



“As an organizational leader, I know you don’t have time to waste on technical and operational issues. That’s where we make *IT EZ!* Call us and put an end to your IT problems finally and forever!”
- Diana Spurgus, BSSI

Volume IV, Issue VI
June 2011
Central Ohio

Inside This Issue...

How Would You Like To Have *This* Corporate Embarrassment On Your Record?.....Page 1

7 Simple Ways To Keep Your iPad SecurePage 2

Shiny New Gadget: MobileMe.....Page 2

Hackers Are Now Targeting MacsPage 3

Do The Words "Anthony Weiner" mean anything to you?.....Page 3

The World’s Funniest Real Ads.....Page 3

How Exposed Are You Online?.....Page 4

How To Get A List Of Ideal Prospects For FREE.....Page 4



Business Bits & Bytes



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

How Would You Like To Have *This* Corporate Embarrassment On Your Record?

Back in April, the largest known e-mail security breach took place when Epsilon, an online marketing corporation, had their *clients’* lists of e-mail addresses stolen by sophisticated cyber thieves.

Epsilon was in charge of maintaining the e-mail databases and campaigns of some of the largest corporations in the country, including 1-800 Flowers, Best Buy, Walgreens, JPMorgan Chase, Capital One, and more. In fact, there’s a good chance that you’ve received multiple “apology” e-mails from these vendors.

While some said the breach didn't cause a whole lot of damage, we disagree. Essentially, these cyber criminals now have the ability to invent highly sophisticated phishing attacks by creating e-mail offers that look like legitimate promotions coming from companies they (the people whose e-mail addresses were stolen) buy from and trust.

And though it’s already common for cyber thieves to impersonate credible organizations with what appears to be legitimate e-mail messages that seek to verify account information, this recent breach of security allows cyber thieves to be smarter and even more targeted with their scams.

Two Key Lessons

First, you need to be a lot more wary of e-mail promotions and communications that ask you to provide your credit card information or to validate your account information (username, password, social security number, etc.). No valid company will ever ask you to send important, confidential information in that manner.

Second, this breach serves as a warning to all businesses that they must have the MOST up-to-date security systems in place for their computer network, especially if you handle client data such as credit cards, bank accounts, social security numbers, passwords, client lists and more. Epsilon has responded to the security breach, apologizing to all of those affected, but the damage is done to their organization, not to mention their clients.

That’s why we urge all of our clients to enroll in our ITEZ Care Program. This service allows us to monitor your network’s anti-virus, firewall and security settings to make sure your network is fully protected against these damaging events.

Get More Free Tips, Tools and Services At Our Web Site: www.BSSI.biz.

Shiny New Gadget Of The Month:

mobileme

If you're a Mac device junkie and have a Mac at home, a PC at work, an iPhone in your pocket and an iPad in your car, check out MobileMe. This software allows you to store email, contacts and calendars — even shared ones — in the cloud and automatically keeps them in sync across all your devices.

Other cool features include the ability to remotely locate a lost iPhone or iPad. And if you're certain it fell into less-than-honest hands and you don't think you'll be getting it back any time soon, you can remotely wipe the device clean of all your data.

The Gallery enables you to create a beautifully displayed online gallery of your photos and share them with others in just a few clicks, allowing your friends and family to add photos of their own. And the iDisk app gives you the power to store and share large files online as well as access them remotely.

MobileMe costs only \$99 for a year's subscription and \$149 for a family pack that gives you one individual account with 20GB of storage and 4 family accounts with 5 GB of storage. Not sure if it's right for you? Then sign up for a free 60-day trial at:

www.apple.com/mobileme

7 Simple Ways To Keep Your iPad Secure



- **Don't leave it lying around**

Although this is common sense, you've probably violated this rule more than once. iPads are easy targets for thieves, so don't let it out of your sight when in a public place — and don't leave it in plain view in your car or you might end up with a broken window in addition to a stolen iPad.

- **Use a passcode**

Although it's not 100% hacker-proof, it will block unauthorized users from accessing your information.

- **Consider enabling automatic data erasing**

You can configure your iPad to erase your data after 10 failed passcode attempts. Clearly this is not a good solution for anyone who constantly forgets a password or those who have kids who might try to endlessly log in to use your iPad.

- **Sign up for MobileMe**

As mentioned opposite, this software will allow you to locate a lost iPad and, if it's not recoverable, you can remotely wipe the device of your private information. (This service will soon be replaced by Apple Inc with a service called iCloud.)

- **Limit its capabilities**

You can set your iPad to restrict certain functions such as access to Safari, YouTube, installing applications and explicit media content using a passcode. In the corporate world, an IT administrator could set these restrictions for company owned devices. At home, you can use this to restrict what your children can do with your iPad.

- **Install software updates**

As with all software, make sure you have the latest security updates and patches installed to protect against hackers and viruses.

- **Only connect to trusted WiFi networks**

Public WiFis are open territory for hackers and identity thieves. Whenever you connect, make sure it's a legitimate, secure connection.

The Lighter Side...

The World's Funniest Real Ads

Believe it or not, these ads actually found their way into newspapers all over the world:

Braille dictionary for sale. Must see to appreciate.

FOR SALE BY OWNER: Complete set of Encyclopedia Britannica. 45 volumes. Excellent condition. \$1,000.00 or best offer. No longer needed. Got married last weekend. Wife knows everything.

For sale, Hope Chest, brand new, half off, long story.

Christmas sale. Handmade gifts for the hard-to-find person.

Wanted, man to take care of cows that does not smoke or drink.

Three-year-old teacher needed for pre-school. Experience preferred.

Tired of working for only \$9.75 per hour? We offer profit sharing and flexible hours. Starting pay: \$7 -- \$9 per hour.

Our sofa seats the whole mob and it's made of 100% Italian leather.

Nordic Track \$300 hardly used, call Chubby.

Joining nudist colony! Must sell washer and dryer \$300.

Free puppies: ½ cocker spaniel, ½ sneaky neighbor's dog.

Snow Blower for sale...only used on snowy days.

Bill's Septic Cleaning: "We Haul American-Made Products."

Cows, calves never bred...also 1 gay bull for sale.

Nice Parachute – Never opened. Used once.

Hummels – Largest selection ever. "If it's in stock, then we have it!"

Tickle-Me-Elmo, still in box, comes with its own 1988 Ford Mustang, 5L, Auto, Excellent condition \$6800.

Hackers Are Now Targeting Macs

Until recently, Macintosh computer users have long enjoyed relative freedom from hacker attacks; however, researchers at Symantec Corporation say online criminals are now setting their sights on Mac users.



Online porn hunters are the latest target. Visitors to certain web sites are led to believe they can download a free video player when in fact they are installing malicious code onto their Macs.

Once the users authorize the transaction, the hackers can redirect the users future browsing to fraudulent web sites and possibly steal the user's information or passwords. Sometimes they simply send ads for other pornographic web sites. This results in thousands of dollars in income for the criminals.

While you may think that Macs are essentially more secure than PCs because they are built better, security experts would argue differently. They believe that the Mac is actually no more secure than a PC. In fact, they note that the relatively low number of viruses, exploits and other cyber attacks directed at Mac users is due to Apple's relatively small share of the computer market.

"I don't think that the Mac OS is more secure than Windows -- I think it is safer than Windows because there are less people trying to attack it. There is a big difference," Natalie Lambert, a senior analyst at Forrester Research recently shared with MacNewsWorld.

With that said, the fact remains that for every single attack on a Mac, there are at least 100 attacks on Windows-based systems.

So what should you do if you own a Mac? Use the same safe online surfing practices as PC users, keep your anti-virus software up-to-date, never open strange e-mails from unknown sources, and only verify user names and passwords by phone with your bank or other financial institutions.

Do the words "Anthony Weiner" mean anything?

If you are an organizational leader that is concerned about employees wasting time online using non-work-related web sites like Facebook or Twitter – OR WORSE, using company resources to access pornography, gambling sites, hate groups or more – then read on.

While it's not uncommon for employees to waste a bit of work time on relatively harmless activities, such as shopping or visiting a favorite sports site, times have changed; employers are learning the hard way that employee use or abuse of a company's Internet system can lead to significant liability and time wasted if not monitored.

For example, one business owner (who will remain nameless) shared that they received a panicked phone call from the office while traveling. The police had shown up and arrested one of their staff for soliciting a minor online. Since he was doing this during work hours from the office, that's where the police showed up to arrest him – clearly a PR nightmare. And stories like this are happening *EVERYWHERE*.

Then there's the wasted time. Social media sites like Twitter and Facebook are addictive. If your employees are constantly "plugged in" to those sites, they won't be nearly as productive at work as they should be.

Protecting your company requires two simple steps at a minimum. The first is to have a written company policy that details what employees can and can't do with company resources or during company hours. Next, you'll want to have a content filtering system in place that will enforce your policy by automatically "policing" your company e-mail and Internet usage, blocking sites and content you don't want your employees to access without hindering their ability to work online.

Get More Free Tips, Tools and Services At Our Web Site: www.BSSI.biz.

How To Get A List Of Ideal Prospects For FREE

With LinkedIn.com, you can build lists of people who match your ideal prospect – and even get introductions – all for the cost of a few clicks.

For example, if you want to reach the HR managers at companies in a certain geographic area, simply go to LinkedIn and follow these steps:

1. Set up an account and connect with your clients, friends and vendors. The more “connected” you are online, the easier it will be to get introduced to new prospects.
2. Click on the “Advanced Search” link located near the main search form.
3. Customize your search by entering in the industries, title, location and keywords that would be related to the prospect you are looking to find. For example, you could enter “HR” or “Human Resources Manager” in the title search, and then narrow your results down using the “Postal Code” lookup and “Within X Miles” setting.
4. Unless you want a particular industry, leave that area unchecked.
5. When the list comes up, do a sort by “Relationship” so that those with the closest relationship to you or your contacts are ranked towards the top. If you find someone you want to connect with, look for people YOU know who can introduce you.

How Exposed Are You Online?

Is privacy in America dead? With all the camera phones, online tracking software and social media sites, you can pretty much bet on it. But that doesn't mean you can't protect yourself.

For starters, go to Google Maps and search on your name to see if they have a picture of your home mapped out. If so, you can request to be removed. Next, set up a Google alert for your name (and company name if you're a business owner). Google will e-mail you any time something is posted about you with a link so you can keep an eye on reviews, photos, etc. Next, go to www.Spokeo.com and search on yourself – you might be shocked at how much information is posted about you, your home, your income and personal life. You can request to be removed from this site by going to www.spokeo.com/privacy.

Who Else Wants To Win A \$25 Gift Card?

Take our monthly “Trivia Challenge” and you could win too!

The Grand Prize Winner of last month's Trivia Challenge Quiz is Beth Borgan-Cooper of the Mondri Akrosil Group. She was the first person to correctly answer my quiz question from last month:

What was put on sale for the first time in May of 1886?

- a) United States Savings Bonds b) Coca-Cola c) Mother's Day Cards

The correct answer is b) Coca-Cola. Congratulations, Beth Borgan-Cooper you've won a \$25 Gift Card to Starbuck's!

Now, here's this month's trivia question. The winner will receive a gift card to Starbuck's.

What inventor averaged one patent for every three weeks of his life?

- a) Thomas Edison b) Benjamin Franklin c) Alexander Graham Bell

Call us right now with your answer! 740-681-9753

Client Spotlight: Central Ohio Plastic Surgery, Inc.

(www.centralohioplasticsurgery.com)

Dr. Jason B. Lichten and his team offer a full range of plastic, reconstructive, and cosmetic surgeries including breast and body contouring, facial rejuvenation, and breast reconstruction throughout central Ohio. Dr. Lichten maintains that patient satisfaction begins with a skilled surgical technique, but he is also dedicated to providing personalized patient care throughout each phase of treatment and recovery.

BSSI has the privilege of managing the computer environment at Central Ohio Plastic Surgery and has for over 3 years now. We are very proud to be a part of Dr. Lichten's team. If you need a nip or a tuck, make sure to check them out! :)

Get More Free Tips, Tools and Services At Our Web Site: www.BSSI.biz.