TECHNOLOGY TIMES

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

KAMIND®

WHAT'S NEW

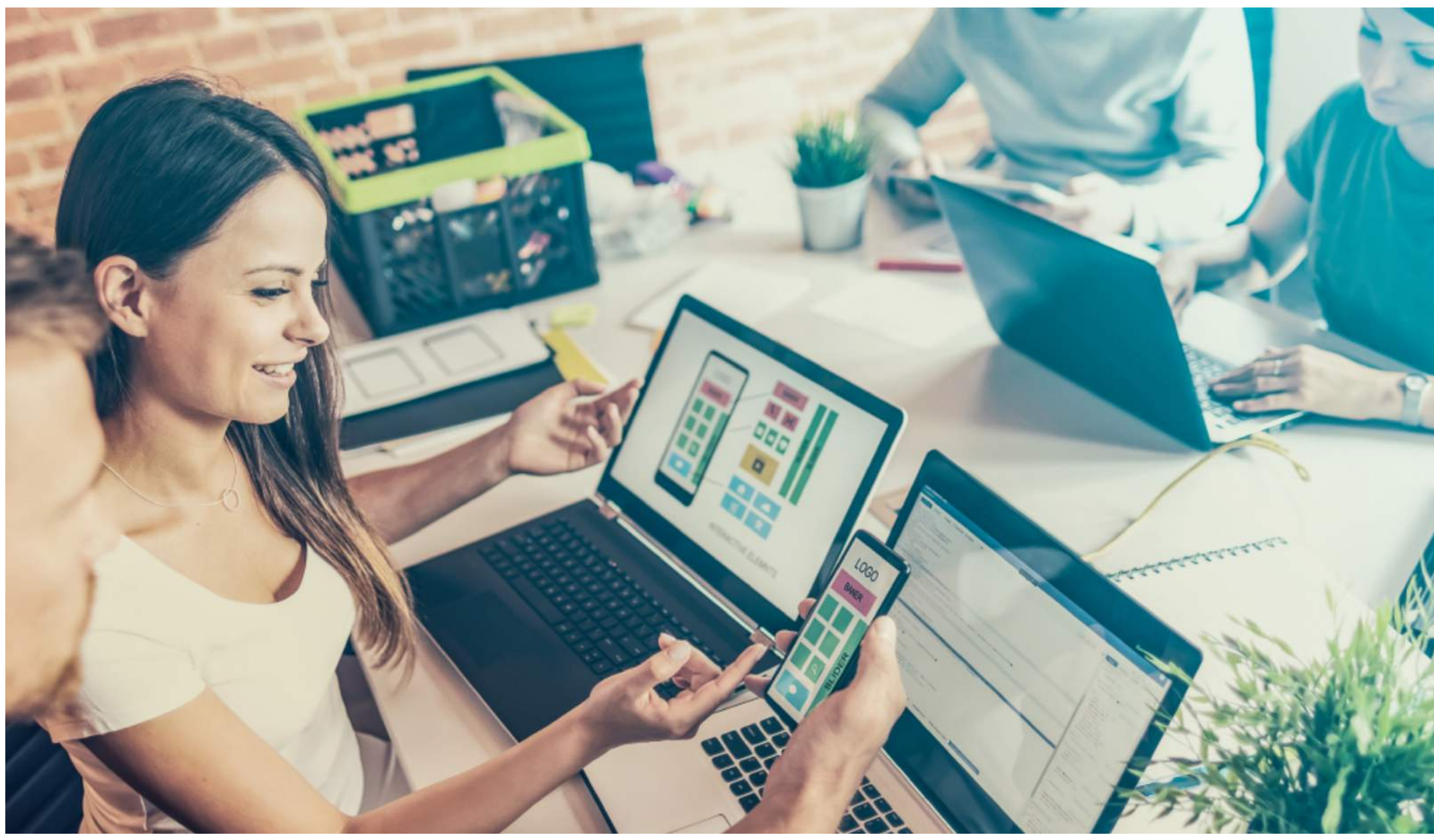
KAMIND IT is hosting our quarterly Hands - On Training Seminar **September 9th through the 12th.** Remember to mark your Calendars!

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

AUGUST 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"



3 IT Investments You Should NEVER Skimp On

What is standing between your business's data and hackers a world away? What's your plan when your on-site server fails? When you skimp on technology and IT solutions for your business, the answers to these two questions are simple:

There is nothing standing between your business's sensitive data and people who want to take advantage of that data; and there is no plan.

It happens way too often. Businesses "save" on certain aspects of their technology to save a few bucks up-front. You may even know someone who has done just this. They jump at the chance to outfit their office with a huge monitor and a PC with top specs (even though they don't need it) and then they decide that IT security isn't a priority. They aren't willing to pull out the credit card for a security solution because they don't want to deal with a monthly or yearly cost. But "saving" on security can cost them dearly in time, money, resources and clients.

When it comes to investing in IT, here are three things you never want to "save" on. Security. Far too many businesses – from small to large – underinvest in IT security. We touch on this topic a lot because we see it a lot. These are business owners and managers who fall into the mindset of "It won't happen to me." This is a dangerous line of thinking. For small businesses, a data breach can be devastating. Not only is data compromised and potentially copied or stolen, but your clients will also immediately question whether or not they should trust you. There's a good chance they end up taking their business elsewhere – and they may even sue you.

When IT security isn't a priority and you invest in the cheapest option available, it's like asking hackers to let themselves in. One study by the security firm Imperva found that over 50% of all Internet traffic is made by bots. Many of these bots are looking for security holes.

Continued Page 2

Continued From Page. 1

They test websites and networks, looking for a way in. If they find their way in, they can do some serious damage. Investing in solid IT security – with an experienced team of IT specialists behind that security – can prevent that damage from ever happening in the first place. It's not only about protecting your business assets but also protecting your clients and giving them another reason why they should trust you.

Backups. You keep all of your data on-site with no backups. It's all stored in one central location and that's it. This is a recipe for disaster if you get hacked, but it can be an even bigger disaster if a hard disk or server fails.

Suddenly, you find yourself unable to access client information, invoices, phone numbers – you name it. Having a backup on-site or in the cloud means everything you do has an extra layer of protection. A backup gives you the ability to restore your data should the worst-case scenario occur.

It's even better to go a step further and have a backup for the backup. Have one on-site solution and one cloud-based solution. Even if the backup to the backup is as simple as a 4TB hard drive from Amazon, it has the potential to save your business should anything go wrong.

Of course, you also need a system in place to make sure data is being regularly and accurately updated. Another mistake businesses make is buying a backup or backup services, but not making the best use out of it. For example, they simply never bother to set it up. Or it is set up but isn't configured correctly and isn't backing up data as intended – or is backing up data too infrequently to be useful.

Updates. How old is your technology? Think about the hardware you're running – and the software on that hardware. Letting your technology fall behind the times can spell trouble. Not only are you opening yourself up to security vulnerabilities, but you may also be operating on technology that's no longer supported by the developers.

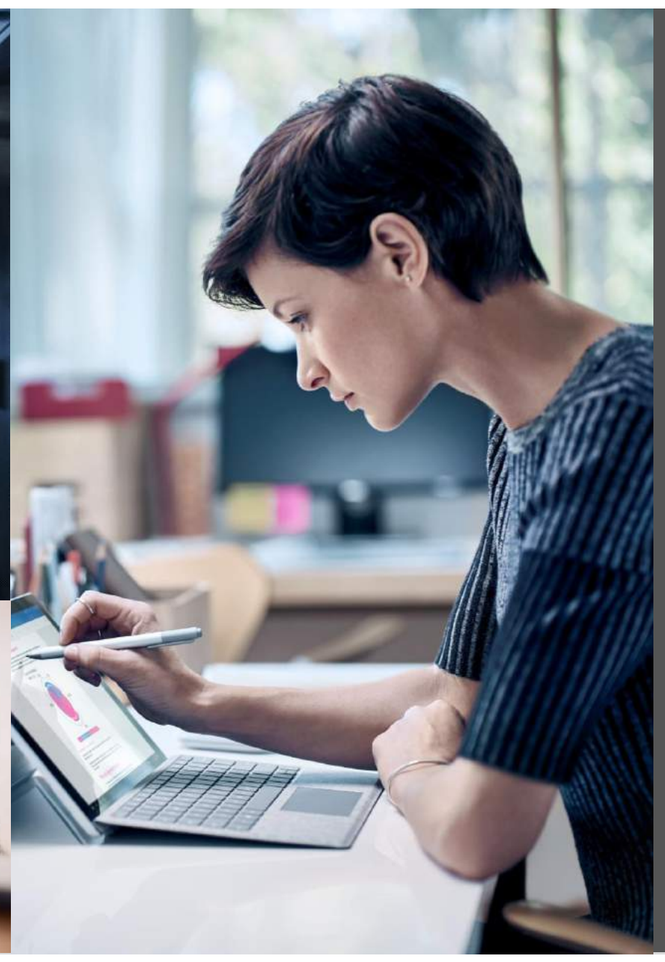
If the developers are no longer publishing updates or supporting the software, this is a huge security red flag that you need to update. On top of that, should you or an employee need to troubleshoot a piece of unsupported software, you may find yourself going up against walls. There might be no one to call, and if a Google search doesn't help, you may be out of luck.

The potential headaches don't end there. If you're running unsupported software on shiny, new hardware, you may be voiding the warranty of that hardware (always check your warranties and the fine print of any hardware you buy).

Alternatively, if you're trying to run brand-new software on old hardware, chances are you're going to run into compatibility issues. That wonderful piece of software might not work, or work the way you expected it to, all because you didn't want to update your old hardware.

It's not always fun to reach into your pocketbook to invest in good IT security, cloud backup storage or new hardware, but when you cut corners and skimp out, you will end up paying for it later, one way or another. When that bill comes, it's going to be a lot bigger than if you had committed to those IT investments in the first place.

"... when you cut corners you will end up paying for it later..."



Shiny New Gadget of The Month

Don't Get Jacked with The Juice Jack Defender!

Juice-Jack Defender is a charger defense system that you can slot your charging cord in and plug to the USB power charging station. This way, it blocks end-to-end transfer of data from your device and the connecting station. Thus, no cybercriminal can move data out or into your device; you remain protected from malware installation and data theft.

Malware installation and info theft have led to fraud. Many innocent people who have had their bank details stolen via using public provided utility service such as the USB power charging stations have had money withdrawn from their accounts by scammers. Some other victims have had their identity used by someone else to con unsuspecting clients or family members.

The **Juice-Jack Defender** was first used by the White House to protect its staff from malware installation and identity theft.

It is currently available for shipping at Amazon. It sells for $10

4 Reasons CEOs Should Plan For Failure And Encourage Risk-Taking

Every successful company leader will tell you that failure is a part of business, but far fewer will admit they plan for failure. Growing a business requires taking risks, and failure is a frequent outcome on the journey to achieving success.

In their best-selling book Switch, co-authors and brothers Chip and Dan Heath describe how world-renowned design firm IDEO (perhaps best known for its work with Apple) plans for failure during its design process. The company's designers even created a process chart that factors in the excitement and hope at the beginning, the emotional lows of when things aren't going as planned and the joy of victory at the end.

It's a brilliant way to view risk-taking and how leaders can plan for failure while on the road to success. It's an approach I embrace at Petra Coach and recommend to the member companies that we consult. Here's how you do it:

1. Plan For Failure By Knowing The Risks

When taking a risk, make sure it's a calculated one. Evaluate the upsides and downsides and what they mean to your business. Have answers to key questions like: does the undertaking align with your company's vision and mission? Do the activities and tasks support company goals and priorities? Did we plan for failure, and do we know how to respond if things go sideways? Remember, a failure that is aligned with your business's goals is still a step in the right direction.

2. Learn From Your Mistakes

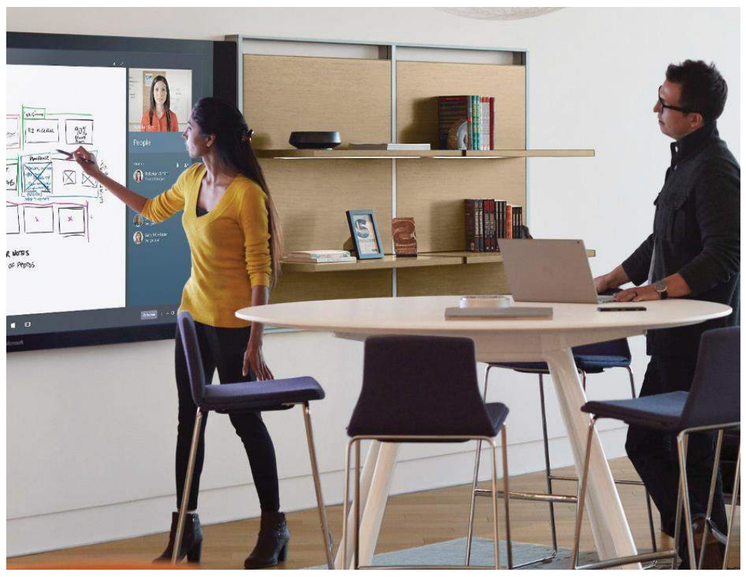
Every failure experienced will provide important lessons that can be applied to your business. Roll up your sleeves and find out what went wrong. Were your expectations incorrect? Did you misjudge market demand? Was your strategy not on target? Be brutally honest about the hows and whys, but don't dwell on it or point fingers. Get your team together to determine the necessary changes and move forward.

3. Celebrate Failure

Failure is part and parcel of running a business, so don't feel ashamed when things don't go as expected. Failure means you're taking action to grow your business. Celebrate each failure by publicly applauding team members who had the courage to take a chance and accept the consequences. Hold a "failure party" or create an award for the biggest risk taken. It will foster a positive attitude toward smart risk-taking.

4. Encourage Open Discussion About Failure

All business leaders have failed at some point during their careers. To foster a culture of smart risk-taking, encourage team members to share their highs and lows about projects where they took a chance. Make it acceptable to talk about mistakes so team members are encouraged to share their experiences and ideas. It will create a more open and creative environment and help build healthier teams. In today's world where business seems to move at the speed of sound, the biggest risk is not taking any risk at all. Few, if any, business leaders have succeeded by sticking to their original idea. A planned, detailed strategy to deal with failure will keep your team energized and in a positive mindset when they tackle the next big idea.



*As the founder of Petra Coach, **Andy Bailey** can cut through organizational BS faster than a hot knife through butter, showing organizations the logjams thwarting their success, and coaching them past the excuses we all use to avoid doing what needs to be done. Andy learned how to build great organizations by building a great business, which he started in college. It then grew into an Inc. 500 multimillion-dollar national company that he successfully sold and exited.*

Do You Have These 3 Things Every Business Needs To Be Successful?

You have a solid team. People are everything in business – that includes your employees. You strive to hire the best team (who match your core values and company culture and who bring top-notch skills to the table) and you train them well (they understand your systems and processes). On top of that, they're happy!

You have purpose behind what you do. We all need purpose to not only be happy but also to thrive. When your team knows what they're working toward and understand the value of their work, that gives them purpose. You've clearly laid out the objectives and everyone is on the same page. When your employees know why they do what they do, they're happier and more productive for it.

You are passionate. You don't just love what you do, you love the people you work with and you love the difference your business makes in the community or the world. When you have passion, it's infectious. It inspires people around you. When your team is inspired, they'll go the extra mile and your business will find success likes it's never found before.

Inc.com, 5/20/2019

What The Heck Is An AUP ... And Why Do You Want It?

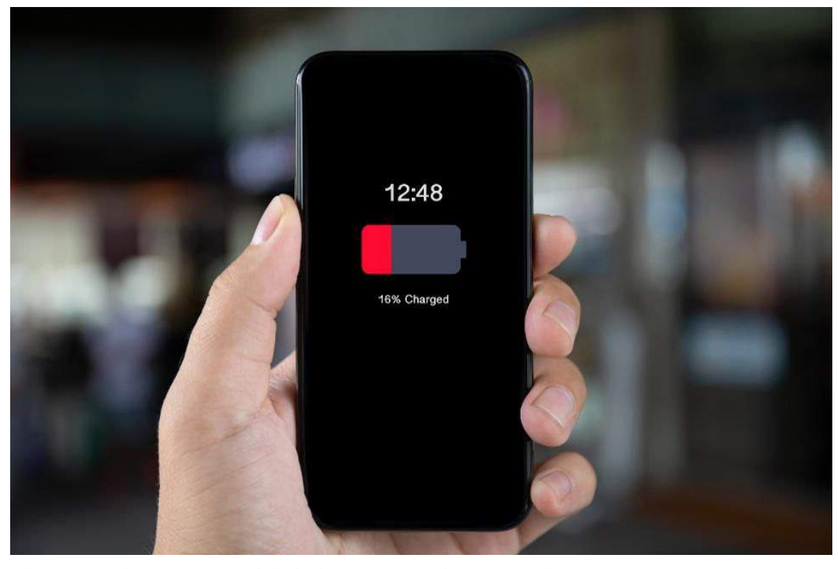
With so many access points, from cell phones to laptops and home computers, how can anyone hope to keep their network safe from hackers, viruses and other unintentional security breaches?The answer is not "one thing" but a series of things you have to implement and constantly be vigilant about, such as installing and constantly updating your firewall, antivirus, spam-filtering software and backups. This is why clients hire us – it's a full-time job for someone with specific expertise (which we have!).

Once that basic foundation is in place, the next most important thing you can do is create an Acceptable Use Policy (AUP) and train your employees on how to use company devices and other security protocols, such as never accessing company e-mail, data or applications with unprotected home PCs and devices (for example). Also, how to create good passwords, how to recognize a phishing e-mail, what websites to never access, etc. NEVER assume your employees know everything they need to know about IT security. Threats are ever-evolving and attacks are getting more sophisticated and cleverer by the minute.

If you'd like our help in creating an AUP for your company, based on best practices, call us. You'll be glad you did.

Never Use Airport USB Charging Ports – Or Cords Laying Around

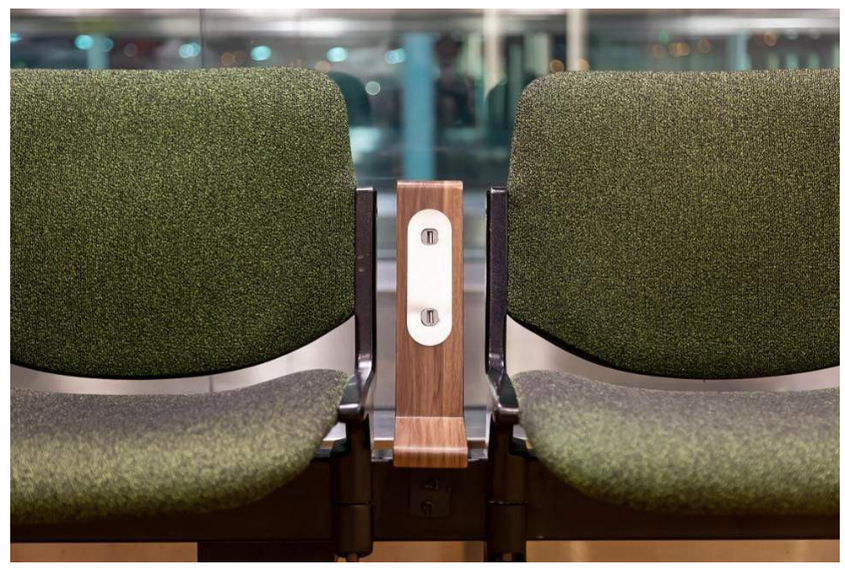
Those oh-so-handy USB power charging stations in the airport may come with a cost you can't see. Cybercriminals can modify those USB connections to install malware on your phone or download data without your knowledge.
"Plugging into a public USB port is kind of like finding a toothbrush on the side of the road and deciding to stick it in your mouth. You have no idea where that thing has been," says Caleb Barlow, Vice President of X-Force Threat Intelligence at IBM Security. "And remember that that USB port can pass data."
It's much safer to bring your regular charger along and plug it into a wall outlet or, alternatively, bring a portable power bank to recharge your phone when you're low on bars. If you insist on using public USB ports, Barlow recommends investing $10 for something called



Almost out of juice? Be careful of where you turn for a power boost.

a Juice-Jack Defender. "It's a little dongle you can put in front of your charging cord that basically blocks any data from passing down the cord. It only passes the voltage," says Barlow. While these precautions may seem excessive to the average traveler, Barlow says it's smart to worry about public USB power stations. A growing number of nation-state hackers are now training their sights on travelers, according to new research from IBM Security. The 2019 IBM X-Force Threat Intelligence Index reveals that the transportation industry has become a priority target for cybercriminals as the second-most attacked industry — up from tenth in 2017. Since January 2018, 566 million records from the travel and transportation industry have been leaked or compromised in publicly reported breaches.

Suzanne Rowan Kelleher
June, 2019


They're handy, but airport USB charging stations may pose a risk to your personal data.

Want more informative and comprehensive stories? Check out **KAMIND IT**'s Blog at **www.kamind.com/blog**

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**

Which page on kamind.com can you find important articles about Cyber Security, Licensing, Etc.?

A. www.kamind.com/security
B. www.kamind.com/blog
C. www.kamind.com/eos
D. www.kamind.com/software-audits

KAMIND®
Cloud Solutions Advisors

Microsoft AEP Authorized Education Gold Partner

Microsoft Partner
Microsoft
Gold Cloud Platform
Gold Cloud Productivity
Gold Windows and Devices
Gold Enterprise Mobility Management
Gold Small and Midmarket Cloud Solutions