



“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 finally and forever!”

- Rick Johnston

Information Management Systems

April 2010
 Fargo, ND

Inside This Issue...

SPAM and Why You Should Care.....Page 1

The Droid: Good, Bad & Bottom LinePage 2

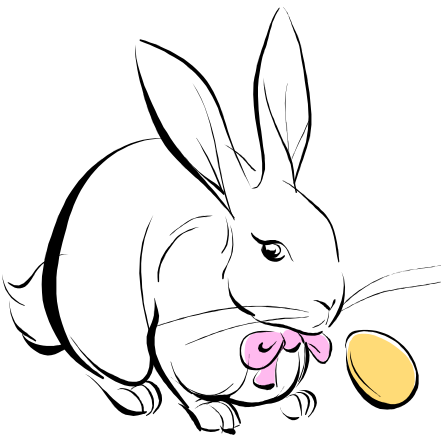
Proof That The Details Really Do Matter.....Page 3

Security Alert.....Page 3

Protect Your Kids From Online Predators.....Page 4

Spring Clean Your ComputerPage 4

it’s simple, it’s service



Technology Times

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

SPAM and Why You Should Care

If you ask ten people to define spam, you will get ten different answers and one request; how can I stop it?

The short answer is this: spam is the abuse of electronic messaging to send unsolicited bulk-mail messages indiscriminately. E-mail spam is the most widely recognized form of spam. There are similar abuses in instant messaging, newsgroups, web search, blogs, mobile phone texting, junk faxes and social networking spam.

Most people are concerned about e-mail spam.

If you are old enough, you may remember SPAM as a canned meat product, produced in the Unites States by Hormel. What you may not know is that post-war England survived in a large part due to the use of this type of imported meat product, while it rebuilt its agricultural base. The most prevalent was a “corned beef” product from Argentina. It was widely used and widely hated.

Enter “Monty Python’s Flying Circus” and the famous café sketch of 1970, where the only item on the menu in many disguises was SPAM. Off stage a chorus is singing the words SPAM over and over, in effect “spamming” the dialogue. It wasn’t until the 80’s that BBS users would type the word “spam” over and over to push other users’ text off the screen. After that it took several years until it became a part of our language.

Why spam? The answer is that it can be commercially viable. If a spammer can convert a spam to a sale, then it becomes economically worthwhile. It can also be a way for malware to enter your system.

In February 2010, Microsoft’s Digital Crimes Unit shut down the Waledac Botnet. A Botnet is a series of PCs that have been hijacked and used in a remote control fashion to aid in the distribution of spam. It was estimated the Waledac Botnet had infected hundreds of thousands of computers around the world.

Between December 3 and 21, approximately 651 million spam e-mails went to Hotmail accounts alone from the Waledac Botnet. The capacity of the Botnet was in excess of 1.5 billion e-mails a day. So if you are pushing a pharmacy product and you convert 1 in 12 million, you can make money sending spam. In 2009 Cisco systems reported the origins of spam by country (in trillions per year):

1. **Brazil: 7,700,000,000**
2. **USA: 6,600,000,000**
3. **India: 3,600,000,000**
4. **South Korea: 3,100,000,000**
5. **Turkey: 2,600,000,000**
6. **Vietnam: 2,500,000,000**

Continued on page 2

Want to Lock-in your IT Costs for the Next *THREE* Years? Sign up for IMS Total Care Services *TODAY!*

Shiny New Gadget of the Month



Motorola Droid Phone

Here's a quick run-down of the good, the bad, and the bottom line on this new phone.

The good: Most users of the new Motorola Droid Phone really like its display screen; fans cite the phone's large, crisp picture and vivid graphics.

The phone also has a pretty fast Web browser, (reportedly much faster than that of the Blackberry), a Google Maps Navigation app, and better messaging and contact management. With Verizon as its carrier, the Droid has very reliable service.

The bad: The QWERTY keyboard seems to be a bit awkward, especially if you don't exactly have dainty hands. Some people dislike its weight, too, since it weighs a full ounce more than its closest competitor.

Also, because the dialpad control is restricted to the home screen, driving and making a phone call is rather difficult.

Not surprisingly, music and video capabilities are not as strong as the iPod's. In addition, there's no Bluetooth voice dialing.

The bottom line: Overall, the Droid is a good smart phone with good service, useful Google maps, and a killer display screen. It's a great touch-screen upgrade from the Blackberry and gives its competition a run for the money.

- 7. **China: 2,400,000,000**
- 8. **Poland: 2,400,000,000**
- 9. **Russia: 2,300,000,000**
- 10. **Argentina: 1,500,000,000**

On the receiving end, handling SPAM can be expensive. In a study done in California for the year 2007, it was found that spam cost US businesses \$13 Billion. That was for lost productivity, additional equipment, software and manpower to combat the problem. The direct cost is in the consumption of computer and network resources and the cost in human time and attention. The indirect costs are more difficult to measure; they are mostly borne by the victims and the crime that accompanies it: financial theft, identity theft, data and intellectual property, virus and malware infection, child pornography, fraud and deceptive marketing.

As spammers have gotten more sophisticated, so have the anti-spam devices.

Even with the Waledac Botnet out of business, there are still many out there. Most recently, in February 2010, Symantec Labs reported that 80% of all spam is sent out by 10 Botnets that average 135 billion messages a day and have 5 million computers in their Botnets. What can you do to avoid spam?

The answer is its very unlikely you can avoid it, but there are several things you can do to lessen its impact on your life. For example:

- Make sure your computer is up to date with the latest service packs and security updates; don't avoid updating because it is inconvenient
- Keep your anti-virus program up to date
- At home you can install Microsoft Security Essentials from www.microsoft.com; it is an excellent additional tool to catch malware that comes in through e-mail spam or web spam
- Be careful about opening e-mails from people you don't know
- Be careful about opening e-mail from what appears to be legitimate companies, like Microsoft, or EBay, Amazon or an address that simply says support, if you are not expecting an e-mail and you have no previous relationship ... that's a good clue it's spam

At the corporate level, there are good cost-effective means of stopping spam, especially if you host your own e-mail. We recommend GFI's MailDefense Suite., <http://www.gfi.com/maildefense>. If you are having a "spam" issue, give us a call and talk about how we can help you be more productive and keep more of your dollar in the bottom line.

Easter Humor

- Why did a fellow rabbit say that the Easter Bunny was self-centered?
Because he is egocentric
- What do you call ten rabbits marching backwards?
A receding hareline
- Why shouldn't you tell an Easter egg a good joke?
It might Crack up!



The Lighter Side... Slow Down

A state police officer sees a car pattering along at 22 MPH on the highway. He turns on his lights and pulls the driver over.

Approaching the car, he notices that there are five old ladies - two in the front seat and three in the back - wide eyed and white as ghosts. The driver, obviously confused, says to him, "Officer, I don't understand. I was doing exactly the speed limit! What seems to be the problem?"

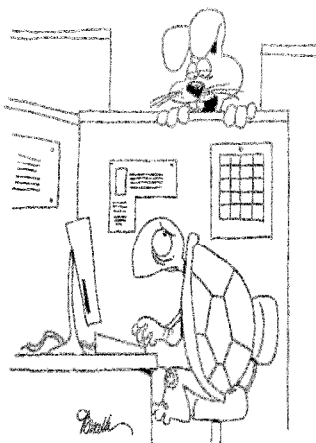
"Ma'am," the officer replies, "You weren't speeding, but you should know that driving slower than the speed limit can also be a danger to other drivers."

"Slower than the speed limit? No sir, I was doing the speed limit exactly....22MPH!" the old woman says a bit proudly.

The officer, trying to contain a chuckle, explains to her that "22" was the route number, not the speed limit. A bit embarrassed, the woman grinned and thanked the officer for pointing out her error.

"But before I let you go, Ma'am, I have to ask...Is everyone in this car ok? You all look a bit shaken."

"Oh, they'll be alright in a minute, officer. We just got off Route 119."



"You didn't hear it from me, but the other hares in the office think you're getting your work done too quickly."

Security Alert: Hackers And Cyber Criminals Are Now Concentrating Their Attacks On Small Business

At the recent 2009 Visa Security Summit a new trend was revealed: hackers and cyber criminals are now turning their efforts to small "mom and pop" businesses instead of large enterprise corporations. Why? Because small business networks offer a much easier "lock" to pick, unlike large enterprises who invest far more man power and money into high security for their network.

"As the security becomes better at large companies, the small business begins to look more and more enticing to computer criminals," said Charles Matthews, President of the International Council for Small Business, "It's the path of least resistance."

Think your network is secure? Take a look at these surprising statistics:

- One-fifth of small businesses don't have up-to-date antivirus software installed.
- Sixty percent don't encrypt their wireless links.
- Two-thirds of small businesses don't have a security plan in place.
- Eighty-five percent of the fraud occurs in small and medium-sized businesses.

Why is security so poor for small business? Primarily for two reasons:

Lack of knowledge. Most small businesses believe that nothing could ever happen to them, and therefore don't take the necessary precautions to secure their network, monitor their systems, and train their staff.

They are also unaware on HOW to get this done. The second reason is that they are **being frugal in the wrong places.** Some simply refuse to spend money on securing their network. That's akin to having a beautiful home full of expensive furnishings and valuables, but refusing to buy a good lock for the door because it "costs too much."

So what should you do at a minimum to protect your company? Here are 7 fundamentals:

1. Educate your users on security basics such as using strong passwords, shutting down PCs at night, and not downloading "cute" screen savers and illegal music. Some companies make computer security rules part of their standard HR policies and make each employee sign that they understand the rules.
2. Install a web filtering software to police users and prevent accidental (or intentional) slip-ups on the above-mentioned usage policies.
3. Install a good virus protection system on all computers on your network and maintain it (for our IMS Total Care Services clients, we do that for you.)
4. Install a firewall and check the logs periodically (again, we manage that for our IMSTCS clients).
5. Remove all unessential services and applications installed on your servers. After e-mail, this is probably the biggest security vulnerability. If a hacker gets in, this will reduce their ability to use a forgotten service or application to exploit your network.
6. Keep all your servers updated with all the latest security patches.
7. Never keep any of the manufacturer's default settings on any of the appliances or software you install. Hackers know what these settings are and will use them to gain easy access to your network. This item nails more systems administrators than care to admit it.

For those of you on our IMSTCS, you can rest assured we are taking good care of issues 3 through 7; however, if you would like us to conduct a training class and develop an AUP (acceptable use policy) for your staff and then install a content filtering software to help enforce the policies, give us a call (701) 364-2718!

This training and software is a small price to pay for the peace of mind you'll have over your network's security. And since better than 80% of all security breaches happen because of an end-user mistake, you'll also be taking a big step towards protecting your assets.

Want to Lock-in your IT Costs for the Next **THREE** Years? Sign up for IMS Total Care Services **TODAY!**

Protect Your Kids Online For Under \$30

Nearly 90% of 8-16 year olds have seen inappropriate images online. Most of them stumble upon it as a result of conducting research for their homework. With frightening numbers of pornography, child predators, and other harmful online risks, protecting your children's online activity is a MUST.

With the following 4 features, Net Nanny Parental Controls software by ContentWatch (\$29 at www.hermanstreet.com) helps you do just that.

1. Blocks "Mature"

Games. The software scans the online game for its ESRB ratings (like movie ratings, but for computer games). If the game isn't kid-friendly, the computer blocks it.

2. Filters Facebook. Net Nanny can provide parents with a report on who their kids' "friends" are, what pictures and videos they are looking at, and their Facebook Instant Message conversations.

3. Prevents Proxy Sites From Working. Content filters work by making a "blacklist" of sites that it won't allow. If you tried to type in a blacklisted website address, you wouldn't get very far. But there's a sneaky way around this called a "Proxy Server."

Proxy Server web addresses are usually content neutral, so users can go there without flagging the blacklist system. Once in, your child can navigate to their original blacklisted site. Net Nanny prevents this by blocking both proxy server entries and the inappropriate website itself.

4. Keeps Parents Informed. If your child is trying to gain access to something you have blocked, Net Nanny sends you an e-mail alert.

Proper Disposal of All Things Electronic

As much as you'd like to, it's really not safe to just throw away old computers, network equipment, or any electronics like TV's, cell phones, and DVD players. If disposed of improperly, these items contain toxic chemicals, like arsenic and mercury that can harm the environment. How do you dispose of these things properly? Check out these two tips:

1. Reuse. This is the most environmentally friendly of the disposal methods. Find another use for your old equipment. For example, you might be able to use an old PC as a firewall, run a basic program like an older voicemail system, or make it a toy for your kids or grandkids to beat up.

2. E-cycle. Some major retailers, like Best Buy and Dell, offer recycling programs for computers and home electronics. If it's your cell phone you are looking to get rid of, you can find a local program by going to www.earth911.org or www.mygreenelectronics.org

Spring Clean Your Computer For Maximum Performance

With Spring in the air, now is a good time to do an annual clean up of the computers, servers and electronic equipment in your office, both inside and out.

Failure to thoroughly clean your computer at least once or twice a year will result in decreased performance and possibly even system failures.

Here's why:

- Dust clogs the computer's cooling system causing it to heat up, damaging sensitive electronic equipment. Dust can also cause fan noise and (believe it or not) slow performance!
- Crumbs and dirt in your keyboard can cause keys to stick and make crunchy sounds when typing. Plus, it's just gross and unhealthy; Do you know there are more germs on your computer keyboard than the average public toilet?
- Dust, fingerprints and dirt build-up will make your computer monitor dim and fuzzy.

But the physical "dirt" is only the beginning...

- ◆ Delete temporary files and unused programs taking up space and slowing things down.
- Defrag your hard drive (Start > All Programs > Accessories > System Tools > Disk Defragmenter).
- Get rid of clutter on your desktop by removing shortcuts and files you don't need.
- Make sure you have the latest security patches and updates installed and configured properly.
- Check your backups and conduct an emergency "restore" of the data. Remember, the best time to check your backups is when you DON'T desperately need to recover your data!

Want Us To Spring Clean Your Network? Call Us For Any Service Between Now And April 30th To Receive...

- 10% off any service, repair or upgrade
- A FREE Spring Network Tune-Up
- A FREE Computer Cleaning Kit to keep your keyboards, monitors and LCD screens squeaky clean

Fair Warning! This Offer Ends Friday, April 30th!

Call: 701-364-2718, send an email to info@imsnetworking.com