

INSIDE THIS ISSUE

How To Safely Share Passwords With
Employees • P. 1

FREE REPORT:
The Cybersecurity Crisis
How To Protect Your Accounts, Data,
Information And Reputation From
Cybercrime • P. 2

Does My Business Really Need Cyber
Liability Insurance? • P. 3

JOIN THE 7 FIGURE ACADEMY

By Mark Anthony

Most business owners have a difficult time stepping away from their work. They want to profit as much as possible, which means they believe they must give all of their time, effort and attention to the business. But what if you could run a profitable business without sacrificing everything else? In *Join The 7 Figure Club* by Mark Anthony, you'll learn how to increase sales, improve staff accountability, devise ways to reclaim your free time and much more. Anthony offers practical advice for readers and shares the seven pillars of a thriving business. If you're ready to take your business to the next level, add *Join The 7 Figure Club* to your reading list.



WANT TO BECOME A BETTER LEADER?

Learn How To Manage Yourself First

Every business owner and leader wants to lead and inspire their team effectively, but this is easier said than done. You're going to face challenges within your business that will put your mettle to the test. Many of these obstacles will stem from your team as you learn to manage different personalities and overcome communication barriers. If you want to lead your team properly, you must take a step back and focus on yourself first.

Many employees look to their leaders for support, encouragement and guidance. As their leader, you have to remember you are setting an example for your team, so you must stay aware of every action you take. Pay attention to how you talk to people and how you're spending your time while at work. You should be acting in the same manner you would expect from every other member of your team. If you're not, it's time to make some adjustments. Your business's success and your employees' behavior begins and ends with you. Become the leader you would want to work for, and your employees will respond positively.

Is It Time For A Vacation From Work?

Business leaders want their companies to be profitable and often dedicate hours of overtime every week to ensure everything



runs smoothly. While this might give your business a boost, it can be damaging to your mental health. Many leaders have a hard time taking a break from their business and end up burning out before reaching the pinnacle of success. Don't fall into this trap.

Here are a few warning signs to pay attention to that tell you it's time to take a break from work.

- **You feel anxious or nauseous every morning before work.** Your body will tell you when it needs a break. Listen to it!
- **You make careless mistakes.** Overworking ourselves can take away from our focus, which causes us to make mistakes we wouldn't normally make.
- **Your motivation has vanished.** If you feel like you have to force yourself through the motions at work, it's likely time for a vacation.

CYBERTOOLS CHRONICLE

Insider Tips To
Make Your
Business Run
Faster, Easier And
More Profitably

WHAT'S NEW AT CYBERTOOLS

Cybertools is a sponsor for this wonderful event!! Join us for an amazing evening and be uplifted, inspired, and dream big as this year's Women to Watch take the stage and share their personal stories.
September 14th
5:00-7:30 p.m.
Silver Cloud Point Ruston
Scan the QR code
to get your tickets!!!



SEPTEMBER 2023

This monthly publication is provided courtesy of David & Aubri Stone, Owners of Cybertools, Inc.



OUR MISSION:

To build a community of success-minded entrepreneurs that inspires excellence, encourages collaboration and expands the capacity of all members to achieve great things.

HOW TO SAFELY SHARE PASSWORDS WITH EMPLOYEES

If you ask a security professional, you get by-the-book advice about sharing passwords: "Don't share passwords." But we know, in reality, that doesn't work. Your office might be sharing a single password for apps like SurveyMonkey right now to save cash on buying additional users, and some social media accounts don't even give you the option to have multiple log-ins.

Sharing passwords in your office is sometimes necessary for collaboration, and the best way to do this is by using a password manager. Affordable (some platforms even offer free versions), layered with security and simple to use, password managers are the safest and easiest way to store and share your company's private passwords.

Reasons You Would Need To Share Your Passwords

Shared accounts are the biggest reason

businesses share passwords, whether their employees work from a physical office or at home. It improves collaboration and makes employees' jobs a lot easier.

Medical leaves, turnover, vacations and "Bob isn't coming in because he ate bad fish last night but has our Amazon log-in" are other reasons passwords get handed around like a plate of turkey at Thanksgiving dinner.

However, unsafe sharing habits will put your private passwords in the hands of greedy hackers, who can fetch a high price for your data in dark web markets. IBM Security reported that in 2022, 19% of all breaches were caused by stolen or compromised credentials.

So, how do you share passwords safely?

continued on page 2...



...continued from cover

First, Avoid These Common Password-Sharing Mistakes

When it comes to password sharing, remember:

- 1. **Don't send passwords via e-mail:** E-mail is the #1 target of hackers, and many e-mail services aren't encrypted. Those that are encrypted are still risky because e-mails are stored in several servers on their way to or from your account. That means your e-mail is sitting in a Sent folder, ripe for the taking by anyone who gets into your e-mail account, encrypted or not.
- 2. **Never text or chat passwords:** Like e-mails, SMS messages or messaging apps like Slack aren't secure. Once a text is sent, it is available for anyone to see.
- 3. **Stay away from storing passwords using pen and paper and shared documents:** Sticky notes, memo pads, Google Docs – NEVER write down your passwords.
- 4. **Avoid the temptation to store passwords on your device:** If your device gets hacked, nothing stops that perp from taking every password you saved.

The Best Way To SAFELY Share And Store Your Passwords

We recommend using reliable password managers because they have multiple layers of encryption so only those with a key (your master password) can see it, AND they include more robust security and sharing features like:

“

IBM Security reported that in 2022, 19% of all breaches were caused by stolen or compromised credentials.

- **Zero-knowledge architecture:** Not even your password manager service can see the information you save in your vault.
- **Multifactor authentication (MFA):** For added log-in security.
- **Unique password generation:** Creates strong, random passwords to improve log-in security.
- **Fake log-in page warnings:** Warns you if a page is spoofed by hackers.
- **Breach or weak password notification:** Alerts you if one of your passwords was leaked or if your current password is weak.
- **Simple, secure built-in password sharing:** Some password managers let you choose which passwords your employees can see and keep others in a private vault. Others, like Keeper, let you share documents or records without exposing credentials.

To use password managers, you only need to remember one password – the master password. One downside is that whomever you share a

password with needs an account for the same service. However, most password managers have corporate accounts, so this shouldn't be a problem.

A Word To The Wise: Look out for password managers with a bad security track record, like LastPass, which was breached in 2022, 2021, 2016 and 2015.

Smart Businesses Use Password Managers

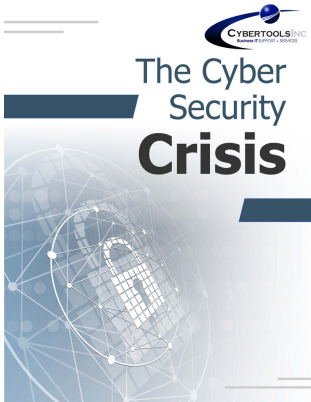
It's a good idea to avoid sharing passwords as much as possible, but when you have to, use a reliable password manager to ensure you have control over exactly who sees your credentials. Talk to your employees about safe password hygiene, host regular security-awareness training for employees and use MFA with every account. It's not just safe business – it's smart business. If you're not sure which password manager to use, give us a call and we'll get you set up with one.

FREE REPORT:

The Cybersecurity Crisis: Urgent And Critical Protections We Are Urging All Clients To Have In Place NOW To Protect Their Bank Accounts, Client Data, Confidential Information And Reputation From The Tsunami Of Cybercrime

As a local IT support company, we work day and night to protect our clients from these attacks – and unfortunately we see, on a regular basis, hardworking entrepreneurs being financially devastated by these lawless scumbags. We are determined to WARN as many businesses as possible of the VERY REAL threats facing their organization, so they have a chance to protect themselves and everything they've worked so hard to achieve. If you want to have any hope of avoiding a cyber-attack, you MUST read this report and act on the information we're providing.

Download Your FREE Copy Today At www.cybertools.us/new-cybersecurity-crisis



CARTOON OF THE MONTH



“Son, there are three things I want you to never forget... never give up on a dream... marry for love... and use 8-digit complex passwords!”

DOES MY BUSINESS REALLY NEED CYBER LIABILITY INSURANCE?



Businesses, regardless of their size, face the risk of cyberattacks and data breaches in today's digital landscape. While larger companies may have the means to recover from such incidents, small and medium-sized businesses (SMBs) often lack the necessary resources and protection. This brings us to the question: do SMBs need cyber liability insurance? In short, yes. Cyber liability insurance offers essential protection for SMBs against cyber threats. Here's why:

- **Wide-reaching Threats**
SMBs are mistaken if they believe they're immune to cybercriminals. Any entity that handles customer or employee data becomes a potential target. Cybercriminals often focus on SMBs due to their weaker cybersecurity measures.
- **Financial Safeguard**
Cyber liability insurance provides financial security in the event of a data breach. It covers costs like data recovery, system restoration, legal fees, and other expenses associated with cyber incidents. Some policies even extend coverage to business losses resulting from cyberattacks.

- **Access to Experts**
SMBs may lack the resources to bounce back from cyber incidents. Cyber liability insurance grants access to breach response teams and legal support, aiding in recovery and damage control.
- **Meeting Compliance**
Cybersecurity regulations vary across industries and locations. Cyber liability insurance helps SMBs meet these obligations and avoid penalties.. In conclusion, SMBs should seriously consider investing in cyber liability insurance to shield their finances and reputation from cyber threats. Even if not mandated, the potential impact of cyber incidents makes this insurance a valuable asset. Many SMBs underestimate their vulnerability to cybercriminals. Any organization handling personal or financial data can be a target. Cyber liability insurance proves crucial for financial protection, covering costs such as data recovery, legal fees, and more. Additionally, some plans extend coverage to business interruptions caused by cyber events.

SHINY NEW GADGET OF THE MONTH

The Nuzzle Pillow



Nobody likes waking up in the middle of the night because of an uncomfortable pillow. Sometimes, your pillow gets too hot, and you have to flip it over to the cooler side, while other times it's gone flat and requires a quick re-fluff before you can get comfortable again. With the Nuzzle pillow, you don't have to worry about either problem.

Using fabric developed for NASA space suits, these pillows remain cool on the hottest nights. The Nuzzle pillow is made up of Nanocoil gel fibers that help it retain its shape while keeping your neck and head supported throughout the night. If you're ready for a better night's rest, try the Nuzzle pillow today!

Limited internal resources can hinder SMBs from effectively managing cyber aftermath. Cyber liability insurance provides access to external expertise, including breach response teams and legal advice, easing recovery efforts and minimizing operational and reputational damage. For compliance, industries and locations dictate varying data protection rules. Cyber liability insurance aids SMBs in adhering to these regulations and avoiding penalties. In conclusion, cyber liability insurance is a wise investment for SMBs. It offers a safety net against cyber risks, ensures financial stability, provides access to expertise, and aids in compliance with data protection laws.

NEED DIGITAL MARKETING? Cybertools is offering digital marketing for our clients. Want an online presence? Call us to find out more. (253) 875-3777