

## What's New

### Android Has A Big Problem And You Need To Know About It

Android is the most popular mobile platform in the world. Because of this, it's also the target of countless hackers and cybercriminals who want to break into the platform and exploit its users.

As Android ages, fewer people upgrade to the latest version of Google's mobile operating system. They don't upgrade because their devices don't support the latest updates or their phone manufacturer (or service provider) is slower to roll out updates to its users. These updates are critical to keeping users safe from outside intrusion.

However, these problems are only the tip of the iceberg for Google. Many phone makers – particularly Chinese phone makers like Xiaomi, Oppo, Vivo and Huawei – are either in the process of adopting a new operating system that is not Android or thinking about it. It could mean Android's dominance is starting to fade, and we could be looking at a future with a little less Google in our lives.

*Forbes, May 14, 2021*

## August 2021



This monthly publication provided courtesy of Frank M. DeBenedetto, President of TRTG.

“As a business owner, you don't have time to waste on technical and operational issues. That's where we shine! Call us and put an end to your IT problems finally and forever!”



## Don't Let The Dog Days Of Summer Wreak Havoc On Your Technology

Heat and technology don't mix. We're talking about things like PCs, servers and everything inside of them. A lot of manufacturers try to make sure the heat generated by hardware has a way to escape, but it's not always enough. And what about heat from the *outside*? This is where problems can really get out of control.

Right now, we're in the dog days of summer. The temperatures are high and air conditioners are running at full capacity in an attempt to keep us cool. As you run your business, your technology is running and generating its own heat, as well. If it can't keep cool, the end result can be disastrous.

### Why Every Business Should Take Heat Seriously

Smaller devices like laptops, tablets and more compact desktop computers are especially susceptible to heat damage simply because they

are not as efficient at removing heat internally. As they heat up, their performance degrades. If they get hot enough, it can cause irreparable damage. Most devices will automatically shut down if they get too hot – you want to avoid getting to that point as much as you can.

Overheating can also cause damage to specific components. There have been reports of graphics cards catching on fire due to heat and heat-caused electrical issues. Heat can also destroy CPUs. While CPUs are designed to withstand the high temperatures created by processing data, they have their limits. If the computer is forced to overwork as it tries to stay cool, the end result can be a melted CPU!

To make matters worse, as heat intrudes on your devices, they will struggle to function correctly. For example, you may even start to

*Continued on pg.2*

*Continued from pg.1*

notice slowdowns when using your laptop. Programs may take forever to load, and they may even freeze, leaving you without a way to work!

For any business, this can be devastating. When you're dealing with clients and customers, the last thing you need is for your systems to fail. Suddenly, productivity falls through the floor, and you're left scrambling as you try to figure out what to do next. It can bring your business to a standstill.

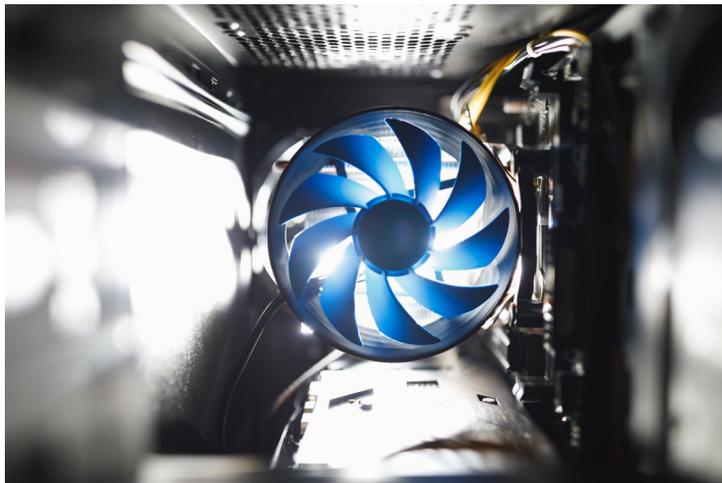
*But it doesn't end there!* If your systems overheat – either due to internal issues (such as inadequate heat dissipation), external issues (summer temperatures) or a combination of both – you could lose valuable data. Heat is a common cause of data loss. Heat can damage hard drives and solid-state disk drives. If you don't have an off-site backup (whether it's local or cloud-based), that data may be lost forever.

And if you lose that data, it can be *incredibly* costly to get your business back up and running. It's not only data lost, but also it's time and money lost. It can be as devastating as a data breach or cyber-attack and can leave you with few options.

### What Can You Do?

First, it's important to assess your cooling needs. Does your business have adequate air conditioning? If you have a data or server room, does that have adequate air conditioning? Look at individual devices – do they have adequate cooling or do they need to be supplemented?

**“If the computer is forced to overwork as it tries to stay cool, the end result can be a melted CPU!”**



Second, assess your data security needs. Do you keep all of your data on-site? In the event of an emergency, and if your data is compromised, do you have a contingency plan? Do you regularly back up your data?

There are a lot of questions to consider, but they're all important. Your data and the health of your

business is top priority. If you have questions about your technology cooling needs – as well as data protection and backup – consider partnering with a managed services provider (MSP) or an

experienced IT services firm. They can help you solve all of these problems and get you through the dog days of summer like it's nothing!

## Free Report: What Every Small-Business Owner Must Know About Protecting And Preserving Their Company's Critical Data And Computer Systems

### PROTECT YOUR NETWORK

“What Every Business Owner Must Know About Protecting and Preserving Their Network”



Don't Trust Your Company's Critical Data And Operations To Just Anyone!

This report will outline in plain, nontechnical English the common mistakes that many small-business owners make with their computer networks that cost them thousands in lost sales, productivity and computer repair bills and will provide an easy, proven way to reduce or completely eliminate the financial expense and frustration caused by these oversights.

To claim your free Report

Send your request to [kmarquez@tworivertech.com](mailto:kmarquez@tworivertech.com)

## Shiny New Gadget Of The Month:



## See The World A Little Closer With StarScope

There's something magical about having the ability to bring the world a little closer to you. But the StarScope Monocular isn't magic – it's all science! The StarScope is a compact monocular featuring 10X magnification that can deliver high-quality optics directly to your eye or your smartphone! The StarScope can be attached to virtually any smartphone camera to improve the zoom function, giving you stellar photos. Even better, the StarScope is compact for easy travel; just put it in your pocket or bag and go. And you don't even have to worry about the weather – it's waterproof, fog-proof and ready for your next adventure. Check it out at [Bit.ly/3opQIhz](https://bit.ly/3opQIhz).

## 3 Types Of Questions You Should Never Ask As A Leader Of A Major Company

At ghSMART, we make it our mission to advise CEOs and other leaders of large companies on the biggest, most important decisions that they face – the decisions that can make or break a business. How do we do that, exactly? Well, without getting into the weeds, we usually guide our clients through their decision-making process by simply helping them ask the right questions.

The “right questions” are typically the kind that get to the heart of the issue. They produce answers, and thus actions, that lead to the best possible outcome from the initial decision. However, where there are “right questions,” there are also wrong questions that can lead to crippling initiatives that could affect an entire business. If you don't want that for your company, here are three common types of wrong questions that you should avoid:

### 1. Questions Having To Do With Potential Ethical Dilemmas

In my experience, some of the wisest leaders in business are the ones who, when faced with a potential ethics question, respond the same way: “If you have to ask, then don't.”

What I mean by that is if there's even a shadow of a possibility that saying “yes” to a question about business leadership could propel you into morally gray territory, then it's not a question worth asking at all. In fact, even if your decision could be misinterpreted as unethical, you should avoid the question. At ghSMART, we call this practice “having 110% integrity” – 100% for avoiding ethical dilemmas, and an extra 10% for avoiding dilemmas that could even just seem to make your company appear unethical. In summation, if you ever have to ask, “Would it be ethical if ...” then it's better to leave the question unasked.

### 2. Questions About Whether Someone Is Underperforming

A good rule of thumb for underperformance is this: if you ever question whether someone is underperforming in service to your team's vision, they are absolutely underperforming. Subordinates typically follow a fairly predictable

work pattern – one that pretty clearly indicates their strengths and weaknesses. If you catch yourself asking, “I wonder if so-and-so will ever rise to the challenge and display qualities and strengths I haven't seen yet,” then the answer should be clear. Their strengths do not match the role they are in, and you should probably find someone more suited for their role and your vision.

### 3. Questions About Whether You Can Trust Your Boss

I've heard it said that people don't quit companies, they quit bosses. I think that line of thinking has a lot of truth to it. If you have to ask if you can trust the person you're working for to look out for your best interests and the best interests of your company, then you probably can't trust them. You should find a boss who cares about your career goals and who will help you succeed and accelerate toward them. If you don't have that kind of leadership, it might be best to look elsewhere for work.



*Dr. Geoff Smart is the founder and chairman of ghSMART, which helps Fortune 500 companies, CEOs and successful entrepreneurs alike make smart decisions when it comes to curating talented teams. For three consecutive years, Forbes ranked ghSMART as the best management consulting firm in its industry, and it has produced three best-selling books outlining their principles. Additionally, Dr. Smart published Leadocracy: Hiring More Great Leaders (Like You) Into Government, which was a New York Times best seller.*

## Services We Offer

*Cloud Services ~ Managed Networking Services  
Cybersecurity ~ Hosted Voice over IP*

# TRTG Happenings



## Ransomware Attacks Surge in 2021

Ransomware is a particularly nasty form of cyber extortion perpetuated by bad actors typically in third world countries. When a system is compromised, all the files on the computer (Word, Excel, PDFs, etc.) are encrypted and rendered unreadable. The demand to decrypt the files can range from thousands to millions of dollars and is payable in untraceable cryptocurrency such as Bitcoins.

Two recent ransomware attacks by the same cybercriminal gang called REvil were carried out on the Colonial Pipeline and the world's largest meat packing plant, JBS.

Those two breaches resulted in almost \$15 million dollars being paid in ransom.

<https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password>

<https://www.wsj.com/articles/jbs-paid-11-million-to-resolve-ransomware-attack-11623280781>

**This event comes right after another significant security concern called PrintNightmare.** The vulnerability was uncovered last week after security researchers accidentally published a proof-of-concept (PoC) exploit. While Microsoft hasn't rated the vulnerability, it allows attackers to remotely execute code with system-

level privileges, which is as critical and problematic as you can get in Windows. Microsoft is working on a patch, but until its available the company recommends disabling the Windows Print Spooler service.

<https://www.theverge.com/2021/7/2/22560435/microsoft-printnightmare-windows-print-spooler-service-vulnerability-exploit-0-day>

**With that said, we are STRONGLY encouraging our clients to begin backing up their local workstations.** In the past, we focused mainly on backing up our client's data which is stored on the cloud in either OS33 or Microsoft Office 365. With ransomware, however, your local computer may need to be restored to a point in time prior to an attack. Without a backup, we would be forced to reinstall the entire computer which could easily triple the time it would take to recover.

Our Workstation Cloud Continuity backup product by Datto eliminates data loss and will help our clients get their employees back up and running quickly. This reliable, image-based, all-in-one BCDR solution provides backup direct to the Datto Cloud, screenshot verification, and multiple layers of recovery capabilities including Bare Metal Restore, Rapid Rollback, and File/Folder Recovery. In the event of a lost or stolen PC, ransomware attack, or other disaster, we can quickly and easily get our customers up and running, exactly as they had been before.

We will be making Workstation Cloud Continuity a requirement for all new clients going forward as we feel it is that important in our overall cybersecurity strategy. Again, this may seem like a belt and suspenders approach, but this is designed to minimize the time it may take for recovery should that day ever come.

To our valued clients, we appreciate your patience while we navigate through the latest threats. We will continue to communicate with you as they evolve and, as always, we will continue to keep cybersecurity at the top of our priority list.

## IT Security Tip of the Month

You'd like to access the company website or a site for one of your vendors from work. When you click on your favorite browser, it opens to your homepage: msn.com, yahoo.com, aol.com, espn.com... You get the point. You then select the bookmark for the desired website and go. BIG problem! Most websites these days have tracking cookies, microdots and other advertising and data-collection bots that sit on them. These little spies are now following you across your browser session. Be careful with your information. Web portal sites like I listed are filled with ads, and the site's overhead is paid for with information they get from you.

1. Consider changing your homepage to something like <https://startpage.com/>. They don't spy.
2. Always open a new browser tab when navigating to a new website. Close the last one to keep things tidy after the new one loads.
3. Consider using add-ons in your browser to cut down on ads and spies. Not sure how? Ask us.

