NEWSLETTER

■ May 2020

3 WAYS TO STOP CYBERCRIMINALS COLD IN TODAY'S CRAZY TIMES

You've seen it. You've probably even experienced it. For what feels like forever now, just about everyone has been forced to modify priorities. As a business owner, you've likely shifted your focus to your business to accommodate this world crisis. You may even be investing more of your time in retaining customers and generating new cash flow. If you're like most people out there, you've barely had time to think about cybersecurity and protecting your important data.

Maybe you've heard the saying, "Never let a crisis go to waste." It's as if cybercriminals wrote it because that "crisis" shift is precisely what they're thinking right now. They're probably working overtime right now to craft new malware while our lives have turned upside down. Yes, as you're focused on your business, hackers are finding new ways into your IT network. Their objective is to steal data and passwords, compromise your clients' private information, and even demand large ransoms.

Did you know that cybercrime is expected to grow to $6 trillion by the year 2021? But, now is when hackers are expected to be most dangerous.

Here are three strategies you can use right now to help protect your business data, money, and productivity during these unusual times.

1. Guard Your Inbox.

People aren't paying as much attention as they usually do, which makes it the perfect time for cyber-attackers to send e-mails with dangerous malware, worms, and viruses. Always carefully inspect every e-mail received and make sure you know the sender.

Here's another tip: avoid clicking links in the e-mail unless it's abundantly clear where they go. Also, don't ever download an attachment unless you know who sent it and what it is while it takes a few extra seconds, double check by calling the person who sent you the attachment. Better safe than sorry.

Make sure you communicate these safeguards to everyone on your team, especially if they are working from home.

2. Secure Your Company-Based Technologies.

During crises like this one, your passwords are a critical first line of defense. Don't wait for your company's financial data to be compromised. Make a point now to reevaluate

Continued on page 2

COMPUTER MAGIC

Welcome to our monthly publication provided to you by Samantha Boneck, Marketing Associate of Computer Magic, Inc.

Our Mission: We help you reach your long-term objectives, enable you to drive real growth in your company, and to secure greater return on investment.

WHAT'S NEW

Computer Magic is here for you! We're available 24/7 for anything you need. Do you need help with remote access? Or, do you have questions regarding your remote team? Give us a call and we would be more than happy to assist you – no purchase necessary.

Samantha Boneck
Marketing Associate
Computer Magic, Inc.

Continued on page 2

your passwords and direct your team to create stronger passwords. Too many employees are guilty of using the same password across multiple applications. Use a unique password for every single application.

Your team may tend to save your passwords in their web browser. Don't do this. A skilled hacker can bypass the PIN required to access your saved passwords. Once they have the password or PIN to access your web browser, they can steal as much as they want – credit card information, customers' private data, and more!

We recommend that our clients use a password manager. It's convenient, but more importantly, it's far more secure.

3. Secure Your Home-Based Technologies.

With the coronavirus pandemic, far more businesses are encouraging their employees to work from home. That means many people are working from the living room or kitchen without giving a second thought to security. This negligence is an invitation to new cybercrimes.

Here are a few tips to ensure your work-from-home employees are keeping your network and data secure: make sure your employees and contractors are not using their home computers or devices when they are working from home. Add a firewall to ALL computers and devices that will be utilized at home. Finally, your network and data are not truly secure unless your employees utilize a VPN (virtual private network).

There's no need to invite in more problems by letting your computer and network security slide during these times. We would be happy to help you create or even improve your work-from-home environment.

While this coronavirus scare has negatively affected countless businesses, we are proud to say we are open and continue servicing our customers. If you need additional security advice or would like to have a consultation to discuss how to keep your data safe or how we can help you work more effectively, connect with us today.

HOW TO DEAL WITH INCREASING CUSTOMER EXPECTATIONS

The more you do for customers, the more they expect. That is the nature of customer service.

Excellent service providers scramble to meet the expectations of customers who have become accustomed to excellent service. Aggressive competitors continue to bump up their offerings in an attempt to take your customers from you. As a result, this has turned into a perpetual desire by customers for more, better, different, and improved services.

In most cases, "good enough" isn't enough.

The great art and science of business are to improve product or service offerings without giving up margins or increasing prices beyond what customers are willing to pay. It is about adding value without spending too much to do it.

Any business that can't do this will be relegated to competing at the low end of the market on price alone, and that is a difficult place to be.

Rally your team, from engineering and manufacturing to sales and support, to regularly brainstorm how you can profitably grow your value proposition. Customers will increasingly demand it.

Here are eight things you can do about them.

1. Find out what is important to customers: what they require and what they desire. You're not clairvoyant, so routinely ask customers for input.

2. Explain your value proposition when you must say no. If you can't do something the customer wants, explain why. But see if there is something acceptable you can do instead.

3. Educate customers about the value you create for them. If they don't know about it or appreciate it, it isn't valuable.

4. Hold quarterly sessions with your team to brainstorm how to add value to the customer experience.

5. Evaluate the entire customer experience. Look for failure points and irritations that can be eliminated and improvements that can be made.

6. Pay more attention to your customers than to your competition. Know what your competitor is doing, but put your customer at the center of your focus.

7. Pleasantly surprise customers whenever you can. Work with your team to brainstorm ideas on how to do that.

8. Treat better customers better. Treat all customers well, but those who spend more should get preferential treatment.

Business goes to the bold and innovative. Creativity and imagination are the best tools for continually rethinking your value proposition. Proper execution delivers and makes customers glad they keep coming back to you for more.

IT Security Tip of The Month

DO THESE 3 THINGS TO MAKE SURE YOU DON'T GET HACKED DURING COVID-19

Take advice from the secret service, FBI, and FTC warning american's on how to avoid becoming targets.

Cybercriminals have been impersonating authority figures to profit from desperate individuals reaching for any means of relief from COVID-19.

If you come across a claim that mentions anything to do with relinguishing the COVID-19 disease – be advised – this may be a scam! This includes blogs and articles mentioning alternatives to combat the virus including oil of oregano, garlic pills, elderberry or any other "natural" cure has not been proven to cure this virus and should be taken with a grain of salt.

Tips To Practice Cyber Safety

- BE AWARE of fraudulent emails claiming to contain "new information" about the virus requiring people to share sensitive information in order to gain access.
- Fake fundraisers is another area that has been used.
- Always double check before clicking on a link; this poses the threat of installing malware on your device.
- If you have the slightest bit of doubt, believe it and don't do whatever is being asked of you without making that phone call from a known number. ALWAYS DOUBLE CHECK!

> ***"Success is going from failure to failure without losing your enthusiasm."***
>
> *Winston Churchill*

3 WAYS TO GROW YOUR BUSINESS WITHOUT SPENDING A DIME

Follow a thought leader in your industry

Whether you follow them on social media or their blog, keep up-to-date with the issues. Then do further research into those issues. Staying updated with current trends keeps you in the know and more likely to learn something you can easily apply to your own business.

Use your best testimonials

If someone posts a great review on Google, for example, reach out and ask about using it in your marketing. Or reach out to customers who you already have a good relationship with and ask if they're willing to give you a testimonial. It builds credibility.

Partner up

It pays to develop partnerships with existing vendors or other businesses that are adjacent to yours. That is to say, look for opportunities to share customers. If you have a customer who's looking for a specific service you don't offer, point them to someone who does (your partner). And your partner will do the same. Reach out into your business community and see what kind of relationships you can form.

Business Insider, Feb. 13, 2020

DO THESE 3 THINGS TO MAKE SURE YOU DON'T GET HACKED

Train Up.

Get your entire team trained on IT security fundamentals and best practices. They should know how to create strong passwords, how to safely access the web and how to securely use e-mail – including how to identify phishing scams. They should have a clear understanding of today's threats and how to be proactive in addressing those threats.

Invest in good tech.

You should be invested in solid malware protection, including antivirus software and firewalls. All of your data should be backed up to the cloud and expertly secured using encryption software. You should also be invested in threat monitoring.

Establish relevant systems and processes.

Have standard operating procedures (SOP) in place to train employees, respond to threats and access networks. For example, are employees connecting with unverified devices from home? Establish rules on what can and cannot happen. Another example: are your cloud backups set up correctly? Is someone checking it? Again, have SOP in place to address these kinds of issues.

Small Business Trends, Feb. 13, 2020

TECH TRIVIA QUIZ ENTER TO WIN!

You can be the Grand Prize Winner of this month's Trivia Challenge Quiz! Just be the first person to correctly answer this month's trivia question and receive a **$25 Amazon gift card**. Ready? Call us with your answer!

'.MOV' extension usually refers to what kind of file?

A) Image File
B) Animation/Movie File
C) Audio File
D) MS Office Document

Call us right now with your answer!

608-291-9723

COMPUTER MAGIC

608-291-9723 computermagic.us
101 Nichols Rd, Monona, WI 53716
tom@computermagic.us