TECH TIPS

TECHNOLOGY INSIGHT THAT BUILDS BUSINESS

HODGSON
CONSULTING & SOLUTIONS

Inside This Issue

WHAT'S NEW

BOOK RELEASE

COMING SOON What's next for Hodgson Consulting & Solutions?

SMALL BUSINESS TECH DAY WISCONSIN

HODGSON

October 2022

This monthly publication provided courtesy of Robert Zehnder President of Hodgson Consulting & Solutions.

Our Mission:

To eliminate every technical frustration, obstacle and inefficiency for companies with multiple locations and/or a remote workforce.

Keep Your Information Secure

By Using Strong Passwords

We use passwords for just about everything. Most of us have to enter a password to get into our computers, then enter more passwords to access our e-mail, social media profiles, databases and other accounts. Even our cell phones and tablets can and should be password-protected. In fact, if you aren't securing all of your devices and accounts with passwords, you should definitely start. It could help prevent your business and personal information from becoming compromised.

Why Passwords?

We use passwords to ensure that those who don't have access to our accounts can't get access. Most of our devices hold large amounts of personal information. Think about the potential harm someone could do if they gained access to your personal cell phone. They would immediately be able to see all of your contacts, pictures and applications. They might even be able to log in to your e-mail, where they could obtain your banking information. If this type of access falls into the wrong hands, it could be detrimental to your life. Passwords offer the first line of defense to prevent others from obtaining sensitive information.

This becomes even more important if you own a business. Each of your employees should be utilizing strong passwords to access company information. If your business is not using passwords— or is using simple passwords— you could be opening yourself up to hackers and cybercriminals. If a cybercriminal gains access to your company's private information through a weak password, they will gain access to customer information, which could damage your reputation and open you up to lawsuits. That being said, everyone within your business needs to utilize complex and unique passwords.

Making A Strong Password

Not all passwords are created equal. When it comes to making a strong

Continued on pg.2

Continued from pg.1

password, you must think about it. If you use a password that you can't remember, then it's essentially useless. And if you use a password that's too easy to remember, your password probably won't be strong enough to keep cybercriminals out. Your password should be long, have a mix of lowercase and uppercase letters, utilize numbers and special characters, have no ties to personal information, and should not be a word from the dictionary.

In the grand scheme of things, it's not enough to just create complex passwords. They also need to be unique. In addition to this, you should use a different password for each and every one of your accounts to help maximize their effectiveness. Think about it this way: let's say you use the same password across your business e-mail accounts, social media accounts, and bank accounts. If someone decrypts the password for your Facebook page, they now have the password for more valuable accounts. If you can't tell that your social media account was compromised, the cybercriminal could try to use that same password to gain access to more important accounts. It's a dangerous game that can be avoided by using unique and complex passwords for every account you use.

> **"You should use a different password for each and every one of your accounts to help maximize their effectiveness."**

Remembering All Of These Passwords

You may be worried about remembering all of your passwords if you have to create a unique one for each of your accounts. Your first thought may be to write them down, but that might not be the most secure option. If someone gets their hands on your little black book of passwords, they'll immediately gain access to all of your accounts with a handy directory showing them exactly where to go. Instead, you should utilize a password manager to help keep track of all of this sensitive information.

With a password manager, you only have to worry about remembering the master password for your password manager. All of your other passwords will be securely hidden. Password managers also give you the option to create random passwords for your accounts to bolster their security. That way you can have the most complex password possible without worrying about forgetting it. Additionally, password managers can also help remember the answers to security questions and more, so that you never get accidentally locked out of one of your accounts. They're easy to use, convenient and secure.

Passwords are an important part of your cyber security plan. Make sure you and your employees are using complex and unique passwords. It can also help you implement some training so your employees understand the importance of secure passwords. When used correctly, passwords will help deter any would-be cybercriminals from accessing your sensitive information.

Why Are Cybersecurity Insurance Claims Raising?

Cybersecurity insurance protects businesses in the event of online attacks. Insurance providers can absorb a considerable amount of the impact, allowing companies to recover faster and get back on track after experiencing a cyber breach. Recent data shows an alarming rise in the cybersecurity claims made by businesses across various industries around the world.

Let's try to figure out why this is happening.

The Upsurge of Cyber Claims for Cybersecurity Insurance

With continuous and rapid technological developments, online threats have also advanced considerably. Social engineering and ransomware attacks have risen dramatically. As a business owner, you must understand what has been happening to protect your company from impending threats.

Pandemic-Related Threats

During the pandemic, most people were online most of the day, either for work, for school, or stuck at home with nothing else to do. As the remote population ballooned, so did the number of unprotected home-based employees. The companies they worked for became much more vulnerable to disastrous attacks.

A New Approach to Ransomware Involving Cybersecurity Insurance

Initially, hackers targeted individual users and small companies with this malicious software. But recently, they have realized that they could earn more from big corporations willing and capable of paying any ransom amount. Some hackers have shifted their focus to providing ransomware as a service or RaaS to users who wish to launch an attack but do not have the know-how. With easier access, it's no surprise that more businesses and individuals are becoming victims and filing claims with their cybersecurity insurance providers.

Social Engineering Strategies

Many current cybersecurity claims stem from these new social engineering attacks. These attacks come in many forms, such as phishing, baiting, scareware, pretexting, and many more. It's interesting how social engineering tactics produce so many victims when it is one of the easiest cyberattacks to identify and avoid.

AVOID A CYBERSECURITY NIGHTMARE

Treat yourself to these security best practices...

HANDLE ATTACHMENTS WITH CAUTION
Turn off the option to automatically download attachments in your email. Download applications from trusted sources or marketplaces. Scan attachments before opening and keep anti-virus software up to date.

BEWARE OF OBSCURED URLs
Pay close attention to web addresses. Malicious persons fool unsuspecting users by changing the spelling of URLs.

PROTECT PERSONAL INFO
Call companies & individuals who seek sensitive information to verify that the request is legitimate.

REPORT SECURITY BREACHES
Report suspicious data or security breaches to your supervisor or incident response team immediately.

THE SCARIEST STATS ABOUT CYBERSECURITY

95% of cybersecurity breaches are made possible by human error.

Since the start of the COVID-19 pandemic, there has been a **300%** increase in the number of cybercrimes in the USA.

In 2022, businesses around the globe face a ransomware attack every **11 seconds**.

By the end of 2022 cybercrime is expected to cost the world **$7 trillion**. This figure will climb to **10.5 trillion** by **2025**.

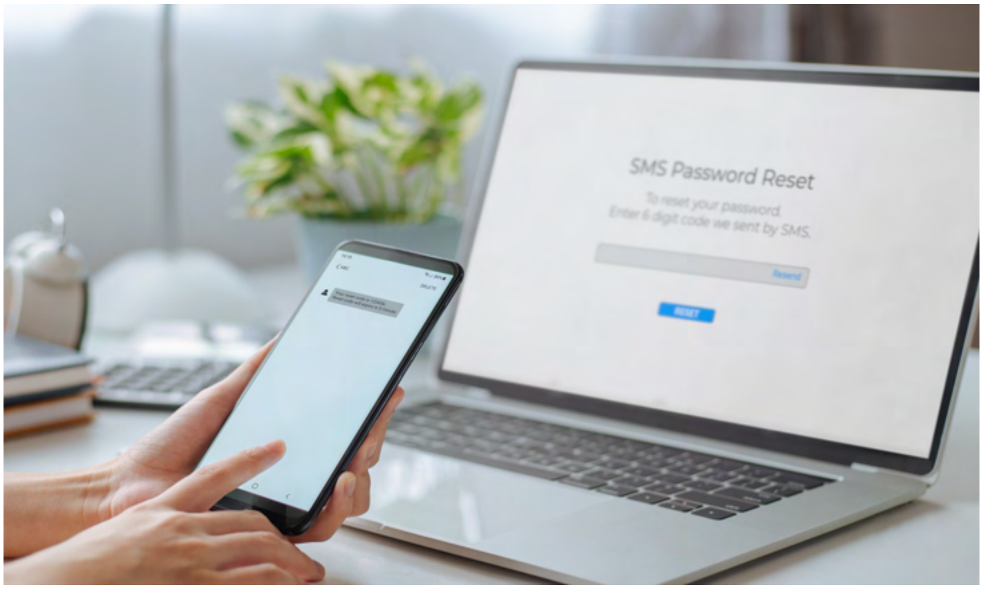
60% of organizations have experienced a cyberattack in the last 2 years.

61% of cybersecurity professionals believe that their team is understaffed.

85% of all data breaches involve human interaction.

HODGSON CONSULTING & SOLUTIONS

Take Advantage Of Google Reviews



When you are deciding on a restaurant to dine at, you might check the Google reviews to help with your decision. The same thing goes for your business. Before people come in to buy your product or services, they might check your Google reviews – so it's important that your reviews positively reflect your business. If you own a company, you should understand how Google reviews work and do everything you can to encourage customers to leave positive ratings and comments.

If you haven't already claimed your Google business profile, you should do so immediately. It will allow you to add pictures and a description so customers know what to expect from your business. When customers have completed a purchase with you, encourage them to leave a review if they had a positive experience. Some customers may need help with the review process, so teach them how to leave a review if they have never done it before. Make sure you thank customers who leave positive reviews and try to fix the issues explained in your negative reviews. Being a responsive owner will reflect positively on your business. When you use Google reviews to your advantage, you will see a boost in clientele.

3 Easy Ways To Make Your Mac More Secure

Data breaches and malware attacks have been on the rise over the past few years, so you must take the necessary precautions to protect your devices. Below you will find three easy ways to make your Mac more secure.

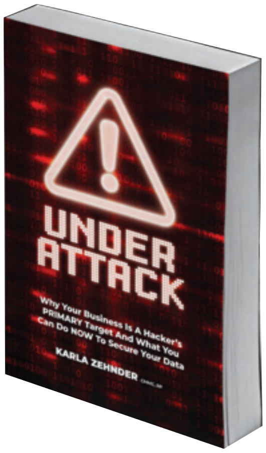
- Install a mobile device management profile so you can give an administrator remote access to the device. If your Mac is ever stolen, you can locate it and lock it before any of your data becomes compromised.

- Utilize multifactor authentication, which will require you to confirm your login on another device. This adds an extra layer of security to your Mac.

- Backup your data to protect yourself from ransomware attacks. Consider buying an external hard drive or a cloud storage solution and backup software to do so.

WHAT'S NEW

BOOK RELEASE


UNDER ATTACK
Why Your Business Is A Hacker's PRIMARY Target And What You Can Do NOW To Secure Your Data
KARLA ZEHNDER

We are excited to announce a new book release, *Under Attack*, written by our CEO Karla Zehnder. This book is jam packed with valuable information, tips, and strategies on how to PROTECT your business from cyber threats, regulatory action, scams, and business crippling disasters.

Read this book and you'll discover:

- How your business RIGHT NOW is at risk for losing considerable productivity, sales, customers, lawsuits, and money from malware attacks
- Why YOUR BUSINESS is the #1 target for cyberattacks, and why YOU are your business's weakest link
- What are the TOP NINE ways cybercriminals HACK your network and what you can do now to stop them
- What exactly is CLOUD COMPUTING and how it can enhance your network security while increasing productivity and lowering costs
- The major risks of allowing your employees to work from home and the FOUR SIMPLE STEPS to ensure this business model never compromises your network
- And so much more!

Order Your FREE Copy Here: www.hodgsonconsulting.com/underattack

COMING SOON

What's next for Hodgson Consulting & Solutions?

SMALL BUSINESS
TECH DAY
WISCONSIN

We are extremely proud to host the first ever **Small Business Tech Day** in Wisconsin on **December 15, 2022!**

The event is designed to help small businesses equip themselves with the best technology and practices available today to increase productivity and profitability and protect them against online threats.

On this FREE online event, you will get to hear from:

- ★ **Kevin O'Leary** - Shark Tank celebrity and entrepreneur
- ★ **Eric O'Neill** - former FBI counter-terrorism and counterintelligence operative
- ★ **Mike Michalowicz** - best-selling author and entrepreneur extraordinaire
- ★ **Karla Zehnder** - our award-winning CEO

and more...

Scan the QR code to watch a promo video

Stay tuned and follow us on social media for more information about the upcoming Small Business Tech Day.