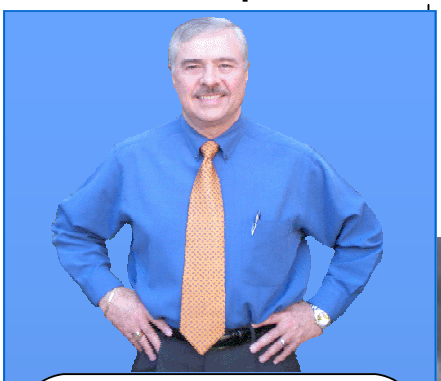
BUSINESS CONSULTANTS WITH A TECHNOLOGY FOCUS ISSUE 40 June 2012

TECH SAGE TECH TALK

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



"As a business owner, you don't have time to waste on technical and operational issues. That's where we *shine*! Call us and put an end to your IT problems finally and forever!"

John Hill,
TechSage Solutions

Inside This Issue . . .

Important Alert:
The FDIC "Misunderstanding" That Business Owners Need To Know About

Here's an important question about your finances with a shocking answer: If a cyber-criminal were to gain access to your company's bank account and steal all of the money in it, could you get it back? In many cases, the answer is *no*.

Many small business owners falsely believe they are protected by Federal Deposit Insurance Corporation (FDIC) laws and that the bank (or Federal government) would replace money stolen by a thief. Not so. The FDIC protects bank accounts against *bank failures*, not theft or embezzlement. So if your money is taken by a criminal—be it a completely anonymous person or even a "trusted" employee or vendor—the bank is not responsible for replacing the funds.

What's really concerning about this is the fact that online criminals are becoming more and more sophisticated in their attacks. Criminals are also targeting small businesses since they are the "low hanging fruit"—small businesses often don't have the security systems in place to prevent these attacks.

One Real Example That Cost One Business Close To $100,000

Sign Designs Inc. is an electric-sign maker in Modesto, California that had almost $100,000 stolen from their account by an unknown group in Eastern Europe. The first sign of trouble was a phone call from Bank of Stockton, their local community bank. It had just received a call from Chase Bank's anti-fraud team regarding a $9,670 electronic payment to a Chase customer in Michigan. The owner confirmed he had not set up or authorized that payment, and when he looked further, he discovered that 17 similar transactions had already been processed the previous day from his bank account.

Although the owner's bank notified all the banks that had received the funds, a large chunk of the money had already been withdrawn by "money mules" (people who launder money for online criminals, usually in Eastern Europe). The biggest problem for Sign Designs is that the Bank of Stockton isn't accepting responsibility for the losses, claiming its systems were never breached. Hackers had planted a malicious program on the computer of Sign Designs' controller and used that program to steal his online-banking credentials. The bank also points out that…(Continued on the next page.)

Shiny New Gadget Of The Month

The Levitron

Okay, I admit it; this month's gadget is not something that will increase productivity, make some daily task easier or put some extra money in your pocket. This month is just pure fun for the geek in all of us!

The Levitron is a small desktop gadget that gives you a mesmerizing way to display small objects. The device allows you to levitate and slowly rotate your collectibles, toys, small office supplies—pretty much anything weighing up to 12 ounces.

To float an object, you first levitate the included small magnetic disc over the base. Four LED lights on the base station help guide the alignment. Next, place your item of choice on top of the disc and instantly the object appears to be floating over the base. Cool! The Levitron automatically compensates for changes in weight by making up to 1,000 corrections per second to the electromagnets contained within the base. If you watch the online video at www.VAT19.com, you can see them pouring water into a glass being levitated without a single drop spilled.

For only $99, it's a great gift for the executive or geek in your life!

Sign Designs failed to implement proper security measures on its network that might have averted the losses.

How To Protect Yourself

1. Keep Your Network SECURE!

Hackers are focusing on small business computer networks because they are far easier to crack than a bank's network. Weak passwords, out-of-date anti-virus, security patches that aren't updated, and unmanaged (or non-existent) firewalls are the simple security checks that hackers are counting on you to neglect. Don't be an easy target! Of course, our **TechSage Network Shield** clients know that we're watching over their network and making sure the gateway to your data is safe.

2. Educate Your Staff

While up-to-date anti-virus will protect you against a LOT of threats, it's not 100% effective in protecting you. That's because the most common way criminals access financial accounts is through e-mail: phishing scams, malware attachments in documents or links, or brute-force password guessing/reset attacks. The first two are made possible through human error; employees or trusted account holders "giving" hackers access by accidentally downloading malware, typing passwords in an e-mail, clicking on a link in an e-mail they believe to be safe, and so on. That's why it's important that anyone accessing financials should know NOT to click on strange links, open questionable attachments or send any account information via e-mail.

3. Talk To Your Bank

Find out exactly what their policy is for fraud and what you can do to prevent problems. Ask your bank to set up "dual controls" on your account so that each transaction requires the approval of two people. You might also establish a daily limit on how much money can be transferred out of your account, and require that all transfers be prescheduled by phone or confirmed via phone call or text message. If possible, impose restrictions on adding new payees.

4. Watch Your Account Daily

You should also get into the habit of checking your accounts daily at the end of the day and notifying your bank immediately of any questionable withdrawals. Money is laundered quickly; the sooner you catch the mistakes, the better your chances are of recovering the funds.

5. Make Sure Your Accountant Has Proper Security Controls

If you have someone doing your payroll and/or accounting, make sure they are following the same strict security procedures of your own computer network. Sign Designs was hacked by accessing the controller's PC and using his credentials to make the transfers. Therefore, it's essential that any and every employee, vendor or person accessing your financial accounts is following even tighter security controls on their PCs or other devices used to log into your bank, credit card account, etc.

If you're not certain your computer network is secure from these attacks, call us for a FREE Network Security Audit and find out for sure if you're protected…or not: 210-582-5814 or e-mail: contact@techsagesolutions.com

5 Critical Facts Every Business Owner Must Know Before Moving To The Cloud

If you need to upgrade your current computer network and are considering cloud computing to save money and simplify IT, the insights in this report will arm you with the right information and questions to ask to avoid getting "sold" a solution that doesn't work for you. You'll discover:

- What cloud computing is and why it matters to small and medium sized businesses.
- The various types of cloud solutions you need to know about and how to determine which is right for you.
- What you should expect to save on IT costs initially and over time.
- 15 critical questions you must know the answer to about the cloud.
- The most important thing you need to know about security and where your data is hosted.
- Little known facts about moving to the cloud most IT consultants don't know or won't tell you that could end up costing you big.

Request this free report today at contact@techsagesolutions.com

How Small Businesses Should Budget For IT Expenses

A question that seems to come up a lot lately with clients, in some form or fashion, is "How should I properly budget for IT expenses?" While this is a great question, there are a lot of variables that determine the answer, so I can't provide a "one-size-fits-all," simple answer. However, below are some general guidelines that should help you figure this out:

1. **Hardware Refresh.** No one likes the cost of a network upgrade, but it IS necessary approximately once every 3 to 4 years. PCs and servers older than that tend to run slow, crash frequently and generally become more expensive to fix and support than to replace. Therefore, your budget should include an IT refresh of all equipment every 3 years to be on the safe side.

2. **Maintenance.** There is no "set it and forget it" when it comes to network maintenance. With cyber criminals becoming more sophisticated and aggressive, you MUST constantly monitor and update your network against cyber-attacks, malware, data loss, etc.

3. **Data Backup.** Another expense you must account for is backing up your data to an offsite location (often called "cloud backup"). Since all businesses generate MORE data year after year, the backup will grow. Start by assessing the growth of your data over the last couple of years to uncover a trend. From there, forecast those additional expenses going forward at the same rate (don't expect this to stay static year after year).

4. **Expansion.** Another factor for your IT budget is upgrading software, line of business applications, CRM systems and accounting packages that can no longer support your growing company. As your company grows, systems, processes and data become more complex requiring more sophisticated (and often more expensive) software and systems. Make sure you are looking ahead year upon year to see this coming and to properly budget for it. There's no "magic" formula for this because the timing and cost of your upgrade is unique to your company, situation and what you are trying to accomplish.

Many of our clients have opted for our **TechSage Shield Protection Plans**.as an easy way to budget for IT on a monthly basis.

If you have at least 10 workstations and one server, we offer a free onsite network audit. All you have to do is go to and www.techsagesolutions.com sign up on our opt in form.

Is Your Email Inbox Out of Control ?

Do you come in the morning and your email grew by leaps and bounds from people you don't know and don't care to know? **We have a solution!** This is the statistics of **my email address** by using a spam filter. Increase your productivity and protect your computer from viruses. *For more information, call 210-582-5814*

Year to date statistics:

- 303,390 messages delivered successfully.
- 981,140 messages blocked as spam.
- 123,614 messages sent outbound.
- 99 viruses blocked.

Confusing VoIP

Terminology Explained

Technical terminology with what seems like millions of acronyms is among the most difficult to understand. If you listen to IT people speak, it can often sound like nothing but a string of abbreviations with the odd technical sounding word thrown in for good measure. The same goes for VoIP, Voice over Internet Protocol.

Here are seven of the most commonly used VoIP terms and what they mean.

Internet Service Provider - ISP. The company that provides your company with Internet access. **Private Branch eXchange - PBX**. A system within a company that allows internal phones to connect to an outside line. This is also referred to as a switchboard in larger businesses. An IP PBX, Internet Protocol Private Branch Exchange, is the same thing, but it handles VoIP calls as well. **Analog.** The old system that transmits voice over telephone lines. Your normal landline telephone connection is most likely analog. In many countries, this is also called the Plain Old Telephone System - POTS for short**. Analog Telephone Adapter - ATA.** A piece of hardware that allows you to use a traditional telephone for VoIP calls. Digital. Any information, including sound, that's on a computer. VoIP is a form of digital communication, because it uses a digital system, the Internet, to transfer your voice. **Integrated Services Digital Network - ISDN.** A telephone network that allows digital signal e.g., VoIP, to be transmitted over traditional phone lines. **Softphone.** A VoIP application that is run strictly on your computer.

There's a lot of technical terminology out there, the majority of it in acronyms. Don't be afraid to ask us for more information. If you'd like to learn about ways you can use VoIP in your company, please contact us.

www.techsagesolutions.com/blog
Published with permission from TechAdvisory.org.

A Google Search Secret You Must Use Prior To Any Sales Call

There are more than 16 billion online information searches conducted via popular search engines each month, with more than 65% of them done using Google (and in the business world, it's my experience that Google has a 95% search market share). Yet even though Google is very easy to use, most people only access a small portion of what Google has to offer.

It's imperative that, prior to any sales call, you gather information about your prospect so you can customize your pitch. A standard sales call that gives the same pitch or voice-mail message to everyone just doesn't cut it (yet it's surprising how many people still "smile and dial").

I'm not talking about just visiting someone's web site. Rather, a good Google search can reveal detailed information that helps you better personalize your pitch and your examples to things that your prospect or client cares about. If you're a true sales pro who understands that information is power, here is a Google Search secret that can help you get the inside information on companies, industries, and people.

Search Secret: Type the name of a company in Google. If the company name is more than one word, put the name between quotation marks (e.g., "acme corporation"). On the Google results page you'll see a link that says "More Search Tools." Click on that link and you will see one of the options is labeled "Custom Range." Click on this and you'll see an option to enter a date range. Put in the range you are interested and you'll see the results for that company within that range. Imagine prior to a sales call that you conduct this sort of search. You click search on the current month and pull up press releases and articles. Even historical information is valuable, as it will show you how the company has progressed over time, past partnerships, and it even might reveal past or current vendors. Knowing the latest information helps you become educated about your prospect and will help you build instant rapport.

Guest Article Provided By: Sam Richter
Considered the "modern day Dale Carnegie," Sam Richter is the founder of the #1 rated Know More! sales training program and an best-selling author of the award winning "Take the Cold Out of Cold Calling" (http://www.takecold.com). Sam delivers his keynote presentations and sales workshops to organizations around the globe where he'll shock you with how to find information, and inspire you with how to use it to create relationship value. Learn more at http://www.samrichter.com

Why Encrypt Email?

With an **increase in regulatory pressures**, identity theft and highly publicized security breaches in the media, companies that do not encrypt emails containing sensitive information are at risk of regulatory fines, lawsuits, negative PR and a loss of company intellectual property.

Companies dependent on building a relationship of trust with their customers and business partners cannot afford to risk such potential damages to their brand image. **Email encryption** is, therefore, an important piece of the security puzzle; it protects your company, your customers and business partners. The question then becomes how to implement this critical business process. *Call 210-582-5814 for more information.*