes all aspects of your company, not just remote work. However, remote work is unique, and you may need to take extra steps to protect your business if you allow it.

This includes installing security software on devices and enforcing multifactor authentication on their device, on work applications, and when accessing the company's network. Train your team on at-home security, like how to spot phishing emails, create strong passwords, and keeping kids or other family members away from work devices.

Three Cyber Security Threats *your team MUST know about*

Your employees are you first line of defense in cyber security and their training is as crucial as the cutting-edge tools you've invested in. Are you overlooking this vital element?

We strongly advise you make an ongoing commitment to regular cyber security training for every single one of your team members. That means keeping them up to date on the latest cyber threats, the warning signs to look out for, and, of course, what to do should a situation arise.

If you're not already doing that, arrange something now (we can help!)

While you wait, here are three urgent cyber threats to address right away:

Admin attack: Email addresses like "info@" or "admin@" are often less protected due to perceived low risk. But several teams may require access to these accounts, making them an easy target. Multifactor Authentication (MFA), as simple as using a smartphone, can double your security. Don't neglect it.

MFA fatigue attacks: MFA can feel intrusive, leading employees to approve requests without scrutiny. Cyber criminals exploit this complacency with a flood of fake notifications. Encourage your team to meticulously verify all MFA requests.

Phishing bait: Phishing remains a top threat. Cyber criminals mimic trusted sources with deceptive emails. Teach your team to inspect email addresses closely. Implementing a sender policy framework can also enhance your protection.

Cyber security training doesn't have to be tedious. Try simulated attacks and think of them like an escape room challenge - fun, yet enlightening. It's about identifying vulnerabilities, not fault-finding.

Don't exclude your leadership team from training. They need to understand the response plan in case of a breach, much like a fire drill.

Training your staff is not just smart - it's crucial. If you need help getting started, get in touch today. We can help you put together a training program best suited to your needs and company environment, as well as a response plan.

Did You Know

Edge is stripping features to keep up with Chrome?

In another bid to tempt Google Chrome fans over to Edge, Microsoft is removing features.

Sounds counterproductive, right? But some of its less popular (read 'failed') features have left the browser a little bloated and overcrowded. These are the features that are being deprecated:

Math Solver
Picture Dictionary
Citations
Grammar Tools
and Kids Mode

New to Windows 365

New features are coming to Microsoft 365 on Android

Microsoft has updated its Android interface, adding features to promote Bing Chat, Edge, and Microsoft 365. You can now access options like 'Search in Edge', 'Bing Search', and a new 'Microsoft 365 Note' feature when selecting text in apps like Gmail.

However, this update has hidden some essential features like 'copy' and 'select', particularly on Samsung phones. You can work around this by selecting 'copy' in the extended menu.

5 Habits Your Remote Workers *should always practice*

Remote work has become a way of life very quickly, hasn't it? Loads of businesses and their people are reaping the rewards of flexibility and convenience. With the holidays coming up, you may see even more people requesting to work remotely.

But, working remotely also brings cyber security challenges that demand your attention. Of course, this should always be a concern, but when you have employees working from home, a coffee shop, or anywhere else for that matter, you need to make sure they're making wise decisions that put the security of your data at the forefront.

In addition to what we covered in our WFH Strategies article earlier in this newsletter, here are 5 habits that your remote workers should adopt straight away:

Choosing your work location wisely. Working from a favorite coffee shop or a picturesque park may seem like a dream come true, but it can expose you to more cyber security risks. Over-the-shoulder attacks, where cyber criminals discreetly snoop on your screen in public spaces, might seem unlikely, but they have real potential to lead to data breaches. Employees should choose to work in quieter, more private settings to minimize this risk.

Beware of public Wi-Fi. Public Wi-Fi networks are a common breeding ground for cyber threats. If your people must work from a public place, ask them to avoid connecting to public Wi-Fi. These networks can be less secure and make you vulnerable to hacking. Instead, use your phone's hotspot for a safer internet connection. Bonus: use a VPN (Virtual Private Network), as it encrypts data.

Invest in security software. These serves as a protective shield against malware and cyber attacks. It's a valuable addition to both company-provided and personal devices. Not only does it safeguard business data, but it can also shield your personal information, such as credit card details and sensitive documents. In our opinion, this should be a non-negotiable term of working remotely. If you provide your employees with devices, this software needs to be provided and maintained properly by you and your IT team. If you allow employees to work remotely from private devices (which isn't our favorite thing, but we know it's sometimes the best option), you can't force them to install software onto their own devices, but you can - and should - reject remote working requests until a secure device can be obtained.

Keep everything updated. Regularly updating all your devices is not just about gaining access to new features; it's also about staying secure. Software updates contain crucial security fixes that patch vulnerabilities. Remember, it's not just laptops and phones that need updating, but also routers and any IoT (Internet of Things) devices connected to your network.

Manage household risks. Even within the confines of their homes, computers hold sensitive business information. If your employees have housemates, children, or other family members sharing their space, ask them to consider implementing parental controls and other appropriate precautions to prevent accidental data breaches.

By adopting these smart habits, as well as taking the right security measures, you can let your people enjoy the benefits of remote work - while everything stays safe and secure.

Technology Update

New battery-saving features coming to Windows 11

Microsoft has introduced a new Windows 11 preview build with some exciting features.

The Snipping Tool has a combined capture bar for easy screenshot and video switching, including voiceovers. And Notepad gets an auto-save feature, eliminating prompts and restoring content when you reopen it.

These updates aim to improve usability and battery life for people using Windows 11. While they're only in preview now, we expect to see a general release after testing.

Who will be your November Quiz Champ?

Loser sacrifices their leftover Halloween candy!

1. **Mozilla Firefox originally launched under what name?**
2. **What is Google's Android mascot officially known as?**
3. **A "platform upgrade" involves swapping which core PC components?**
4. **When was the first SMS text message sent?**
5. **Who coined the term "Artificial Intelligence" (AI)?**

The answers are on page 8.

Question: I'm still using the original version of Windows 11 (21H2), should I upgrade?

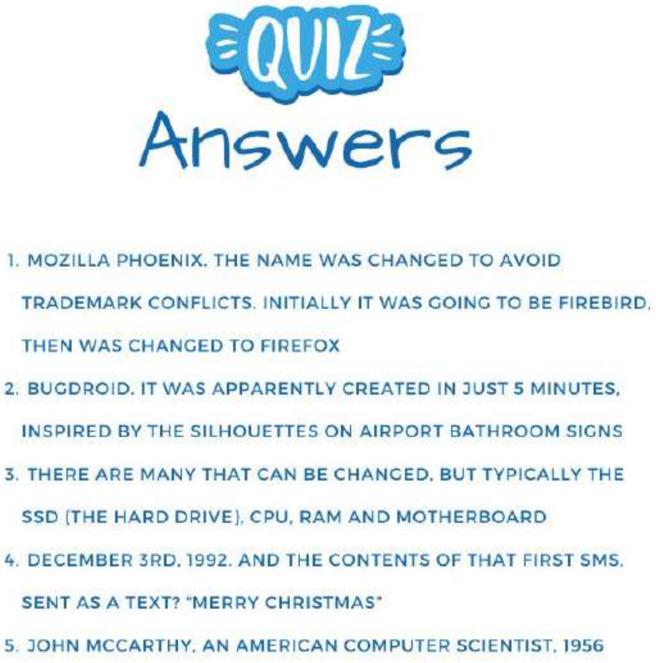
Answer: Yes! Upgrade to 22H2 as soon as possible. Support for 21H2 ended last month (October 2023). That means there will be no further updates and you may be at increased security risk.

Question: I've had an email to say a recording of a Teams meeting has expired and been deleted. Is there any way I can recover it?

Answer: Don't panic. Go to your Recycle Bin, find the recording, and hit 'restore'. Remember, though, you only have a 90 day window to do this. Once the recording is recovered, it is no longer subject to automatic expiration dates.

Question: Will Google penalize my website if I use ChatGPT?

Answers: No. There's no reason to worry about Google penalties when using ChatGPT for your website content. Chatbots don't negatively affect the SEO of your website. But do get a human to review everything written by AI, to ensure it reads well, is factually correct and that it makes sense.



QUIZ Answers

1. MOZILLA PHOENIX. THE NAME WAS CHANGED TO AVOID TRADEMARK CONFLICTS. INITIALLY IT WAS GOING TO BE FIREBIRD, THEN WAS CHANGED TO FIREFOX
2. BUGDROID. IT WAS APPARENTLY CREATED IN JUST 5 MINUTES, INSPIRED BY THE SILHOUETTES ON AIRPORT BATHROOM SIGNS
3. THERE ARE MANY THAT CAN BE CHANGED, BUT TYPICALLY THE SSD (THE HARD DRIVE), CPU, RAM AND MOTHERBOARD
4. DECEMBER 3RD, 1992. AND THE CONTENTS OF THAT FIRST SMS, SENT AS A TEXT? "MERRY CHRISTMAS"
5. JOHN MCCARTHY, AN AMERICAN COMPUTER SCIENTIST, 1956

WCI TECHNOLOGY SOLUTIONS

81 Mill Street, Suite 300
Gahanna, OH 43230

@WCITech

WCI Technology Solutions

@WCITech

Airline Ticket Scams are Soaring

Scammers love travel season. They know your eyes are peeled for a cheap ticket and have devised convincing ways to get their hands on your money. Tricked consumers have spent months of their lives dealing with the consequences of these scams and lost thousands of dollars in the process.

In a recent plague of travel scams, criminals are pretending to be "travel agents" selling plane tickets. Between 2020 and 2021, digital fraud in travel and leisure increased 68.4% globally, according to TransUnion's 2022 Global Digital Fraud Trends Report.

How Plane Ticket Scams Work

Travel scammers use a handful of tactics to steal your information. They create fake websites, pose as travel agents and send you "confirmation" emails that don't include an airline ticket. Some call your phone to "confirm your information" for a flight, asking for your credit card, bank or personal information. Or they use social media ads or emails advertising free or cheap tickets. These are all major red flags to watch out for. Before clicking or booking anything, pay attention to these travel tips to avoid getting scammed out of thousands of dollars of your hard-earned vacation savings.

Here's How to Avoid & Identify Travel Scams:

Always verify that an agent or agency is legit. **In the U.S. and Canada, you can use the Better Business Bureau (BBB) or travel associations like the International Air Transport Association to verify agent credentials. Read customer reviews and look for weird grammar errors in emails and on websites. However, the BBB recommends booking directly through hotels or airlines.**

Check for a ticket confirmation number. **If you don't get a ticket number with your confirmation email, a scammer may have reserved you a seat instead and stolen your money.**

Watch out for online deals. Scammers use fake emails and ads to boast amazing deals on hotels or flights. If you think they are too good to be true, they are.

Be skeptical of "confirmation calls". If you get a follow-up call from an agent to verify your personal information, it's probably a scam.

Stay informed, pay attention and implement these practical tips for your next adventure.

Safe Travels!