Dead Trees

A PUBLICATION OF QUESTIONABLE VALUE FROM William Blinn COMMUNICATIONS

179 Caren Avenue • Worthington • Ohio 43085
614-785-9359 • Fax 877-870-4892 • www.Blinn.com

July 2002

Spam: Is legislation the answer?

Not in my opinion. As much as I detest spam, I don't buy the argument that it can be legislated away. But when a topic hits USA Today, you know it's a top-of-mind issue for a lot of people. And most people don't like it.

In a single 24-hour period, I received the following "offers". I note the country of origin in parentheses. The country of origin can be easily determined by looking at a message's Internet routing headers; in fact, that's the only way to figure out where it came from because most spammers forge the "from" and "reply to" part of their messages.

The slop bucket overflows with:

- Two medical warnings that included a pitch for a worthless and possibly harmful "medicine". (Australia)
- Many offers for 100 million e-mail addresses. (Most from China and Korea; a few from the US)
- Two illustrated messages for 4 porn sites. (US, Korea)
- Two offers for a program that harvests ("steals") e-mail addresses. (China, Korea)
- An offer from an "erotic photographer" who prefers "young subjects". (Russia, Korea)
- An offer for "incest pictures". (Netherlands)
- An offer for cheap toner cartridges. (Korea)
- Several casino offers. (US, India)
- Two offers for "cheap Viagra". (Netherlands)
- Numerous offers for "hot babes live". (Hungary)
- Lolitas on-line. (South America, country not clear)
- At least a dozen offers for "human growth hormone". (One was sent via the US military "Defense Net", which apparently has an open relay.)
- A dozen or more offers for "life insurance quotes", most of which were made to appear to be coming from Canada. (Most were from Italy, Russia, and China)
- Lots of offers for "Noni juice". (Nearly all from Korea)

Well, you get the idea. A total of 81 messages in less than 24 hours. Nearly all of them for products that are useless at best. Call me overly cautious if you want, but I'm not about to buy "medicine" from somebody who hides behind a fake address, uses a one-time "drop box" to retrieve replies, and steals mail transport services to send me a message. After a week out of town, I returned to find 600+ messages, more than 400 of which were spam.

And keep in mind that the exact kind of information that would be needed for a legitimate insurance quotation would also be ideal for the person who's planning a little identity theft. Are Russian, Chinese, and Italian insurance agents licensed in the US? Would a legitimate insurance agent send a message from an offshore server?

Is this situation out of control?

I'm old enough to remember CB radio. It seemed like a good idea at the time. We could talk to each other from car to car. But then the crap (sorry, but there are no words for it more polite than this) started. Within a few years, everyone with the exception of truckers and trash-talkers had decided that the advantages of having a CB radio didn't outweigh the disadvantages.

That could happen to e-mail. It could happen to the Internet. Despite the enormous advantages that the Internet in general and e-mail in particular bring us, many users are today doing everything they can to keep their address private.

A friend visited a website to learn about "sheriff's auctions" and "foreclosure sales". Within 20 minutes, he had received his first spam touting "no-cash house purchases" and he now receives at least half a dozen of these unwanted messages every day. He's incensed and he has every right to be.

There ought to be a law?

Despite all this, I'm still not suggesting that legislation is the answer. Laws can be passed making spam illegal, but a lot of spammers (even though they're located in the US) use spam-friendly operators in China, Korea, and Russia.

In other cases, they use "open relay" systems (computers that don't much care who uses them) that are rampant in Central Europe, Eastern Europe, and much of Asia. US colleges also have a terrible record regarding open relays.

There are organizations that identify open relays and make this information available on a subscription basis. If your Internet service provider and mine subscribed to these services and used the information to set up mail blocks to stop mail from known open relays, spam would drop dramatically.

And if those same organizations identified "spam friendly" service providers and blacklisted mail from them, the legitimate users would force the service providers to eliminate the spammers. About a year ago, an Internet service provider refused mail I sent to one of its subscribers. A quick check

What the heck is this?

Dead Trees is the **William Blinn Communications** newsletter. It's published whenever I feel like it, although I generally feel like it when I'm preparing the month's invoices. If you didn't receive an invoice with this newsletter, kindly contact me and we'll rectify that situation. Please note that despite the name, of the publication, I bear no particular animosity toward trees. The name is simply an acknowledgment that paper is made from, well, dead trees.

revealed that my website host had been identified as hosting a spammer.

I was on the phone within 10 seconds to the company that hosts my website. By that time, they had identified the spammer and they had terminated the account under the "terms of service" that nearly every website provider has (but some don't enforce). In less than a day, the problem was solved. The ISP that has 100 honest paying customers and 1 spammer will be more than happy to get rid of the spammer.

So my theory is that ISPs could stop spam without anybody's help if they wanted to. In fact, AOL could probably do it alone by:

- Refusing all mail from any computer that's been determined to be an open relay and
- Refusing all mail from spam havens (Russia, China, and Korea are the worst) until those countries clean up their acts.

We don't need any new laws, either. What we do need is somebody with the guts to enforce the laws we do have. If somebody sent my 17-year-old daughter a package promoting pornography via the US Postal Service, that person would receive a visit from the postal inspectors. If somebody tried to run the Nigerian bank fraud scam by phone or mail, the law would reach out and touch them. But when creeps and crooks use the Internet they get away with it.

The government isn't going to help. It's up to the Internet service providers and to those of us who are users to find a way to stop the flood.

The solution

If AOL, Mindspring, Time Warner, and the various Baby Bell ISPs worked together to block spam, the spam would be gone. Until then, all you can do is use a program such as SpamKiller or JunkSpy. These programs examine your inbound mail and sort it into two categories – junk and good mail. Sometimes spam gets through and sometimes a good message shows up in the trash. So you must at least glance at the messages that have been identified as spam to see if you want to pull any of them out of the trash.

Anti-spam legislation is a bad idea for a number of reasons, not the least of which is that we don't need more laws. Some state attorneys general (with New York's attorney general in the lead) are going after big spammers who are breaking existing laws. When you con consumers, you're breaking the law. But what if you pass a law that makes spam illegal in the US? All the spammers will up accounts in Korea or China. And what would that accomplish?

Contact your Internet service provider. Tell them that you want them to work with other ISPs to identify the source of spam and to reject mail from those sources. The patchwork of weak anti-spam efforts by most ISPs (with some notable objections) have little effect on spammers. Only a concerted, coordinated effort will get the job done.

And in the meantime, invest in anti-spam software such as SpamKiller (now included in McAfee Antivirus software). If you want to use the Internet to further your own business, it's time to start running the shysters out of Dodge! ß

BB, phone home!

After spending a week in New York City, I can tell you that connecting a computer to a cell phone works. Maybe not well just yet, but it works.

I was able to collect (slowly) my e-mail without the need to use a wired phone.

Verizon is rolling out its 3G system and Sprint PCS will have some 3G cities soon. 3G could mean 3rd generation (which it does) or it could refer to 3GHz (where many of the phones will operate). As far as I know, the 3G name has nothing to do with the frequency.

The big thing that 3G phones will offer is the ability to transfer data faster and by the end of this year several major cities will have 3G services. Of course, that means you'll have to buy yet another new phone if you want to use 3G's capabilities. And because 3G is new technology, you'll need a phone that operates with older technologies, too. In other words, if you want good coverage, you may need a "3-band" phone.

The first generation of cell phones were analog. Most cell phone users today probably have 2nd generation phones. These are digital. They offer fewer dropped calls, but the sound of a digital connection still leaves a lot to be desired. The 3rd generation phones will also be digital, but they'll operate on different frequencies.

GSM (Global System for Mobile communication) is widely used in Europe and other parts of the world. GSM uses a variation of time division multiple access (TDMA) and is the most widely used of the 3 digital wireless telephone technologies (TDMA, GSM, and CDMA). GSM digitizes and compresses data, then sends it down a channel with two other streams of user data, each in its own time slot. It operates at either the 900MHz or 1.8GHz frequency band.

TDMA (time division multiple access) is a technology used in digital cellular telephone communication that divides each cellular channel into three time slots in order to increase the amount of data that can be carried.

CDMA (code-division multiple access) refers to any of several protocols used in so-called second-generation (2G) and third-generation (3G) wireless communications. As the term implies, CDMA is a form of multiplexing, which allows numerous signals to occupy a single transmission channel, optimizing the use of available UHF bandwidth (800MHz and 1.9GHz) systems. It's enough to make my head hurt. ß