TECHNOLOGY TIMES

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

WHAT'S NEW

From our team here at **KAMIND IT**, we'd like to wish everyone a happy and safe Mothers Day!

Meet our newest team member that is here to assist in growing our business at KAMIND IT. **Dacoda Engelman** is our new Inside Sales Representative, locating organizations that need assistance solving business problems with the use of The Microsoft Intelligent Cloud! Please welcome Dacoda to our team.

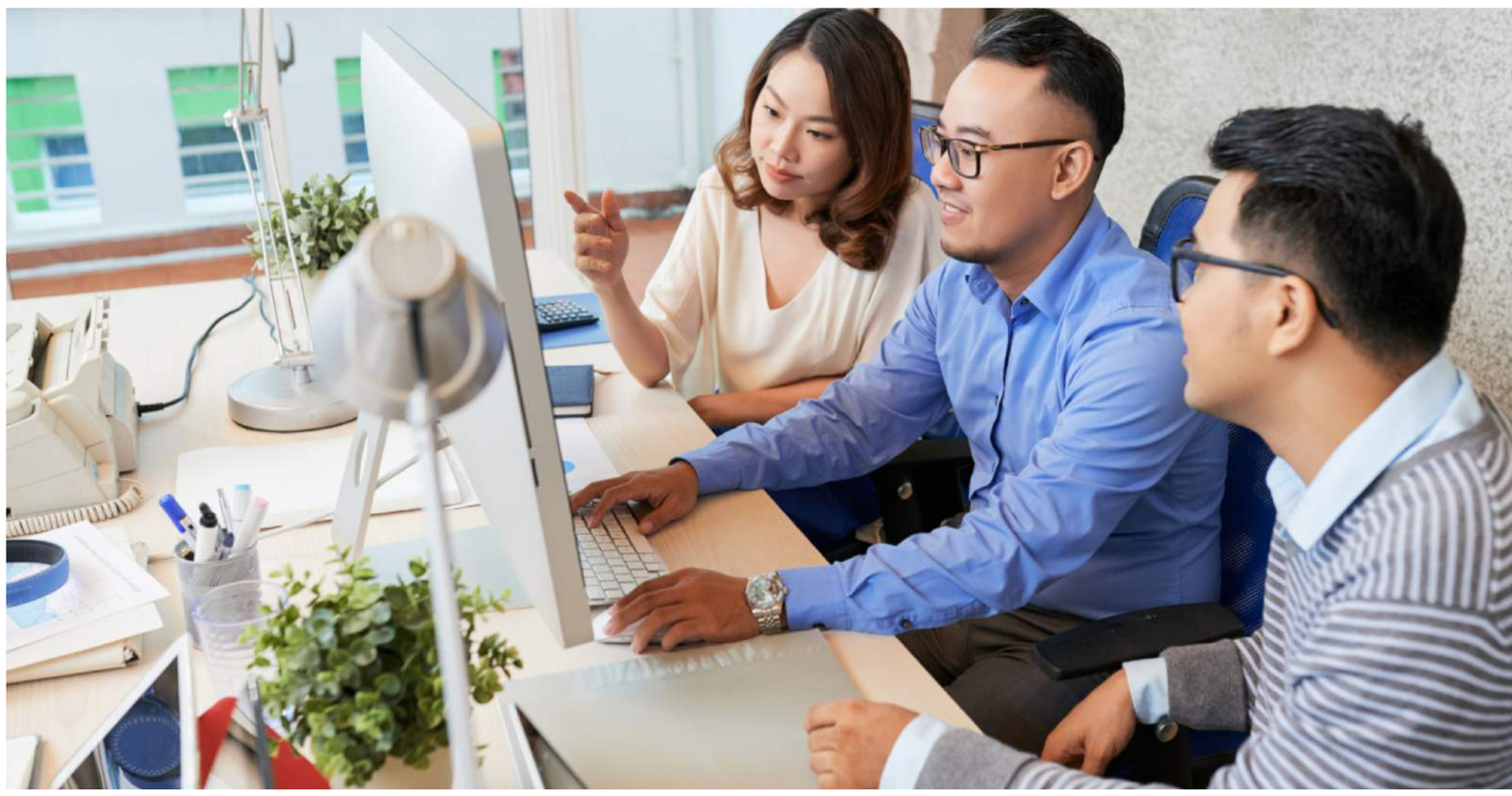
May is small business month, and in honor of that KAMIND IT is offering any small business owner a free copy of Matt Katzer's book **"Moving To Office 365, Planning and Migration Guide"** Go to the URL below to request your free copy!

https://www.kamind.com/freebook/

MAY 2019

This monthly publication is provided courtesy of Matt Katzer, CEO of **KAMIND IT**

Our Mission: "We help our clients solve business problems with the use of The Microsoft Intelligent Cloud"



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. Without that ongoing support, Windows 7 users will become fish in a barrel to sophisticated cybercriminals looking for a quick buck.

Continued Page 2

Continued From Page. 1

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

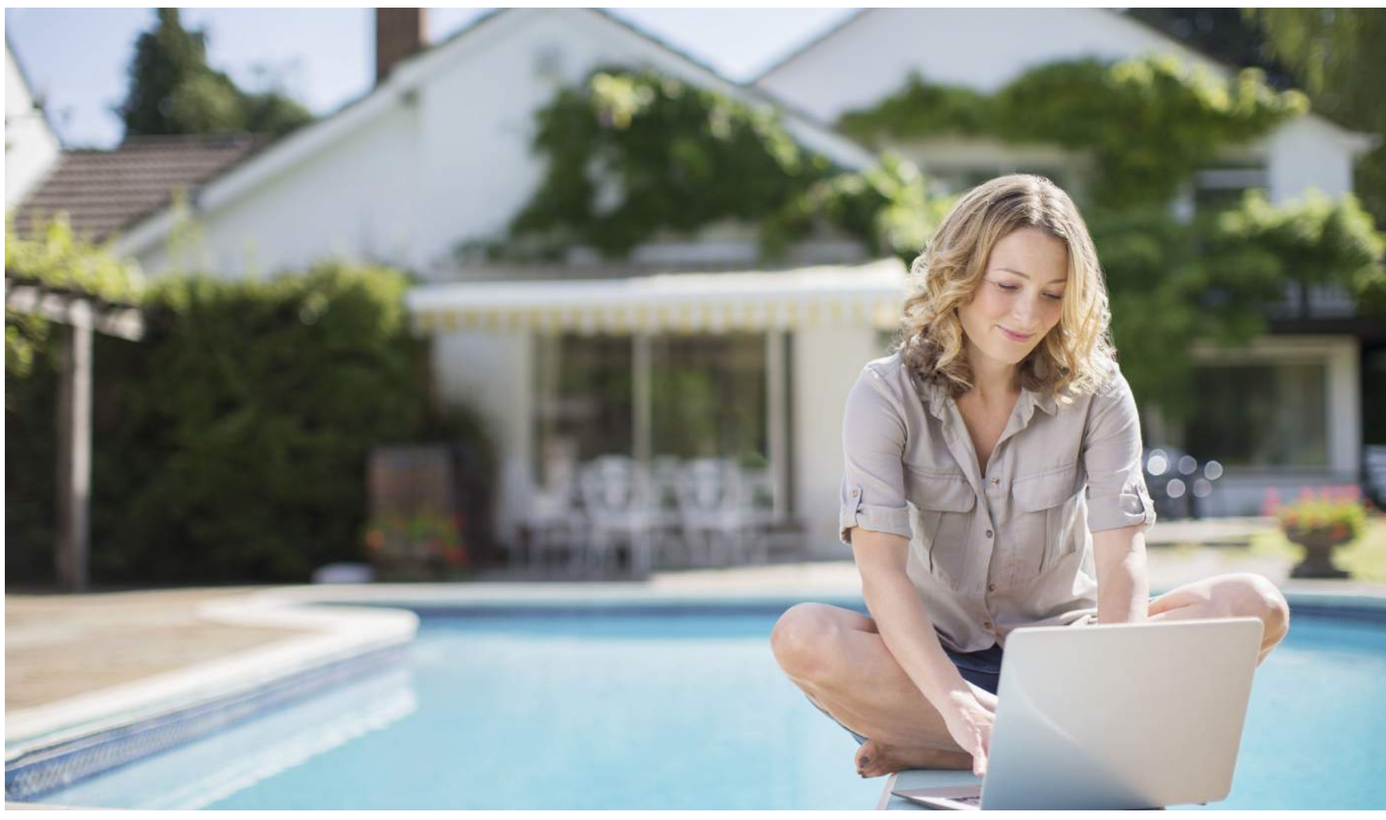
Upgrading your operating system well in advance of the Windows 7 end-of-life date may seem like a decision you should make for your peace of mind, but it's even more critical than that. Of course, as time leaves Windows 7 behind, it's certain that pieces of software will steadily become incompatible 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 alwaysfind a new way in. Thus, the developers hastily put together a new patch, and the cycle continues. 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.

"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."

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.



15% Off First Year Subscription of Microsoft 365 Business or Office 365 Business Premium (Ends May 31st, 2019)

Take Advantage of **KAMIND IT**'s Security Plans with these Exclusive Benefits.
Office 365 enhances your productivity and security, helping you save money and gain peace of mind. Get powerful services to transform your business, including:

- **Secure Desktop**
- **Business class email**
- **Online storage**
- **Teamwork solutions**
- **Mobile Application Management**
- **Advance Threat Analytics to defend against Phishing**
- **Upgrade early versions of Windows Pro to the latest Windows 10 Pro**

Visit **WWW.KAMIND IT/PROMO15** today!

Shiny New Gadget of The Month

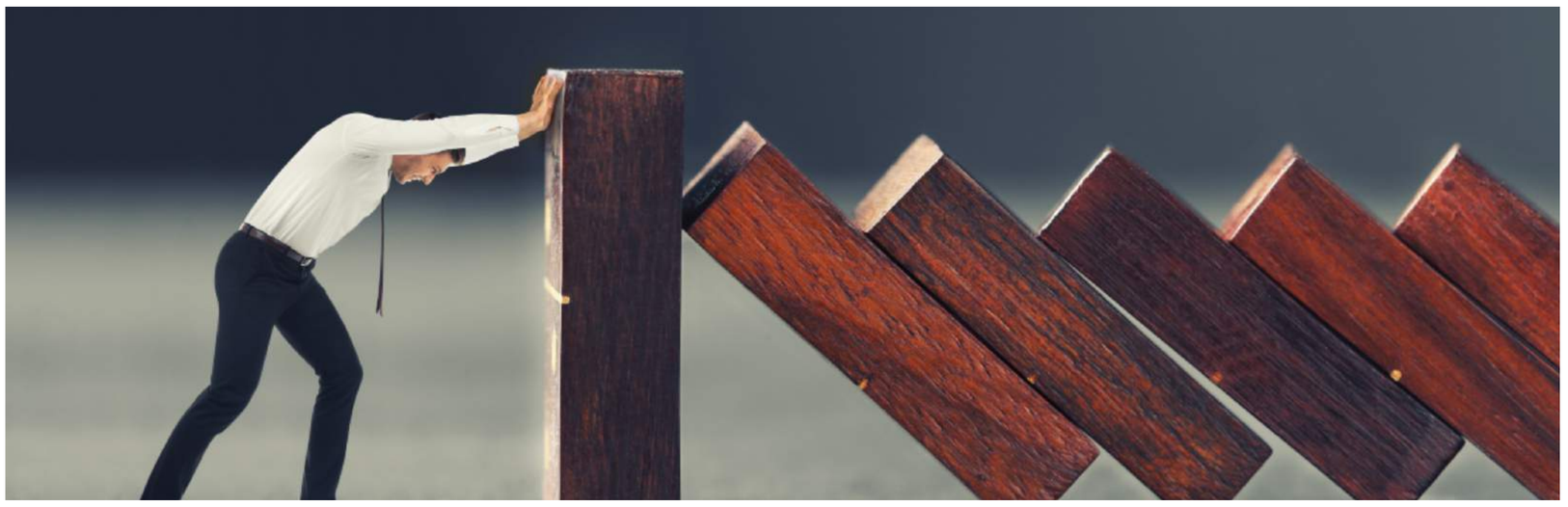
VIZR Hopes To Revolutionize Your Dashboard

When it comes to driving, the forces that aim to keep us safe seem to be in constant battle with the pull of convenience. We're supposed to keep our eyes glued to the road while trying to navigate through Google Maps without missing a single turn. It's an inherently dangerous combination.

With their new VIZR tool, FIXD automotive hopes to fix that. After selecting the feature you want, you connect the device to your phone and place it on your dashboard, where it creates a transparent display. This way, FIXD says, you can seamlessly navigate without ever glancing at your phone and putting your life in jeopardy.

Though VIZR is a great idea, the reviews indicate it might not be all it's cracked up to be. You might want to wait until all the bugs are sorted out. For now, just keep your eyes on the road the old-fashioned way.

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.

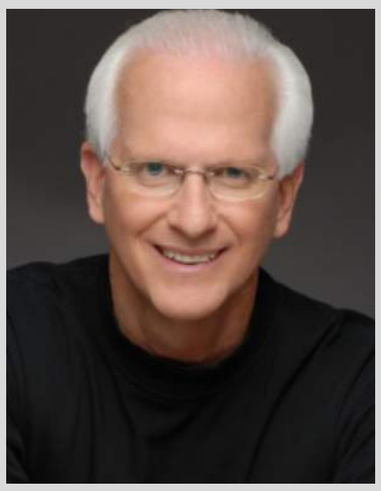
Put yourself in their shoes. Ask yourself if you have ever made a mistake. A bad decision? Have you ever said something you regret? Ever disappointed your boss? Jumped to the wrong conclusion? Done something foolish or outright stupid? Everyone has. Sometimes a simple reminder of our past failings enables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

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.

1/3/2019

Easy Ways To Prevent Great Hires From Getting Away

Today's labor market is tighter than it's been in years. With this in mind, it's essential that you do all you can to attract top talent. One of the best and simplest ways to do that is to improve your hiring process.

First, make sure the job description sounds like a true sales pitch. You should feature the benefits of working in that job above the preferred credentials. Once the applications start coming in, ensure you're keeping in regular contact with your prospects. When it comes time for interviews, make the process as straightforward and comfortable as possible and cater to their scheduling needs. Finally, ask for feedback about your hiring process – checking into reviews on sites like Glassdoor can provide valuable insight. **Inc.com, 2/1/2019**

5 No-Brainer Tips to Avoid Getting Hacked

A new week, a new retailer getting hacked. With headlines about security breaches occurring at Target, Neiman Marcus and Michaels, cyber attacks are front and center. Obviously, these types of data breaches are upsetting for large retailers, but don't think they could only happen to the "big guys." Hacking happens at all levels of business.While some cyber hacking is so sophisticated that it would be incredibly challenging for any entrepreneur to avoid, there are some careless mistakes you or your staff might be making which could be putting you at greater risk for hacking.
Limit your exposure now by making sure you're avoiding these five mistakes that open up easy hacker entry points to your network.

1. Not logging out of all your accounts. You've been traveling and working and you want to curl up in this hotel room and try to get some sleep before your client meetings tomorrow. So you simply shut the top of your laptop and don't bother to log out of your open accounts. Seems innocent enough. But just because your laptop's closed doesn't mean your accounts are too.
Related: Cyber Security a Growing Issue for Small Business
Logging out of your open email, wp-content admin sites and other online accounts helps secure your information. While it's not a guarantee of security, it's a good policy to protect yourself against easy exposure to hacking. Keep this in mind for public places too. If you're working on your laptop in a public place, always log out and lock your computer before stepping away, even for a moment

2. You don't update your passwords often and don't make them complex. I know it's annoying, but it's a good practice to make your passwords complex and to update them often (at least quarterly). That means upper and lower case letters, numbers and yes, symbols. Generic and unchanged passwords are incredibly easy to guess and hack into. (If your name is Bob and your birth year is 1968 don't make your password Bob1968.)
With the brilliance of social media comes the incredibly public nature of most of your private information. A hacker could pretty easily figure out your name, find you on socials and put together enough combinations of your name and date of birth to hack your accounts quickly and easily. So use a little more creativity and update your passwords periodically to make hacking harder.
Related: Your Password Is 123456? Wow. Seriously?

3. You don't secure your Wi-Fi network or you use public Wi-Fi. Wi-Fi networks are really easy entry points to your computer, accounts and network. If you offer free Wi-Fi in the lobby for your clients, do it on a separate network than your own office network. And always make sure your Wi-Fi network is password protected.
If you use public Wi-Fi networks like those at airports or local coffee shops, use caution.

4. You click on links in emails you don't recognize. Likely, you already know that you shouldn't open the email from the professed brother of the deposed king of Angola, you know the oen that wants to offer you the investment deal of a lifetime. That kind of spam and phishing email is easy to avoid. But what about the inquiries for the job you just posted on Craigslist? How legit are those emails? Are they submitting links in their email for you to access their online portfolio? Seems legit, right? And it probably is, but keep in mind your gut check when reviewing unknown emails. If something feels funny, don't open it or click on it. Pay attention to suspect emails as more and more hackers are getting really sophisticated in the way they write them these days. If something seems out of place, or too good to be true, do some research before opening an email or clicking a link.

5. You download from unknown sites. Just don't do it. Don't download free printables, desktop wallpapers or music-streaming software from sites you don't inherently know and trust. It's a quick and easy way for hackers to infiltrate your system.

Matthew Toren
Contributor **01/31/2017**

Who Else Wants To Win A $25 Gift Card?

You can be the Grand Prize Winner of this month's Trivia Challenge Quiz! Just be the first person to correctly answer this month's trivia question and receive a $25 Amazon Gift Card! Email your answers to **trivia@kamind.com**

Who invented the Graphical User Interface (GUI)?

A. Microsoft
B. Apple
C. Bell Labs
D. Xerox
E. HP