Diversified Digital

DIVERSIFIED DIGITAL

DIGEST

THE 3DS KEEPING YOUR DENTAL PRACTICE SAFE, SOUND & UP TO DATE

QUARTERLY JOURNAL • ISSUE 8 • WINTER 2022

Issue 8 Winter Newsletter 2022

Antivirus Software: A Must for your Practice, Mobile Device Safety Tips, Start 2021 with Organizational Tips, 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's something you would like to talk about, explain or share, email me with your request at lisa@diversifieddigital.com. We're here for you!

OUR PARTNERS:

Cybersecurity Myths – Busted

(Excerpts taken from The Hacker News)

Even with the growing awareness about cybersecurity, many myths are prevalent. These misconceptions can be a barrier to effective security. The first step to ensure the security of your business is to separate the false information, myths, and rumors from the truth.

Myth #1 Too much security diminishes productivity. The common idea is that increased security makes it difficult for employees to access what they need, not just the hackers. Strict security policies such as regular monitoring and access control can hinder productivity at work.

Truth: Enhanced cybersecurity can boost productivity. The modern cybersecurity approach uses security tools with built-in security features that integrate seamlessly into your system.

Myth #2 Cyberattacks are only caused by external threat actors. Insider threats are on the rise and can include employees, vendors, business partners OR an external intruder trying to impersonate them.

Truth: Cyberattacks can very well start from someone you know. Use a combination of privilege and access management settings, along with security awareness training to educate your employees about the dangers and how to detect them.

Myth #3 Cybercriminals only attack large businesses. Small and medium-sized businesses are top targets for hackers, especially those with a collection of private information.

Truth: NO business-whether large or small, is immune to hacking and malicious attacks. Hackers DON'T discriminate when it comes to their victims.

Myth #4 Antivirus software or antimalware software is enough to secure your business. Antivirus software is essential, but it only secures one entry point. Hackers have many ways to bypass that software. Even if you have anti-malware in place, they have plenty of room for entry.

Truth: Antivirus software can only protect you from a unique set of recognized cyber threats, not from other emerging threats. You need much more to secure your data from hackers as a business. An all-encompassing security solution uses applications like Diversified Digital Security Suites that continuously monitors threats and provides end-to-end, twenty-four seven protection from cyber risks.

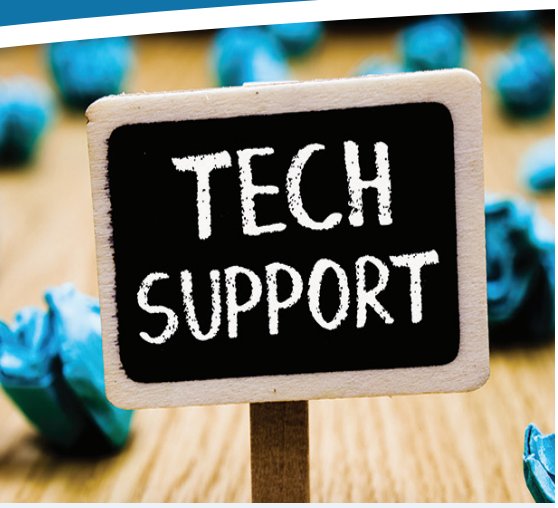
Myth #5 Cybersecurity is too expensive. The average cost of a data breach in 2021 is $4.24 million. This number does not include the damage from reputation or customer loss.

Truth: The cost of a good cybersecurity solution is nothing compared to the price of a successful attack. Invest in a solid security solution and take additional measures like strong passwords, multi-factor authentication, access management, and employee training.

Myth #6 You've achieved total cybersecurity. Cybersecurity is a continuous process that needs to be updated and changed to the threat landscape. Any business will always be susceptible to existing and emerging threats.

Truth: There is no such thing as total or perfect cybersecurity against cyberattacks. You could easily be the next target. It's vital to conduct security audits, review policies, and invest in upcoming updates in security methods to keep you as safe as possible.

Diversified Digital



Tech Tips: Definitions

Computer Security:
Also called cybersecurity, it's the protection of computer systems and information from harm, theft, and unauthorized use.

Cybercrime:
Any type of illegal activity undertaken on a computer, including network intrusion, identity theft, and spreading computer viruses.

Encryption:
The process of encoding data to prevent theft by ensuring it can only be accessed with a key.

Malware:
Short for "malicious software." Malware is a program developed to do harm to other computers. Types of malware include viruses, worms, and spyware.

Breach:
The moment a hacker successfully exploits a vulnerability in a computer or device and gains access to its files and networks.

Virus:
Malware aimed to corrupt, erase or modify information on a computer before spreading to others.

Pen-testing:
Short for penetration testing, this practice is a means of evaluating security using hacker tools and techniques with the aim of discovering vulnerabilities and evaluating security flaws.

How to Keep Your Printer in Top Condition

Printers are an essential machine in any office or business. Even though we're attempting to go digital, no one can deny the need for a well-functioning printer.

1. Keep your printer clean:
   Most printer issues are caused by dusty or dirty machines. Smaller parts are especially vulnerable.
2. Check for paper jams:
   Getting materials stuck in the printer will affect speed, and output quality. If left unaddressed, parts could easily get damaged. By carefully clearing a paper jam, you can save potential headaches or expenses in the future.
3. Choose the RIGHT cartridges:
   When your ink cartridge is low or empty, it can be tempting to buy an off-brand or take advantage of a special deal, but be sure you aren't sacrificing quality or compatibility. An incompatible cartridge can jam, cause your printer to fail, or damage the printer parts. Remember to read the instructions carefully before replacing the cartridge.

4. Use the latest software and drivers:
   Update your printer with the latest manufacturer software and drivers as they become available. By staying updated, you keep your printer working productively for your practice.

Celebrity Anagrams

Can you unscramble these celebrity anagrams? Each set of letters can be rearranged to spell the name of a current celebrity — someone you might see on stage or in a movie.

Example: whits mill = Will Smith

1. monk hats
2. perm restyle
3. twinkles eat
4. rote music
5. scowlers rule
6. big lemons
7. oil jar buster
8. o green ecology
9. madman tot
10. my rice jar

One Liner Laughs...

Are people born with photographic memories, or does it take time to develop?

I just got kicked out of a secret cooking society. I spilled the beans.

It was an emotional wedding. Even the cake was in tiers.

A recent study has found that women who carry a little extra weight live longer than the men who mention it.

Just burned 2,000 calories. That's the last time I leave brownies in the oven while I nap.

OVERNIGHT OATS

Yield: 1 serving | 236 Calories | 6 Proteins | 34.5 Carbs | 10 Fats

INGREDIENTS:

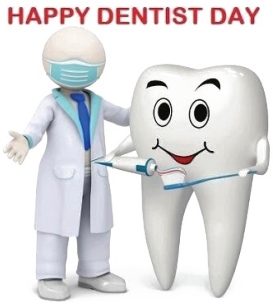
- ¼ Cup of Quick Oats
- ½ Cup Unsweetened Almond, Skim or Soy Milk
- ¼ Banana – Sliced
- ½ Tablespoon Chia Seeds
- 4-5 Drops of your favorite sweetener
- Pinch of Cinnamon
- Toppings: any chopped nut, granola, or additional fruit

DIRECTIONS:

1. Place all the ingredients (except toppings) in a jar, shake or stir well.
2. Cover and refrigerate.
3. The next morning, add your toppings and enjoy!

Recipe from Skinny Taste Cookbook
I often make Gina's recipes because, I love them so much!

—Lisa



February is National Children's Dental Health Month

Winter Hacks - *Have you tried any?*

1. Pack an extra pair of socks in your glove compartment. If you need to shovel or step in a slush puddle, you'll have dry socks to change into. Put your mismatched socks to good use! Use the socks over your wiper blades, too.
2. Use your ceiling fan in the winter too! Flip the switch to reverse the spin and turn the fan on low to blow warm air down from the ceiling.
3. Keep kitty litter in your car. If you get stuck in deep snow or slick ice, sprinkle kitty litter (NON-CLUMPING) at the base of the tires to add some traction and get you moving. You can also use your car floor mats to help.
4. Another use for hand sanitizer is to unfreeze your car door locks. Ice will melt instantly.
5. Forgot an ice scraper? Use an old gift card or loyalty card- it works well. (Don't use a credit card- it damages them!)
6. Duct Tape! Not only does it fix everything, it's very flammable and great to get a fire going in an emergency. You can also tape the word "SOS" on the back and side windows.
7. Use cooking spray on a snow shovel to keep snow from sticking.
8. Remove road salt from shoes with diluted white vinegar.
9. Use tin foil as a fireplace cleaner. Place a two-fold layer of tin foil at the base of your fireplace before starting a fire. Once the fire dies out, all you need to do is to pull out the ash-covered tin foil and toss it out.

Diversified Digital

WHO IS DIVERSIFIED DIGITAL LLC?

We're 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 entire office and network needs- from hardware and software to Internet service providers and third-party solutions.

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 is 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. You can also email Don 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're in the planning stages for advice to ensure a smooth transition. We'll be needed on the day you switch services, and proper planning reduces frustration, eliminates potential down time, and guarantees you a spot on our schedule.

Celebrity Anagrams

1. Tom Hanks
2. Meryl Streep
3. Kate Winslet
4. Tom Cruise
5. Russell Crowe
6. Mel Gibson
7. Julia Roberts
8. George Clooney
9. Matt Damon
10. Jim Carrey

BLACK TALON SECURITY

"HELPING YOU BUILD A MORE SECURE PRACTICE"

Gary Salman
Chief Executive Officer

Cybersecurity Helps Your Practice Succeed

Ten of the Best Practices for Keeping Your Business and Data Secure

Preventing the theft of your data and protecting business continuity must be the primary focus for your business. Below is a list of best practices to help enhance the security of your organization.

1. Enable Multi-Factor Authentication (MFA) or Two-Factor Authentication (2FA) for any application or website that supports it. MFA sends a unique code to your phone or activates an authentication app to validate your login.
2. Use strong passwords EVERYWHERE. Create strong passwords by combining a minimum of 12 characters, numbers and special characters like @, $, #, !, &, etc.
3. NEVER use the same password across multiple websites or applications. Every website and/or application should have a unique password.
4. Utilize password management tools like LastPass or Dashlane to manage and create strong/unique passwords.
5. Utilizing remote access tools can prevent tremendous risk to your organization. Make sure you are using the paid business versions of these technologies as well as MFA and strong passwords.
6. Train your entire organization on how to recognize threats such as phishing, spear phishing, social engineering, business email compromise (banking wire fraud) and proper use of removable devices. Test them using a phishing simulator.
7. Utilize a cybersecurity firm to evaluate your firewall(s) and to perform real-time vulnerability management to uncover exploitable devices on your network that may expose you to a breach or ransomware attack.
8. Have an annual penetration test performed by a cybersecurity company to identify risks and how you could be breached.
9. Have a security risk assessment performed by a cybersecurity company to evaluate how and where you may be attacked.
10. Have a cybersecurity company deploy artificial intelligence (AI) based threat detection and mitigation technology known as Extended Detection and Response (EDR) software on all computers and servers.

We are excited to announce that Don will be hitting the road sharing his experience and knowledge.

Don's first stop will be speaking at the Greenbriar Study Club in April on "Security – The facts and only the current facts about security for your dental practice."

We are in the beginning stages of planning an evening event with Don and Gary from Black Talon Security as the speakers. We look forward to sharing the information with you as it comes together.