The Tech Chronicle

Brought to you by bridge IT SUPPORT

Insider Tips To Make Your Business Run Faster, Easier And More Profitably

What's New in February

We have launched a new weekly cybersecurity training tip email program. In January the Department of Homeland Security asked IT providers to review and step up their security protocols. Since the criminals are now targeting people more than hacking into systems, we felt one of the best ways to accomplish this is to educate computer users on how to identify and handle security threats. If you are not already receiving this FREE weekly security tip, please call or email us to be added to the list.

February 2020

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

Our Mission:
To positively influence the quality of life in West Michigan by directing our God-given talent of fixing and maintaining computer systems to our loyal clients so they can deliver the same to their clients.

You Shouldn't Trust Your Backups! But You Should Get Them VERIFIED

Ronald Reagan said it about the Russians, and it applies to your practice's data backups: "Trust... but VERIFY."

If you're reading this right now and your backups give you a nice green checkmark or a "Success!" email, and you haven't had anyone fully check them, I've got some bad news for you: unless you've had those backups VERIFIED, they can't be trusted. **You could be in a situation where your backups could be silently failing or giving a "false positive" without you knowing it, a situation all too common.**

Backup verification is a multi-step process. First, you have to verify all the data is identical to the "live" server. If a backup failed to copy correctly and it didn't warn you, how would you know? Your tapes could be blank, or filled with corrupted data, and the only way to know for sure is to check.

Second, you have to make sure you can restore. You may have a situation where the data copied correctly, but isn't in a format that can be restored. The disk could have errors or be damaged, or the backup could be missing core files or configurations. By actually rebuilding a Server with the data, you can prove that it is all there and working, beyond a shadow of a doubt.

Even if everything else is configured correctly, systems that use databases (like almost all EHR and Practice Management Systems) require special care. If, as an amateur would do, you simply copy the files, your backup will fail, and it will never warn you, because it will look like it succeeds. **It won't be until the day you try to restore that you find that your database is corrupted and unreadable, requiring costly DB repair services and upwards of weeks of downtime – if the data can be recovered at all!** Backup verification can discover these issues before they become a disaster.

Continued on page 2...

.. continued from cover

If you're currently rotating a set of disks or tapes, taking one home… is your backup encrypted? Do you know for certain it is? Has anyone tested and verified the encryption? Not only that, but how often are drives rotated? All too often, we find such a situation where a business owner believes the drives are rotated daily, but the staff member in charge isn't doing it. What does that mean? If there was a fire, flood, or theft, there would be no recovery – everything would be lost.

"What about Carbonite, Crashplan or other Cloud Backups?" These can suffer from data corruption or database configuration issues just like a tape or disk system. Even if you have cloud backups that are configured directly, a situation like server hardware failure or ransomware can be far more costly than it seems. For an average-sized practice, your data could take upwards of eight hours or more to download from a cloud service! After that, you then need an IT professional to spend upwards of four to eight hours of time to set your system backup, restore those backups properly, reconnect all the computers, etc. Basically, consider having no computers – no X-Rays, no electronic insurance claims, no patient charts, nothing – for two full business days, minimum. How many thousands of dollars would that cost you? How much trust would you lose from your patients, having to send them home?

As an example, Bridge IT Support recently went in to a dentist office in the West Michigan area. They thought the backups were rock solid – every day, they got an email that said it was successful, and the office manager was dutifully swapping the disks. **When we attempted to verify, we found that the backups actually contained no practice data at all!** The basic "Windows" operating system was backed up, but the disks were completely missing their medical records, charts, and X-Ray images. The kicker was that this was a Server that was only 3 months old, and we verified that the backups were simply set up wrong at that point.

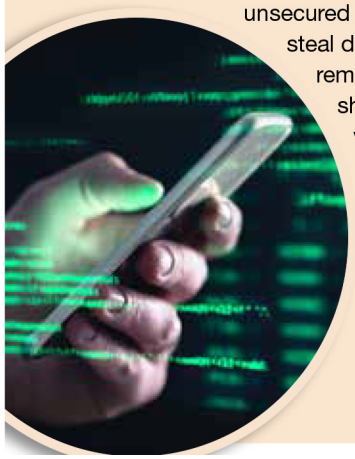
Don't let it happen to you. Bridge IT Support can set you up with a secure, managed, disaster recovery and business continuity solution, rather than relying on fallible backup tapes. **Call today.**

Dentrix users!
Now that your office is running Windows 10 and Dentrix, does it seem a little sluggish at times? After working with Dentrix on this for several offices, they suggest the best way to remedy this is to leave "Patient Chart" open. Do not close it each time and restart between patients.

Top Ways To Protect Your Remote Employees From Cyberthreats

Allowing employees to work remotely comes with its share of benefits, like increased productivity and employee happiness. But it comes with challenges as well, including staying ahead of cyberthreats. Here are three ways to protect remote employees who work from laptops, tablets and smartphones.

1. Avoid unsecured public WiFi. It may be convenient, but cybercriminals can use unsecured networks to steal data. Instead, remote workers should utilize a virtual private network (VPN). Personal hotspots are another option.



2. Require endpoint security, such as firewalls and malware protection, installed on remote workers' devices. All remote employees should use the same endpoint security so you know everything is up-to-date.

3. Develop 'cyber security best practices' for your business. Everyone, including remote workers, should be on the same page when it comes to cyber security. Make sure your employees know the threats and how to stay vigilant online. *Inc., Feb. 12, 2019*

6 WAYS TO MAKE YOUR BUSINESS MORE EFFICIENT

1. Cut the clutter. Have any outdated systems and processes that are cluttering up your business? Get rid of them. Look for inefficiencies or redundancies you can eliminate, then do it!

2. Block interruptions. When you need to work, it's okay to put up barriers. Block out your calendar when you don't want calls. Turn off all phone notifications. Only check e-mail twice a day. Set limits!

3. Look to automation. Whether you're scheduling e-mails or social media posts, look at what you can automate to avoid wasting time.

4. Balance tech and traditional. It's okay to rely on texting, e-mail and online chat to communicate with customers, but don't forget the power of real, face-to-face communication.

5. Say no to multitasking. Multitasking is a myth. You can either do several things at once and deliver mediocre results or do one thing right the first time and deliver stellar results.

6. Invest more in cyber security. There are countless threats out there, so don't get caught without good IT security across the whole of your business. Don't risk it! *Small Business Trends, Nov. 4, 2019*

Continued on Page 3 ...

3 SIMPLE WAYS INTROVERTS LEVERAGE THEIR STRENGTHS TO THRIVE IN THE WORKPLACE

Introverts can be drained by social interaction and stimulation. They need to recharge regularly, so days off are important in order for them to be at their most productive. Here are three ways introverts can be at their best in the workplace:

- **Manage energy more than your time.** When you feel most energized, that's the right time to focus on creative work that requires more brainpower. Structure your days around your energy.
- **Cultivate the right environment.** Work in a space that calms you and energizes you. Set the right light (such as natural lighting) and invest in noise-canceling headphones.
- **Say what needs to be said.** Introverts constantly think but don't always speak up. Don't let communication fall to the wayside. Remember, we're all working together. *Business Insider, Nov. 19, 2019*

Security Byte: Secure Boot

This is a technology built in to modern computers and in to Windows that makes it so a computer can only boot into Microsoft Windows – and not into, say, a virus that is trying to take over the computer. Bridge IT Support enables Secure Boot on all new computers sold running 64-bit operating systems.

Top 3 Ways Hackers Will Attack Your Network - And They Are Targeting You RIGHT NOW

You might read the headline of this article and think, "That has to be an exaggeration." Unfortunately, it's not. Every single day, small businesses are targeted by cybercriminals. These criminals look for vulnerable victims, then attack.

Hackers have many methods they use to break into your network, steal data or put you in a position where you have to pay them money to get your data back. They use a combination of software and skill to make it happen. Here are three ways hackers and cybercriminals attack your network in an attempt to get what they want.

1. THEY GO THROUGH YOUR EMPLOYEES.

That's right, they'll use your own employees against you, and your employees might not even realize what's happening. Let's say a hacker gets hold of your internal email list, like the emails you have posted on your website or LinkedIn. All the hacker has to do is send an email to everyone at your company.

The email might be disguised as a message addressed from you asking your employees for a gift card, which is becoming an increasingly common scam. Another email tactic is making a message look like it's from a fellow employee, asking everyone else to open an attached file, which is likely malware or ransomware.

2. THEY ATTACK YOUR NETWORK DIRECTLY.

Some hackers aren't afraid of forced entry. Hackers and cybercriminals have access to black market tools and software that helps them get into networked devices – particularly unprotected networked devices.

For example, if you have a PC that's connected to the Internet and your network doesn't use any firewalls, data encryption or other network protection software, a hacker can break in and steal data from that PC and potentially other devices connected to that PC, such as portable hard drives.

3. THEY HOLD YOUR DATA HOSTAGE.

Hackers are relying on ransomware more and more to get what they want. Hackers rely on email, executable files and fraudulent web ads (such as banner ads and pop-ups) to attack networks with ransomware. All it takes is someone clicking a bad link or file and the next thing you know, you're locked out of your network.

All of these points are why you need to take a hard look at IT security solutions and use them. Hackers are just looking for easy targets and, sadly, a lot of small businesses fit the bill. Just because you haven't had any major problems yet doesn't mean you won't in the future. The threats are out there and they're not going to go away. Invest in security, partner with an IT security firm and protect yourself. This is one investment that is truly worth it!

bridge
IT SUPPORT

601 3 Mile Rd NW, Suite C
Grand Rapids, MI 49544

Inside This Issue

Cartoon Of The Month