TECH TIPS
TECHNOLOGY INSIGHT THAT BUILDS BUSINESS

HODGSON
CONSULTING & SOLUTIONS

Inside This Issue

June 2021

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.

Breaking Bad Habits 4 Ways Your Employees Are Putting Your Business At Risk Of Cyber-Attack

Your employees are instrumental when it comes to protecting your business from cyberthreats. But they can also become targets for hackers and cybercriminals, and they might not know it. Here are four ways your employees might be endangering your business and themselves — and what you can do about it.

1. They're Not Practicing Safe And Secure Web Browsing. One of the most basic rules of the Internet is to not click on anything that looks suspicious. These days, however, it can be harder to tell what's safe and what isn't.

A good rule of thumb is to avoid websites that do not have "https" in front of their web address. The "s" tells you it's secure – https stands for Hypertext Transfer Protocol Secure. If all you see is "http" – no "s" – then you should **not** trust putting your data on that website, as you don't know where your data might end up.

Another way to practice safe web browsing is to avoid clicking on ads or by using an ad blocker, such as uBlock Origin (a popular ad blocker for Google Chrome and Mozilla Firefox). Hackers can use ad networks to install malware on a user's computer and network.

2. They're Not Using Strong Passwords. This is one of the worst IT security habits out there. It's too easy for employees to use simple passwords or to reuse the same password over and over again or to use one password for everything. Or, worse yet, all of the above.

Cybercriminals love it when people get lazy with their passwords. If you use the same password over and over, and that password is stolen in a data breach (unbeknownst to you), it becomes super easy for cybercriminals to access virtually any app or account tied to that

Continued on pg.2

Continued from pg.1

password. No hacking needed!

To avoid this, your employees must use strong passwords, change passwords every 60 to 90 days, and not reuse old passwords. It might sound tedious, especially if they rely on multiple passwords, but when it comes to the IT security of your business, it's worth it. One more thing: the "tedious" argument really doesn't hold much water either, thanks to password managers like 1Password and LastPass that make it easy to create new passwords and manage them across all apps and accounts.

3. They're Not Using Secure Connections. This is especially relevant for remote workers, but it's something every employee should be aware of. You can find WiFi virtually everywhere, and it makes connecting to the Internet very easy. A little too easy. When you can connect to an unverified network at the click of a button, it should raise eyebrows.

And unless your employee is using company-issued hardware, you have no idea what their endpoint security situation is. It's one risk after another, and it's all unnecessary. The best policy is to prohibit employees from connecting to unsecured networks (like public WiFi) with company property.

Instead, they should stick to secure networks that then connect via VPN. This is on top of the endpoint security that

should be installed on every device that connects to your company's network: malware protection, antivirus, anti-spyware, anti-ransomware, firewalls, you name it! You want to put up as many gates between your business interests and the outside digital world as you can.

4. They're Not Aware Of Current Threats. How educated is your team about today's cyber security threats? If you don't know, or you know the answer isn't a good one, it's time for a change. One of the biggest threats to your business is a workforce that doesn't know what a phishing e-mail looks like or doesn't know who to call when something goes wrong on the IT side of things.

If an employee opens an e-mail they shouldn't or clicks a "bad" link, it can compromise your entire business. You could end up the victim of data breach. Or a hacker might decide to hold your data hostage until you pay up. This happens every day to businesses around the world – and hackers are relentless. They will use your own employees against you, if given the chance.

Your best move is to get your team trained up and educated about current threats facing your business. Working with a managed service provider or partnering with an IT services firm is an excellent way to accomplish this and to avoid everything we've talked about in this article. Education is a powerful tool and, when used right, it can protect your business and your employees.

> **"Education is a powerful tool and, when used right, it can protect your business and your employees."**

FREE Report: 12 Little-Known Facts Every Business Owner Must Know About Data Backup And Disaster Recovery

You will learn:

- The only way to know for SURE your data can be recovered if lost, corrupted or deleted – yet fewer than 10% of businesses have this in place
- Seven things you should absolutely demand from any off-site backup service
- Where many backups fail and give you a false sense of security
- The #1 cause of data loss that businesses don't even think about until their data is erased

Claim your FREE copy today at
www.hodgsonconsulting.com/protect-your-data

Are You Backing Up Your Backups?

Back up your backup. Google can't protect you from negligent insiders.

62% of insider incidents are caused by negligence.

23% of insider incidents are caused by malicious insiders.

Is your Google Workspace backed up?

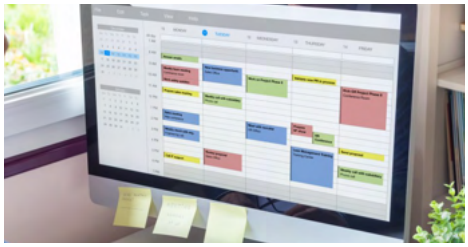
- Yes
- No
- I don't know

69% of survey respondents agree that the top cloud security concern is data loss.

Eliminate Workplace Distractions To Maximize Your Productivity

While most of us accept that distractions will be a part of our day, if your intention is to get things done and to stay productive and focused, you'll need to minimize those distractions. No, we'll never be able to eliminate them 100%, but we can certainly try. Here's what you can do to cut distractions.

Block Time On Your Calendar (And Stick To It). Use your calendar to its full advantage. Mark time off for e-mails, for *all* projects, phone calls, Zoom calls, you name it! If it's part of your normal day, put it on your calendar. Even throw on time for miscellaneous stuff. Then share it with all relevant parties and stick to it. If you're working on a project between 1:00 p.m. and 3:00 p.m., that's the word.



Use Sound To Your Advantage. A common source of distraction is sound: it can be office chatter in the background or even neighborhood sounds (for those working from home). Find a sound that complements your workflow. It might be chill music or the sounds of rain or a babbling brook. Find the right sound that helps you zone in and blocks disruptive sounds.

Forbes, March 15, 2021

The 2 Best Investments You Will Ever Make

Practically every successful person has something in common with every other successful person. Millionaires and billionaires share these habits – habits that are absolutely crucial if you want to achieve the success that's on your mind.

1. Read, Read And Read Some More. Warren Buffett and Bill Gates are prime examples of this, but it's one of the most common traits among the most successful businesspeople in the world ... They are constantly reading: books, blogs, newspapers, magazines and anything else that enriches their personal and professional lives.

2. Get Educated. Whether you hire a private coach, take courses (like continuing education) or hire consultants, there are pros who can teach us more about what we do (or want to do) and how to improve ourselves or our businesses. While we may be good at what we do, there is always room for improvement – you just have to be open to it.

Inc., Feb. 24, 2021