The Tech chronicle

Happy Holidays!

Looking back on 2020, there are a lot of sentiments that come up as we review a year like no other. For us what comes to mind is gratefulness and resilience. Our customers have been overwhelmingly kind and understanding as we (along with most of you) moved operations to a 100% remote workforce. Successfully navigating this, along with many other unforeseen challenges is what 2020 was all about. We want to express our gratitude for our clients and we wish you all a happy holiday season as we begin to look forward to 2021 and the opportunities that it may bring!

December 2020

This monthly publication provided courtesy of Craig Covington co-owner Canon Capital Technologies

Our Mission

To enhance our customers quality of life and the health of their business.

4 Critical Cyber Security Protections to Have In Place Now To Avoid Being Hacked

Did you know the average website is attacked 94 times every day? As cybercriminals become better equipped with advanced technology, that number will increase. Small-business websites are the most at risk for attack. Small businesses are tempting targets because SMB websites are often a direct link to that SMB's network, where all kinds of goodies are stored, including sensitive business and customer data.

This is data cybercriminals want.

Cybercriminals and hackers can be aggressive when it comes to attempting to access your network and data. They use malware, ransomware, phishing scams, bot attacks and even direct attacks to get to your data. If you don't have protections in place against these kinds of incursions, you are putting your business in harm's way.

There are many "barriers" you can put between your business and the bad guys, but there are four things you can do (and should do) right now to put yourself ahead of the curve. These will protect your business and protect your data.

1. Create A Culture Of Awareness. Education is a powerful tool, and that is 100% true when it comes to cyber security. There are several steps you can take to create a culture of awareness. This includes ongoing employee cyber security training which keeps everyone in your organization informed about the latest threats and the latest ways to combat those threats.

Training helps your team identify threats and recognize when someone is trying to break into your network (such as through a phishing scam). Cyber threats are constantly evolving and ongoing

Continued on pg.2

Continued from pg.1

education will keep these threats top of mind, so as the threats change your team is right there on the frontlines ready to take on whatever may be around the corner.

2. Monitor Threats 24/7. This is where partnering with an experienced IT services firm really comes in handy. Coming back to point #1, an IT services company can help you create that culture of awareness, but more than that, they can keep two eyes on your network 24/7. This way, if something or someone attempts to force their way into your network, they can stop it before it becomes a problem.

Even better, threat monitoring helps protect your team from more common types of attacks, such as malware or ransomware attacks. Should an employee accidentally click a harmful link or download a malicious program, it can be isolated before it takes hold and spreads.

3. Make Sure Protections Are Up-To-Date. Practically every piece of hardware and software you use needs to be updated at some point. When you don't update, you put yourself at serious risk. Hackers are constantly looking for vulnerabilities in the apps and devices you use. CRM software is a good example. This software connects your business with customers, and it can be used to store all kinds of information, from very basic contact information to very sensitive customer-specific data.

Should a vulnerability be found, hackers won't waste any time attempting to exploit it. In response, the makers of that CRM software should send out a security patch. If you do not make the update (or have the update automatically installed), your risk increases significantly.

Again, working with an IT services firm or a managed services provider can help you address this minor – but very important – step. They can ensure everything under your roof is up-to-date and that you have all the latest protections.

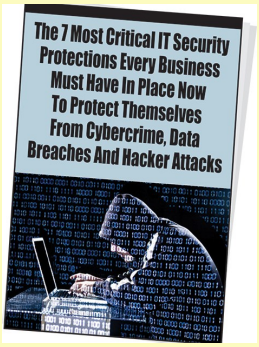
4. Have A Plan. Every single person on your team should be on the same page. They should all change their passwords every 60–90 days. They should all be required to use secure passwords. They should know how to identify potential phishing scams. They should know who to call if the network or their devices go down for any reason. You should know exactly what to do if your on-site data becomes compromised in any way, whether it's due to malware, a natural disaster (flooding, fire, etc.) or hardware failure.

> **"You should have an IT handbook – a plan that spells out every detail of your IT protocol and cyber security strategies."**

In short, you should have an IT handbook – a plan that spells out every detail of your IT protocol and cyber security strategies. This goes hand in hand with the three points we've already discussed: awareness, threat monitoring and keeping hardware and software updated. When you have a plan, you know exactly what to do when threats come your way. You're ready and aware.

Cyber threats are always going to be out there. There isn't anything you can do about that. But there are things you can do for yourself and your business to prepare for those threats. Put these four points into action, work with an IT services provider and give yourself the advantage over those who want to take advantage.

FREE Report: The 7 Most Critical IT Security Protections Every Business Must Have In Place Now To Protect Themselves From Cybercrime, Data Breaches And Hacker Attacks



Three hundred sixty thousand NEW malware threats are being released every day, and businesses (and their bank accounts) are the No. 1 target. To make matters worse, a data breach exposing client or patient information can quickly escalate into serious damage to reputation, fines, civil lawsuits and costly litigation. If you want to have any hope of avoiding a cyber-attack, you MUST read this report and act on the information we're providing.

Download your FREE copy today at
www.ccmgtech.com/cybercrime

4 Ways to Improve Email Productivity

As work situations have gone remote, email has become even more vital for communication. And as the end of the year finds us reevaluating and taking stock, this is a perfect time to make sure your email habits are efficient! Here are four strategies to help clean up your email productivity as we enter 2021:

Rethink Your Subject Line. Tell the recipient as much as possible in as few words as manageable and make sure to let the recipient know if any action is needed on their part.

Establish Addressing Rules. It's annoying to be copied on an endless series of email replies. Establish team rules about who needs to pay attention to which emails by properly utilizing the "To" and "CC" fields.

Use Caution When BCC-ing. Blind copying people on emails comes across as sneaky. Refrain from it as much as possible. Only use it for bulk emails or when you want to politely drop someone from a chain they no longer need.

Don't Draw Things Out. If you can't resolve something in three emails or less, it's time to pick up the phone. Sometimes email just doesn't work.

2 Secrets To World-Class Service — And It's Not What You Think!

Nick Stoyer, Learning and Development Leader at Four Seasons Resort Orlando, revealed some secrets to world-class service at our summit and he and his firm agreed to allow us to share them with you.

How does the Four Seasons deliver world-class service across the globe? Below are excerpts from the conversation which help answer that question. I hope you find the insights as powerful and as useful as we did.

Geoff: Four Seasons Hotels and Resorts is known as the gold standard for service worldwide. It has achieved more five-star ratings than any other hotel/resort brand in the world. The experience is unique, and it's consistently awesome. Any company in any industry can benefit from learning from your example. The question is, "How do you do that?"

Nick: Before it was fashionable for CEOs to want to do good in the world and treat stakeholders (also known as "people") well, Four Seasons was practicing the Golden Rule: treat others as you wish to be treated. Our founder, Issy Sharp, started Four Seasons in 1961 in Toronto. It seemed to him that if you wanted to build the best hospitality company in the world, you had to treat your colleagues and guests the best.

Geoff: Easier said than done.

Nick: For us, it's all about the people we hire, the way we develop them and the culture we build together. That's what we focus on in order to give our guests the best possible experience. One of our guests said that she defines luxury as "the absence of worry." We thought it was brilliant, and we rolled it out as our definition of luxury. So, we need to hire the best people, develop them and give them a culture of support (alleviating them of worry as a team member), so they can do their best to free our guests from worry.

Geoff: Beyond developing and coaching people, what's the culture like at Four Seasons?

Nick: It's very positive, even in failure. We have a saying: "You either win or you learn something." Everything we do, we try to make it as fun and engaging as it can be. We innovate constantly. We build micro-videos of best practices. We constantly huddle and talk about if a guest or a colleague needs something special. That's the culture. It's one of overwhelming support and encouragement. This permits our folks to focus on the guests, observe what they need and take action.

Geoff Smart, chairman and founder of ghSMART is a co-author, with colleague Randy Street, of the New York Times best-selling book *Who: A Method For Hiring.* Geoff also co-created the Topgrading brand of talent management and is the founder of two 501(c)(3) not-for-profit organizations. SMARTKids Leadership Program™ provides leadership tutoring, and the Leaders Initiative™ seeks to deploy society's greatest leaders into government. Geoff earned a Bachelor of Arts in Economics from Northwestern University and a Master's and Doctorate in Psychology from Claremont Graduate University.