Bits & Bytes

Insider Tips On How To Use Technology To Make Your Business Run Faster, Easier, And More Profitably

TAG Technical Action Group Inc
we're I.T.

"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 and put an end to your IT problems forever."

Joe Stoll, President
Technical Action Group (TAG)
JStoll@TechnicalActionGroup.com

Inside this issue:

Volume III, Issue VI **June, 2011**

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 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 "apology" e-mails from one or two 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 To Apply In Your Business—No Matter What Size You Are

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 insurance 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 insurance 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 one of our managed computer support service plans. With a managed service plan, we monitor your network's anti-virus, firewall and security settings to make sure your network is fully protected against these damaging events.

Shiny New Gadget of the Month:

Camtasia Studio

With online video becoming a hot trend and an effective way of engaging visitors with your web site, you might be wondering how you can quickly and inexpensively create your own web videos. Or maybe you want to create a video tutorial to train employees how to perform a certain process or task without having to repeat the training over and over again. Or perhaps you want to create welcome videos and tutorials for new customers. All these are possible using Camtasia Studio.

Since the software comes in versions for Windows and Mac users, anyone can create professional-looking videos. The cost is $300; compared to hiring someone to do this for you, it's a steal. There is a bit of a learning curve, but TechSmith (the makers of Camtasia Studio) offer several web videos to assist you. TechSmith also offers a 30-day trial so you can see if you like it before you commit to buying.

E-Mail / Spam Filtering Explained Simply And Why *Every* Computer In Your Business MUST Be Protected With It

"E-mail filtering" aka "Spam filtering" – two terms you have heard tossed about, but do you really know what they mean and why they are a vital component in protecting your business against data theft, crippling viruses, as well as protecting your company's reputation?

What Does Filtering Do Exactly?

Filtering is available in varying degrees of sophistication depending on what solution is purchased; however all of the solutions do the following:

Every E-mail Gets a "Score"

99% of all e-mails sent globally are spam. The artificial intelligence in a filtering solution looks at three key elements within an e-mail and attempts, through a "scoring" process, to determine whether the e-mail is spam or legitimate by looking at the 3 key elements in every e-mail:

Element #1 – The Sender
a) Is the domain of the sender trustworthy (i.e does it have a known history of sending spam?).

b) Is the server sending the message authorized to send it on behalf of the sender's domain. (i.e. Is the message coming from JohnSmith@xyz.com coming from a server authorized to send mail on behalf of xyz.com)?

Element #2 – Subject Line
Does the subject line contain words or keyword groupings commonly found in spam? Common offenders being "free", "Viagara", sexual wording, etc.

Element #3 – E-mail Message
a) Message Text. The body of the message is reviewed for word strings that are common in well known spam attacks such as "donate to", "free", etc. E-mail hoax writers have a tendency to use emotive, "over-the-top" style of writing peppered with words and phrases such as "urgent", "danger", "worse virus ever", and so on.

b) ALL CAPS: Another indication of a hoax is writing in ALL CAPITAL LETTERS for added emphasis.

c) Invisible Commands. Hidden commands such as directions to open a web link within the background and installing a malicious application on your computer that would do things like steal your passwords or your Outlook e-mail addresses which could be used to spam and infect everyone in your address book through e-mails sent under your name – without you knowing it.

d) Attachments. Attachments to the e-mails are reviewed to determine the likelihood that it is safe for the recipient to open.

Taking Protection One Step Further

Cloud based e-mail / spam filtering services such as MxLogic / McAfee take protection one step further. They have a database they share with their competitors that looks at real-time, up to the second e-mail patterns throughout the world. These services have the ability to detect hundreds of thousands of e-mails that are similar, increasing the likelihood that these are spam. In turn, these e-mails are detected by the filter and prevented from getting delivered to your inbox.

How Is E-Mail / Spam Filtering Delivered?

In one of two ways:

a) Through software that is installed on your server or your firewall; or
b) Provided via a service in the cloud. Those of our clients who buy spam filtering and web defense services from us are purchasing in the cloud.

Why It's *Essential* That Every One Of Your Computers Have E-Mail / Spam Filtering

Inbound Filtering

a) The filter looks at all e-mails coming into your domain from the outside. This helps you and your staff stay more productive without having to deal with sifting through and deleting spam messages throughout each day.

b) Reduces the likelihood of you / your staff missing / deleting an important e-mail while deleting spam.

c) Reduces the risk of inviting a virus or malicious attack on your internal network by unwittingly opening a spam e-mail containing a program that would introduce a virus into your network.

Outbound Filtering

Even with the best spam filtering solution in place, nothing is 100% with cybercriminals working to be one step ahead. Though with a filter in place the chance of an infection is reduced by 99%, in the event your network does become infected, a spam attack could be launched to the outside world from your network without you knowing it. In the event this happens your domain will be blacklisted by organizations on the internet, and stop delivery of ALL of your e-mails to companies that subscribe to that blacklist. This means your clients and prospects could stop getting your e-mails. To resolve requires costly effort for technical support and could take up to 30 days to clear your domain from the blacklists.

Having outbound filtering in place is vital to prevent the above from happening, and to protect the integrity of your domain. When you send a message to a client or prospect, the filter makes sure that the messages are not infected leaving your network. It also ensures that your domain's reputation on the internet is trustworthy which decreases the likelihood of your e-mails being categorized as spam by the recipient, and not delivered via their spam filter.

In the event of a hijack or virus in your network, outbound filtering will suspend spam mail from leaving your network until the spam issue can be handled by your technical support team. Resolution of this issue is a lot quicker than removing you from a blacklist.

Workhorse Filtering. No Horsepower Needed From Your Network

Cloud based services offer the enhanced benefit of filtering being done outside of your network which reduces the load on your internet connection, server, and computers. Also, as cloud based services leverage collaboration and have increased sophistication in spam identification they are able to learn spam patters at an accelerated rate, reducing the likelihood that any spam will enter your network.

State of the Art Protection Costs Less Than You'd Think

A full solution for inbound and outbound filtering costs only between $3 and $5 per month per staff member per month.

DO YOU KNOW HOW WELL YOUR BUSINESS IS PROTECTED?
If not, call us for a free "Stop the Spam!" consultation.

Tools to Drive Productivity Using Your Smartphone

New apps are constantly emergency for iPhone, BlackBerry, Palm webOS, Windows Mobile and Android that help boost productivity in business. I've listed 2 of them here. Check back next month for more!

App: Evernote

Company: Evernote Corp.

Why It Rocks:
Evernote captures your brilliant ideas and entrepreneurial insights the moment they strike, documenting them as text, photos or audio recordings and auto-synchronizing all content to your devices (desktop computer, phone, iPad). Features include geo-location tagging and multiple language support

Available On:
Android, Blackberry, iPhone, Windows Mobile, Palm webOS

Price: Free

App: Bento

Company: FileMaker

Why It Rocks:
Bento organizes the details of your life, no matter how large or how small. Its 25 ready-to-use, customizable database templates manage contacts, schedules, inventory and other professional and personal information.

Features:
iTunes-style searching and sorting, integration with other apps

Available On: iPhone

Price: $4.99

8 Tips To Keep You (and Your Kids) Safe on Social Networking Sites

1. Keep your firewall's security and anti-virus software up-to-date.

2. Never log in from public hotspots. Social networking sites generally do not have secure logins available (that's the https with the lock icon in the search bar). That means your username and password can be swiped at any time.

3. Use strong passwords that contain a mix of upper- and lowercase letters, symbols and numbers.

4. If you wouldn't do it or say it on a public street, don't post it online.

5. Be wary of all links and files. Hackers post links in comments to trick you into downloading an "update," "security patch" or "game."

6. Keep an eye on what your friends post about you. Many people have been fired or lost an important client because of online pictures and content.

7. Be careful who you 'friend.' It feels great to have hundreds of friends, but the reality is, you really know only a fraction of them.

8. Be wary of all add-ons. Many of the games and plug-ins are written by third-party companies, not the social network itself.

What Are QR Codes And How Can You Profit From Them In Your Business?

The last time you were flipping through your favorite magazine, or some time when walking down the street, you may have noticed a small, digital-looking image on an advertisement. What is it? A "Quick Response" code or QR code for short.

A QR code is a specific matrix barcode (or two-dimensional code), readable by dedicated QR barcode readers and camera phones. The code consists of black modules arranged in a square pattern on a white background. The information encoded can be text, URL or other data.

This concept was initially created by Toyota for tracking parts in vehicle manufacturing; however, QR codes have been largely adopted by advertisers that want to target mobile phone users (known as mobile tagging). QR codes can be used to display text to the user, to add a vCard contact to the user's device, to open a URL or to compose an e-mail or text message. Users can also generate and print their own QR codes for others to scan and use by visiting one of several free QR code–generating sites.

So how could you use this? Some companies are smartly using this technology to drive sales by allowing people flipping through a magazine or waiting at a bus stop to get more information on a product, connecting the dots to get people to buy much faster than these types of media originally offered. Others are putting QR codes on permanent coupons or on their business

How To Get Your Sales & Marketing E-Mails Delivered

Since e-mails are cheap and easy and deliver instant results, there's a good chance you are (or plan on) using e-mail broadcasts to communicate with your clients and prospects. But with so much spam, how can you make sure your e-mails stay OUT of the spam filter and get safely delivered to your recipients' inbox? Here are a few tips:

1. Send e-mails only to people who have opted in or requested to receive e-mails from you. Otherwise, you'll risk being flagged as a spammer and will get your account or server blocked.

2. Use a legitimate e-mail broadcasting service. This goes along with the above recommendation. These services have entire teams of people working to make sure the e-mail broadcasts sent from their servers are delivered – a huge task that is no simple thing in the online world. That's why it's better to use these services versus broadcasting from your own server. It takes only one person to flag you as a spammer to get your server shut down.

3. Send text e-mails instead of HTML. A study by AWeber.com shows that plain text messages are undeliverable 1.15% of the time and HTML-only messages were undeliverable 2.3%. If sending HTML, always send a plain text alternative message, also called text/HTML multi-part mime format.