

What's New

Our own Scott Huxley spoke with WFMZ-TV regarding a recent Lehigh Valley Health Network incident in which a ransomware group hacked into a physician's computer. Following is an excerpt from the article (wfmz.com):

Cyber security expert Scott Huxley says LVHN is doing the right thing by not paying the ransom. "Just because you pay it, it doesn't mean you will get the data back and in many cases they are still sharing that information, even though they were paid," Huxley said.

Huxley says, unfortunately, the damage has been done. "There's not a lot you can do, the only thing you can do as a citizen potentially is invest in some mechanisms that may protect your data, that alert you, you'll receive credit monitoring in these types of instances."

April 2023



Syscom Business Technologies is dedicated to technology success for your business. We support businesses throughout Michigan and Pennsylvania from

our offices in Grand Rapids, Traverse City, Greater Metro Detroit and the Lehigh Valley. Over many years, our clients have truly seen increased success through our business relationship.

Scott Huxley, Managing Principal



Improve Your Cyber Security Awareness Learn About Today's Most Common Types of Cyber-Attacks

If you've turned on the news sometime during the past few years, you've probably heard of more than one instance of a business closing due to a cyber-attack. You may think your business is too small for hackers to target you, but this couldn't be further from the truth. Every business is at risk of cyber-attack and should be well-prepared to defend against these threats. With the right type of attack, a cybercriminal can gain valuable information about your business, customers and employees, which can be used to damage your reputation and hurt you financially.

If you're a business owner or leader and you want to ensure your business is well-protected, check out the most common cyber-attacks that are affecting companies today. From there, you can implement cyber security plans and tactics to ensure your business is protected.

Phishing Scams

Phishing is a type of social engineering where an attacker sends a fraudulent message designed to trick a person into revealing sensitive information to the attacker or to deploy malicious software on the victim's infrastructure. Phishing scams can wreak havoc on your business and personal life. You may have seen an e-mail from someone claiming to be Amazon or your credit card company asking for sensitive information. Often, the e-mail address does not line up with who the person is claiming to be.

When a phishing scam targets your business, they'll likely request valuable information from your employees such as passwords or customer data. If your employees fall for the scam, they could give a cybercriminal unprecedented access to your network and systems. This may also allow the cybercriminal to steal private employee and customer

Continued on pg. 2

Continued from pg. 1

information, leaving your employees vulnerable to identity theft. Phishing scams can be averted by using common sense and providing cyber security training to your employees. Most companies will not request private information over e-mail. That being said, if an employee receives a suspicious e-mail, they should do their due diligence to ensure the e-mail is genuine before responding in any way.

Malware

Malware is software installed on a computer without the user's consent that performs malicious actions, such as stealing passwords or money. There are many types of malware, including spyware, viruses, ransomware and adware. You can accidentally download malware onto your computer by clicking on sketchy links within e-mails or websites. You might not even notice you have malware on your computer right now. If your computer is operating more slowly than usual, web browsers are taking you to random sites or you have frequent pop-ups, you should scan your computer for malware.

Prevention is key in stopping malware from affecting your business. Hiring and utilizing a managed services provider is the best way to protect your business, as they will continually monitor your network for exploitable

“Every business is at risk of experiencing a cyber-attack and should be well-prepared to defend against these threats.”

holes. With malware, it's always better to play it safe than sorry. If a cybercriminal is able to use ransomware on your network, your business could be stuck at a standstill until you pay the ransom. Even if you can pay the ransom, your reputation will still take a hit, and your business could be greatly affected. Be careful where you click on your phone, too, since malware attacks on cellphones have become more common.

Attacks Involving Passwords

How do your employees access your network or computer systems? They most likely use a password to log in to their computer, access their e-mail and much more. What would happen if someone with bad intentions gained access to one of your employee's passwords? Depending on the individual's access, they could obtain sensitive information about your business, customers and employees.

Your team should be using long, complex passwords for their accounts, and each password for every account should be different. Encourage your employees to use password managers that will allow them to create the most complex passwords possible and keep track of them more easily. You can also incorporate multifactor authentication to ensure nobody can steal a password and gain access immediately. You should make your employees aware of this during your annual cyber security training.

If your business falls victim to a cyber-attack, it could have lasting consequences for everyone involved. Now that you know the most common types of cyber-attacks, you can start implementing plans to ensure you and your business stay protected.

Free Report Reveals The Critical Protections Small Businesses Need Today: Don't Be A Sitting Duck for Cyber-Attack!

If you don't think you're in danger of being targeted by cyber criminals because you're "small" and not a big target like a Target or Home Depot, it is extremely important that you read this special report: **"7 Urgent Security Protections Every Business Should Have In Place Now."** This report reveals:

- The #1 threat to your business that even the BEST firewalls and antivirus software can't protect against.
- The biggest security risks with cloud computing and what you need to do to stay safe if you're going to store client data, confidential data and financial information in the cloud.
- A common misconception about business bank fraud that will shock you – and 3 simple things you can do to protect your bank account from unauthorized access and theft.
- How to keep your network secure with the proliferation of mobile devices, cloud applications, e-mail, and social media sites connecting to your computer network.



Get your FREE copy today at www.syscombusiness.com/sittingduck

Working Remotely

Continued from pg. 4

work in a toxic workplace and no business owner wants to run one, but how do you know if your business is gradually becoming more toxic? Here are a few warning signs to watch out for.

Mass Turnover: Are employees quitting in droves? Do you know why? You should be holding exit interviews with the employees who are leaving to determine why they want to work elsewhere. Allow them to speak openly, and you'll gain valuable insight.

Low Employee Morale: If your employees are not enthusiastic about their work or tend to work on individual tasks more often, you may have a morale problem. Hold a meeting with your team and allow them to speak freely to understand where the morale issue stems from.

Gossiping Employees: Are your employees talking negatively about each other or the business? If so, you must correct it as soon as possible. Figure out why gossip has increased at your company and develop solutions to solve the root problem.



"I think these, 'take your kid to work' days are just a ploy to get free tech support."

Don't Come Back To Work

Don't come back to work. Instead, move forward in leading your company and managing your career by embracing remote work. Even though ghSMART has been remote-only for over 26 years, I never fully realized how enthusiastic I am about remote work until I heard that many companies are forcing workers to come back into offices.

Before the COVID-19 pandemic, "work where you want" was a rare concept - but during the pandemic, basically every company that could function with people working remotely shifted to that mode out of necessity. I thought that mode would stick, and we'd see the landscape of cities shift from "places people go to work every day" to "places people go to work sometimes, eat, shop, learn and play." But it seems I was wrong.

There isn't a great argument against the idea of remote work, but there is one *for* it. Remote work improves financial and operating performance and productivity for companies while also improving job and life satisfaction for employees. A 2015 Stanford University study published in the *Quarterly Journal of Economics* showed a 13% performance increase from remote working, and employee attrition rates fell by 50%.

Even with all of the research and information available that shows remote work is beneficial, there are still some myths floating around. For example, many say you can't build a great company culture when your business operates remotely. This is entirely false. I think an excellent culture begins with doing what's best for people. Making people commute to offices daily does not seem to be in anybody's best interests.



Another common myth states that people don't work as hard remotely as they do in an office. I believe that if you have a transparent culture where performance is measured, you can pay people according to the value they are creating. They will be incentivized to work productively and not lollygag - even if they are working remotely. But I guess many companies have not yet figured out how to pay employees based on a scorecard of measurable results and instead pay based on hours worked. They should be worried about lollygagging anyway, both in the office and for people who work remotely.

If you run or own a company, please continue to experiment with allowing your people to work remotely when possible. I believe this is the future of work, both because of the demonstrable benefits to companies in operating and financial performance and the benefits to workers due to having more control over their time.



Dr. Geoff Smart is chairman & founder of ghSMART, a leadership consulting firm that exists to help leaders amplify their positive impact on the world. Dr. Smart and his firm have published multiple New York Times bestsellers. He stays active in his community and has advised many government officials.



37257 Mound Rd, Suite B
Sterling Heights, MI 48310

81 Highland Ave, Suite 210
Bethlehem, PA 18017

Inside This Issue

The Most Common Types of Cyber Security Threats | 1

The Critical Protections Small Businesses Need Today: Don't Be A Sitting Duck for Cyber-Attack! | 2

Don't Return to The Workplace | 3

Working Remotely? Improve Your Work-Life Balance In 3 Steps

As many businesses continue to utilize remote workers, some employees are struggling to find a proper work-life balance. They constantly find themselves drawn back to their work after completing all tasks for the day, which takes away from their ability to enjoy hobbies or spend time with their families. Maintaining a proper work-life balance is beneficial to all aspects of our lives, including productivity and overall happiness. If you're struggling to maintain your work-life balance, here are three ways to include more personal time in your daily routine.

Set Boundaries: Don't allow yourself to be pulled back into work. Turn off your work phone and e-mail when your shift has ended for the day.

Create A Workspace: Do not work in the same areas you use for relaxation. This will make it more difficult to relax when you've finished working.

Dress Professionally: It might be tempting to wear sweatpants while working from home, but try to wear the same clothes you would wear if you had to go into an office. When the workday comes to a close, you can dress in



more comfortable clothing, allowing you to easily unwind.

Is Your Workplace Becoming Toxic? Watch Out For These Warning Signs!

Over the past year, the idea of toxic workplaces has garnered quite a lot of attention. No employee wants to

Continued on pg. 3