PALMTECH
I.T. Solutions For Business

THE LEGAL TECH TIMES

PalmTech Computer Solutions February 2021

The Worst Passwords Of 2020

Password manager NordPass recently revealed the worst passwords of 2020. The list included several passwords that were on the list in 2019 (and the year before that). These are passwords that hackers and cybercriminals LOVE. It makes getting into accounts super-easy.

5. 12345678
4. password
3. Picture1
2. 123456789
1. 123456

One of the reasons these passwords are so frequently used is because they are easy to remember and they require little effort to type. As a general rule of thumb, the easier a password is to type (like 123456) or remember, the easier it is for a hacker to crack. Never use these passwords!

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.

You NEVER See It Coming! But Once It Hits, Everyone Says, "I Wish I Would Have_____"

A year ago, no one could have predicted that countless businesses would shift to a remote work model. The pandemic hit hard and fast, and small businesses had to think on their toes. Many had only a few weeks to adapt. It was stressful and extremely challenging.

Looking back on it, many SMBs wish they'd had a plan in place that would have made things easier. When the pandemic hit in February/March 2020, SMBs had to absorb the huge cost of getting their employees up and running off-site. Not only was it costly, but it also took a lot of coordination and on-the-fly planning. This meant things slipped through the cracks, including cyber security.

As they say, hindsight is 20/20. You may wish you had a plan in place or had more time, but you didn't. A vast majority didn't. However, you can still plan for the future! While you never know when disaster is going to strike, you CAN be prepared for it. Whether that disaster is a pandemic, flood, fire or even hardware failure, there are steps you can implement today that will put you in a better place tomorrow. Here's how to get started.

Put Your Plan Into Writing.

First and foremost, you should have a standard operating procedure to call on should something go wrong. For example, in early 2020, many SMBs didn't have a security plan in place, let alone a remote work security plan. They had to make it up as they went, which just added to the challenges they were already experiencing.

continued on page 2

To get over this challenge, work with an experienced IT services company or managed services provider (MSP) to put together a plan. This plan should include a cyber security protocol. It should define what malware software employees should be using, what number they should call for 24/7 support, who to contact when they receive suspicious e-mails, how to identify suspicious e-mails and so on.

More than that, it should outline exactly what needs to happen when disaster strikes. Pandemic? Here's how we operate. Fire? Here's what you need to know. Hardware failure? Call this number immediately. The list goes on, and it can be pretty extensive. This, again, is why it's so important to work with an MSP. They've already put together plans for other SMBs, and they know where to start when they customize a plan with you.

Invest In Security And Backups.

While every business should have network security already in place, the reality is that many don't. There are a ton of reasons why (cost concerns, lack of time, lack of resources, etc.), but those reasons why aren't going to stop a cyber-attack. Hackers don't care that you didn't have time to put malware protection on your PCs. They just want money and to wreak havoc.

When you have IT security in place, including firewall protection, malware software, strong passwords and a company-wide IT security policy, you put your business and all your employees in a much better place. **All of this** should be in place for both on-site employees and remote workers. With more people working from home going into 2021, having reliable IT security in place is more important than ever before.

> **"When you have IT security in place, including firewall protection, malware software, strong passwords and a company-wide IT security policy, you put your business and all your employees in a much better place."**

On top of that, you should have secure backups in place. Investing in cloud storage is a great way to go. That way, if anything happens on-site or to your primary data storage, you have backups you can rely on to restore lost or inaccessible data. Plus, having a solid cloud storage option gives remote employees ready access to any data they might need while at home or on the go.

Where Do You Begin?

Some SMBs have the time, money and resources to invest in on-site IT personnel, but most don't. It is a big investment. This is where partnering with an experienced IT services firm can really pay off. You may have employees in-office or you may have a team working remotely – or you may have a mix of both. You need support that can take care of everyone in your organization while ensuring the protection and integrity of your business and its data. This is where your IT partner comes into play. They are someone you can rely on 24/7 and someone who will be there for you during a pandemic or any other disaster.

Contact us at 561-969-1616 to learn about our IT support services.

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

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

Production Vs. Connection : The Ailment And The Cure

Recently, I had what we like to call an "aha moment" while listening to a sermon one Sunday. The minister made the observation that our society as a whole has swung to the extreme side of *productivity* at the expense of our *connections*. It hit me that this is one of the greatest ailments we see as coaches with our member companies and leaders, especially as of late.

Culture →Appreciation →Connection

We know the best-performing companies are those that devote significant effort to creating a culture that their team members *want* to be a part of. And where does that culture come from? People crave appreciation in the workplace – and we're talking sincere, heartfelt appreciation, not the casual "pat on the back" or quick "thanks" in passing. *Real* appreciation only occurs if there is a *real* connection between people. Connection is valuing the other person more than yourself or having an "others first" mindset. It takes effort, vulnerability and emotion. True culture cannot exist without both of these key elements.

The Ailment

Unfortunately, in our "all about me" culture, connections tend to be shallow and unemotional. It's not what can I do for you, it's what can you do for me. As a society and in business, we have become so laser-focused on overachievement and beating the competition that our connections receive little attention. Especially today, when companies are striving to get back on their feet, push out new offerings and make up for lost time from the pandemic, connections are starving due to the demands of winning.

But At What Cost?

There have never been higher instances of job discontentment, disconnected families, depression, suicide and overall lack of joy. Our extreme focus on production and achievement has come at a huge cost to society. Extremes at either end of the pendulum never end well.

So, Now What?

Back to our coaching perspective, I think we have it right when we help our companies focus on culture by viewing their team members as human beings and not just a means to productivity. In addition, we all know that you cannot truly separate the business side from the personal side and that you have to be equally intentional in both areas to create the life you want, which involves real connections to who and what we love.

It's time to swing the pendulum back, ease off the production pedal and give more attention to treating each other with compassion and putting others first. It may seem strange, but the companies that have done this well typically outperform on the production side, too, because connection is a great motivator for betterment – both personally and professionally.

Gee, maybe there's really something to the old Golden Rule thing.

David Pierce spent the first 30 years of his career in the corporate world. As a CPA, he spent a decade with Deloitte and PcW, and another 20 years in a C-level post in regional banking. He also launched one of the first stand-alone online banks in the US. As an entrepreneur, he eventually said goodbye to the corporate world and started his own consulting firm, and became a Four Decisions Certified Gazelles International Coach and a Petra Coach.

A Quick Refresher

As we move forward, taking advantage of the energy the new year offers to start implementing and executing our annual plans for growth, sometimes we find ourselves biting off more than we can chew since we now know the unexpected is all that can be expected. So let's have a quick refresher.

***On what, you ask?* Smart, safe, and sane cyber practices.** The smart and safe are obvious, but sane? Well, we can lose our mind if we try to comprehend all of the things that we need to know. And sometimes that means we shut down from feeling overwhelmed at the notion of trying to learn anything. Small bites are what this is about, or should we say, small bytes. So here are a few to get those walls around your identity and data strengthened.

Like changing batteries in your smoke detector, you need to change your passwords when there's a beep – or in this case, alert that you've been compromised. Do it right away, and make sure that your new password is not the same as your old password with a number slapped onto the end of it. Make it a phrase or quote that you love. Make the E's into 3's. Mix it up with a special character. Just change it – and ensure that the same password isn't used elsewhere. If so, change those. Yes, all of them. Use a password manager that offers to create and save strong passwords for each account. ALWAYS use two-factor authentication when it is available. Did you know that many web browsers save your password and will alert you if you have compromised accounts? A quick search or consult with your IT company can help you to do this.

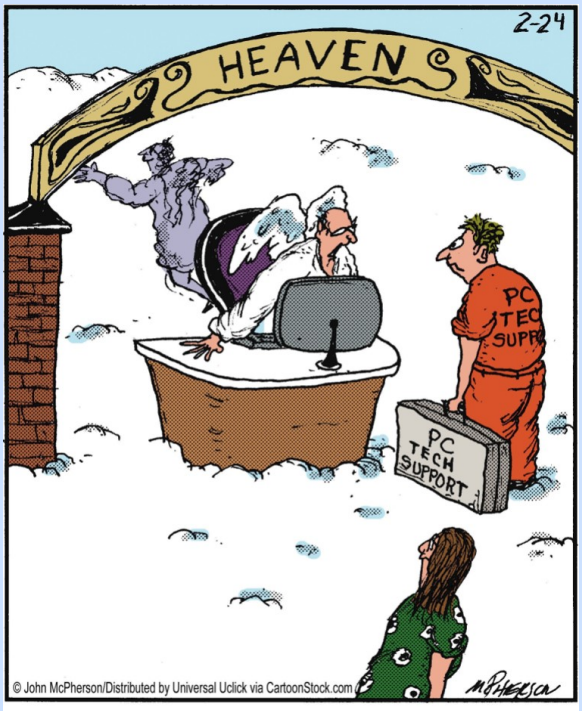
Refresh your clicker skills. When you get an email with a link, what should you do? Well, we'd like you to NOT click on anything, but if you have an itchy twitch to do so, hover first. Does the link that pops up match the site you're being told it will direct to? Hackers can cleverly disguise emails, links, names, and entire sites to look identical to the one you see in an email. Clicking on a fraudulent link can take you to corrupt site, or worse, it can deploy a virus to your entire system. Sometimes you don't realize it's been deployed until months go by and it has silently collected invaluable data for the entire time. As a safety measure, if an email comes from your bank for example, click out of the email and go to the bank's official site to see if the messaging in there too. Call them if you aren't sure – using the number you know, not the one in the email.

Network, but do it safely. Gone are the days of professional networking events – at least for now. It just isn't safe, and neither are public networks of the coffee shop kind. Free Wi-Fi will set you up for exposure to people that are just waiting to see you connect so that they can collect. Your data, that is. Create a hotspot with your phone or wait until you are safely at home using your secured network. Are you not sure how-to setup a hotspot? Your wireless carrier or IT support team can help with that. Ask about using a VPN, which stands for *Virtual Private Network*. This provides an additional layer of security for you and your devices.

We all need a nudge sometimes to mind our manners here and there. The same goes for these little things that we do regularly as we can become lazy or a little sloppy over time with the redundancy of doing them. Consider this your reminder to sit up straight and be secure. Your identity depends on it.

If you need assistance related to smart cybersecurity practices, contact PalmTech at 561.969.1616 or at info@palmtech.net. Visit **https://www.palmtech.net/enhanced-security/** to learn more.

Cartoon Of The Month



"Sorry we had to kill you, but it was the only way we could get some computer tech support up here."