

TECHNOLOGY BYTES

Insider Tips to Make Your Business Run Faster, Easier & More Profitable

“As a business owner, you don’t have time to waste on technical and operational issues. That’s where we *shine!* A true professional IT support team you can count on available 24/7.”



– Doug Johnson , CyberTrust IT Solutions
Contact us:- (949) 396 1100



Exclusively for CEOs!

DID YOU KNOW?



Are YOURS There Too?

• To know, visit pg.2

What's Inside

Page 1

3 Ways To Stop Cybercriminals Cold In Today's Crazy Times

Page 2

Free Dark Web Scan For CEO's

Page 3

Expect, Inspect, Correct

Page 4

3 Things To Make Sure You Don't Get Hacked

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 probably been focused on shifting 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 even had time to think about cyber security 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’s exactly what they’re thinking right now. In fact, they’re probably

working overtime right now to craft new malware while our lives have been turned upside down. Yes, as you’re focused on your business, that’s exactly what they’re thinking right now. In fact, they’re probably working overtime right now to craft new malware while our lives have been turned upside down. Yes, as 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 cost \$6 trillion (that’s a 6 followed by 12 zeroes!) by the year 2021? But, now is when hackers are expected to do their absolute most damage. 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 time 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 finance data to be compromised. Make a point now to reevaluate 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 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 a lot of 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 continuously 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, simply connect with us today.

“Did you know that cybercrime is expected to cost \$6 trillion (that's a 6 followed by 12 zeroes!) by the year 2021?”

The Dark Web is Overflowing With CEO's Credentials...

Are YOURS There Too?

Find Out Right Now With Our FREE & Confidential Dark Web Scan
EXCLUSIVELY for CEOs!

Get The Peace of Mind That Your Credentials,
Company Financials and Customer
Records are 100% SAFE! !

FREE Dark Web Scan for CEO's

Go To: <https://bit.ly/2KPABqR> and fill out the form
Or Call: (949) 396 1100



Shiny New Gadget Of The Month:



Zepp Golf 2 Swing Analyzer

Improve your golf game with a device smaller than a golf ball. The Zepp Golf 2 is a remarkable piece of tech that attaches to the back of any golf glove. It's packed with sensors and delivers real-time analysis of your game.

Using Bluetooth, the Zepp Golf 2 pairs with your smartphone. As the data is analyzed, it's displayed on the accompanying app. It tracks your club speed, backswing positioning, hip rotation, consistency and much more. The Zepp Golf 2 also has a long-lasting battery - up to eight hours - so it will definitely make it through your next game without a hitch. The Zepp Golf 2 is compatible with both iPhone and Android devices. Learn more at [Amazon](https://www.amazon.com/zepp-golf-2) or [Zepp.com](https://www.zepp.com).

EXPECT, INSPECT, CORRECT



It's no coincidence that we have so many ways to say we made a mistake: botched, flubbed, mishandled, misjudged, mucked, messed, screwed or goofed up - just to name a few.

As a leader, you'll hear each of these (some more than others, and likely some more explicit than the ones I've named here) pretty often. When you do, it's important to first try to remember that whoever made the mistake probably didn't mean to.

Put yourself in their shoes. Ask yourself if you have ever made a mistake. A bad decision? Have you ever said something you regret? Ever disappointed your boss? Jumped to the wrong conclusion? Done something foolish or outright stupid? Everyone has. Sometimes a simple reminder of our past failings enables us to be a little more tolerant of others' missteps.

Mistakes don't have to be the end of the world. Mistakes are inevitable

and are often essential to learning and progress. They should guide you, not define you, on you and your employees' journey to success. Mistakes show effort, and if you learn from them, they can be some of the best tools for growth.

I've heard it said before that the only people who don't make mistakes are those who do nothing at all. To me, the most interesting part about errors is the gradual evolution in how they're classified. First, they start as mistakes. Then they turn into lessons, followed by experiences and finally as gifts that help us succeed.

Therefore, the only real mistake is the one from which we learn nothing. Keep that in mind as you're dealing with your employees or considering your own shortcomings. It's one thing to recognize that mistakes are learning opportunities - it's another to actually implement that concept in your organization.

WAIT!

BEFORE You Set Up A Work-From-Home Environment For Your Employees

READ THIS FIRST...

Learn The 3 Essential Steps You Must Take Now To Keep Hackers Out While Your Team Works Remotely



Read More - <https://bit.ly/2YTJT22>

■ **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

To Avoid Cyber Attacks



- Practice Good Password Management
- Use Long Passwords
- A Strong Mix Of Characters
- Update Your Passwords Periodically

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 anti-virus 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? checking it? Again, have SOP in place to address these kinds of issues.

Small Business Trends, Feb. 13, 2020

Need Help Getting Your Employees SECURELY Set Up to Work From Home?

We Can Help!

■ **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 they're talking about. Then do further research into those issues. This 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

THANK YOU

FRONTLINERS

FOR YOUR SERVICE TO THE NATION WE SALUTE YOU!

PLEASE STAY SAFE!