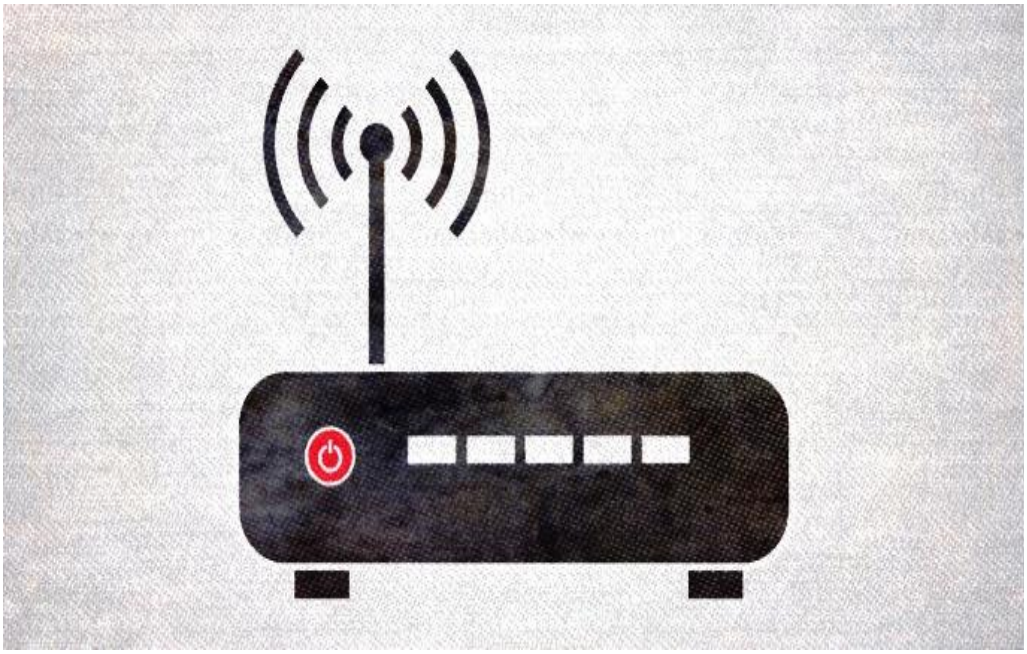

Dimensional Dispatch

7th Dimension

7th Dimension

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

IN THIS ISSUE

Tech News for June 2018

This June, the latest updates include how to Uber and connect online securely.

Uber Panic Button

In April, Uber announced that it was preparing to add direct 911 calling to its app. This June the feature is available to all riders.

The emergency button isn't the only addition to the app. You'll find that button in the app's new safety toolkit. The safety toolkit is accessible from the app's home screen while you're riding in an Uber. It includes a safety center where riders can check out Uber's policies to find out how drivers are supposed to behave. There's also a sharing option, which lets you send your ride details and location to a contact.

While 911 operators currently have a difficult time determining a mobile caller's location, Uber is working on a pilot program to deliver accurate GPS locations to 911 call centers.

VPNFilter

Hackers possibly working for an advanced nation have infected more than 500,000 home and small-office routers around the world with malware that can be used to collect communications, launch attacks on others, and permanently destroy the devices with a single command, researchers at Cisco announced late last month.

To date, VPNFilter is known to be capable of infecting enterprise and small office/home office routers from Linksys, MikroTik, Netgear, and TP-Link, as well as QNAP network-attached storage (NAS) devices.

Both Cisco and Symantec are advising users of any of these devices to do a factory reset, a process that typically involves holding down a button in the back for five to 10 seconds. Unfortunately, these resets wipe all configuration settings stored in the device, so users will have to reenter the settings once the device restarts. At a minimum, Symantec said, users of these devices should reboot their devices. That will stop stages 2 and 3 from running, at least until stage 1 manages to reinstall them.

Users should also change all default passwords, be sure their devices are running the latest firmware, and, whenever possible, disable remote administration.

Is your router and firewall protecting your business?

Call us at (916) 221-0855 to schedule a Security Review.

How to Keep Employees from Leaking Confidential Information

Read this for tips on keeping your company info top secret.

Page 2

How to Buy a New Phone This Summer

Use these tips when making your next smartphone purchase.

Page 3

How to Keep Employees from Leaking Confidential Information.

Back in 2014, Code Spaces was murdered. The company offered tools for source code management, but they didn't have solid control over sensitive information — including their backups. One cyberattack later, and Code Spaces was out of business. Their killer had used some standard techniques, but the most effective was getting an unwitting Code Space employee to help — likely via a phishing attack.

When it comes to cybercrime that targets businesses, employees are the largest risks. Sure, your IT guys and gals are trained to recognize phishing attempts, funky websites, and other things that just don't seem right. But can you say the same thing about the people in reception, or the folks over in sales?

Sure, those employees might know that clicking on links or opening attachments in strange emails can cause issues. But things have become pretty sophisticated; cybercriminals can make it look like someone in your office is sending the email, even if the content looks funny. It only takes a click to compromise the system. It also only takes a click to Google a funny-looking link or ask IT about a weird download you don't recognize.

Just as you can't trust people to be email-savvy, you also can't trust them to come up with good people still use birthdays, pet names, or even "password" as their passcodes — or they meet the bare-minimum standards for required passcode complexity. Randomly generated passcodes are always better, and requiring multiple levels of authentication for secure data access is a must-do.

Remember, that's just for the office. Once employees start working outside of your network, even more issues crop up. It's not always possible to keep them from working from home, or from a coffee shop on the road. But it is possible to invest in security tools, like email encryption, that keep data more secure if they have to work outside your network. And if people are working remotely, remind them that walking away from the computer is a no-no. Anybody could lean over and see what they're working on, download malware or spyware, or even swipe the entire device and walk out — all of which are cybersecurity disasters.

Last but not least, you need to consider the possibility of a deliberate security compromise. Whether they're setting themselves up for a future job or setting you up for a vengeful fall, this common occurrence is hard to prevent. It's possible that Code Space's demise was the result of malice, so let it be a warning to you as well! Whenever an employee leaves the company for any reason, remove their accounts and access to your data. And make it clear to employees that this behavior is considered stealing, or worse, and will be treated as such in criminal and civil court.

You really have your work cut out for you, huh? Fortunately, it's still possible to run a secure-enough company in today's world. Keep an eye on your data and on your employees. And foster an open communication that allows you to spot potential — or developing — compromises as soon as possible.

UNSURE IF YOUR NETWORK IS SECURE?

Contact us at 916-221-0855 or visit 7thdi.com to schedule our Network & Security Audit today!

Shiny New Gadget of the Month

Calling all **Nintendo fans**: the gaming giant is bringing back the NES Classic and the Super NES Classic Edition systems. "Fans have shown their unbridled enthusiasm for these Classic Edition systems, so Nintendo is working to put many more of them on store shelves," Nintendo said last year. If your inner child is rejoicing at the opportunity to play games like Metroid, Super Mario Bros. 3 and The Legend of Zelda, you can pick up your very own system on June 29th.

How to Buy a New Phone This Summer

With hundreds of options, this guide can help narrow your choices to choose the right device for your budget.

For the most part, a phone's cost lines up with its performance. Expensive handsets will have the "best" features, fastest processors and the most advanced cameras. You'll be able to do more on them, and brag to your friends.

Midrange devices are value plays that pack in pretty good features with a slight trade-off in speed, camera tools and nice-to-have extras that most people can live without. If you can happily spend your days without a curved screen or wireless charging, phones in this range will suit you fine.

Finally, low-cost phones are great options for people watching their budgets, first-time phone users and those looking for a secondary or backup device.

We have provided a list of things to look for when you are comparing items

Top tips:

Know what you care about most: Is it screen size, camera quality, battery life? This will help narrow down your choices.

Don't discount the midrange: You can get a great phone that does almost everything that a premium phone can do, for a fraction of the price.

Shop the sales: Look for deep discounts around major holidays. And find out your grace period in case you need a quick return or exchange.

Last year's phones are a great deal, too. Wait for this year's launch to get last year's phone for less.

Hold the phone at a store first: You may love or hate the way it looks and feels in person.

If you buy a global phone, make sure it works with your carrier bands first.

Have you already bought a lot of iPhone apps and iTunes movies? Stick with iPhone if you still want access to them. Likewise, if you've invested in any Android-only software, you'll want to stay on that side of the fence. Otherwise, it's simple enough to switch platforms.

Buy a case and glass screen protector: You'll protect your phone from costly damage, and will increase the phone's resale or trade-in value for when you're ready to move on.

Other features to consider:

- Camera quality
- Battery life and performance
- Water resistance
- Wireless charging
- Fingerprint scanner

Last but not least, remember you will be using this device every day. Choosing a device you like will lead to less headaches down the road. (cnet.com)

UNSURE IF YOUR CREDENTIALS ARE FOR SALE ON THE DARK WEB?

Contact us at 916-221-0855 or visit 7thdi.com to schedule our Dark Web Scan FREE of charge.
Contact us TODAY to get scheduled!

7TH DIMENSION

IT without limits

5005 Windplay Drive, Suite 1, El Dorado Hills, CA 95762
(916) 221-0855
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.