KAMIND®

TECHNOLOGY TIMES

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

WHAT'S NEW

Meet our newest team member that is here to assist in growing our business at **KAMIND IT**. **Brendan McDonnell** is our new **Corporate Sales Executive** assisting our clients solve business problems with the use of The Microsoft Intelligent Cloud! Please welcome **Brendan** to our team.

From everyone at **KAMIND IT**, we wish you a spooky and safe **Halloween!**

OCTOBER 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 Ways To Prevent Your Employees From Leaking Confidential Information

A lot of businesses need to come to terms with the fact that their employees are their greatest IT threat. As a business owner, you may be aware of cyberthreats to your business, but your employees might not be. They might not know about the threat of cyber-attacks or malware. They might use unsecured WiFi on company equipment. As a result, your employees may be putting your business at serious risk.

What can you do to change that?

1. It all starts with education.

One of the biggest reasons why employees put their employer at risk simply comes down to a lack of education. They don't know about the threats targeting businesses or that small businesses are a major target of hackers and scammers.

You need to do everything you can to train your employees. Give them the education and resources to be a line of defense rather than a risk. Develop a consistent training regimen. If you need to bring in IT professionals to help, do it. Don't make assumptions about critical IT security training if you aren't sure. Professionals can answer questions and make sure you and your employees have everything you need to know to keep your business secure.

Another important thing is to hold this training regularly. Threats evolve, and you need to stay ahead of the curve. Keep IT security on the minds of your employees. When they forget about it, that's when the risk is highest.

2. Say NO to unsecured, public WiFi.

This is a big problem for businesses with remote employees, employees who work from home or employees who use company technology outside of the business walls. According to a Spiceworks study, 61% of employees said they have connected to unsecured WiFi while working remotely. This is cause for concern. Connecting to public WiFi is like leaving the front door of your home wide-open while posting on social

Continued Page 2

Continued From Page. 1

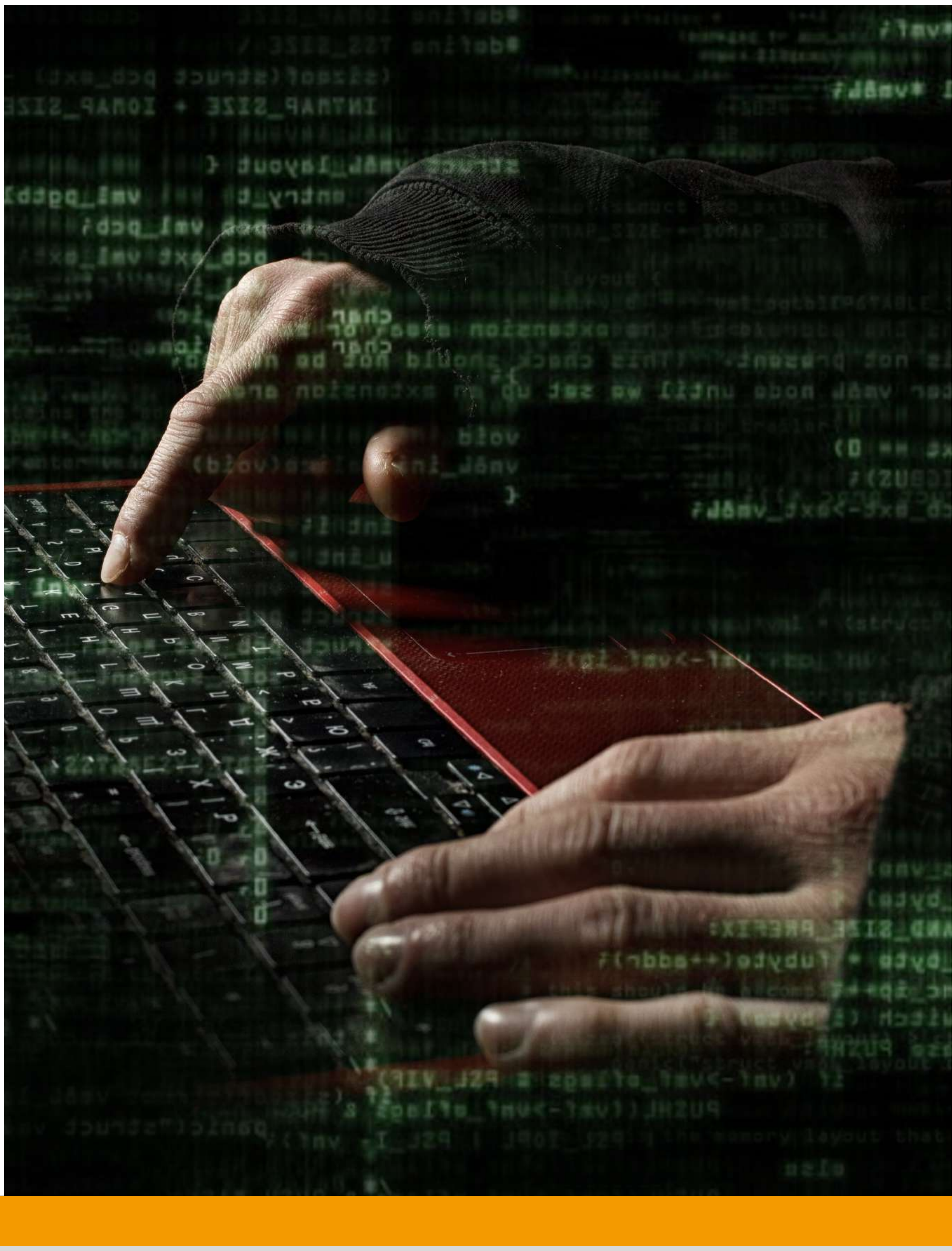
media that you're going to be out of town for a week.You never know who is going to let themselves in and snoop around. Hackers use public hot spots to circulate malware and steal data. Sometimes they even set up fake hot spots with the same name as a legitimate hot spot to trick users into connecting to their WiFi, which makes data theft even easier.

Discouraging your employees from using unsecured, public WiFi is a good step to take, but don't be afraid to take it further. Don't let them connect company equipment to unsecured WiFi at all. And place a bigger focus on endpoint security – make sure your equipment has up-to-date software, malware protection, local firewalls, as well as a VPN (virtual private network). The more layers of security, the better.

3. Protect ALL of your data.
Your employees should never save personal or business data on portable/external hard drives, USB drives or even as printed material – and then take that data out of the office. The theft of these types of devices is a real threat. An external hard drive is a tempting target for thieves because they will search the drive for sensitive data, such as financial or customer information that they can use or sell. If you have remote employees who need to access company data, put a method in place to do just that (it should be discussed as part of your regular company IT security training). They need to know how to properly access the data, save the data or delete it, if necessary.

"It's all about understanding the threats and taking a proactive approach to security."

Many businesses go with a secure cloud option, but you need to determine what makes the most sense for your business and its security. While these three tips are great, nothing beats helping your employees develop a positive IT security mindset. It's all about understanding the threats and taking a proactive approach to security. Proactivity reduces risk. But you don't have to go it alone. Working with experienced IT security professionals is the best way to cover all your bases – and to ensure your employees have everything they need to protect your business.



26+ Cyber Security Statistics & Facts For 2019
Collection of the latest cyber security statistics and trends to help keep you informed

- Roughly 1 out of 5 files aren't protected
- Cyber crime is quickly becoming more profitable than the illegal drug trade
- Users in the U.S. open around 1 in 3 phishing emails
- Information loss accounts for 43 percent of the costs in cyber attacks
- By 2020, there will be 300 billion passwords utilized across the world
- Over half of millennials experienced cyber crime in the last year
- Personal data can be purchased within the range of $0.20 to $15.00
- The lowest cyber crime rate award goes to the Netherlands. The highest goes to Indonesia.
- If they have a data breach, it typically takes companies over 6 months to notice.

Shiny New Gadget of The Month

The Philips Somneo Sleep & Wake-Up Light

Research suggests that when you wake up naturally (that is, you aren't jolted awake by an alarm or radio), you feel more refreshed and energized during the day.

The Philips Somneo Sleep & Wake-Up Light puts this research to the test. It's designed to simulate a natural sunrise right in your bedroom. You can set it to your specific needs, and it will slowly and steadily brighten when you need to wake up. It can also simulate a sunset for the opposite effect when you're going to bed!

You can even use the light as a reading lamp — and it has a built-in radio, too! **The Philips Somneo Sleep & Wake-Up Light** is a versatile device, perfect for anyone who wants to get a better night's sleep. Find it at Amazon and many other electronic retailers.

The Power Of Punctuality

Personally, I am not a fan of people who are always late. Sometimes, things happen that we have no control over, such as car accidents, traffic jams and unexpected family emergencies, to name a few. I am not addressing those situations.

What I am addressing is how punctuality can do wonders for your success.

Have you ever thought about what being punctual says about you? It shows you are in control, disciplined, able to keep track of things, trustworthy, reliable and respectful of another person's time. Being late demonstrates none of those things. In fact, being late shows you are unreliable, disorganized, disinterested and inconsiderate. When you look at it from that perspective, you would never want yourself described that way.

Do you want to hire someone who is unreliable? Not me. How about disorganized? A disorganized person will make mistakes — and mistakes cost money. Let's take a closer look at disinterested. One of the definitions of disinterested is having or feeling no interest in something, unconcerned, uncaring and unenthusiastic. That sounds like someone you NEVER want to have on your team. Then that leaves us with inconsiderate, defined as thoughtlessly causing hurt or inconvenience to others, unthinking, selfish, impolite and rude.

Associates, bosses and customers have NO fondness for lateness. I heard one person express it this way: "If you are chronically late, you are chronically rude." If you are looking to be promoted to a leadership position, it will be difficult to prove yourself reliable when people are having to wait for you to show up. Punctuality is a product of discipline, proper planning and respect for others. In simple terms, preparedness and punctuality are two of the most important qualities of a leader.

When you are late, you are saying, "My time is more valuable than yours." That is not a great way to start anything. The celebrated writer Charles Dickens once said, "I could have never done what I have done without the habits of punctuality, order and discipline." I feel that by being punctual, you are paying a courteous compliment to those you are about to see or serve; it's a respectful gesture of how you value their time.

Chronic lateness sets a tone about accountability. If you want a culture in which people are accountable to customers, associates and even to themselves, then make punctuality a priority. Start all meetings on time regardless of who is missing. The word will get out, and people will start showing up on time.
Being on time may seem a bit trivial to some people, but it's a good idea to start making accountability part of your corporate culture. Shakespeare once stated: "Better three hours too soon, than a minute late." There truly is power in being punctual.

Scan me

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.

KAMIND IT
5200 MEADOWS ROAD
STE #150
LAKE OSWEGO, OR 97035

Prsrt Std
U.S. Postage
PAID
Permit No. 2358
Portland, OR

These Are The Biggest Privacy Threats You Face Online Today

Webcam Access – While it's rare, there are known exploits that allow others to access your webcam (such as malicious software or software security flaws). Putting electrical tape over your webcam isn't a bad idea, but more webcams are coming with kill switches and shutters for peace of mind.

Phishing Scams – Don't ever expect these to go away. People still fall for them. NEVER click links in e-mails from anyone you don't know (and even if you do know them, verify that they sent you a link — e-mail addresses can be spoofed).

Web Browser Plug-ins – Vet every browser plug-in and extension you install. Many extensions collect your browsing history and sell it. Read the terms of service before you click install (a good rule of thumb for software in general).

Ad Tracking – Web ads (and web ad providers, such as Facebook and Google) are notorious for tracking users. They want to know what you like so they can cater ads directly to you in the hopes that you'll click the ad, which gives them ad revenue. It's one of the many reasons why people use ad blockers.

Device Tracking – If you have a smartphone, chances are it's being used to track your every move. Again, it comes back to delivering ads that are relevant to you so you'll click on them. For companies like Facebook and Google, users are the product.

Inc. 7/19/2019

Capitalize On This Strategy To Improve Your Bottom Line

Want to boost your bottom line? The answer may be in cashless payments. It's all about taking your current systems and updating them to current trends. Outside of the U.S., particularly in Europe and much of Asia, cashless payments are king. More people are relying on smartphones as payment processing tools (both in the consumer and business worlds). Of course, you don't want to rely on cashless — you want to be able to accept any money your customers are spending, whether it's cash, card or electronic. Look at your point-of-sale system — is it ready for cashless? If not, look into it, research your options, ask around and see what option makes sense for your business (and bottom line).

Small Business Trends, 6/26/2019

Top IT official names China as main cyber threat to US

A top IT government official on Wednesday said China poses the biggest cyber threat to the U.S. Speaking at a cybersecurity summit, Federal Chief Information Security Officer (CISO) Grant Schneider said China has the "capacity and the capability and the intent" to work against the U.S. in cyberspace more so than other countries.

China is "an adversary that has displayed their intent, has clear means to get into and attack our critical infrastructure systems, our government systems, you name it, both from an intellectual property theft point of view, as well as an espionage point of view," Schneider said at the 10th annual Billington Cybersecurity Summit in Washington.

He added that American dependence on information technology systems only compounds the potential security vulnerabilities that countries like China could exploit and emphasized that threats to networks have evolved. "It's really the nation-state actor, and the one particular nation state with the capacity and the capability, and the intent is really the one that concerns me the most," Schneider said.
Schneider's comments come amid President Trump's escalating trade war with China. The yearlong dispute has at times focused on potential security issues regarding Chinese telecommunications giant Huawei.

The Trump administration cited national security concerns when it blocked U.S. companies from doing business with Huawei, one of the largest telecom products providers in the world. The U.S. has also put pressure on allies not to allow Huawei into their 5G wireless networks.

Schneider spoke on a panel alongside former Federal CISO Gen. Gregory Touhill, who also discussed the key cyber threats to the U.S. While Touhill did not mention China, he emphasized that cyber risks to critical infrastructure and vulnerabilities posed by the increasing amount of Internet of Things devices, or any product with the ability to connect to the internet, as potential security problems.

"The advent of the Internet of Things continues to expand the risk of exposure, and the price of entry for somebody to engage in malicious mischief and criminal activity, the price for them is pretty low," Touhill said. "I see the threat landscape continuing to expand, the risk exposure continuing to be high."

The role of federal CISO was created in 2016, with Touhill serving as the first federal CISO until January 2017. Schneider served as acting federal CISO until he was appointed to the position by Trump in 2018.

Maggie Miller - 09/04/19

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

KAMIND®
Cloud Solutions Advisors

Microsoft
AEP
Authorized Education
Gold Partner