directive

TECHMinutes

May 2014

Your Small Business Technology Information Source!

This Issue:

The Top 3 Highest Grossing IT Trends

As the global economy experiences recovery and growth, businesses have extra capital freed up to spend on information technology. IT spending is surging, but where exactly is all of this money going? In a recent study, Gartner shines some light on IT's hottest trends. Compared to last year, total IT spending is projected to increase by 3.2%, which equates to worldwide projected spending of $3.8 trillion, give or take a few bucks.

Read the Rest Online! http://bit.ly/1i850fN

About Directive

We are a technology consulting firm specializing in technology implementation and management for businesses. We're known for providing big-business, Enterprise-Level IT services to small and medium-sized businesses.

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

Should Increased Mobile Malware Attacks Deter You from BYOD?

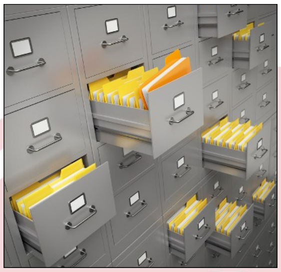
The trend of employees bringing in their own mobile devices to the office and using them for work purposes (BYOD) is growing rapidly. In fact, a new report from Juniper Research forecasts that by 2018, more than one billion employee-owned devices will be used in enterprises. A trend this big means that organizations have to take BYOD seriously.

To put this BYOD projection into perspective, that many devices will account for almost 35% of all tablets and smartphones in use. With more than one third of mobile devices in use projected to contain valuable information from businesses, there's no doubt that hackers and thieves will follow this trend and focus more of their attention on mobile devices, which is actually something hackers have been doing steadily over the past few years.

The growth of BYOD and its projected dominance of the future present a challenge to IT professionals. Unlike an in-house network that can have its security easily managed, mobile devices that access a company's network present security risks that are hard to completely

(Continued on page 3)

Retro 1800s Business Practices Can Cost Your Company Money!



Trivia time! Do you know what device was invented in 1892 that changed the face of offices around the world? If you guessed the fax machine then you're close, but you need to think further ahead by almost 50 years (the first fax machine was patented in 1843 by Alexander Bain). More influential than even the fax machine is the file cabinet, established in 1892.

File cabinets and fax machines both revolutionized their time, but now that we're living in the next millennia, it's safe to say that the time of these two innovations has passed. Yet, how many modern offices contain a fax machine that feeds paper into file cabinets? If this describes your office, then you might as well equip your staff with green eyeshades and mustache wax because you're doing business in the 1800s!

Cheap 1800s Technology is Expensive to Operate

These technologies are outdated because handling files digitally is a much more efficient way of doing things. When it comes to document gathering and transferring tasks like filing away papers, digging through the file cabinet, and sending and receiving faxes (sending a fax averages 30 seconds per page), you may be surprised to learn that an employee in a "modern office" can spend as much as 90% of their time just handling documents!

Considering all the trips an employee makes to and from the file cabinet, all the time spent digging through files to locate a specific document, and all the time spent organizing file cabinets by moving old documents to storage boxes, and the fact that you're paying an employee to do all of this work, it makes sense that the standard-sized file cabinet has $25,000

(Continued on page 3)

What is a Botnet Attack and How Do You Stop It?

Hackers have many different tools at their disposal to access your computer. Some of these tools can even control your machine! When a hacker controls your PC, your computer is now part of a network made up of other compromised devices that they control. This compromised network is known as a botnet, and you don't want to be part of it!

What makes a botnet network unique is that it's often made up of a variety of different Internet-connected devices from all over the world. A typical botnet network is more than just compromised workstations and smartphones, although these technologies certainly make up the majority of the compromised devices. Basically, anything that connects to the Internet can be controlled by a hacker and incorporated into their botnet network.

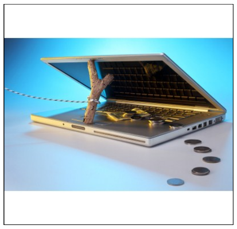
This makes botnet attacks especially dangerous in the upcoming years as "the Internet of things" expands exponentially. The Internet of things refers to the vast amount of devices that are constantly being added to the Internet. Many of these devices are pieces of equipment that one would have never thought would be Internet enabled, like cars and home appliances. The majority of new Internet-connected devices includes small gadgets that have a singular purpose like gathering valuable data and using the Internet to feed a database the collected information in real time. This includes devices such as: Security cameras, fitness trackers, temperature gauges, media players. Many businesses employ these small Internet-connected devices for analytics purposes, so much so, that IDC projects the total number of things connected to the Internet will be 212 billion by the end of 2020.

Botnet attacks will indiscriminately go after all of these different devices connected the Internet and find success with a variety of them. Therefore, a hacker with their own botnet network may potentially have thousands of devices at their disposal and under their control. A hacker's control may be over just a few functions of a device, or it may extend to controlling the device entirely.

Due to the hobbled-together nature of a botnet network, botnet attacks are often likened to a zombie virus. Just as a hacker's compromised network often consists of random devices that they have some control over, so does a zombie hoard consist of people from all different shapes and sizes with limited move-

(Continued on page 4)

Avoid These 3 Bad IT Service Traps



It takes a special kind of person to give great customer service. If someone can't pick up on social cues, or if they have a low tolerance for repetitive questions, they will end up offending a lot of customers. To assist our clients with their IT problems, we make sure to hire the most helpful customer service representatives that we can find.

Because Directive spends extra time screening our IT technicians and training them on how to properly handle the phones, you can rest assured that you won't get stuck having mind-numbing phone call like in these three examples.

Being Read to Like You're Stupid

While it's important to be thorough and informative, reading straight from a prepackaged script is highly annoying. To make matters worse, some people have a way of reading that's a dead giveaway that they're reading, like using a monotone voice, not pausing between sentences, and using zero voice inflection.

Being read to during a support call is annoying because you know how to read, and thanks to Google Search, you can probably find the answer to your technology problem yourself. Yet, despite the fact that you know how to Google the answer, you still call tech support for assistance. Why? Because you want help fixing the problem. The last thing you want is to have to read an instruction manual. Therefore, it's counterproductive and frustrating when you call IT support and someone reads a manual to you.

Looking for an Excuse to Not Help You

"I'm sorry; we can't help you with that." -click- Technology companies can be very particular about which technologies they support and which ones they don't. Terms of technology support are spelled out in what we call an SLA, or Service Level Agreement. SLAs are the way that IT companies define the parameters of a service contract in order to not lose money by having to service technologies they don't support. For example, think how far you would get with Microsoft if you called them about fixing your iPhone. Microsoft would shut you down rather quickly because the iPhone issue would lie outside of the SLA.

To protect ourselves and define the boundaries of service, Directive uses an SLA with our clients, but we see ourselves first and foremost as a solutions provider. This means that we won't immediately hang up when we discover that the the nature of the problem lies outside of the SLA. Instead, we will work hard to find a solution that both meets your needs and fits the SLA. At Directive,

(Continued on page 4)

Should Increased Mobile Malware Attacks Deter You from BYOD?

(Continued from page 1)

control, and these risks grow with the addition of every mobile device. It's no wonder that Juniper also predicted that over half of all mobile devices in the US will have security apps installed on them by 2018.

New network security scenarios presented by BYOD are proving to be quite the challenge for businesses that lean on in-house IT technicians. This was found to be the case in a recent survey of IT professionals by Ponemon Institute. According to this survey, mobile security will be one of the biggest issues in the IT industry for years to come.

71% of respondents say endpoint security threats have become more difficult to stop or mitigate in the past two years.
This trend can be directly attributed to the proliferation of mobile devices in the workplace, and subsequently, the increased attention given to mobile devices by hackers. Basically, more devices around the office translate to more points a hacker can use to infiltrate a company's network.

68% say their mobile devices have been targeted by malware in the past year.
This statistic will surely rise as hackers target mobile devices associated with businesses even more; and it may actually be higher than 68% because this figure only applies to cases of known malware attacks.

41% say their enterprise has 50 or more malware attacks a month.
This averages to multiple malware attacks every day. Arming your staff with a fleet of mobile devices will dramatically increase the amount of attacks on your company's IT infrastructure.

39% of respondents list advanced persistent threats as one of their most concerning security risks.
Hackers are stepping up their game on all fronts and those in charge of overseeing a company's network security are feeling the pressure. When it comes to IT security, the more precautions you have in place, and the more help you have, the better they will protect your company and help to relieve all the stressful situations that come from the barrage of increasing malware attacks.

Having workers use their own devices for work increases the security risks for your business. However, an increased level of risk shouldn't deter you from enjoying the benefits of BYOD. Studies have shown that both employee satisfaction and productivity are improved with the allowance for BYOD. Therefore, as is the case with any major business decision, you have to determine if the benefits outweigh the risks.

Directive is here to help your business go mobile and implement the best security tools you need for BYOD. This includes assessing your mobile needs and reviewing your options. For example, it may be less risky for your business to provide employees with mobile devices that can be managed, instead of allowing them to use their personal devices. You can also take advantage of hosted data solutions so that sensitive information is not stored on random devices, thus reducing the risk from a data breach due to a lost or stolen device.

Read the Rest Online!
http://bit.ly/1hHHXd3

Retro 1800s Business Practices Can Cost Your Company Money!

(Continued from page 1)

worth of company time sunk into it! We're pretty sure that you can think of better things to spend $25,000 on than a crusty old file cabinet.

The Digital Revolution Trumps the Industrial Revolution Every Time
In addition to the waste of time and money it is to manually handle paper documents, relying on paper can be extremely limiting. For example, let's say that your business takes you on the road and you wind up needing a copy of an important document buried deep in a file cabinet at your office. Your only option would be to give your office a call and have someone on staff retrieve the document and then find a way to get it to you. This would either be done by faxing it to you, or scanning it and then attaching the file to an email. Both of these processes are time consuming.

Having your business go paperless is a great solution that will save you money and give everyone on your staff more time to invest in tasks that make you money. By taking advantage of digital solutions like fax servers and cloud computing, you will be able to ditch the fax machine and file cabinet and even save some trees while you're at it. Not to mention it's MUCH easier to back up your data when it's digital.

A fax server solution from Directive will allow you to send and receive faxes as PDF files from your email inbox. Another good paperless solution is storing your company's files to the cloud, which allows anybody on your staff to access any file, on any device, from anywhere, saving you the hassle of telegraphing your straw-hat-wearing clerk and giving them the "what's for" about sending you the printed form via Pony Express.

To equip your office with technology from this century, give Directive a call at 607.433.2200.

Share this Article!
http://bit.ly/1hHIuLV

Avoid These 3 Bad IT Service Traps

(Continued from page 2)

we understand that people calling us about technology problems are looking for answers, not excuses.

Dragging Out a Phone Call to Make More Money

Some break-fix IT companies charge by the hour for their remote support. When it comes to this model of IT support, it's easy for the customer to be suspicious if the break-fix company is taking their sweet time to fix the problem, typically by giving the customer what's called "the runaround." This is a way for the company to leverage their expertise to intentionally lead clueless customers down a series of dead ends for the purpose of eating up expensive minutes off the clock.

At Directive, we remove this suspicion by offering remote support with an all-you-can-eat approach. This works out best for both parties because we're motivated to efficiently find a solution to your problem, and you and your employees don't have to hesitate about contacting us to fix the problem for fear of running up a major bill.

In addition to all of this, our IT technicians are trained to be excellent customer service representatives, which means that you won't get frustrated working with a dud of a customer service rep. Taking advantage of remote IT support is a sure way to come to a fast and satisfying solution that won't leave you wanting toss your phone across the room. To receive excellent IT support from Directive, give us a call at 607.433.2200.

Share this Article!
http://bit.ly/1hHJgbU

We partner with many types of businesses in the area, and strive to eliminate IT issues before they cause expensive downtime, so you can continue to drive your business forward. Our dedicated staff loves seeing our clients succeed. Your success is our success, and as you grow, we grow.

What is a Botnet Attack and How Do You Stop It?

(Continued from page 2)

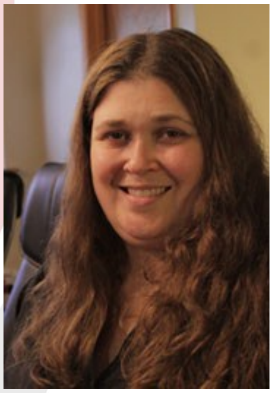
ment; and, just like a zombie horde is dangerous with one goal in mind (BRAINS!), a hacker's botnet network can do some serious damage when they direct everything they control to do one attack (known as a distributed denial of service attack, or DDoS).

How do you know if your computer or Internet-connected device has been breached by a Botnet attack and is subsequently in the control of a hacker? It can be very difficult to tell if you've been compromised because many successful botnet viruses embed themselves in a system and will just sit there dormant, awaiting to receive a command from their creator via Internet connection to do something (like a spiral-eyed "your wish is my command" situation). Therefore, it's good to stay vigilant with your virus scans that look specifically for the latest botnet infections, instead of waiting to take care of a botnet attack only after you notice symptoms.

The way to remove your device from a botnet network is to interrupt communications to the hacker's command-and -control server. This can be achieved by simply disconnecting the device from the Internet. However, once the device is reconnected to the Internet, it will send a signal to its hacker commander, telling them that it's ready to resume its task. This is why it's so important to remove the Botnet code entirely because the hacker can find their target from anywhere over the Internet.

Read the Rest Online!
http://bit.ly/1hHINq8

Chris Chase
Solutions Integrator



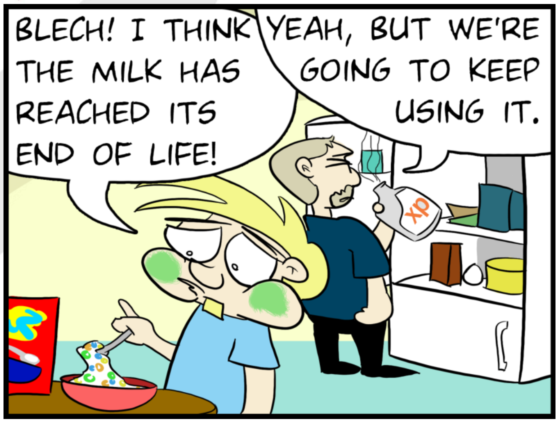
Charlotte Chase
Solutions Integrator

Directive

330 Pony Farm Road
Suite #3
Oneonta, NY 13820
Toll-Free 888-546-4384
Voice: 607-433-2200

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

newsletter@directive.com
facebook.directive.com
linkedin.directive.com
twitter.directive.com
blog.directive.com


BLECH! I THINK THE MILK HAS REACHED ITS END OF LIFE!
YEAH, BUT WE'RE GOING TO KEEP USING IT.
XP