Dimensional Dispatch

7th Dimension Newsletter

May 2018

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

IN THIS ISSUE

Tech Updates for May 2018

Google and Microsoft release their updates for May.

Gmail Refresh

Google announced at the end of April, a major facelift for Gmail. While these new changes are primarily aimed at business customers using **G Suite**, many of them will be coming to the free consumer version of Gmail as well. Now, artificial intelligence can scan your email.

The update includes new security features, Smart reply, Nudging and High priority notifications. **Confidential mode** adds several new features to email that allow much more control over information after it leaves your inbox. You can even turn on two-factor authentication on individual emails. Messages can be further protected through **IRM**, or information rights management. That means an email can be tagged to not allow it to be forwarded, downloaded or even printed.

Smart Nudge reminds people if they didn't respond to an email after a set amount of days. **High-priority** notifications looks through your emails, determines what's important, and chooses which ones to notify you about. **Smart Reply** offers canned responses to emails. Users can shut off these features if desired.

Microsoft April 2018 Update

Microsoft's semi-annual update to Windows 10 is finally here and it's called Windows 10 April 2018 Update. By far the most exciting feature of the new Microsoft update released on April 30th is a feature called "**Focus Assist**." It allows users to keep notifications at bay in order to reduce distractions.

Focus Assist works like this: You can set times when you don't want notifications to bother you, such as during key work hours or when you plug in a second display for a presentation or when you're playing a game. During those periods, Windows will keep alerts to a minimum.

Another feature of this update is called "**Near Share**" which allows users to send movies, music and files from one nearby computer to another.

A bit of the trusted Disk Cleanup tool has made its way to Settings. Go to Settings > System > Storage and click **Free up space** now and Windows will run a scan of your drive and suggest which files you can remove to free up some needed drive space. (Cnet, 2018)

9-Step Checklist to Ensure Your Data Is Safe

With ever-increasing cyber-attacks, this quick to-do will get you geared up for 2018.

Page 2

Protect Your Smart Devices While Traveling

Use these tips when preparing for your next trip.

Page 3

9-Step Checklist to Ensure Your Data Is Safe

Summer is upon us… Time for a stroll in the park…softball…fishing…a few rounds of golf…

Yet how could you possibly relax if some random bit of malware, software glitch or cyber-attack catches you off guard just as you're walking out the door? A well-designed secure computer network gives you the confidence that "all systems are go," whether you're having fun in the sun, or just getting things done with your team.

Here's a quick nine-step checklist we use to ensure that a company's computer network, and the data for that business, is safe and secure from disruption, if not absolute devastation:

1. A written recovery plan. Simply thinking through what needs to happen when things go south, and documenting it all IN ADVANCE, can go a long way toward getting your network back up and running quickly if it gets hacked, impacted by natural disaster or compromised by human error.

2. Have a clear communication plan. What if your employees can't access your office, e-mail or phone system? How will they communicate with you? Make sure your communications plan details every alternative, including MULTIPLE ways to stay in touch in the event of a disaster.

3. Automate your data backups. THE #1 cause of data loss is human error. If your backup system depends on a human being always doing something right, it's a recipe for disaster. Automate your backups wherever possible so they run like clockwork.

4. Have redundant off-site backups. On-site backups are a good first step, but if they get flooded, burned or hacked along with your server, you're out of luck. ALWAYS maintain a recent copy of your data off-site.

5. Enable remote network access. Without remote access to your network, your staff won't be able to keep working in the event that you can't get into your office. To keep your business going, you need a way for your IT specialist to quickly step in when needed.

6. System images are critical. Storing your data off-site is a good first step. But if your system is compromised, the software and architecture that handles all that data MUST be restored for it to be useful. Imaging your server creates a replica of the original, saving you an enormous amount of time and energy in getting your network back in gear, should the need arise. Without it, you risk losing all your preferences, configurations, favorites and more.

7. Maintain an up-to-date network "blueprint." To rebuild all or part of your network, you'll need a blueprint of the software, data, systems and hardware that comprise your company's network. An IT professional can create this for you. It could save you a huge amount of time and money in the event your network needs to be restored.

8. Don't ignore routine maintenance. While fires, flooding and other natural disasters are always a risk, it's ever more likely that you'll have downtime due to a software or hardware glitch or cyber-attack. That's why it's critical to keep your network patched, secure and up-to-date. Deteriorating hardware and corrupted software can wipe you out. Replace and update them as needed to steer clear of this threat.

9. Test, Test, Test! If you're going to go to the trouble of setting up a plan, at least make sure it works! An IT professional can check monthly to make sure your systems work properly and your data is secure. After all, the worst time to test your parachute is AFTER you jump out of the plane.

BE CERTAIN THAT YOU HAVE ALL 9 STEPS FULLY COVERED WITH OUR FREE DISASTER RECOVERY AUDIT.

Contact us at 916-221-0855 or visit 7thdi.com to schedule our Disaster Recovery Audit FREE of charge, now through June 15. Contact us TODAY to get scheduled!

Shiny New Gadget of the Month

Snapchat launches Spectacles V2 that allows users to take photos and videos. The sunnies are underwater capable and lighter than the V1 predecessor. You can bring the carrying case with you to charge your glasses up to 4 times – and you don't need to bring your phone with you to use them. You can simply sync all of your photos and videos at your leisure. Available in 3 color options and customizable to fit prescription lenses, these upgrades may allow these camera glasses to become a success. One hindrance that many reviewers have pointed it out is that Snapchat has made it difficult to share the content to other apps such as Instagram or Facebook. You can own your very own pair of Spectacles V2 for $150 directly from Snap.

FAST FACTS

33%

According to a recent study, 33 percent of the 15 million Americans who have been victims of identity theft had their devices hacked while traveling, so it's very important to protect connected devices before taking off and while on vacation. (Experian, Survey Findings 2018)

43%

43% of Americans confirmed they use a public Wi-Fi connection to shop online. . (Experian, Survey Findings 2018)

50%

Half of Americans don't think they're likely to ever experience identity theft because they believe poor credit makes them unappealing targets. (Experian, Survey Findings 2018)

Protect Your Smart Devices While Traveling

Travel season is ahead of us. Use these tips to protect your privacy on your devices while on vacation.

Before Traveling:

1. Update your operating systems, apps, antivirus and firewall.
2. Enable passcode to unlock all of your devices.
3. Delete sensitive information and store it on a device at home.
4. Install Find My Phone or a remote wipe app to disable access in the event it is stolen.
5. Password protect files and folders.
6. Turn off tracking and Bluetooth if possible to prevent hackers from accessing your phone.

Before Traveling:

1. Disable Wi-Fi while you're not using it so your phone doesn't connect automatically to networks set up by hackers.
2. Avoid public Wi-Fi. Although using free public Wi-Fi seems convenient on vacation, it can come at a cost. Public unsecured networks are very vulnerable because any information transferred between your device and the computer you are accessing can be intercepted by anyone using the network. This includes everything from usernames and password to private personal data – even if the website you're accessing has an https address. Security experts recommend not using free public Wi-Fi at all.

After Returning:

1. Check your activity on social media to ensure there is no suspicious activity.
2. Review your bank account activity for any unauthorized purchases.

As a final note, be aware when traveling. Be careful who you trust to protect your privacy. (Stay Safe Online, 2018)

Want a free check of your information on the Dark Web?
Call us at (916) 221-0855 to schedule a Dimensional Dark Web Scan.

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.