eSudo Technology Solutions, Inc | 408-216-5800

Innovations

Happy Valentine's Day!

Never Apologize For Having High Standards. You And Your Business Deserve The Best!

In-house or outsourced IT? That is the question on many business owner's minds. Can we swing it with an internal IT guy? Will that person be able to handle the volume of work in our office? Will they know all they truly should to keep our company safe? Maybe, but are you willing to risk it? Take a look at these essential questions to consider before you settle for less with your company's IT management. After all, your business needs a good foundation to flourish.

Why in-house IT management may cost more and lack luster. IT is the single largest administrative cost for most businesses today. So, the big question is, and no you won't get a diamond ring out of the deal, should you outsource or pay someone in-house to manage your most valuable assets? Ask yourself these important questions first; Are you prepared to hire a full-time IT administrator? Do you know what to look for in a trusted advisor? Can you be confident that person will know how to keep your company safe and stay on top of new threats? Relationships are all about trust, if you have to play detective to ensure your IT management is up to your standards, it's time to move on. Quality of service is just the tip of the iceberg. Are you prepared to add a fifty to one-hundred thousand to your IT budget just to have someone onsite? Oh, and don't forget to add hardware, licensing, and software costs to the final annual bill too.

Aren't outsourced IT solutions just as expensive if not more? We won't sugar coat it, outsourced IT services can be more expensive to get started especially if your company needs to purchase new items like firewalls, computers or software to meet service standards. However, in most cases, the overall costs are reduced and the only major drawback is that your IT manager isn't just the guy across

(Continued on page 2)

What's Inside

Lovely

"Love has nothing to do with what you are expecting to get — only with what you are expecting to give — which is everything.

~ Katharine Hepburn

"The greatest happiness in life is the conviction that we are loved; loved for ourselves, or rather, loved in spite of ourselves."

~ Victor Hugo

"To love is nothing. To be loved is something. But to love and be loved, that's everything."

~ T. Tolis

A Day For Love

Valentine's day is just around the corner. Did you know on February 14th an estimated 150 million cards will be exchanged and over $3 billion worth of merchandise from jewelry stores will be gifted? How did this lovely idea start?

Valentine's day roots. According to www.History.com, at the end of the 5th century, Pope Gelasius declared February 14th St. Valentine's Day however at this time, there was no correlation with love or gift giving. As a matter of fact, there are a variety of stories about how Valentine's day began with a focus on sacrifice rather than romance and love. Many cultures also associated this time of year with the beginning of spring and over time correlated it with the mating season for birds.

Valentine's day evolved. Over 1,000 years later, annual celebrations were taking hold. By the late 1700's a British publisher took off with the idea of sentimental verses for young lovers who couldn't put words to

(Continued on page 3)

eSudo™
PEOPLE • TECHNOLOGY • SOLUTIONS

www.eSudo.com
Service@eSudo.com

408-216-5800

Never Apologize For Having High Standards...

(Continued from page 1)

the hall. You'll need an open line of communication between your staff and your new outsourced IT department to keep things running smoothly.

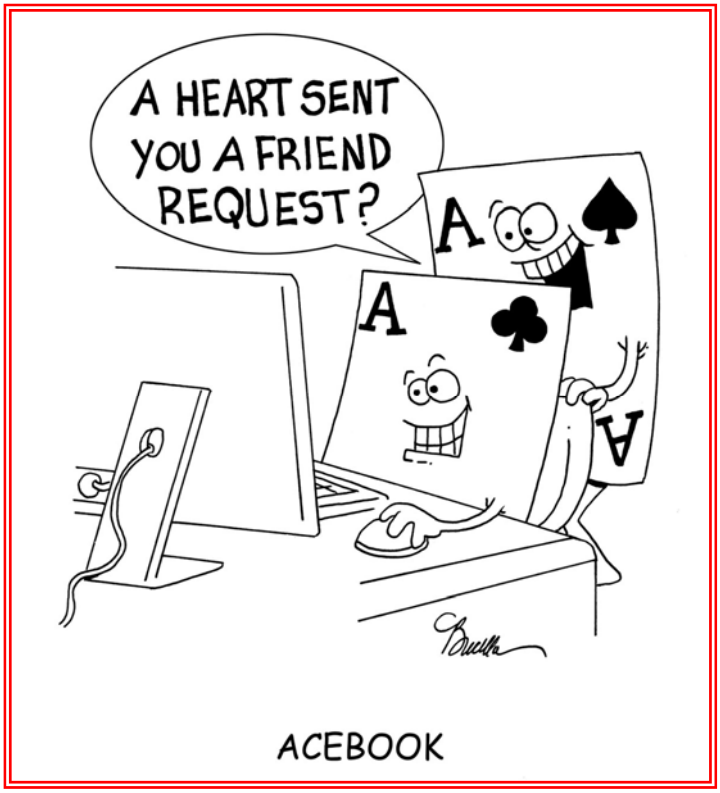
Outsourced IT benefits that can't be beat. Outsourcing your IT needs to a team of experts extends an invaluable pool of knowledge, understanding, and experience to your business. You no longer have to rely on just one person's comprehension of security, backups, and networking to keep your company operating. Outsourced IT companies generally keep technicians on staff with varying specialties to better serve their client base. In addition, their daily interactions with security issues, threats, and the ever changing landscape of business needs gives your organization the upper hand in resolving IT situations quickly. Here are a few more added benefits to outsourcing your IT management:

- ***A shoulder to cry on when you're down.*** While no one can guarantee an outage won't happen, you won't be alone with an outsourced IT department. In your time of need, an outsourced IT provider will have a team of resources ready to listen and help you get things back up and running smoothly. Instead of waiting hours for one IT guy to repair everything, you will experience less downtime with multiple resources at your fingertips.
- ***Predictable billing and costs.*** Transparency is big in any relationship. IT shouldn't be any different. When your company needs something new, you should be presented with the best options and upfront costs for everything from hardware to labor. In addition, outsourced IT solutions allow you to pay regular monthly fees you can budget for just like utility bills.
- ***They speak the language when you need help with vendors.*** An outsourced IT provider brings more relationships and experience with critical vendors to the table. They are able to work with other technical service departments and translate your needs into solutions.
- ***A deeper connection to new technology.*** Outsourced IT extends a deeper knowledge base for your company to tap into and resolve issues. Chances are if you're experiencing come crazy symptoms with your computer, they have seen it, researched it, fixed it and can do it for you too.

Don't settle for less, your company deserves the best. If you're tired of waiting on the IT guy, unsure if your company is truly safe, or just worried about your backups give us a call. We will conduct a FREE Network Security audit to get a full picture of your present standing. Then present our findings and offer solutions to bring your company up to your standards for operation.

FREE Network Security Audit

eSudo (408) 216-5800



Malware Defense

Malware has become a nasty little issue for businesses around the world. Here are a few great ways to combat this epidemic with ease.

Use antivirus software and keep it updated. Updates help keep your antivirus program abreast of the newest threats. Attackers are always coming up with new ways to do things. Antivirus updates give your systems a sort of inoculation for the current strands of viruses and malware.

Install patches as soon as they are available. Patches cover vulnerabilities in your current antivirus program. These critical changes will help close any weak points for current threats. Hacking is not an exact science so there are always new approaches. Patches are a way vendors can improve on the software they've already sold you and enhance the effectiveness of their program.

Audit your network regularly. Take time semiannually to conduct an audit of your entire network to ensure all your computers and devices are updated and patched. Antivirus programs are not the only types of software you should update. Specialty software and web browsers may also require special attention to stay safe.

A Day For Love...

(Continued from page 1)
their feelings. Printers began producing cards featuring the touching verses and small sketches dubbed "mechanical valentines."

Paper Valentine's took flight. By the 19th century, England opened one of the first factories to create fancy Valentine cards featuring real lace and ribbon. In 1835 a staggering 60,000 Valentine cards were sent out in Britain alone. In just five years, the cost for postage came down with the invention of the postage stamp, and over 400,000 valentines were mailed out.

The U.S. caught on. Just a few years later, the U.S. began to mass-produce Valentine's day cards in Worchester, MA. Today, the U.S. Greeting Card Association estimates a staggering 190 million valentines are sent each year.

Technology changes the pace for cards. While chocolates, stuffed bears, and jewelry will never lose momentum during this loving holiday, the Internet has slowed mailing trends. It's estimated that over 15 million e-valentines are now sent out each year.

Happy Valentine's day! No matter how you celebrate, we hope you have a very Happy Valentine's day.

5 Reasons Why Office 365 Is A Good Fit

Office 365 could be a great way for your business to boost productivity and streamline workflows. Take a look at these five benefits for businesses.

1. Say goodbye to your Exchange server. For year, businesses of all sizes have been maintaining e-mail servers hosted onsite. This brings a continue stream of maintenance with patches, updates and service packs. Office 365 (O365) takes your e-mail to the cloud. There is nothing physically onsite to maintain and it's so much easier to administer accounts.

2. Save money on management and licensing. Buying and maintaining an e-mail server are both costly ventures that may feel like a endless investment. With O365 you will really be keeping more money in your pocket with the minimal upfront migration costs and with the regular monthly licensing. In addition, your O365 solution is scalable on the fly. So, when you grow you can add people and resources as you see fit.

3. Productivity boost for your staff. Everyone will be happy using their favorite devices from apple to android and Windows, O365 preforms beautifully. In addition, this robust tool is available anytime your employees are on the Internet. O365 even has a 99.9% uptime guarantee. This allows staff to work from home or the office with no excuses. If that isn't enough, the applications and collaboration features will surely win your heart keeping everyone on the same page.

4. Security maintained and backed by Microsoft. There has been a huge buzz in the media over the past year about security in the cloud. Microsoft has made it their mission to create an e-mail service with the most robust offerings. Not only are O365 applications accessed through 128-bit SSL/TSL encryption, but they have built-in antivirus, malware protection, and anti-spam filtering features to keep your company information safe.

5. Applications to die for. The final icing on the cupcake is the web versions of the Microsoft suite of products. No more compatibility issues, everyone will be able view and make quick edits as needed.

Questions? Give us a call today for your O365 migration quote. We'll help dial you in with e-mail and applications.

How Long Does Pepper Spray Last?

We don't recommend pepper spraying intruders at the office, but thought this catchy headline might draw your eye to the often over looked issue of physical security.

Keep your technology physically safe. More often than you'd think, physical access to your network is the easiest way for an intruder to break in and get what they want. Just because people enter your office building doesn't mean they should automatically gain access to your network too.

Policies to protect your staff and data. When clients or new visitors enter your office make sure to make a policy requiring them to identify their business with your company. Require anyone coming through the door to register at a receptions desk, present their name, and the nature of their business. Restrict physical access to specific areas of your office like server rooms or closets that house your network devices. Only allow personnel that work on these systems to access and grant access to your network devices.

Surveillance and security doors. If your company houses sensitive information, make sure it's monitored and locked up tight when you leave. Surveillance services are a relatively inexpensive way to alert you of intruders on your off hours. Authenticating security doors are another good option to keep thieves at bay.

Hackable Employees

Business e-mail compromises have cost businesses billions according to recent figures from the FBI. So, what can you do?

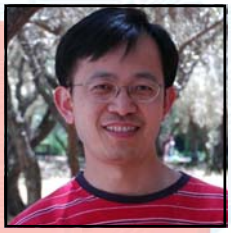
Set an example in your office with these basic guidelines for security:

1. Don't share log-in credentials with anyone. Sure your coworker may just need the computer for a minute, but they should be able to access what they need on their own.

2. Always use a strong password. According to SplashData, the most common passwords used in 2017 are still "123456","123456789", and "qwerty".

3. Don't install applications without consulting IT. If you're not an expert, don't pretend to be. Ask for a full review and assistance.

4. Use your company programs. Don't view, save or send your company data using personal accounts online.



"We make all of your computer problems go away without the cost of a full-time I.T. staff"

Ask us about our fixed price service agreements — Computer support at a flat monthly fee you can budget for!

~ Matthew Kaing, Director, eSudo Technology Solutions

Inquiring Minds...

Ransomware Threat Grows; Small Businesses At Risk.
A recent increase in hackers using ransomware to take their victims' data hostage means that organizations should aggressively move to back up data -- and teach employees how hackers work. According to PC Magazine, in a ransomware attack criminals deploy malicious code through e-mail or websites. The code then encrypts computer data so that the company can no longer access it. Criminals then demand payment for unlocking it. The technique has been very successful.

Ransomware attacks grew over 250% in 2017. Some extremely high profile cases have made big news, such as the U.K.'s National Health Service data that cost the organization $100,000 in ransom and an estimated $1 billion in damages. However, small businesses are just as likely, or more likely, to have a ransomware attack. In fact, according to PC magazine, some criminals exclusively target small businesses these days because they rarely have the IT resources in place to prevent such attacks. One attack on a small business can not only disrupt commerce, but likely poison relationships with larger companies.

Employees themselves are often responsible for letting the hackers in by downloading malicious files through e-mail. These e-mail attachments can masquerade as innocuous pdfs, but, in fact, they are executable programs. Train all your employees not to click on an attachment in e-mail if they do not recognize the sender. Even legitimate websites can often host malicious programs and one visit to such a website can mean ransomware infection. Malicious links are one way these programs take over.

Preparation is key. Update all your computers regularly. Updates might seem like such a pain, but they are critical since they often address security issues. Cybercriminals love old operating systems. They know how they work what to do to wiggle in your network. Experts now recommend deploying hosted endpoint security to manage computers, networks and mobile devices too. These inexpensive security programs provided by companies such as F-secure, Webroot Secure, and Avast are a great layer of defense.

Avoid ransomware with a sound backup solution. If all else fails, a full backup of your data is the best way to recover your environment. Sophisticated solutions exist that allow a company to maintain several layers of backups that can be rolled back to a time before hackers compromised the data just like nothing ever happened. Don't just dole out the money your attackers ask for, restore your computers from your backup and move on.

If you are attacked, should you pay? Experts say no — easy to say, but not easy to do if you are facing catastrophic data loss. Remember, these are criminals. There is no guarantee they will restore your systems in their entirety after you pay and every chance they really won't.

eSudo™
PEOPLE • TECHNOLOGY • SOLUTIONS

www.eSudo.com
Service@eSudo.com

408-216-5800

Ready For The Perfect Union?

Give us a call today for your FREE Network Security Audit and we will propose!

Do your computers seem to be working against you? Are you tired of wondering when your IT guy can fix things or will even show up? Feeling like you may be missing some of the benefits of a stronger commitment?

Give us a call today to claim your **FREE Network Security Audit (a $947 value).** We will bring our best tools, comb through every piece of your network, and even get down on one knee to *PROPOSE real solutions that will streamline and secure your business.*

eSudo (408) 216-5800