PALMTECH
I.T. Solutions For Business

THE LEGAL TECH TIMES

PalmTech Computer Solutions January 2021

Don't Let The Bad Guys Win

If you haven't changed your passwords recently, now is the perfect time to do it! What better way to kick off the new year! It only takes a few minutes, and it's one of the simplest ways we can protect ourselves against cybercriminals. Cyber security experts suggest changing our passwords every 1-3 months, but the more often you do it, the better. Hackers work overtime trying to break into apps and websites. They want usernames and passwords they can sell or exploit. If hackers get your passwords, they will try to use them. If you change your password frequently, it becomes MUCH harder for hackers to take advantage. So, put the bad guys in their place and plug in a new password!

This monthly publication provided courtesy of Chuck Poole, CISSP, CEO of PalmTech Computer Solutions.

Our Mission

To equip small and midsized businesses in the West Palm Beach area with a smooth running and seamless IT platform that enhances productivity, improves efficiency, and creates a competitive advantage.

Finally Shed The Old This Year
It's Costing You Much More Than You Think

New year, new technology! If your business is still relying on older and aging technology, it's time to think about updating that technology. As it ages, the effort to keep it running comes with many hidden costs. While it may seem financially savvy to keep older hardware and software running, you may be setting yourself up for **major** costs down the road.

It's understandable why many small businesses shy away from investing in new equipment and software. They do the math and see a number that keeps rising. While the upfront costs of new technology — hardware or software — *can* be high (or higher than you would like), you have to consider what you would be paying for versus the cost of keeping aging technology running.

Let's start by looking at some of the "hidden" costs that come with using older or outdated technology. First, consider **the cost of productivity**.

The older technology gets, the less efficiently it runs. This applies to hardware and software. Hardware has a tendency to lag, even if it's well-maintained. Devices simply wear out with use. This cannot be avoided. But the productivity issues that come with aging hardware only get worse when you bring aging software into the mix. Over time, you will start to lose support from developers, and this comes with all sorts of problems. Here are three examples.

Loss Of Integration Older apps lose stable integration with companion apps. At one point, your CRM software may have worked perfectly with your billing

continued on page 2

software. As developers focus on newer versions of their apps, they stop updating past versions. The end result is more hiccups or errors. You risk losing data.

Loss Of Compatibility Older apps aren't always compatible with newer apps. What should you do when still using an old software and your vendors or customers use the up-to-date version? It can result in a lot of aggravation on everyone's part, and you can end up losing customers. One Microsoft survey showed a vast majority of consumers – 91% – would walk away from a business if that business were using older technology.

Loss Of Time And Money Factoring in slow equipment and a loss of integration and compatibility, aging tech makes it harder for your team to do their jobs. A recent study by Currys PC World found that employees lose an average of 46 minutes **every day** due to aging technology. That adds up to about 24 days per year and an average loss of about $3,500 per employee – though that number can vary wildly from industry to industry. You can be sure the cost in time and money has a ripple effect throughout the entire business.

While productivity takes a hit, there's another major issue that comes up when your business relies on aging technology: **security**.

As your tech ages, and as developers end support, this means you'll see fewer security patches. Eventually, there will be *zero* security patches, leaving you vulnerable.

> **"One Microsoft survey showed a vast majority of consumers — 91% — would walk away from a business if that business were using older technology."**

Developers may stop supporting older products, but hackers and cybercriminals will keep on trying to break into those products. They know small businesses tend to update their systems at a slower pace, and this gives criminals an advantage.

If you get caught using outdated software and a hacker is able to break into your network, the costs associated with this kind of a data breach can put a business under. It's devastating. The problem is made worse if you had limited IT security in place (or none at all) and weren't backing up your data. It's like handing your business over to the criminals! The importance of IT security cannot be overstated, and if you are working on older computers with outdated software, risks are greater.

So, What Can You Do? As we said before, many small businesses assume that keeping their technology up-to-date is cost prohibitive. They don't want to deal with the upfront cost that comes with investing in new hardware and software. While it can be costly, depending on your needs, there are ways to mitigate those costs.

One great example is through a Hardware-as-a-Service (HaaS) and Software-as-a-Service (SaaS) company or program. These allow small businesses to stay current without having to drop a tidy sum in order to make it all happen. These services are often offered through managed service providers (MSPs) that are dedicated to helping small businesses with all of their IT needs, including keeping their technology updated and their network secure from outside intruders.

When you factor in the loss of productivity (and the frustration that comes with that) along with the costs that come with data breaches, malware infections or cyber-attacks, it can easily be worth it to kick your old tech to the curb and embrace the new!

Are Your Employees' Credentials For Sale On The Dark Web?

Visit www.palmtech.net/darkweb/ For A Free Scan!

6 Time Management Tips For The Busy Entrepreneur

Face it, there will never be enough hours in the day to accomplish everything you need to do. But, if you methodically review how you spend your days and instill focus and discipline while completing daily priorities, you will soon find more time to work on the long-term success of your business. Here are six ways to do it.

1. Conduct A Time Audit.

Sit down and review three months of activity. The data from the analysis will show where you spent your time (which projects, tasks and priorities demanded your attention) and with whom you collaborated to get the work done. The audit will also shed light on areas where you were distracted, where you were the most productive and which tasks/projects took more (or less) time than anticipated.

2. Eliminate Time Drains.

These are the kinds of things that sneak up on you and steal time that can be put to better use growing your business. Look for these time drains: not delegating tasks, not managing meetings efficiently (tip: always have an agenda!) and spending too much time writing/responding to e-mails. If you've done your job as a leader, members of your team can handle a majority of meetings and e-mails. You hired great people. Now let them do their jobs.

3. Take Control Of Your Calendar.

Remember, *you* drive your schedule; don't let others drive it. Block time throughout your day and guard against changing your schedule to work on tasks that are not important or urgent. The way you allocate your time has a direct correlation to your effectiveness as a leader and, ultimately, the performance of your business. Prudent calendar management will also send a strong signal to your team that you should take this seriously.

4. Plan Your Day.

When you know your priorities for the day, you will be better prepared to reset your work schedule if the unexpected comes your way. Once your schedule is set, block off chunks of time to work on your priorities. I

recommend 90-minute blocks so you can concentrate on big-picture items or work on a group of related tasks. Stay disciplined and don't allow yourself to go over that allotted time.

5. Limit Interruptions.

Now comes the hard part. Once you start working on each priority, you need to remain focused. Close the door and don't answer the phone unless it's a critical issue. Avoid checking your e-mail. Don't let distractions slow you down.

6. Hold Yourself Accountable.

Share your tasks, priorities and deadlines with a colleague. Meet with that person at least monthly to review how well you managed your time. The probability of success increases when you have someone watching your progress and coaching you until you the cross the finish line

Andy Bailey is the founder, CEO and lead business coach at Petra, an organization dedicated to helping business owners across the world achieve levels of success they never thought possible. With personal experience founding an Inc. 500 multimillion-dollar company that he then sold and exited, Bailey founded Petra to pass on the principles and practices he learned along the way. As his clients can attest, he can cut through organizational b.s. faster than a hot knife through butter.

Know Better, Do Better

The end of the year in the usual circumstances brings about reflection even if it hasn't given us challenges to face or decisions to look back on. This year was one of extraordinary circumstances, and while the situation was unprecedented, the summary of what transpired lends itself to the age's old advice: **Preparation is key.**

The poet Maya Angelou is credited with saying "When you know better, you do better." And in knowing better, would that have meant that:

1. We would have prepared for assembling and supporting our businesses and employees in remote and work from home setups?
2. We would have had adequate training to recognize the scams and attack methods that cybercriminals would deploy when trying to breach our systems?
3. We would have taken inventory on what equipment we have, and what we might need in dire situations to run our business?
4. We would have done a security risk assessment to know what gaps were in existence within our businesses so that we could address them immediately and not risk further exposure in these new situations?

The list could undoubtedly go on and on. But even these few basic "we would haves" are enough items to put on our to-do list from the experience of 2020.

Knowing this, and that **humans are the greatest risk to your business or your client's businesses** when it comes to data breaches and the likelihood of not recovering from a breach, you need to ask yourself: Am I doing better?

A solid and ongoing training program is one of your best defenses when it comes to fighting cybercrime. The threat of it happening isn't going to diminish and will likely continue to increase in both chances of happening, as well as methods of attack, for the foreseeable future, if not forever.

So, what are you doing to make sure that you are prepared? We all know better now than to ever say "that probably won't happen". But do we know better ENOUGH? If you don't have a training program in place, speak with your IT provider and insist that one is implemented. Call us at 561-969-1616 and we will answer any questions you may have.

Remember, when you know better, you do better. **Let's all do better.**