Diversified Digital

DIVERSIFIED DIGITAL

DIGEST

THE 3D'S KEEPING YOUR DENTAL PRACTICE SAFE, SOUND & UP TO DATE

QUARTERLY JOURNAL • ISSUE 6 • SUMMER 2021

Issue 6 Summer Newsletter 2021

DarkSide: They may have you in their sight, Tech Tips: Cyber terms you may not know, Secrets for the perfect summer cook out, and much more!

Diversified Digital is excited to share our Quarterly Newsletter, which is specifically designed for your busy dental practice. We want to provide you with articles and information that can help you achieve your IT practice goals, helpful hints and tips for the staff, contests and humor to make you chuckle & smile!

We want this newsletter to be valuable for you. If there is something you would like to talk about, explain or share, email me with your request at lisa@diversifieddigital.com. We are here for you!

OUR PARTNERS:

BLACK TALON SECURITY · WatchGuard · Kaseya

CYLANCE · DUO · DELL

Microsoft Surface Pro · ergotron · Infrascale

ICWGROUP Insurance Companies · NOVASTOR · Venga

MFA The Next Level of Protection for Your Practice

Passwords continue to be a major headache for your practice and employees. Our brains are simply not designed to remember long, complex phrases-especially not more than one. This means that we are constantly tempted to take the easy way out and make them easy to remember, especially when we are required to share access of apps and services with our co-workers. Using easy passwords can lead you into possible trouble. We all have read articles about cyber-attacks in all forms of businesses. The new threats posed by cyber criminals is on the rise, it is no longer targeted for big businesses. The practice's data is worth three times as much as financial data on the black market, meaning that health care organizations are increasingly vulnerable to cybersecurity attacks.

Security is an ever-evolving challenge, and with Muti-Factor Authentication (MFA) this will add another layer of protection to each computer and your practice. MFA is a means for protecting data requiring multiple login credentials to access data or a software application. It is a tool used to verify that users are who they appear to be. According to a report released by Microsoft, by implementing MFA, organizations reduce their cybersecurity risk by 99.9%. The most common cause of cyberattacks stem from stolen login credentials.

In previous newsletters and mailings from Diversified Digital, we have talked about MFA and the added protection it will bring to your practice. Our staff has been working on the best way to provide that protection for you in the practice while making it as painless for you as possible. We have personally tested and used this process in our office to make sure it would work like it needs to for your practice.

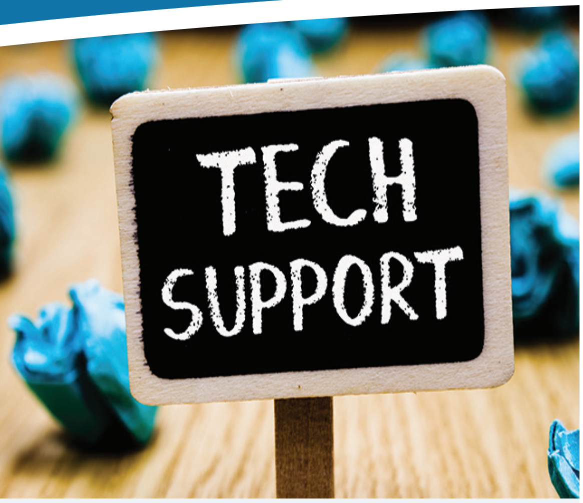
Our DD Security Suites include:

1. Firewall/Router
2. Endpoint EDR
3. MFA

Are you ready for another layer of protection with MFA? For more information or questions please call us at **Diversified Digital 888-734-3701**.

— WE WANT TO PROTECT YOU FROM THE BAD GUYS! —

Diversified Digital



Tech Tips: Cyber Security Terms You May Not Be Familiar With

Encryption: TA security method that makes information unreadable to anyone who does not have a key to decipher it; commonly used to secure online purchases and other transactions. When a website indicates it is "secure," that usually means the data you send and receive is encrypted.

Firewall: A hardware or software device, or both, that controls network access and communications between a network and the Internet, or between one part of a network and another.

Malware: Derived from "malicious software." Software designed to do harm by causing damage to systems or data, invading privacy, stealing information, or infiltrating computers without permission. Includes viruses, worms, Trojan horses, some keyloggers, spyware, adware, and bots.

Social Engineering: A method of deceiving users into divulging private information, social engineering takes advantage of our natural tendency to trust one another rather than rely solely on technological means to steal information. Often associated with phishing, pharming, spam, and other Internet-based scams.

Spoofing: Forging an email or instant message to appear as if it came from someone or somewhere other than its true source.

Spyware: Software that collects information about your computer and how you use it and relays that information to someone else over the Internet. Spyware ordinarily runs in the background, and in some cases installs itself on your computer without your knowledge or permission.

Trojan Horse: A malicious program disguised as legitimate software; often gives someone else the power to take remote control of your computer; may also attack data or systems. Unlike viruses and worms, Trojan horses cannot replicate or propagate themselves and therefore must rely on other methods of distribution.

What is a Phishing Kit?

Phishing kits make it easy for cyber criminals, even those with minimal technical skills, to launch phishing campaigns. A phishing kit bundles phishing website resources, and tools, that need only be installed on a server. Once installed, all the attacker needs to do is send out emails to potential victims.

Some phishing kits allow attackers to spoof trusted brands, increasing the chances of someone clicking on a fraudulent link. The common denominator among phishing attacks, is the disguise. The attackers spoof their email address, so it looks like it's coming from someone else. They set up fake websites that can look like ones the victim trusts, and use foreign character sets to disguise URL's.

There's a variety of techniques that fall under the umbrella of phishing. A couple of different ways to break attacks down into categories is, by the purpose of the phishing attempt. Generally, a phishing campaign tries to get the victim to do one of two things:

•Hand over sensitive information. These messages aim to trick the user into revealing important data — often asking for a username and password that the attacker can then use to breach a system or account. The classic version of this scam involves sending out an email tailored to look like a message from a major bank; by spamming out the message to millions of people, the attackers ensure that at least some of the recipients will be customers of that bank. The victim clicks on a link in the message and is taken to a malicious site designed to resemble the bank's webpage, and then hopefully enters their username and password. The attacker can now access the victim's account.

•Download malware. Like a lot of spam, these types of phishing emails aim to get the victim to infect their own computer with malware. Often the messages are "soft targeted". For instance, an HR staff with an attachment that seems to be from a job seeker's resume. These attachments are often .zip files, or Microsoft Office documents with malicious embedded code.

These were the top brands attackers used:

•PayPal 22%	•eBay 6%
•Microsoft 19%	•Amazon 3%
•Facebook 15%	

Other times, attackers might send soft targeted emails to someone playing a particular role in an organization, even if they don't know anything about them personally. Some phishing attacks aim to get login information from, or infect the computers of a specific person. Attackers dedicate much more energy to tricking those victims, who have been selected because the potential rewards are typically quite high.

There also are several steps you can take and mindsets you should get into that will keep you from becoming a phishing statistic, including:

•Always check the spelling of the URLs in email links before you click or enter sensitive information.

•Watch out for URL redirects, where you are subtly sent to a different website with identical design.

•If you receive an email from a source you know but it seems suspicious, contact that source with a new email, rather than just hitting reply.

•Do not post personal data, like your birthday, vacation plans, your address, or phone number on any on social media.

Article information from CSO – CSO provides news, analysis and research on security and risk management.

Famous Quotes

"The five most efficient cyber defenders are: Anticipation, Education, Detection, Reaction and Resilience. Do remember: "Cybersecurity is much more than an IT topic."
— Stephane Nappo

"If security were all that mattered, computers would never be turned on, let alone hooked into a network with literally millions of potential intruders"
— Dan Farmer

"It takes 20 years to build a reputation and few minutes of cyber-incident to ruin it."
— Stephane Nappo

2021 is The Best Year Ever for Section 179

The 2021 Section 179 deduction has been raised to $1,050,000 (that is one million, fifty thousand dollars). This means your company can buy, finance, or lease new or used equipment, and write off the full purchase price on your 2021 taxes. This can result in substantial savings.
To use Section 179 for 2021, the equipment must be purchased (or financed/leased) and put into service by midnight 12/31/2021. To claim the deduction, use Form 4562.

Tech Humor

HAVING MULTIPLE PASSWORDS DOESN'T SEEM TO STOP HACKERS, BUT IT SURE STOPS ME.
RETRY

JOKES:

Q: Why is the cell phone wearing glasses?
A: It lost its contacts!

Patient: Doc, I need your help. I am addicted to checking my twitter!
Doctor: I'm so sorry, I don't follow you.

MOVIE NIGHT QUIZ—Answers

1. Cool Hand Luke 1967.
2. Titanic 1997.
3. Moonstruck 1987.
4. Rocky 1976.
5. Jaws 1975.
6. Sudden Impact 1983.
7. Finding Nemo 2003.
8. When Harry Met Sally 1989.
9. The Sandlot 1993.
10. Dirty Dancing 1987

Secrets for the Perfect Summer Cookout

These easy ideas will help you host a perfect summer cookout! By doing some of these tips, I have been able to kick back, relax and enjoy the party too!

Clean the grill with an onion— Rub a cut onion on the hot grates and the enzymes in the onion loosen up baked up grime & grit while seasoning your grill.

Keep everyone comfortable— Keep a basket filled with everything your friends/guests might need: from bug spray & sunscreen to hand sanitizers. For an evening party even have a few lightweight blankets available and an outside hand washing station.

Keep things Mini— Instead of large burgers, mini burgers or sliders result in less waste and are easier to cook and serve. Fruits chopped into bite sized pieces are less messy to deal with and ready to eat at a party or cookout.

Use a Muffin/Cupcake tin for toppings— Serve a gourmet meal without too much fuss. A muffin/cupcake tin, regular or large size, makes a great multi-topping holder for things like ketchup, mustard, pickle relish etc. for hamburgers & hot dogs. If you have baked potatoes, sour cream, bacon bits, cheeses, and veggies fit easily. Taco bar items are easy if you put some jalapeno peppers, taco sauces, and beans in the tins. It's also great for a variety of toppings on ice cream sundaes.

Keep your drinks chilled— Who needs store bought ice? Be creative and use a blow-up kiddie pool from a dollar store for a cooler. Fill up with frozen water balloons to keep your drinks cold. Best part is you can have an impromptu water fight once the ice has melted. Small size balloons also work in a cooler! Another COOL idea…Pesky ice cubes water down your drink but we need them when its hot outside. Freeze juice, coffee, fruit, herbs, lemon juice, or just water and lemons into ice cube trays. These cubes will look stunning in your drink no matter what it is you're drinking.

Did someone say S'mores— Too hot for a fire but got a craving for s'mores, here is easy solution. Think outside the box and make sheet pan s'mores. Avoid all the mess and make a double batch because they will go fast. Check out the recipe I included below.

I hope you can use one or more of these ideas at your next get together!

Chocolate S'mores Bars from the Taste of Home

INGREDIENTS:

- ¼ cup butter, cubed
- 1 package *(10 ounces)* large marshmallows
- 1 package *(12 ounces)* Golden Grahams cereal
- 1/3 cup milk chocolate chips, melted

DIRECTIONS:

1. In a large saucepan, melt butter over low heat. Add marshmallows; cook and stir until blended. Remove from heat. Stir in cereal until coated.
2. Press into a greased 13x9 inch pan using a buttered spatula. Drizzle with melted chocolate. Cool completely before cutting.
3. Store in an air-tight container. You can also line your paper with parchment paper if you would prefer.

Enjoy!

Diversified
Digital

DIGITAL LLC?

We are an IT company that SPECIALIZES in Dentistry. At Diversified Digital we can provide you comprehensive solutions to meet your business goals.

Our team consists of highly trained professional technicians. Your calls will always be answered by a LIVE person during office hours by Lisa or Marlene.

Need help outside of business hours or on the weekend you can call our 888-734-3701 for assistance.

We oversee the entire office and network needs, from hardware and software to printers and Internet providers. We also provide 3rd party support.

We partner with Black Talon Security, Cylance, Kaseya, Watchguard and others to provide you with the best coverage for your practice.

The team at Diversified Digital are committed to provide the INDIVIDUAL care and service you need for your dental office.

Call us to find out how we can PARTNER with you to take the headache out of your IT worries at 888-734-3701 or email us at Don@diversifieddigital.com

*** For Your Information ***

Thinking of changing ISP (Internet Service Provider) or Phone Systems?

Please take the time to call us while you are in the planning stages for our advice to help make a smooth transition. There are times that we are needed on the day of the switch over and having that planned saves you a lot of frustration, possible down time and puts you on our schedule for that day.

Diversified
Digital

Creating a partnership for all your IT needs.

Follow us on Facebook for updates and more articles like these!

Small and Medium Businesses: DarkSide Has You in Their Sight

BLACK TALON
SECURITY
"HELPING YOU BUILD A MORE SECURE PRACTICE"

Gary Salman
Chief Executive Officer

As most of you are aware, a recent cyberattack crippled the Colonial Pipeline effectively stopping the flow of petroleum products to southeastern states. Somewhat terrifying, unexpected by many, but eye-opening for everyone. What does this attack and being a dentist have in common? Both are targets of a highly-effective ransomware group called DarkSide. These attacks result in the complete interruption of business operations for 1-2 weeks…oil/fuel for Colonial Pipeline and patient treatment for dental practices. Black Talon Security has, unfortunately, had to interact with DarkSide to recover stolen and encrypted data on numerous occasions.

One of the biggest issues we see in the dental technology space is that practices rely on generalists, your IT company, to protect their practice. Instead, they should be working with specialists, a cybersecurity company who is dedicated to providing advanced security solutions to protect your livelihood. Do you honestly believe your IT vendor has the knowledge and resources to protect you from a threat group that has the capacity to take down our national infrastructure?
The answer is **NO**.

These ransomware threats and data extortion groups do NOT care if you are a dentist or a large corporation such as Colonial. Every business is at risk. In the end, the cyber criminals can easily hit hundreds of dental practices and make $30,000+ per attack...Ultimately costing you $100,000+. Over the course of a few weeks, they can walk away with millions of dollars.

In a recent attack against an orthodontic practice, the threat actor indicated that they stole ALL the practice's data. The doctor did not believe them and asked for proof that they had their data. The threat actor sent us 12 photographs of 12-14 year old children who are patients of the orthodontist. You can only imagine the devastation that this orthodontist felt. He did not want his data sold on the Dark web and had to pay $30,000 for the decryption and deletion of his data. We all want to believe that this will never happen to us and that our IT company has us protected. Unfortunately, this is just not the case.

Please take this opportunity to really understand the threat landscape and learn from the unfortunate life-changing events that your colleagues have had to endure. You need to change the trajectory of this ransomware pandemic now by engaging with specialists to help you secure your life, your critical patient data, and your practice that you have worked so hard to build.

We are partners with Black Talon Security, if you would like more information call us at 888-734-3701

Movie Night Quiz

Now that the weather is better, and we are not sitting on the couch as much binge-watching movie and TV shows lets put your memories to a test! Below are famous lines from movies can you name the movie???

1. "What we have here is failure to communicate."
2. "I'm king of the world"
3. "Snap out of it"
4. "Yo, Adrain!"
5. "Your gonna need a bigger boat"
6. "Go Ahead, make my day"
7. "Just keep swimming"
8. "I'll have what she's having"
9. "Your killin' me, Smalls"
10. "Nobody puts Baby in a corner"

(Answers on page 2)

Help us **"WELCOME"** Daniel O'Grady to our team! Dan grew up on the west side of Cleveland and is a graduate of St. Edwards High School and Cleveland State University. He started as a software developer for Sherwin-Williams and then Modgility, from there he went to Lake Erie Electric as a systems technician before he joined us in April. He is married and enjoys golf, baseball, fantasy books and is a dog lover. Dan brings new talent to the Diversified Digital Team that will help us keep moving ahead of the bad guys to protect your practice and to continue to help your offices run smoothly.