



The War Against SPAM – Part 1

Measures and Countermeasures

© René Mente – September 9, 2005

Background

Since the dawn of the Internet (AKA: *The Epoch*, circa 1970), sending text messages (E-Mail) between computer users has proven to be a very effective means of communications, and has grown exponentially in popularity. Today even cell phone users are capable of communicating via text messaging. While this is a most convenient way to communicate short messages amongst computer users and cell phone users, it has also become an effective communications medium for those with more nefarious and sinister motives, most notably, SPAMMERS.

If you don't know what SPAM is, then you are not an e-mail user. Just about everyone on the planet with an e-mail address has received unsolicited junk e-mail - more commonly known as SPAM – at one time or another.

In the 1970s, there were very few computer users that even knew that the Internet existed; in fact, there were relatively few computer users, period. And of those few computer users, even fewer knew what a computer network was. It's probably safe to say that the number of e-mail users in the 1970s numbered less than 10,000 worldwide. Computer users in the 1970s were most likely employees of large computer companies or involved in some way in computer/networking research and development. Because the computer user population was so low in the 1970s, the use of e-mail was strictly confined to sending work-related messages, and once in a while scheduling technical conferences. Sending SPAM was unheard of, and unthinkable in the 1970s.

The 1980s gave rise to the Personal Computer (the PC), and to fledgling software companies like Microsoft. In the early 1980s, most PCs were standalone systems that were primarily used for applications like word processing, and spreadsheets. As PCs started to proliferate, the need for connecting – or networking – these high-tech business appliances became a necessity. Towards the end of the 1980s, more and more PCs were being connected via Local Area Networks, and more offices were being interconnected via Wide Area Networks. The high-tech companies were able to interconnect remote offices together using a maturing public network called The Internet.

At first, PC users were able to send e-mails to each other, but if they didn't have an Internet connection yet, these e-mails were restricted to only those users within the same office building. As more businesses started getting connected to the Internet, users found themselves being able to communicate via e-mail with an ever-increasing number of other users. But e-mails were still by-and-large restricted to business-related messages. A computer user with an e-mail address was still relatively rare by the end of the 1980s, and so was SPAM. In fact, if any user received a SPAM in the 1980s, they would *flame* the offending sender. Flaming is the electronic equivalent of humiliation in a public forum, such as putting petty criminals in the stockades in the town square.

In the late 1980s and throughout the entire 1990s, shrewd businessmen saw the potential of the Internet as a potentially viable means of turning a profit, and thus gave rise to a new industry called Internet Service Providers (ISPs). The mid-1990s saw one of the largest ISPs get off the ground: America On-Line (AOL). Large ISPs like AOL and Earthlink saw the home consumer as their primary customer base. While most Fortune 1000 businesses were already connected to the Internet and had well-established domain names (the *dot coms*), the home consumer had no access to e-mail, and had no e-mail address until companies like AOL and Earthlink came along. Now the home consumer could have an e-mail address too, such as johndoe@aol.com.

To the well-established e-mail user, AOL users, Earthlink newcomers, etc. were known as *newbies*. Prior to the millions of newbies that joined the Internet in the 1990s, there were no rules or regulations governing the use of the Internet (and in fact, the Internet is still largely unregulated today). It was like the wild, wild west. Internet users abided by an unwritten code of ethics; one of the most noteworthy unwritten rules was that “Thou shall not send SPAM to other e-mail users”. Violators of this rule were almost always flamed in newsgroups (a public discussion forum facilitated by the Internet).

However, all this changed once the hoards of AOL and Earthlink newbies got Internet connections. Suddenly anybody with a product or service to sell started *advertising* their goods and services via e-mail. It was impossible to flame millions of AOL newbies in newsgroups. And because the Internet was unregulated, it didn't take long before commercial SPAM shops started popping up all over the planet. The most notorious commercial SPAMMER was Alan Ralsky (operating out of the greater Detroit, Michigan area).

Early SPAM Strategies

In the beginning, there were only two types of SPAMMERS: the individual SPAMMER with something to sell, and the commercial SPAMMERS that offered SPAMMING as a “service” to others with goods or services to sell.

Unfortunately, there were millions of individual SPAMMERS by the mid 1990s. There wasn't much anyone could do about these unscrupulous individuals except to delete the unwanted e-mails from their mailbox. Sure, you could complain to your network administrator or ISP, and ask them to complain to the SPAMMER or their ISP, but most of the time this turned out to be an exercise in futility.

The commercial SPAMMERS, such as Alan Ralsky, would set up mail servers (SMTP Relays) all over the world with the single purpose of sending out SPAM to unfortunate recipients. Fortunately, these SPAM generators were finite in number, and clever e-mail administrators could block any e-mail attempts from these known sources.

As the number of clever e-mail administrators increased, so did the number of commercial SPAM servers and SPAM services. So e-mail administrators found themselves with full-time jobs in trying to keep up with the increasing number of SPAM shops.

The larger commercial SPAM shops somehow acquired lists of AOL users, Earthlink users, CompuServe users, etc., which made their service more valuable to their equally unscrupulous clients. To make matters worse, they were also able to harvest other e-mail addresses from these ISP's mail log files (probably by bribing an inside employee at one-or-more of these ISPs), and now they had millions of legitimate e-mail addresses that their SPAM servers could use to send unwanted messages on behalf of their clients.

Commercial SPAM shops found new ways to make money; in addition to sending out billions of unwanted e-mails per day on their clients' behalf, they soon discovered that they could also sell CDs containing millions of legitimate e-mail addresses to would-be individual SPAMMERS who were looking to “get rich quick overnight”.

The SPAM problem got to be so bad that in 1997, the number of SPAM e-mails equaled the number of legitimate e-mails. By the end of the 1990s, SPAM e-mail outnumbered legitimate e-mail by a factor of two-to-one. Unfortunately, this resulted in e-mail becoming a much less-effective means of legitimate communications.

The avalanche of SPAM got to be so bad that ISPs had no effective way of stopping the onslaught. SPAM was getting out of control, and for a while, it looked like the popularity of e-mail as a communications tool was going to die.

SPAM Countermeasures

As user groups and ISPs started becoming increasingly frustrated by the mounting insurgence of SPAM, websites started publishing the names and e-mail addresses of known SPAMMERS. These lists were used by e-mail users and e-mail administrators to block unwanted e-mail if the sender's e-mail address matched one of the addresses on the anti-SPAM list. However, this countermeasure was not without its flaws; in its early development cycle, anybody could add an e-mail address to these lists, whether or not the e-mail address was used to send SPAM. The organizations that maintained these lists now had to hire moderators to ensure that the sources in these databases were truly guilty of sending out SPAM.

New-and-improved e-mail server software, known as Mail Transport Agents (or MTAs) also emerged in the late 1990s. The updated MTAs were able to incorporate these publicly maintained anti-SPAM lists (such as <http://www.spamcop.net>, <http://www.spamhaus.com>, etc.) and help prevent these unwanted e-mails from being delivered to users mailboxes. Sendmail 8.9.3 (<http://www.sendmail.org>) and Q-Mail 1.0.2 (<http://www.qmail.org>) are examples of MTAs with these capabilities.

New SPAM Strategies

Not all ISPs or e-mail administrators knew how to properly deploy these newer MTAs with anti-SPAM functionality; in fact, few even had updated MTAs at all. This was especially true with companies that didn't have the expertise to install and maintain UNIX-based mail servers. Most small companies with Internet connections would purchase a glorified PC, install Microsoft Exchange with its default settings, and start communicating via e-mail with customers and business partners over the Internet. This seemed easy enough to do, and didn't require much expertise; just plug in the new mail server, load Microsoft NT server software, insert the Microsoft Exchange CD and click on the "Install" button when it appeared. The process couldn't be simpler; unfortunately, the process couldn't be any more insecure either (this was true in the UNIX world also, but not nearly as pervasive).

SPAMMERS took notice of the trend of proliferating unsecured mail servers. They were looking for ways to outsmart the newer MTAs in order to continue profiting by sending out SPAM on their client's behalf. Towards the end of the 1990s, more businesses were doing business online; there was a tremendous increase in e-commerce, e-tailers, online gambling, etc. Naturally, the way to announce their new online stores was through the SPAM channel. This gave rise to a new breed of commercial SPAM shops; instead of sending out SPAM through known SPAM generators that might get blocked by the newer MTAs, they would write programs that would find unsecured mail servers – also known as "Open Relays" – to send their SPAM through.

As the name implies, an Open Relay is a mail server that does not check to see if an e-mail is being sent from one of its authorized users. By its very nature, the Simple Mail Transfer Protocol (SMTP – a part of the TCP/IP suite of protocols established in the early 1970s) was designed to relay e-mail from any source to any destination, as long as the destination e-mail address was legitimate. And every mail server on the Internet uses SMTP protocols as its underlying mechanism to send and receive e-mail.

Simply stated, SPAMMERS were now using the mail servers of legitimate businesses to relay their unwanted SPAM. To the destination mail server, the e-mail appeared to be coming from a legitimate business that was not found on any anti-SPAM database. Therefore, this method of delivering SPAM circumvented the new features found in these newer MTAs.

This is considered to be very unethical to say the least, and even illegal in some countries because the SPAMMERS are now utilizing other companies assets, resources and bandwidth to do their dirty work. Therefore it is imperative that your mail servers are configured securely.

Countering The New SPAM Strategies

So now we have a situation where individual SPAMMERS, commercial SPAM houses, Alan Ralsky, and SPAM surreptitiously sent through Open Relays are all targeting user mailboxes at the same time. What is the already overworked e-mail administrator to do?

The answer comes in a couple of different forms. First and foremost is educating e-mail administrators to all of these potential threats. If e-mail administrators are unaware and ignorant of how SPAM keeps getting through their defenses (assuming that there are some defenses in place), then they have no hope in controlling the SPAM situation. Another countermeasure is beefing up the MTAs some more so they can thwart the latest SPAM strategies.

Once again, user groups and ISPs have found solutions in websites that started compiling and maintaining databases of unsecured Open Relays. <http://www.ordb.org> is an example of just that. The “*ordb*” part of the domain name stands for Open Relays Database. ISPs that have updated their MTAs to include checking mail servers against databases like [ordb.org](http://www.ordb.org) were able to successfully block SPAM illegally relayed through these Open Relays.

Companies whose mail servers appeared in the [ordb.org](http://www.ordb.org) database soon discovered that they had unsecured mail servers because e-mail would bounce back to their users. This forced companies to upgrade their mail servers, and secure their MTAs (if they wanted to do business via e-mail, that is). This countermeasure was quite successful in closing this loophole.

In addition to Open Relays databases, websites with publicly maintained blacklists known as “DNSBL”s also started appearing, and MTAs were quickly updated to take advantage of these anti-SPAM lists as well. DNSBLs are blacklists based on mail servers’ IP addresses that MTAs automatically obtain via Domain Name Services (DNS – a protocol that other protocols such as SMTP and HTTP rely upon). The main advantage of checking mail server addresses against DNSBL databases is that the lookup is **very** fast, which is advantageous for larger mail servers that process high volumes of e-mail.

Countermeasures such as Open Relay Databases, DNSBLs, and new MTAs finally gave e-mail administrators and ISPs an adequate arsenal to use in the war against SPAM.

Welcome To The 21st Century

The end of the 20th century has ushered in the Information age; we witnessed the advent of the Personal Computer; we were able to connect these appliances to the rest of the world via the Internet; we’ve grown accustomed to instant communications and instant gratification. Overall, technology has improved our quality of life. However, as we have seen, technology can also be leveraged against us by the likes of SPAMMERS.

Unless you are a SPAMMER, SPAM is egregious nuisance, a veritable cause of high-tech frustration, and at times, even dangerous. Users could inadvertently delete an important, legitimate e-mail while mindlessly deleting SPAM from their mailbox.

In the past, SPAM would try to coerce users to leave their hard-earned money at online casinos, purchase additional ink jet cartridges, refinance their mortgage for the fifth time in the same month, or even overdose on Viagra. However, like the junk mail that arrives at your home’s mailbox everyday, they were relatively harmless.

Things changed for the worse after the turn of the century. The last couple of years gave rise to a resurgence of e-mail borne viruses. These new breeds of viruses did a lot more than simply slowing down PCs or wipe out data. The new breed of viruses contained computer code that would search through Microsoft Outlook address books and send SPAM out to the e-mail

addresses found within the address books using a small SMTP engine that was also included with the virus. Additional variants of these viruses also sent out SPAM by randomly forging the originating e-mail address with users' e-mail addresses found in these address books (a technique known as *spoofing*).

This caused much confusion among many e-mail users, because the virus would often encounter obsolete or incorrect e-mail addresses, which would then bounce back to the spoofed sender address, resulting in the e-mail user to wonder why they got a bounced message for an e-mail that they were certain that they never sent. That was because an infected PC sent out SPAM using an originating e-mail address that was randomly picked from the infected PC's address book.

In other words, these new viruses exploited flaws in Microsoft Outlook, Microsoft Outlook Express, and Internet Explorer, etc. Since then, Microsoft has been releasing operating system patches and application updates in an attempt to fix these security flaws.

Worse yet, many of these new viruses were actually *worms*. The distinction between viruses and worms are subtle; the main difference is that a worm does everything a virus does, but worms also actively scan the network for more unprotected PCs to infect. These worms have taken down entire networks. *Nimda* (<http://archives.cnn.com/2001/TECH/internet/10/31/new.nimda.idg>) is an example of one of these worms. The one thing that early 21st century worms and viruses had in common was that most of them were spread via e-mail as attachments that unsuspecting e-mail users would open, mainly because it appeared to be coming from someone that they knew. Once the attachment was opened, code would execute on the users' PC and surreptitiously install these worms and viruses. Once installed, the worms would immediately go to work seeking out other unprotected PCs.

In essence, every PC connected to the Internet could potentially become a SPAM server.

21st Century Countermeasures

Older blacklists were rendered ineffective because too many SPAM messages appeared to be coming from legitimate e-mail addresses. The blacklists maintainers couldn't block every e-mail address simply because someone's PC was infected with one of these new viruses.

A different type of blacklist was required; blacklists that could keep track of IP addresses of large ISP's customers that *shouldn't* be operating mail servers. These new blacklists were variations of DNSBLs, which contained entire blocks of IP addresses that ISPs would dynamically assign to their customers (via DHCP protocols). The theory being that legitimate e-mail servers wouldn't have a dynamic IP address (one that keeps changing periodically); legitimate e-mail servers always use static IP addresses, so they would resolve consistently via DNS look-ups and satisfy the security requirements found in the newer MTAs.

Additionally, anti-virus companies (such as Symantec, McAfee, TrendMicro, etc.) started improving their anti-virus software with the ability detect viruses and worms in real-time. However, it was incumbent on the PC user to purchase, install and maintain the anti-virus software on their PCs. The problem was that the average PC user wasn't even aware of these security issues; all they knew was that the SPAM problem seemed to be getting worse or that networks seemed to be getting slower. Fortunately, the mainstream media started reporting these stories as Fortune 500 company's and government agency's networks were crashing (becoming inoperable) because of worms and viruses.

The Rise Of Spies And Zombies

The early 21st century saw the sinister convergence of viruses, worms, and SPAM. Those who thought that the already-dire situation couldn't get any worse were wrong; **very** wrong. Early versions of SPAM-generating viruses contained pre-programmed SPAM messages that could not easily be changed once the virus installed itself on the users' PC. Newer variations (mutations) of viruses would be released that would check with temporary websites to get new messages to send out as SPAM. Commercial SPAM shops started getting more sophisticated by staying a couple of steps ahead of Microsoft's critical security patch releases.

However, Microsoft started increasing the frequency of its patch releases, and started releasing their critical security patch releases on a regular basis (the second Tuesday of each Month, AKA: *Patch Tuesday*).

See: http://searchwin2000.techtarget.com/columnItem/0,294698,sid1_gci1016130,00.html

Many have argued (myself included) that this once-per-month patch release cycle is not nearly frequent enough, as it gives virus authors the rest of the month to find the next unpatched Microsoft security flaw to exploit. This anemic patch release cycle has proven to be fatal, because the next variation of exploits became even more sinister than previous virus variants.

This latest variation of worms and viruses have installed themselves as *Trojan Horses*, which are viruses that contain special code that would allow the virus authors to remotely control an infected PC. This type of code is called a Trojan Horse because – as the historical reference suggests – is executable code that the user had to *invite* onto their PC – most likely by opening up an e-mail attachment or through unsafe file-sharing services. The malicious code would then open up a *back door* on the PC, which can then be used for [usually] sinister purposes, such as turning the now-unprotected workstation into a *zombie*.

Thousands of zombies (collectively known as *bot nets*) can be controlled remotely at the same time by *zombie masters*, who could make these armies of zombies do whatever they want, including sending out SPAM, collecting personal and private information from the users' hard disk for nefarious purposes, and launching Distributed Denial of Service attacks against commercial and/or government networks.

Zombies could also be dormant for long periods of time, doing nothing but waiting for future instructions from their zombie masters, similar to *terrorist sleeper cells*. Zombie bot nets can be rented out to cyber-terrorists, criminal gangs, or unfriendly governments at any time. Currently, there are an estimated 3,000,000 zombies in the world (<http://www.camram.org/zombielogic>).

Also see http://www.usatoday.com/tech/news/computersecurity/2004-09-08-zombieprice_x.htm.

And if that isn't scary enough, there is also a new breed of virus called *Spyware* that is currently installed on an estimated 88% of all the PCs in the world.

http://news.com.com/Research+Spyware+industry+worth+billions/2100-1029_3-5693730.html

Spyware is special software that is designed to collect personal information from PCs – such as access codes for online web banking, for example – and then send that information to an individual or organization who can then use that information to withdraw funds from bank accounts or make online purchases. Spyware can also be used (and often is) to help perpetrate *Identity Theft*.

These are very real serious and very serious threats to personal security, and also potentially to national security.

Gone Phishing

Yet another phenomenon resulting in Identity Theft cropped up in the early years in the 21st century: a phenomenon dubbed as *Phishing*. Phishing is a combines e-mail and web technologies to dupe unsuspecting users in giving out their credit card numbers, expiration dates, the name of the credit card holders, bank account numbers, online web banking passwords, etc. Phishing is a 21st century high-tech criminal enterprise that has bilked users, credit card companies and banks out of billions of dollars per year.

The way phishing works is that a criminal organization (e.g., the Russian Mafia, see <http://www.eweek.com/article2/0,1759,1772686,00.asp>) would set up temporary websites, usually in some remote corner of the world, that is specifically designed to look just like Citibank's website, or Bank of America's website (just to cite a couple of examples).

Next, millions of SPAMs get sent out to users – probably through leveraging a few thousand zombies – requesting them to visit these nefarious websites and update their bank account information or credit card data. Often times, the e-mail addresses to seed these SPAM campaigns were stolen from unsecured e-commerce sites, and in one case, stolen computer backup tapes.

The unsuspecting user then goes to these websites and updates their personal financial data, just as the SPAM had instructed them to do. Since these websites look identical to the actual websites of these financial institutions, unsuspecting users don't give it a second thought. In addition, these SPAMs often spoof e-mail addresses from these financial institutions and/or credit agencies, thus appearing to be even more credible to unsuspecting users.

Phishing operations are difficult to track down and prosecute because the websites that they set up only have an average life span of 4 or 5 days; the zombie-controlled SPAM campaign has an equal life span. However, this is just enough time to generate billions of dollars per year for this new breed of cyber-criminal.

More Countermeasures Are Needed

In addition to frequent releases of Microsoft's critical security patches, large ISPs have also responded to these e-mail security threats by blocking their own SMTP ports (TCP port 25) from inside their own network infrastructures. What this means is that a Comcast customer, for example, would be required to use one of Comcast's outgoing SMTP mail servers in order to send out e-mail.

There are millions of PC users that connect to the Internet using one ISP service (such as a Cox Communications Cable Modem), but use another service (such as [Neptune.Net](http://www.Neptune.Net) or AOL) for their e-mail. This situation exists because companies like Cox Communications provides Internet access via their Cable TV infrastructure, but not e-mail or web-hosting services; and companies like [Neptune.Net](http://www.Neptune.Net) provides e-mail and web-hosting services, but doesn't have a large physical network infrastructure like Cox Communications, Adelphia or SBC. Therefore, millions of PC users subscribe to two (or more) ISP services.

This strategy of large Internet access providers blocking TCP port 25 has helped diminish the amount of SPAM coming from virus-infected PCs and zombies connected to major network backbones (See http://news.com.com/ISPs+versus+the+zombies/2100-7349_3-5793719.html). However, zombie masters are looking for other ways of distributing their remote control software (such as infecting websites), and spyware often uses other TCP ports to transmit the PC users' personal data. Thus this particular strategy is only enjoying limited success.

The anti-virus companies have included Spyware detection features in their recent releases, however not all anti-virus can actually agree on just what exactly spyware is. PC users often install software on their PCs without reading the entire License Agreement (they blindly click on “I Accept”), some of which actually states “by installing this software, the user agrees to allow certain information to be transmitted to the software vendor for market research purposes”.

Then there are those who are advocating special legislation. As I have stated at the outset of this article, the Internet is by-and-large unregulated. There is a very good reason for this; most notably, the Internet is a global network. Unlike legislative bodies, the Internet has no concept of borders or jurisdictions. For example, the United States Congress can enact laws like the *Can SPAM Act of 2003* (<http://www.ftc.gov/bcp/online/pubs/buspubs/canspam.htm>), but how can Congress, the Federal Trade Commission, or the Department of Justice enforce this law in Beijing, Damascus, or Grozny, Chechnya? Until we have one world government, legislation is clearly not the answer.

Other proposed solutions come from the private sector, specifically the technology sector (<http://www.microsoft.com/presspass/misc/billgspam05-21-03.msp>). But let's not forget that technology got us into this mess in the first place; technology might be able to address this issue, but as we have seen, SPAMMERS, virus authors and zombie masters will always find ways to use technology against us.

Some other companies have tried putting the onus on legitimate senders by generating an automatic response to all e-mails addressed to a recipient whose mail server uses *confirmation-based MTA* technology. The automated response is sent back to the sender requesting that they reply back to (confirm) the automated response, and if/when they do, the original e-mail message will be delivered to the intended recipient. Confirmation-based MTAs work under the assumption that zombies and other SPAM generators won't reply to these automated responses.

While this strategy seems like a sound idea at first, these types of mail servers often require additional attention and administration because SPAM messages often stay in the delivery queue for long periods of time. Additionally, these messages get backed up, and sometimes even restored unintentionally. If these SPAM messages contain viruses or worms, they can also start infecting other PCs and servers that are connected to the same network as the mail server.

Another proposal being considered is Bonded Sender MTA technology. This proposed solution acts like a DNSBL in reverse (like a DNSWL, or DBS-based white list); all e-mails coming from users that relay e-mail through Bonded Sender servers will be delivered to the Bonded Server MTA recipient unencumbered; all other e-mail senders will have to prove that they relay e-mail from/through a trusted (certified) source. The problem with this technology is that senders need to register their mail server's IP address with the Bonded Sender server; otherwise the e-mail will be blocked pending certification or confirmation. Also, in order to become a Bonded Sender server, e-mail administrators need to go through a certification process, and also post a financial bond that will get debited every time the certifying organization receives a complaint about SPAM originating from the Bonded Sender (<http://www.bondedsender.com/howitworks.html>). The largest problem with this technology is that this program isn't ubiquitous; if there's not enough critical mass to accept this technology, it merely becomes a nuisance to legitimate e-mail senders (like the confirmation-based MTAs).

Yet another proposal being considered is a pay-per-e-mail system. The premise of the theory behind this proposal is that the reason that SPAM is such a huge problem is that sending e-mail is free. Opponents to this proposal argue that 1) paying bulk mail rates to the U.S. Post Office hasn't cut down on the amount of junk mail that we receive every day, 2) criminal operations running armies of zombies can easily circumvent paying e-mail postage, and 3) the SMTP standard would have to change, forcing everyone to purchase new hardware and software in order to adopt the new protocols and standards.

In Conclusion

The war against SPAM has thus far been a cat-and-mouse game - a chess match of measures and countermeasures. While there are no easy answers to this conundrum, [Neptune Consulting Group, Inc.](#) believes that an opportunity exists for network security experts to solve the SPAM problem by staying far enough ahead of the technology curve to thwart current and near-future cyber threats.

SPAM has come a long way since peddling Viagra to the masses. Who knows what kinds of cyber threats are looming on the horizon. The one thing that is certain is that complacency will only make it worse. Network security and network vigilance is key in keeping computers and networks safe, along with emerging technological trends. And [Neptune Consulting Group, Inc.](#) is on the forefront of both.

In the meantime, the best protection that you have is you. Please practice *safe computing*:

- ❑ Don't open e-mail attachments (or e-mail, for that matter) from senders that you do not personally know.
- ❑ Keep anti-virus definitions files up to date.
- ❑ Perform anti-virus and anti-spyware scans on all your hard drives on a regular basis. Unlike us humans, computers don't need to sleep; the ideal time to run anti-virus and anti-spyware scans is while you are sleeping (not to mention that fact that running these scans might even make you sleep better, because you wouldn't worry as much about computer security).
- ❑ Keep your Operating System and Applications patches current.
- ❑ Change your passwords at least a couple of times per year.
- ❑ Make frequent back ups of your personal data.

The numerous calls for new proposals and countermeasures are on the rise. Even more disturbing are the numerous proposals for new legislation at city, state, and federal levels. As stated earlier, we don't believe that additional legislation will work because there is no effective way of enforcing these laws. And when legislative bodies start considering regulation, taxation is never far behind.

We are of the opinion that education and self-regulation is the best solution. While this alone may not stop the phenomenon known as SPAM, awareness of the problem is the best prevention to becoming a victim of SPAM. Complacency is the enemy, but don't despair, companies like [Neptune Consulting Group, Inc.](#) are your biggest allies in the war against SPAM.



René Mente
President / CEO
Neptune Consulting Group, Inc.