



# Dimensional Dispatch

7th Dimension  
Newsletter

7th Dimension  
5005 Windplay Drive, Ste. 1  
El Dorado Hills, CA 95762  
(916) 221-0855

October 2018

"INSIDER TIPS TO MAKE YOUR BUSINESS RUN FASTER, EASIER AND MORE PROFITABLY"

IN THIS ISSUE

## You're Better Off Giving Your Employees A \$1,000 Bonus Than Being Cheap With Technology

Imagine you're the CEO of a scrappy, promising new start-up. In the beginning, it's just you and two other employees working on dinky PCs out of a 12-by-12-foot office—but times are picking up and the company is heading into the uncharted waters of rapid growth.

As the business moves into the public eye — and, in turn, the hungry eyes of potential hackers — it's become obvious that you're going to need to lock down your data. At this critical stage, a cyber-attack could mean the death of everything you and your team have built.

But the budget is looking lean. Everything you've done so far has been by the skin of your teeth, so why should security be any different? You put one of your more tech-savvy employees on the case, tasking him with finding the

cheapest cyber security solutions available. Sure, he may not be an expert, but he understands computers. What could go wrong?

He scours the web, perusing dozens of "Top 5 Cheap Firewall Software" articles, and, with the help of a scrappy how-to guide, installs what seems to be the best of the lot on your servers and across all your computers. The entire process takes 10 hours, and costs next to nothing.

Potential crisis averted, you turn your attention to other matters. You think, "we'll revisit our cyber security later, once we have a little more financial wiggle room."

Across the following year, the company's success skyrockets—

(Continued on page 2)



### Never Throw Your Boarding Pass Away!

Read why your boarding pass is a security risk.

Page 2



### Google Is Tracking Your Location

What happens when you turn location settings off?

Page 3

(Continued from page 1)

business is flooding in and your profit margin is exploding. You even ended up snagging a feature in Entrepreneur magazine.

Your company is the envy of all your peers. That is, until the day that you get hacked.

One morning, an advanced strain of ransomware easily sidesteps your free antivirus and starts wreaking havoc. It slithers through your systems and locks you out of everything, from client data to basic Word documents, and encrypts it behind a paywall, demanding \$50,000 in Bitcoin or you'll lose access to all of it — forever.

This may sound like nothing more than a horror story, but in reality, this happens to business owners every day. An IBM security study from last December discovered that over half of businesses surveyed had paid over \$10,000 in ransomware payoffs, with 20% paying over \$40,000. That's not even including the millions of dollars of damage caused by other forms of malicious software every year. The fact is, when your time, money and business are on the line, it simply doesn't pay to be cheap when

choosing your cyber security technology.

Think of it this way. Say, with your free antivirus, you're "saving" \$100 a month.



Lo and behold, a virus manages to punch its way through and causes chaos throughout the company server. Even if you're lucky and it isn't ransomware, by the time you've managed to expunge the stubborn virus from your business, you'll have put in countless man-hours, guaranteed to cost you more than that \$100 a month. You'd be better off giving each of your employees a \$1,000 bonus!

Free antivirus software, giveaway cyber-protection, or a \$5 firewall seems like a great idea, until a hacker cuts through your company's defenses like a warm knife through butter. These guys love

when they see these outdated, cheapo barriers guarding your priceless data — those are the paper-thin defenses that keep hackers in business. You wouldn't buy a rusty, secondhand old lock for your house, so why are you installing primitive cyber security software to protect your most precious company resources?

In today's world of rampant cybercrime, it's inevitable that somebody will come knocking at your digital door. When that day comes, do you want a free piece of software that you saw on LifeHacker, or a tried-and-tested, up-to-the-minute, comprehensive security solution?

Don't be shortsighted and risk everything just to save a quick buck. Invest in your company's future, and protect yourself with the most powerful tools on the market.

**READY TO SCHEDULE  
YOUR NEXT IT  
ASSESSMENT?  
CALL US AT (916) 221-0855**

## NEVER Throw Your Boarding Pass Away, Not Even After Your Flight



Everybody knows that a boarding pass is mandatory in order to board a plane. While we're in the airport, we keep a close eye on our boarding passes, clutching them in our hands like they're precious gems. But after we land, pretty much everyone ditches the ticket, whether it's lost on the floor, compacted in the washing machine or thrown directly into the trash.

This may seem innocent enough, until you realize the abundance of personal information encrypted on your pass. You'd be amazed at the information a person can glean just by scanning the QR code on the ticket: your home and e-mail addresses, your phone number and even your bank information! When you get rid of your next boarding pass, shred it. Your bank account will thank you. (Luxuryandqlamor)

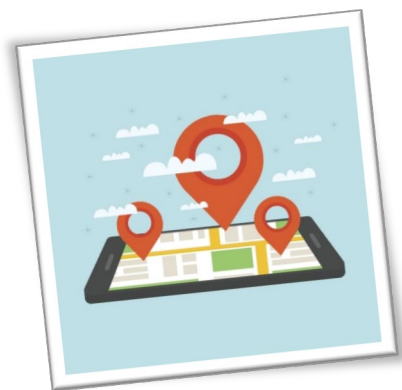
# Google Is Tracking Your Location

Shock horror – it appears Google can track the location of anyone using some of its apps on Android or iPhone even when they’ve told it not to.

That’s according to an “exclusive” from the Associated Press (AP) which describes how Google’s ability to record a user’s location history goes deeper than many realize.

Officially, Android users can turn off tracking using a slider button in the Location section under Settings. Once deactivated, Google no longer stores a timeline and a precise record of a user’s movements when they take their Android device (or iPhone running Google services and apps) with them.

But according to AP’s research, turning off Location History doesn’t stop certain Google apps (Maps and Weather for instance) from storing a timestamped location when you open them.



Confusingly, this isn’t the same as Location Data, which uses a range of techniques (cell towers but especially Wi-Fi geolocation) to track where people are, sometimes to within a few meters.

AP quotes Princeton researcher, Jonathan Mayer, “If you’re going to allow users to turn off something called ‘Location History,’ then all the places where you maintain location history should be turned off. That seems like a pretty straightforward position to have.”

In 2017, a report from Quartz found that Android devices were still having their locations tracked via cell towers even after location history had been turned off, their SIM cards were removed and a factory reset had been initiated.

And it’s not just Google of course – numerous apps are at it, albeit after asking for permissions to do so. It’s not clear how many users decline or turn off location access for apps, but it’s likely to be a minority.

It’s a trade-off in the end. The usefulness of smartphones depends to some degree on navigation apps such as Maps, which require location data. Ditto apps that help to locate lost devices.

The lowdown is clear: if you own a smartphone, you can limit location tracking but for now you can’t turn it off completely. (Sophos)



## 7TH DIMENSION

IT without limits

5005 Windplay Drive, Suite 1, El Dorado Hills, CA 95762  
 (916) 221-0855  
[support@7thdi.com](mailto:support@7thdi.com)



*We love having you as a customer, and quite honestly, we wish we had more like you!*

Simply refer any company and earn up to \$100 when your referral becomes our client.