PALMTECH
I.T. Solutions For Business

# THE LEGAL TECH TIMES

PalmTech Computer Solutions May 2019

## Come See Us at the 2019 Annual Florida Bar Convention!

**Please stop by and see us at booth #113 during the upcoming 2019 Annual Florida Bar Convention held at the Boca Raton Resort and Club June 26th - June 29th!**

**For more information, visit here:**

**www.palmtech.net/events/**

This monthly publication provided courtesy of Chuck Poole, President 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.

# Are YOU Prepared For The End Of Windows 7?

On January 14, 2020, the world will bid a fond farewell to the beloved Windows 7 operating system. Well, sort of. Microsoft has declared that, after that date, it will no longer update or support the system. It's the final nail in the coffin for a trustworthy, oft-touted software package that's been running on fumes since newer versions hit the scene. And, as with any funeral, there are some arrangements to be made for the millions of businesses that have stuck it out to the end. Here's everything you need to know about the coming changes – and what you should do now to prepare.

### The End Of An Era

The news of Microsoft closing down Windows 7 support may come as a surprise to some of us, but the operating system has been on its last legs for a while. In fact, Microsoft stopped adding new features and honoring warranties for the platform back in 2015. When 2020 comes, it will cease releasing patches and updates for good.

This doesn't mean that Windows 7 PCs will suddenly stop working in January; you'll still be able to boot up in the operating system if you keep it installed. But if you value your privacy, your data and your sanity, it's time to upgrade.

Those Microsoft updates that pop up from time to time don't exist just to annoy you; they patch security vulnerabilities and protect you against new viruses and malware.

*continued on page 2*

Without that ongoing support, Windows 7 users will become fish in a barrel to sophisticated cybercriminals looking for a quick buck. That's why it's essential that you call in the professionals to prepare your business for the switch to Windows 10 – or an alternative operating system – now, not later.

**It's A Requirement, Not A Choice**

Upgrading your operating system well in advance of the Windows 7 end-of-life date may seem like a decision you should make for your peace of mind, but it's even more critical than that. Of course, as time leaves Windows 7 behind, it's certain that pieces of software will steadily become incompatible with the OS. Programs your company uses day-to-day suddenly becoming unusable will present serious headaches, but the real problem lies in the security of your network.

Windows developers are in a constant arms race with cybercriminals looking to exploit vulnerabilities in their platform. Each patch brings a host of bug fixes and security upgrades, but cybercriminals almost always find a new way in. Thus, the developers hastily put together a new patch, and the cycle continues.

> **"Like maggots drawn to rotting meat, they flock to the abandoned platform and dig into the networks of those stubbornly clinging to the outdated OS."**

When an operating system loses support from these developers, its users are left completely vulnerable to hackers. Like maggots drawn to rotting meat, they flock to the abandoned platform and dig into the networks of those stubbornly clinging to the outdated OS. This process is expected to be especially nasty after Windows 7's end of life, since so many businesses still use the OS and likely will forget (or refuse) to upgrade.

If you value your business at all, it's not a choice. You need to upgrade before time runs out.

**Avoid The Crunch**

Not only should you enlist your IT experts to facilitate the upgrade, but you should do it ASAP. As the clock ticks down on Windows 7, tech companies are expecting a flood of upgrade requests as businesses scramble to leave the OS behind before it's too late. Many of these IT providers will have a lot on their plate later in the year as they hurry to upgrade hundreds, if not thousands, of individual PCs. If you wait it out, you're likely to find yourself at the back of a long, long line, potentially to the point that you breeze past January 14 without a solution. If you do, you're almost certain to regret it.

Every day, the need for an upgrade becomes more urgent. Give the task the ample time required, and avoid needless stress. Reach out to your IT provider and ask them to start the upgrade process today. If you'd like our assistance, call us at (561)969-1616!

# Read These Top Tips To Avoid Getting Hacked

Everyone knows how damaging data breaches can be to a business, but few actually realize that 81% of these hacks are not the result of elaborate scams carried out by sophisticated hackers. They happen because of poor passwords.

Do what you can to prevent your business from being targeted. Demand that your employees create strong passwords: between 8 and10 characters in length, with letters, numbers and symbols scattered throughout. Instruct them to avoid real dictionary words and to steer clear of the boneheadedly obvious ones like "12345" or "password." You can test the strength of your password online at Microsoft's Security and Safety Center. If you can, enabling two-factor authentication can go a long way toward your overall security.

Even if you use a secure password yourself, you'd likely be amazed (and terrified) to discover how many members of your team do not. In 2019, a strong password is essential. Make sure every one of your employees takes care to create one. If you need assistance with your cybersecurity, contact us at (561)969-1616.

# Expect, Inspect, Correct

It's no coincidence that we have so many ways to say we made a mistake: botched, flubbed, mishandled, misjudged, mucked, messed, screwed or goofed up – just to name a few.

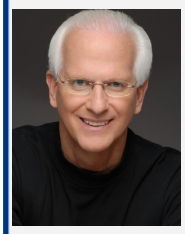
As a leader, you'll hear each of these (some more than others, and likely some more explicit than the ones I've named here) pretty often. When you do, it's important to first try to remember that whoever made the mistake probably didn't mean to.

Put yourself in their shoes. Ask yourself if you have ever made a mistake. A bad decision? Have you ever said something you regret? Ever disappointed your boss? Jumped to the wrong conclusion? Done something foolish or outright stupid? Everyone has. Sometimes a simple reminder of our past failings enables us to be a little more tolerant of others' missteps.

Mistakes don't have to be the end of the world. Mistakes are inevitable and are often essential to learning and progress. They should guide you, not define you, on you and your employees' journey to success. Mistakes show effort, and if you learn from them, they can be some of the best tools for growth.

I've heard it said before that the only people who don't make mistakes are those who do nothing at all. To me, the most interesting part about errors is the gradual evolution in how they're classified. First, they start as mistakes. Then they turn into lessons, followed by experiences and finally as gifts that help us succeed.

Therefore, the only real mistake is the one from which we learn nothing. Keep that in mind as you're dealing with your employees or considering your own shortcomings. It's one thing to recognize that mistakes are learning opportunities – it's another to actually implement that concept in your organization.



*Robert Stevenson is one of the most widely recognized professional speakers in the world. Author of the books How To Soar Like An Eagle In A World Full Of Turkeys and 52 Essential Habits For Success, he's shared the podium with esteemed figures from across the country, including former President George H.W. Bush, former Secretary of State Colin Powell, Anthony Robbins, Tom Peters and Steven Covey. Today, he travels the world, sharing powerful ideas for achieving excellence, both personally and professionally.*

# Are You Prepared For Hurricane Season?

Even if you feel your business is not likely to face the brunt of a hurricane's landfall, you should take steps to prepare for hurricane season. With talk of a busy hurricane season ahead, it is important that any business which might face heavy storms takes extra precautions. Extreme weather of any kind, from tropical depression and storms to Category 5 hurricanes and tornadoes, can not only cause structural damage to your business, but can also cause catastrophic data loss and network damages. Visit www.palmtech.net/hurricane-prep/ to download our Extreme Weather Checklist!

# What Are 2-Step and 2-Factor Authentication

In the digital age, cybersecurity should be one of the top priorities for anyone who goes online. One way is to vet those who are trying to access your systems. But when it comes to verifying users' identity, many are unaware of the two kinds of authentication measures available. Read on to know the differences between two-step authentication and two-factor authentication.

If you want to improve your business's cybersecurity for you and your customers, you should look at your authentication process. Two-step and two-factor authentication are two of the most commonly used options in cybersecurity. Many businesses use the terms two-step and two-factor authentication interchangeably. There are, however, subtle differences between the two.

## Two-step Authentication

A two-step authentication process requires a single-factor login (such as a password or biometric reading) as well as another similar type of login that is essentially sent to the user. For example, you may have a password for your first step and then receive a one-time-use code on your cell phone as the second step.

Two-step authentication adds an extra step in the verification process, making it more secure than single-step authentication (i.e., just the password). However, if a person or business is hacked, it won't be enough to stop hackers from getting a hold of whatever they are looking for.

## Two-factor authentication

On the other hand, there is two-factor authentication (sometimes referred to as multifactor authentication), which is significantly more secure. This type of authentication requires two different types of information to authenticate a user's identity. For example, it could be a combination of a fingerprint or retinal scan as well as a password or passcode. Because the types of information are different, it would require a hacker a great deal more effort to obtain both forms of authentication.

## The difference between the two

In essence, every two-factor authentication is a two-step authentication process, but the opposite is not true. With this information in mind, make sure that you are using the right type of authentication in your business to keep your company and customer information as secure as possible.

Your network needs the best security technology has to offer. The type of authentication you should use is just one of hundreds of choices that must be made to achieve that end. To take the stress out of securing and protecting your network, call us today for all the help you could ever ask for.


## Are Your Credentials For Sale On The Dark Web?

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