VOLUME 5, ISSUE 4 APRIL 2022

MTC TECH TALK

For Humans Not Geeks!

Your resource for the latest technology updates and opportunities for your success.

How To Protect Your Business Against the Reality of Cyber Security in 2022

What's In This Issue?

Meeting Tree Computer
☎ (845) 237-2117

All across the world, hackers are targeting and exploiting security weaknesses and holding data hostage. Last May, the Colonial Pipeline was hit by a cyber-attack that disrupted fuel supplies along the East Coast for several days. The company – and the FBI – paid hackers $4.4 million in Bitcoin to regain control of the system.

Colonial Pipeline was not the only corporation that paid hackers an exorbitant amount of money. The NBA, Kia Motors and JBS Foods have also been victimized by cyber-attacks where hackers demanded millions of dollars. CD Projekt RED, a Polish video game developer, was also a victim of a cyber-attack, but since they had backups in place, they never had to pay the demanded ransom.

While these are all big organizations, that does not mean that small businesses are safe. These stories made the news because companies paid millions of dollars to regain control of their data. When a small or mid-size business gets attacked, they can't pay millions of dollars to recover stolen information, hackers know this. Instead, they will usually go after customer and employee information as well as financial records and statements, which are all worth good money on the DarkWeb. They're in it for the money and could care less that 60% of the SMB's that they attack end up having to close their doors for good.

The year 2021 set a record for cyber-attacks, and 2022 is shaping out to be no different. In fact, the Russian invasion of the Ukraine has prompted the Cybersecurity and Infrastructure Security Agency (CISA) to issue a "shields up" warning. Russia has a history of launching cyber-attacks against those that interfere, putting businesses of all sizes at risk, as the aim will be to cause as much disruption as possible.

This means that you can't afford to slack off on your usual cyber security measures. If there's something you've been meaning to get around to doing, now is the time.

Hire A Managed Services Provider For Your IT Needs

Let's say this again (and again, and again). Every security conscious business needs an MSP. Yes, your time and materials

(Break Fix) IT partner might be cheaper, however, the only time this service provider offers support to your business is when there is a malfunction within your IT infrastructure. You call them when you can't print, they respond and fix the issue. They are not however, set up to keep hackers out and your network secure. And it's a jungle out there.

If you are following our LinkedIn Newsletter - **Bytesize News** - you know that Microsoft recently revealed that more than 35.7 billion phishing emails were sent to its customers last year. Fortunately for us, the tech giant blocked 1,000 of these malicious emails EVERY SECOND. That's about 3.15 billion emails.

While this is great news for those of us who rely on Microsoft's applications on a daily basis, the risk that one of those remaining emails finds its way into your network is still tremendous and only preventative maintenance, security, behind-the-scenes monitoring, and remediation offers hope of protection.

The simple truth is that MSPs can be incredibly beneficial to any business. They're designed to recognize and fix weak points in your IT infrastructure. MSPs work proactively to ensure that your business is fully protected in the cyberworld. They offer around-the-clock monitoring, data backup and recovery, firewall and network protection, real-time threat prevention and so much more.

Implement Appropriate Protections

With or without the support of an MSP there are 5 basic checks you need to implement urgently to keep your data protected from the nefarious activities of hackers:

- The first thing you need to make sure you have in place is a working backup. Should you be hit by a cyber-attack – such as ransomware for example – you will still be able to access all of your data and documents.
- Ensure that all your applications, systems and devices are running the latest updates, and that any relevant patches are in place.
- You should also make sure best practice is being followed when it comes to password hygiene. Make use of password managers to ensure your whole team uses unique passwords that are less susceptible to brute force attacks.
- You should also strongly consider using multi-factor authentication (where you get a login code on another device) across your applications for a higher level of security.
- Check your incident response and recovery plan is up-to-date and that everyone is aware of the steps they should take if they suspect a security breach. Your people need to know who to report a possible breach to, and who is responsible for protecting the business.

Create A Cyber-Secure Culture

Bad results from cyber-attacks often stem from employee error or misunderstanding. When you first hire an employee, train them on cyber security. In addition to this, your current employees should go through a reminder course at least once a year.

Inform them about the dangers of phishing e-mails and texts, downloading malware, social media scams and password protection. If your employees are aware of the risks, they will be more observant and better able to any potential threats. And this really means training for everyone from the most senior employee to the most junior. Your entire team needs to buy into the cyber-secure culture if you want your training to be effective.

In today's day and age, you simply can't be too careful when it comes to your cyber security. If you're unsure that you have the right protections in place, speak to an expert who can help put your mind at ease and make sure your business is as protected as possible. We're here to help. If you have any concerns that your cyber security has fallen behind, call us, and we'll check.

Your Tech Tip of the Month

24 Important Cybersecurity Definitions to Add to Your Brain Bank

Cyber Security touches every part of an organization, and misconceptions around cybersecurity can put your company at risk. To help, we've compiled a list of definitions including some of the most commonly used security terms in the industry.

This list of cyber "jargon busters" is designed to help you better understand the many cybersecurity terms you hear and see every day, including ones you'll read about monthly in this newsletter.

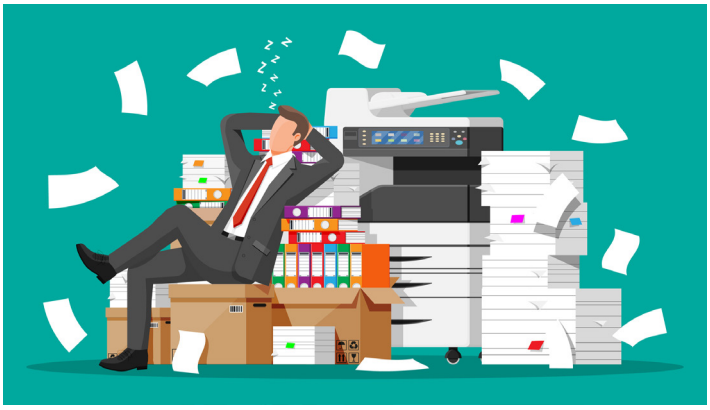
Take a deep dive into cybersecurity with these basic terms:
https://www.meetingtreecomputer.com/tech-tip-75-24-important-cybersecurity-definitions-to-add-to-your-brain-bank/

Are You Forgetting Something?

Don't worry, you haven't missed our birthday.

We're talking about your office printer. When was the last time you thought about it (and we don't mean those angry thoughts when it starts scrunching up paper)?
We mean thinking about it from a data security point of view. That big hunk of plastic and metal needs attention. Because it's on your network. And it probably has an internal memory of all the documents that have been sent to print.

That means it's a threat when it comes to data theft.



Make sure your printer is password protected. That it's secured, accessible by only the relevant people, and that old printers have their memories wiped and are correctly disposed of.

Need a hand? We can help you. Give us a call on 845-237-2117 and we'll make sure your entire network is secure and protected.

Are You Insured For That?

It seems today there's an insurance for everything. From the standard things like cars and our homes, extending to pets and devices... you can insure anything that has the potential to cost a lot of money if something goes wrong.

Does your business have cyber insurance in place?

I'm not trying to sell it to you! But it's definitely something you should consider.

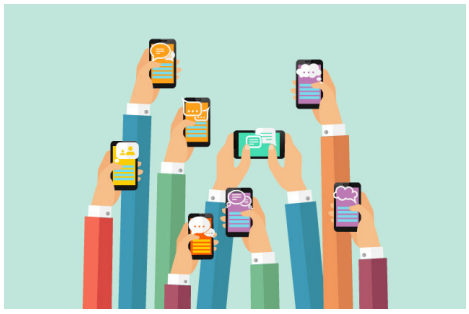
Should you be the victim of, for example, a ransomware attack – where all of your data is encrypted and held ransom until you pay up – it could cost your business dearly. And I'm not even talking about the ransom amount. The real cost is the downtime and getting your systems back up and running.

One of the huge advantages of having cyber insurance is that the insurance companies will insist you meet certain basic safety standards. This is nothing to be scared of. Those standards are designed to reduce your risk of suffering a cyber-attack in the first place.

We are not an insurance company so we can't provide the insurance for you. But we can help you get your cyber defenses to an acceptable level. Just give us a call at 845-237-2117. And if you are looking for a cyber insurance agency that knows what they're talking about, we can help you with that as well.

Keeping Your Business Safe Across All Chat Channels

OK, so work chat won't be 100% productive all of the time. But would you know if your staff's 121 chats ever crossed the line from friendly to inappropriate?



While we don't promote micromanagement or employee monitoring, the rise of private messaging thanks to remote working has led to an increase in sexual harassment and bullying in the workplace.

As usual, Microsoft has got things covered.

This month, Microsoft is rolling out an updated communication compliance feature that will notify you in under an hour if any inappropriate communication has been sent.

The facility will monitor messages sent and received over email, Teams, Yammer, and other third-party platforms, and run them by a set of pre-defined policies. When a breach is identified, the messages will be passed to a team of reviewers, who will then notify you within those 60 minutes.

Previously, this detection and review stage took around 24 hours. And although Microsoft hasn't detailed how it will cut the time so dramatically, it's definitely a real benefit when you're trying to keep your team safe and happy.

Is this a feature that you already make use of? If you don't monitor your employees already, would this feature make you reconsider the need? We'd love to hear your thoughts.

Ps. *Effective May 7, 2022, all New York employers will be required to provide notice to employees of any employer monitoring of work phones, emails, or Internet use. We will keep you informed on this policy change as we get closer to the effective date.*

The 7 KPIs for ROI from IT

How to ensure your business's spend on IT is an investment, and never an expense

No matter what kind of business you run, technology sits at the heart of it today. And it's going to become more and more important in the future.

Big business thinkers see IT as a long-term investment. They understand the correlation between the short-term impact to cash flow, and the enormous long-term benefits of business growth, increased productivity and highly satisfied staff and customers.

To get your Return on Investment (ROI) there are several Key Performance Indicators (KPIs) to track. Our new guide tells you what they are.

https://www.meetingtreecomputer.com/files/2022/03/ROI-from-IT-PDF-Meeting-Tree-Computer.pdf

Teams is great, but how can I make it less distracting?

Click the colored dot next on your profile, and you'll see some status options. Choose "busy" or "do not disturb," for example, when you need fewer distractions. You can also write a message, so your colleagues know when you'll be free.

Should I migrate my in-house systems to the cloud?

This is a big question with a lot of considerations. We've just written a guide all about cloud migration that might help.

Email us if you'd like to get a copy.

How can I make sure my staff stick to cyber security measures?

The very best way is to make sure they're fully aware of the risks, and the extent of damage a cyber-attack could cause.

Regular cyber security training for everyone in the business is also recommended.

Submit Your Question Here:

mduci@meetingtreecomputer.com

This is how you can get in touch with us:

call: 845-237-2117 | email: info@meetingtreecomputer.com
website: www.meetingtreecomputer.com

Follow Us