



Michael Mellott, President

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

Volume V, Issue VI
June 2012

Inside This Issue...

- The FDIC “Misunderstanding” That Business Owners Need To Know AboutPage 1
- Shiny New Gadget: The LevitronPage 2
- Father Knows BestPage 3
- How Small Businesses Should Budget For IT ExpensesPage 3
- Free Report: Is Cloud Computing Right For You?Page 4
- A Google Search Secret You Must Use Prior To Any Sales CallPage 4



5090 Dorsey Hall Dr. Ellicott City, MD 21042
(410) 884-0225 | WWW.XPERTECHS.COM



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

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

Continued on Pg. 2



Get More Free Tips, Tools, and Services at our Website: WWW.XPERTECHS.COM

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!

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 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 XperCARE Proactive Managed IT Service 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 Assessment and find out for sure if you're protected...or not!

The Lighter Side... **Father Knows Best**

"If the new American father feels bewildered and even defeated, let him take comfort from the fact that whatever he does in any fathering situation has a fifty percent chance of being right." - Bill Cosby

"Never raise your hand to your kids. It leaves your groin unprotected." - Red Buttons

"When I was a kid, I said to my father one afternoon, 'Daddy, will you take me to the zoo?' He answered, 'If the zoo wants you, let them come and get you.'" - Jerry Lewis

"Spread the diaper in the position of the diamond with you at bat. Then fold second base down to home and set the baby on the pitcher's mound. Put first base and third together, bring up home plate and pin the three together. Of course, in case of rain, you gotta call the game and start all over again." - Jimmy Piersal, on how to diaper a baby, 1968.

Seize the Opportunity

Did you miss an XPERTECHS webinar that you were planning to attend? Or perhaps you just want to learn more about Cloud Computing, Backup & Disaster Recovery or Microsoft Exchange?

Now you can view our monthly webinars online for FREE by visiting:

www.xpertechs.com/view-webinars



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. A good general rule of thumb is \$400 per month for each server and \$80-\$90 per month per PC.
- 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 XperCARE Proactive Managed IT Service as an easy way to budget for IT. This program allows you to pay a fixed, monthly fee for all IT expenses including 24x7x365 monitoring, antivirus & malware protection, remote & onsite support, helpdesk, backup & disaster recovery, virtual CIO services, network administration and more!



www.XPERTECHS.com



FREE REPORT:

Discover What Most IT Consultants Don't Know Or Won't Tell You About Moving Your Company's Network To The Cloud

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

By: Michael L. Mellott

XPertechns
5000 Unity Hall Drive
Ellicott City, MD 21042
(410) 884-0225

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:

- 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.
- 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.

Download this free report today at www.XPERTECHS.com/cloud-report or give us a call at (410) 884-0225.

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: Google Timeline Search. 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.

One of the options is labeled "Timeline." Click on this and you'll see a graphic timeline by decade, with certain time periods blocked out. Click on one of the blocked out periods and you'll see articles featuring your search results from your chosen time period. Imagine prior to a sales call that you conduct this sort of search. You click on the current month and pull up press releases and articles. Even the 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.

Guest Article Provided By: Sam Richter

The best-selling author of the award winning "Take the Cold Out of Cold Calling"



Video Series

Watch the Top 6 Questions About the Cloud: ANSWERED!



www.XPERTECHS.com/top-cloud-questions



Get More Free Tips, Tools, and Services at our Website: WWW.XPERTECHS.COM