DENTAL TECHNOLOGY ADVISOR

You Care For Your Patients, We Care For Your Technology

Bridge IT Support | January 2019

What's New

Welcome to the inaugural issue of our monthly newsletter!

We are inundated with spam and junk mail just like you, so we are very sensitive to not adding more of this to your life!

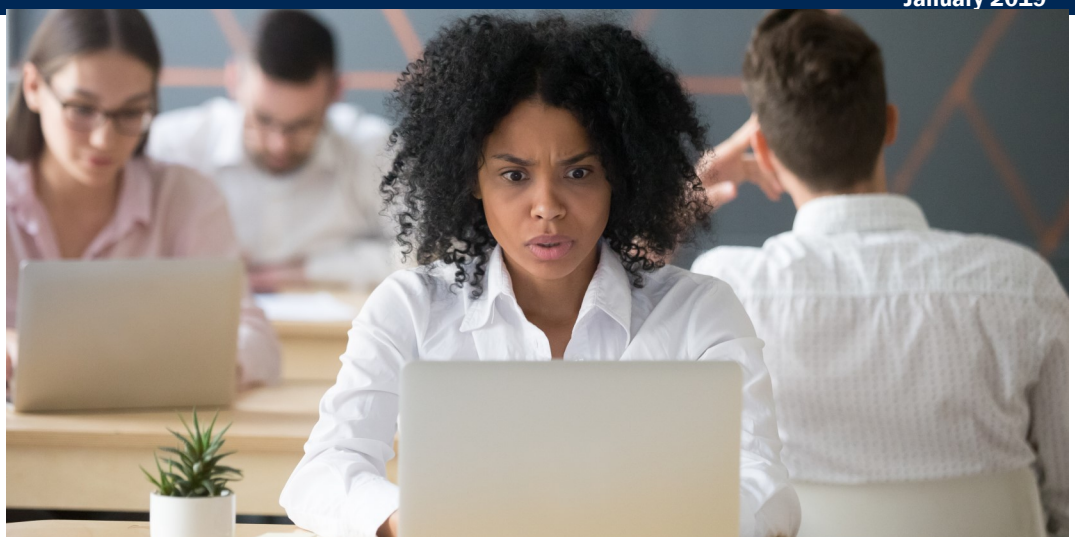
This newsletter will be a worth-while monthly read for you, with information applicable to your practice and personal life. Take a look through this issue and let us know if you agree.

If you have any suggestions for topics or FAQ's, please drop us an email or call.

This monthly publication provided courtesy of Mark VanderWal, President of Bridge IT Support.

bridge IT SUPPORT

Our Mission:
To positively influence the quality of life in Michigan by directing our God-given talent of fixing and maintaining computer systems to dental practices so they can deliver exceptional care to their patients.



4 Ways To Keep Employees From Leaking Confidential Information

Hacking a business today is easier than it has ever been. With nearly every company in America now intimately intertwined with technology, you might think cyber security would be a priority. But the truth is, our protective measures have grown lax, as organizations fall behind the times in their trust of flimsy barriers, trusting in blind faith that they won't be targeted.

Right alongside the rise of software that makes our life and work easier than ever, the tools cybercriminals use have advanced as well, enabling hackers to penetrate precious networks of data with minimal effort. What used to take thousands of lines of code now takes a couple of clicks. And actually, according to IBM's 2016 Cyber Security Intelligence Index, 60% of the time it's not some fancy tool that allows criminals to circumvent your defenses – it's your employees letting them in.

No matter how impenetrable you may imagine your security measures are, they'll be rendered useless if a hapless member of your team clicks the wrong file and opens the floodgates. When it comes to cyber security, your biggest vulnerability isn't your antivirus – it's your poorly trained employees. Here are four ways to prevent them from slipping up and opening your business up to attack.

1. STRONGER PASSWORDS

This may seem like a no-brainer, but it's probably anything but to many members of your team. According to a 2015 survey conducted by TeleSign, close to 75% of consumers use duplicate passwords in their online activity. Twenty-one percent of them use passwords more than a decade old, 47% have been using the same password for five years and a whopping 54% use the same five passwords across an entire lifetime online.

As a business owner, these numbers shouldn't just make you chuckle – they

Continued on pg.2

Continued from pg.1

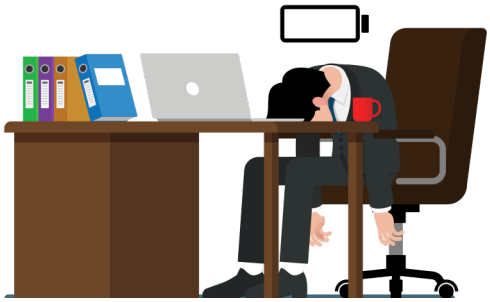
should make you mad. It may be that the entirety of your company's data, everything you've worked so hard to build over years of blood, sweat and tears, could be guarded behind a password as simple as "123456."

Make sure you train your employees on safe password practices. That means mandatory password changes to key business accounts every few months, each of them containing letters, numbers and symbols, preferably without any real words at all. It's a small change, but it can drastically increase your odds against data breaches.

2. MAKE CYBER SECURITY PART OF YOUR COMPANY POLICY

If your business is going to survive a digital onslaught, safe online practices for your employees need to be more than a recommendation. They need to be mandatory company policies. Every new and existing employee needs to know what's expected of them and what the consequences will be if they deviate from guidelines. For example, when an update comes through for a key piece of software, it needs to be installed immediately. Have a set procedure in place for them to follow if they encounter a suspicious e-mail or potentially malicious link. These and other practices, when set in stone, ensure that employees remain personally invested in protecting your company.

> **"60% of the time, it's not some fancy tool that allows criminals to circumvent your defenses — it's your employees letting them in."**



3. CONDUCT A SECURITY AUDIT

The best way to suss out any employee vulnerabilities, though, will always be to do a thorough security audit of all your systems. This means investigating the hardware and software you're using on a daily basis, sure, but most importantly, you need to analyze the habits of your personnel and whether or not they're complying with your high standards of cyber security.

4. TRAIN YOUR PEOPLE

As they say, forewarned is forearmed. This is never truer than when defending your business from data breaches. With comprehensive cyber security awareness training, outlining everything from the biggest digital threats to post-breach best practices, you can turn your biggest security liability into your greatest defense. If employees know the ins and outs of hackers' tricks, it becomes exponentially more difficult for hackers to trick them and find a way into your network.

With all four of these steps, it can be difficult to determine just how to implement these policies within your organization – much less what should be included – but luckily, we can help. Contact us if you would like to discuss or want more information.

Free Report: What Every Dental Practice Must Know About Hiring An Honest, Competent, Responsive, and Fairly Priced Computer Consultant

Bridge IT Support recently released their latest report for the dental industry, which includes:

- The "dirty little secret" of the computer support industry
- 20 Revealing questions you should ask
- 4 costly misconceptions about computer maintenance
- And more……

Visit our website at www.bridgeITsupport.com for your copy, or email us today at info@bridgeITsupport.com

Security Byte

What is the best way to ensure my computers are safe?

Imagine the computer network in your practice as the gold in Fort Knox, with criminals constantly scheming to steal this precious treasure. Protecting this gold is accomplished by multiple layers of security in the form of a perimeter fence, manned guard shack, more layers of fencing, multiple walls in the building, security coded doors, surveillance cameras, etc…

Why did they not just put up one fence and call it good enough? Because someone might figure out a way to secretly get through the fence undetected and steal the gold. However, if there are multiple layers of security, even though the criminal got through one layer of fencing undetected, the probability of getting through more layers of fencing, walls, gates, patrol dogs, camera's etc. is highly unlikely. The moral of this story is more layers equals more protection…

Leaders in the computer security industry recommend the same best practice "layered" approach to IT security. There are many ways to protect a computer network, and they all work in different ways. But just like the security layers protecting Fort Knox, none of them are perfect, so each additional layer can catch something that another could not.

Our future articles will review each of these many security layers in understandable terms to try to remove the mystery of each.

End of Life for Windows 7

-There are HIPAA compliance implications!

On January 14, 2020, Windows 7 will reach "End of Life," meaning Microsoft will discontinue all support and security patches for this product. When a vulnerability is found, Microsoft will no longer release a patch to fix it.

Therefore, after 2019, any computer or server running on Windows 7 or Server 2008 will no longer be secure or HIPAA compliant.

The end of 2019 may seem like a distant future, but it is fast approaching! There are many considerations and implications to properly integrate this project, so planning and budgeting now will help to ensure a smooth and seamless transition for your practice.

Migrating your practice away from Windows 7 will not be a quick fix! We highly recommend coordinating your upgrade as soon as possible to beat the rush leading up to the deadline. This upgrade will require your practice to be shut down for one to as many as five days, depending on your size, so you can see the importance of good planning and schedule coordination.

Your recommended ACTION ITEMS are:

1. Contact us to initiate a technical review of your system, allowing us to put together a "migration plan" for your practice. This will take us a few weeks to complete.

Call: 616-682-5450, or email info@bridgeITsupport.com

2. Schedule a meeting with us to review the plan and make final adjustments based on your feedback. This meeting typically runs about an hour.

3. Check your schedule and contact us ASAP to get on the installation calendar

We encourage you to consider implementing this project immediately to allow you to choose YOUR schedule. Beat the end of year rush, and choose the schedule that works best for your office. Do you have any days or weeks coming up where your practice will already be closed? This is a perfect time to get this project completed.

Our team is available to answer any questions you may have regarding Windows 7 End of Life and how your practice will be affected. To get in touch, call 616-682-5450 or send us a message today.

3 Ways To Protect Your Business From Cyber-Attacks

1. Plan for the worst.
The sad truth is that, no matter how much most businesses prepare their defenses for a cyber-attack, a breach will often occur anyway. That doesn't mean you shouldn't invest in protection, but you should always have a plan in place if and when crisis strikes. Include actions to contain the breach, patch the affected systems, and coordinate teams (not just IT) to stay on top of the problem.

2. Keep your team in the know.
The vast majority of breaches are instigated through minor errors by everyday employees. These noncompliant security behaviors aren't just bad for your business; they're bad for PR. That's why cyber security should be everyone's priority, not just the techies in your business. That means educating everyone on what to watch out for and what to do when hackers come knocking at your door.

3. Budget for robust cyber security.
Of course, all of these measures won't mean a thing if you don't actually invest in cyber security. Instead of a one-and-done task to check off, cyber security actions should be a regular component of your day-today. Include the costs of training, employee time, documentation, consulting and the latest security innovations.
Smallbiztrends.com, 11/20/2018

5 Mistakes Leaders Make That Keep Their Companies From Growing

1. Becoming complacent. No matter how comfortable the status quo is, stagnation only leads to failure down the road.

2. Pouring money into a failing project. When a venture fails, it's best to learn from it and move on rather than dump more resources into a clunker.

3. Entering a new market without the requisite knowledge. Don't overreach – only expand your business's focus when you really know what you're getting into, inside and out.

4. Focusing on the short-term. Never take an immediate win that will jeopardize long-term success.

5. Succumbing to analysis paralysis. Overthinking is fatal. Stay nimble and informed, but don't let it stop you from actually acting. *Inc.com, 11/8/2018*

"I got my e-mail's read receipt back, I just wish I had an understand receipt."

bridge
IT SUPPORT
6080 Fulton St. E
Ada, MI 49301