INDEVTECH

TECHMinutes

Your Small Business Technology Information Source!

This Issue:

Crafting Successful Remote Work Policies

Considering the circumstances of the past couple years, it's no surprise that many businesses have turned their attention towards creating a long-term plan for a remote workforce. There are many considerations that must be brought front and center to create such a remote work policy, many of which require a focused examination of technology and the practices associated with it...

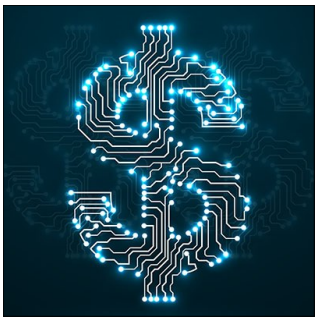
Read the Rest Online!
https://bit.ly/3x9lqjY

About Indevtech Incorporated

We are the IT department for many small businesses in Hawaii, across different verticals such as healthcare, legal, financial, and manufacturing concerns.

Visit us **online** at:
newsletter.indevtech.com

4 Critical Technologies All Small Businesses Need



One of the best things about technology is that it does quite a bit to level the playing field. Smaller businesses can effectively do the work of larger enterprises because they have access to similar technologies. Additionally, technology goes a long way toward helping businesses manage their customer relationships, a key component to any revenue-seeking endeavor. This month we thought we would put together a list of four technologies every small business can use to manage their business and compete in their market.

Human Resources Software

For decades, human resources was manned by people doing constant tasks to help improve working conditions and facilitate business by keeping companies running smoothly. Today, the whole industry is seeing a major shift, in large part, from technology. Today, there are online platforms for recruiting talent, time-tracking software that makes accounts receivable much more efficient, and other applications designed to make the role of human resources easier to manage. With this technology, the communication between HR and the staff is streamlined and secure, the litany of forms needed by a business and outside regulatory bodies has all moved online, and all the performance tracking that HR is responsible for can be audited through a company's technology. Today's HR software also makes

(Continued on page 3)

Here's What Effective Collaboration Looks Like

In order to produce the results that your business' customers demand, it is essential that your team work together. This collaboration comes in several forms, but if one person struggles, it can be a dire development for any project or service delivery. This month we thought it would be useful to outline what effective collaboration looks like and give you some insights into how technology fuels most of your business' collaborative efforts.

Start With Talent

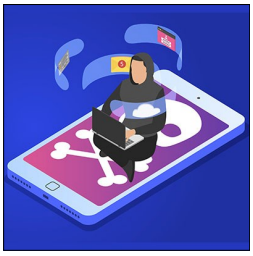
One of the main issues a lot of organizations have with their collaborative efforts is assigning tasks to people who aren't fit for them. Oftentimes this happens as a result of heavier-than-usual workloads on people who would normally undertake the tasks, leaving it to untrained and inexperienced people to complete sections of a project or service delivery. Ultimately, it creates efficiency issues, especially when the work has to be redone. When managing a collaborative effort, ensure that your team is made up of people that have the specific skills the task calls for.

Communication

Of course, communication is a major part of any collaborative effort, not just for access to communication tools that allow for a free exchange of ideas, but also for the checks and balances that make these initiatives successful. In a lot of situations, businesses want to avoid conflict as much as possible, but when workers collaborate, there should be some. After all, collaborative teams are generally made up of people with different perspectives and experiences. A healthy exchange of constructive criticism can bring out the best in a team effort, and can have major impacts on the end result and the revenue generated from it.

(Continued on page 2)

Social Networking Sites are Far From Immune to Cybersecurity Threats



One of the more overlooked parts of cybersecurity attacks involves social media and social engineering tactics targeting it. If you're not careful, you could be putting yourself at risk of attacks through social media. How can you ensure that your staff members are keeping security at top of mind even when using social media? Let's find out.

Fake Accounts

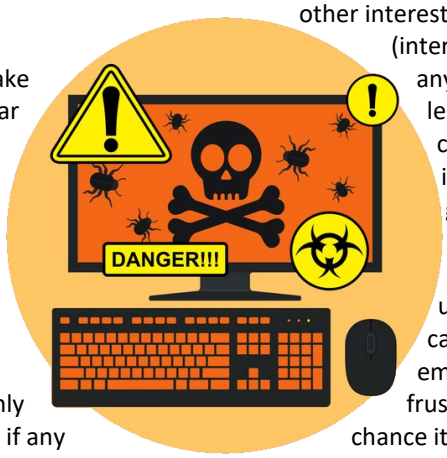
A hacker might set up fake accounts that look similar to those you are familiar with or those who are popular or common. Accounts like these might be quite new, having only a handful of friends or been created recently. These accounts often only have a handful of posts, if any at all, and they are just fishing for "friends" to target.

Unsolicited Messages

Sometimes hackers might use a hacked or fake account to send unsolicited messages to users. The most notorious types of messages received might be from friends who you might not have heard from in a while, and you might ask yourself why they are contacting you out of the blue all of a sudden. While we are all for wanting to trust friends or connections, it's important to vet suspicious messages appropriately before responding.

Phishing Links

Social media is often used to share links to news websites, articles, reviews, or other interesting information (interesting to the sharer, anyway). Before mindlessly clicking on a link, consider who is sharing it, where the link goes, and whether or not you can trust it. Taking a moment to use a bit of scrutiny can save you a lot of embarrassment and frustration on the off-chance it's a phishing link.



Sneaky Quizzes

This one is more insidious compared to the others, as it's not immediately clear or obvious that this is an issue. Essentially, you might see your friends taking quizzes like "Which Golden Girl are You?" If you're not careful, you might be providing the quizzes, and whoever created them in the first place, with information that might be harvested later on for a hacking campaign. While it might be fun to learn these things, be cognizant of the types of questions you are being asked, too.

Training is Incredibly Important

To keep your employees from doing something silly and falling for a social media phishing scam, you need to conduct regular training sessions that make them aware of the dangers they face every day they log onto their social media accounts. Periodically go over social media best practices to ensure that your team is always apprised of what they need to know.

Indevtech can help your business train its employees and reinforce appropriate practices. To learn more about how we can help your team keep security at the top of their minds in all they do, reach out to us at (808) 529-4605.

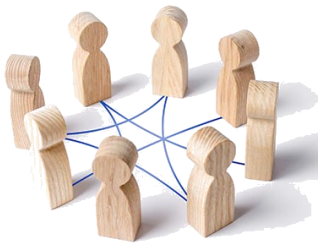
Share this Article!
https://bit.ly/3PXclTX

Here's What Effective Collaboration Looks Like

(Continued from page 1)

Align Your Goals

One of the most important issues surrounding any collaborative endeavor is to have a shared goal. Many businesses get trapped by the belief that all the workers on a collaborative team share the same goals. Typically, they don't. That's why you need a clear set of goals to work from and managers that are good at creating manageable and measurable tasks that will reach the team's goal.



What Technology Can Help?

There are a lot of different ways you can fuel your collaborative teams with technology, but before you just throw technology at your efforts, you should understand what technology is best for your needs. Here are some options that are readily available that can help your business' collaborative efforts:

- **Collaboration apps -** Software that is specifically made for collaboration. These apps are available anywhere on nearly any device and give users the ability to work with a lot of integrated software titles.
- **Video conferencing -** Being able to have impromptu meetings where you can talk to your team is important with all project coordination.
- **Productivity suites -** Cloud-based productivity suites give team members the ability to collaborate on specific documents, presentations, and spreadsheets.

Indevtech technicians can help you get all the technology needed to improve your business' collaborative productivity. Give us a call and have a conversation today at (808) 529-4605.

Share this Article!
https://bit.ly/3NVIJEt

4 Critical Technologies All Small Businesses Need

(Continued from page 1)
reviewing the enormous amount of data available much, much easier.

Customer Relationship Management

The power of customer relationship management (CRM) software is how it combines all the elements that a business needs to manage their relationships with current and even potential customers. What's more, the CRM typically has features that allow for management of projects and services, time tracking, and saves company and project-centric information so that employees that work in different departments can do work for a single project in one easy-to-use interface.

Innovative Payment Methods

Money is seemingly tight everywhere and customers really respond when your business provides advanced payment solutions. Technology like contactless payments are gaining in popularity. These include mobile wallets and card payments (using swipe or tap to pay), which allow your customers to pay online or in person without having to have cash on them.

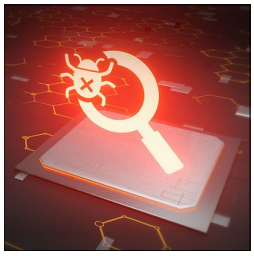
Advanced Data Security

One place where a lot of small and mid-sized businesses lag behind enterprises is with their cybersecurity. Your business needs to invest in security solutions for your brick and mortar locations, for your network and infrastructure, and for the data you take in. Since many businesses are now looking for as much information about their prospective and current customers as possible, having an idea and the tools needed on how to protect that information is crucial to sustaining a positive reputation within your customer base and inside your industry.

Technology can significantly change the way your business operates and can present some pretty great changes to help you tackle all the issues your business may have. Call the IT professionals at Indevtech for more information about getting the technology and technology support your business requires today at (808) 529-4605.

Share this Article!
https://bit.ly/3xkVmUg

Is Your Network a Ticking Time Bomb?



Cybersecurity is not easy to manage, and even professionals have their work cut out for them against modern threats like ransomware and other high-profile security threats. Today, we want to educate you on some of the terminology used in cybersecurity, namely the relationship between a vulnerability and an exploit, as well as what you can do to keep the risks associated with both relatively low.

What Are Vulnerabilities?

Vulnerabilities are small cracks in the code of software and other types of applications that give hackers an entry point into a system. Vulnerabilities are unfortunately a part of the norm in app development and cybersecurity, and they are something that researchers and developers have had to find ways to cope with throughout the years.

Vulnerabilities often go undiscovered for quite some time, only being brought to attention when they are actively exploited or discovered. It's virtually impossible to create an application that is vulnerability-free for its entire life cycle, as the nature of threats constantly rises to meet software developers where they are. Because of this, there is an ongoing battle between hackers and developers, constantly trying to outdo the other. Vulnerabilities are the reasons why patches and security updates are issued as regularly as they are, as they can potentially solve certain vulnerabilities before they become exploits.

What Are Exploits?

Exploits, on the other hand, are vulnerabilities which are being actively used to gain entrance to a system or infrastructure. The big difference between the two is that a vulnerability represents a theoretical weakness that is not currently being used, whereas an exploit is one that is actively being used to target a system. Exploits must be addressed as soon as they are brought to your attention.

What Do You Do?

Adequate cybersecurity practices require the following three approaches:

- Apply patches and security updates as needed to remove vulnerabilities, thereby lessening the chance of suffering from an exploit or data breach.
- Monitor your network for suspicious activity that could be indicative of a data breach.
- Educate your staff on how they can avoid falling victim to phishing attacks that might target vulnerabilities in your infrastructure.

Don't Get Caught Off Guard

We know that cybersecurity can be challenging for some businesses, but it doesn't have to be. Indevtech wants to help your organization optimize security and simplify the patching process. To learn more about what we can do for your business, reach out to us at (808) 529-4605.

Share this Article!
https://bit.ly/3NY4FyY

The FBI is Extremely Concerned About Ransomware; and You Should Be Too

Ransomware is an incredibly disruptive threat that can put your business at risk, but it is increasingly becoming not just a fiscal risk to organizations, but also to the physical health and wellbeing of communities and individuals. The Federal Bureau of Investigation has issued a warning that should have everyone concerned about the future of ransomware attacks, not just in business, but in everyday life.

The Warning

Ordinarily, with ransomware attacks against businesses or individuals, files are locked down with encryption, preventing the organization and the user from accessing them until a ransom is paid. While this is certainly devastating, in a business sense, the worst that can happen is that they will be forced to shut their doors or be subject to massive lawsuits regarding the privacy and protection of sensitive data. But what if these ransomware attacks targeted local governments or agencies?

In this warning from the FBI, they caution that ransomware attacks against local governments can put a halt to services which the public depends on, like healthcare, emergency response teams, and so on. The warning states: "In the next year, local US government agencies almost certainly will continue to experience ransomware attacks, particularly as malware deployment and targeting tactics evolve, further endangering public health and safety, and resulting in significant financial liabilities."

The Implications

Consider what might happen if a hospital or doctor's office cannot access the files of its patients. What might happen if these patients are in critical condition? What about if there is a significant emergency and the response team can't do anything about it because their infrastructure is locked down by a ransomware attack? Not only are sensitive records compromised, but systems in place to prevent or respond to disasters cannot operate effectively.

The fact of the matter is that lives are at risk, and if emergency response systems, healthcare records, and other public government agency organizations cannot access…

Read the Rest Online!
https://bit.ly/3tjKlQu

Indevtech has been serving Hawaii since 2001, providing end-to-end managed IT services to small- and medium-businesses. Our philosophy is very simple: we strive to be the best at what we do, so that you can succeed at what you do. We have a proven framework that, when deployed with a solid commitment from our clients, provides an unshakable foundation on which our clients can build their businesses.

Tech Trivia
eCommerce sales will reach $6.54 trillion globally by 2023.

Indevtech Incorporated

Pacific Guardian Center, Mauka Tower
737 Bishop Street, Suite 2070
Honolulu, Hawaii 96813-3205
Phone: (808) 529-4605

newsletter@indevtech.com

blog.indevtech.com

Visit us **online** at:
newsletter.indevtech.com