DENTAL TECHNOLOGY ADVISOR

You Care For Your Patients, We Care For Your Technology

Bridge IT Support March 2019

What's New

Computer Delivery Delays Are Real!

If you are waiting to schedule your computer equipment update for later this year, we suggest placing your order at least ten weeks prior to your intended installation date.

Just today we received a rescheduled delivery notice from Dell for an order we placed six weeks ago, which is now expected to be an eight week delivery (last year delivery times were 7-10 days!).

Manufacturers and industry experts are suggesting delivery times will get even longer than this as the year progresses due to a worldwide processor chip shortage, combined with Windows 7 End of Life equipment replacement demand.

https://www.techadvisory.org/2019/02/expect-cpu-shortages-until-late-2019/

Thank you for your business!

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.

Occasional Maintenance is No Longer Enough to be Secure!

By: Drew Morrison
-Bridge IT Support Lead Engineer

How often does your IT Company do your System Maintenance? Once a year? Twice? Quarterly? If they're not keeping watch constantly, you could be at risk of being hacked, experiencing a data breach, ransomware, or a full-system disaster.

By now, almost everyone has heard about the Equifax breach, how it has affected nearly 150 million Americans. The company has lost consumer trust, lost an incredible amount of money, and was investigated. The damage to those millions of people is an uncountable amount. But, could it have been avoided?

Equifax was hacked because they didn't install a security patch. Six months before the breach, a patch was released for part of their infrastructure, and their IT department did not install it. Had the patch been installed – had their IT department been doing continual maintenance – it likely never would have happened. What can we learn from this? If you are only doing maintenance once a year or more, you are missing critical security patches and could be vulnerable, just like Equifax!

Let's talk about the WannaCry Ransomware attack. It hit 250,000 computers in 116 countries around the world. Those people had their data totally destroyed unless they paid the ransom – and there's no guarantee they even could. If these were corporate computers, they hopefully had backups – but even if they did, that can be a lengthy, expensive process. As well, backups don't always work, and if they've never been tested and verified there's no way to know that. But, of those quarter million computers, how many could have been prevented?

In March 2017, Microsoft released a critical security patch. Two months later, WannaCry exploited the vulnerability that was patched. Had those quarter million computers been up-to-date on their Microsoft patches, they never would have had to deal with WannaCry ransomware, and could have gone on with their day, watching the news, shaking their heads at the poor souls who got it. What can we learn from this? If you are only doing maintenance once a quarter (three months), you are still missing critical security patches and could be vulnerable to attacks like WannaCry!

Speaking of ransomware, let's talk about the City Government of Atlanta, which back in 2018 was shut down for over a week from a ransomware attack. Not all the details are out yet, but we know this – their computers had been compromised and hacked since April 2017, with the same type of attack as WannaCry above. That means it was only from March to April from when the patch was released to when they got hacked. Had they kept up-to-date, they likely would never have been in that mess. We can still learn something here – even if you do updates once a month, you could still be vulnerable to ransomware attacks, just like Atlanta!

I hear you asking, "Why can't I just run

Continued on pg.2

Continued from pg.1

Windows Update and be fine?” Windows updates break – it is surprisingly common for Windows to stop updating itself, to get stuck in a loop and never properly install, say it is up-to-date when it is not, and more. A Google Search for “Windows Updates not working” returns 30,000,000 results. If you want to be sure you have the security updates, you need an IT company or internal IT staff to install updates, and monitor if they ever fail to install or stop working. Without that, you’re leaving it to chance.

Not only that, there are more updates than just Windows patches that need to be installed. Does your business host a website? Does your Server run your email? Do you have a network firewall? All of these and more should be regularly updated and monitored.

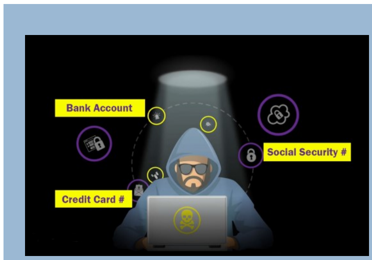
For better or worse, the security landscape has changed. We no longer live in a world where you can slap mediocre antivirus on a computer and consider it “secure”. Hackers and Ransomware authors are increasingly targeting vulnerable computers, especially small to medium businesses who will sometimes skimp on IT resources by thinking “I’m too small for them to notice”. That may have been true 5-10 years ago, but isn’t any more. They know you have more to lose.

“How can I protect myself and my business?” Great question! Here are just a few basic steps you can take to set you on the path to having a more secure system:

- If you’re doing maintenance and patching on a yearly or quarterly basis, find an IT company who can give you constant monitoring and updates, like Bridge IT Support.
- If you’re already on a monthly plan with your IT company, ask them how often they install patches for you. If it’s less than once a week, make sure to question why.
- Make sure all your computers have an up-to-date, trusted antivirus software that is proven against ransomware and other threats, and is monitored by your IT company for problems.
- Install a network firewall appliance from a trusted vendor, and activate security services to scan for potential issues before they even enter from the internet. Make sure your IT company is monitoring this firewall device and keeping it up-to-date.
- Keep all computers on a supported operating system, with a secure, up-to-date web browser.
- Have your IT company ensure all data is backed up, secure and encrypted, in multiple locations, and in multiple formats, and be sure it has a fast recovery time to avoid downtime. Do regular backup verification to mitigate “false positives”.
- Practice good password hygiene – never share passwords, and make a separate password for each website. If you have trouble remembering them – or have a “little book” of passwords, ask your IT company for a Password Manager recommendation.
- There is, of course, much more to good security than just security patching and keeping software up-to-date. Systems must be configured correctly and routinely tested, for example. However, it has been shown, time and time again, that having IT professionals keep your system updated can help prevent attacks and breaches.

> “If you are only doing maintenance once a year or more, you are missing critical security patches and could be vulnerable.”

Call Bridge IT Support today to discuss what we can do for you to help secure your business.



FREE Dark Web Scans!

What is the Dark Web? What used to be the dark street corner for conducting illicit business has now moved to the Dark Web on the internet. Seems every day we hear about another business getting hacked, potentially making YOUR professional and personal logins and passwords available to the public.

We recently enrolled in a Dark Web scanning service, allowing us to scan the web to see if any credentials have been compromised.

We are offering a free scan to the first 10 people to respond to this offer. Simply give us the URL of your practice, or personal email address, and we’ll do a scan for you.

Email us at info@bridgeITsupport.com, or give us a call at 616-682-5450.

Security Byte

This section of the newsletter will remove the confusion and fear concerning cybersecurity and how it relates to your practice and home.

In an earlier newsletter issue, we discussed cybersecurity best practices are to utilize LAYERS of security in your network, like the combination of fences, walls, alarms, guards, dogs, and camera's surrounding the precious gold of Fort Knox.

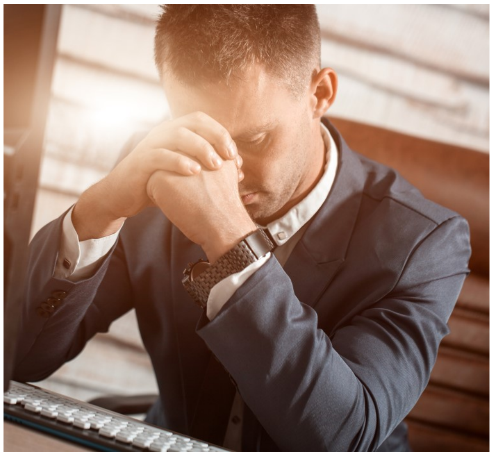
What is Intrusion Detection?

Intrusion Detection and Prevention Systems, often abbreviated as IDS and IPS, take a more active stance to augment a Firewall's passive one. These systems are activated on your firewall to constantly update lists of the latest attacks and exploits, and actively scan network traffic to block these attacks. Without a subscription service, your firewall will not get the updated profiles of all the latest cyber-threats, and therefore becomes less and less effective every day. Make sure your firewall has subscription services activated.

Cyber criminals have a variety of paths into your data, including directly through your firewall as discussed above, but they can also bait you into websites outside of your network to load malicious software vectors. Next month, we will review Web Filtering as a way to protect your network.

Still Not The Person You Always Wanted To Be?

3 Steps To Get You There In 2019



We all aspire to be better people, but too many of us hesitate to roll up our sleeves and tackle the roadblocks that prevent us from achieving that goal. We stay in our comfort zones, fall back on old habits and then question why our life isn't improving.

When I'm coaching CEOs and they tell me they're stuck in a rut, I always have the same response: start changing what you are doing in your life, because the person you are today will not get you to where you want to be.

Here are three guidelines to do exactly that.

1. START BY GETTING FOCUSED.
When planning any journey, the first thing you need to know is where you are. In business, you hold monthly and quarterly meetings to review operations and financial statements so you know how the company is doing. You should be doing the same thing for yourself.

Then you need to figure out where you want to go. What do you want your life to look like one, two or three years down the road? Map out specific goals to achieve this, and then follow them religiously. Stay on task, but don't multitask. Limit your distractions, and control your time.

2. WRITTEN, MEASURABLE GOALS ARE A MUST.
The first and most important step toward achieving and exceeding your goals is to write them down. I cannot stress this enough. Writing down your goals and priorities serves as a reminder of what you need to accomplish. As much as you can, keep them SMART: specific, measurable, attainable, relevant, and time-bound. Carry your list around with you and act on it every day. Do it for 30 days, and you'll be amazed at your progress.

3. LAY A FOUNDATION FOR EXECUTION EXCELLENCE.
If you've ever played sports, you are probably familiar with the phrases "in the zone" or "in the flow." It applies to any profession, from songwriting and acting to computer programming and engineering. When you're in the flow, you feel good, have a ton of energy and get a lot of work accomplished. Find the things you need to do on a daily basis to stay in the flow – whether that's exercise, meditating, reading or anything else – and write them down.

It's also essential that you hold yourself accountable along this path. Find an accountability partner and share with them your tasks, priorities and deadlines to accomplish your goals. You are much more likely to succeed when you have someone watching your progress and ensuring you cross the finish line.

Andy Bailey is the founder, CEO and lead business coach at Petra, an organization dedicated to helping business owners across the world achieve levels of success they never thought possible. With personal experience founding an Inc. 500 multimillion-dollar company that he then sold and exited, Bailey founded Petra to pass on the principles and practices he learned along the way. As his clients can attest, he can cut through organizational BS faster than a

5 Sneaky Tricks Cybercriminals Use To Hack Your Network

1. PHISHING. Woe to you and your business if you haven't heard of this one yet. By using an email, chat, web ad or website impersonating a legitimate organization, hackers get members of your team to click and install malware.

2. BAITING. Baiting uses an enticing item to lure employees into giving up personal data, such as a music or movie download or a mysterious flash drive left around the office.

3. QUID PRO QUO. It's like baiting, except that hackers offer a service instead of an item in return for private data.

4. PRETEXTING. This is a type of phishing in which a hacker poses as a respected colleague or member of your organization in order to boost private data.

5. TAILGATING. It occurs when an unauthorized person physically follows your employees into restricted areas. *SmallBizTrends.com, 9/20/2018*

Don't Wait 191 Days To Realize There's Been A Data Breach — By Then, It's Too Late

According to a 2017 report by research firm Ponemon, it takes an average of 191 days for a company to realize it's been compromised by a data breach. This number should scare anyone. The longer you take to recognize and respond to a breach, the more criminals can steal and the bigger the damage becomes. What's more, your delayed reaction will leave you fewer options to mitigate the disaster. To survive, you need to stay on top of your cyber security with a team of dedicated professionals keeping tabs on attacks, strengthening your barriers and responding within hours, not days, if the worst ever happens. *SmallBizTrends.com, 10/30/2018*

The Ugly Truth About Apps Sharing Your Kids' Data

It's always unsettling when apps secretly gather your data. But when it comes to apps for kids, that's doubly true. Recently, the attorney general of New Mexico filed a lawsuit against Tiny Lab, which develops games for kids like *Fun Kid Racing*, and other companies, including Google and Twitter. The suit alleges that numerous applications violated child privacy laws by tracking and sharing data for users under 13. *The New York Times* looked into it and found that dozens of other kid-targeted apps may be doing the same thing. Keep an eye on the apps your child is using, as well as the data they're sharing. You don't want them becoming a victim of this gross data-sharing. *Wired.com*

© MARK ANDERSON WWW.ANDERTOONS.COM

"All that work to tell you about stuff you could look up on Wikipedia?!"

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

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