Wonder Or Worry?

What Can Be Done To *Brighten* The Internet's Future

MGT 511
David E. Rohr
February 27, 2006

Abstract: The far-reaching capabilities of the Internet have simultaneously created a wonder and worry. That's because along with being an incredible tool for communication, education, commerce and craft, the internet's dark side has come to threaten us in many ways including the dangers posed to our networks and hardware through hackers, spammers, chain letters , urban legends and other menacing phenomenon. In other cases, the threat is more costly with identity theft, cyber terrorism and cyber stalking threatening both our personal and financial security. Combating these will require various combinations of consumer/user education, government/business cooperation and technological innovation.

Problem: From the daily crush of spam and other Internet garbage to the constant threat from hackers and crackers, businesses and the people who make them work are compromised in their productivity. In the case of spam and viruses, the annual costs range into the billions. On top of these threats, the dangers from hackers, crackers, and cyber terrorists force both public and private sectors to devote valuable personnel and financial resources to defensive measures. And the personal threat of identity theft and cyber stalking can make the Internet as dangerous as the darkest alley in the roughest part of town.

Solution: Individuals can do a significant amount to secure themselves, their computers, their financials and their families. From proper management of personal networks and passwords to more prudent and judicious use of anti-spam and anti-virus people not only make their own worlds more secure, they make the shenanigans and wrongdoing less rewarding. It is also clear that personal involvement is a major key to overcoming problems with identity theft and protecting children from cyber stalkers. Finally, software makers, hardware manufacturers, ISPs and others who are behind our online infrastructure can do a great deal to improve the situation. By using the same kind of ingenuity they applied in creating Internet resources to the effort of keeping our online world safe, inventers and entrepreneurs can catch up with and move ahead of those who would misuse the Internet. A combination of consumer and government pressure can help bring this about. Perhaps even a business-government task force or policing agency is required to combat the multitude of threats.

Hackers and crackers. Protecting our digital valuables from cyber burglars

With only 50 employees, my company is reasonably small in the grand scheme of business. Yet, Dixon Schwabl Advertising maintains a healthy concern for both hackers, and crackers, according to IT Director, Bob Hotchkiss. " In my 4 years here, we haven't really seen any attacks or intrusions on our systems. But I have to say that it is something I am always vigilant about. I guess the biggest problem is unauthorized software or an occasional virus that travels in via an employee disk."

I can vouch for Bob's overall IT vigilance from personal experience too. Last summer, knowing that the agency had no wireless capability and knowing that I might soon come across an extra wireless router for my home network. I innocently volunteered to plug the router into an extra CAT 5 jack in my office wall. He nicely, but firmly declined my offer, explaining his concern about mischievous people who might be driving around looking for wireless signals to exploit.

Hackers, of course, come in all shapes and sizes. And their work varies in intensity and scope. Some people actually argue that hackers are good for the computer industry and business in general. This argument is based on the simple notion that hackers perform a service that exposes weaknesses. It is the kind of argument that is Darwinian in scope in that the fittest are who survives. Some believe that hackers are simply adventurous, young people using their

intelligence and curiosity to find out how things work, (Syracuse University Website, 2006).

Crackers are clearly another matter. These people are intent on using the Internet for more antisocial purposes, (Crowley, 2003). However, the practice has also meant business for other organizations looking to profit by selling protection (Chubb Insurance, 2006). From most of the available information it is apparent that companies can be more effective at combating the threat through an integrated program of firewalls, encryption and other security along with well defined policies for computer use, sharing, password protection, computer use for non-business activities, etc. I checked the Dixon Schwabl employee manual and found nothing in it relating to computer and network security and use.

It is worth pointing out that the biggest threat to companies' data and network security does not come from either hackers or crackers. Rather, it walks through the door every in the form of trusted company employees. No amount of firewall protection can stop the people who log on with company-approved passwords. A recent Wall Street Journal article describes the problem in a range of ways from pilfered files sneaking out of company locations on keychain flash drives, to sensitive information stolen from emails to customer records falling into the wrong hands at outsourced call centers, (Totty, 2006). It says that no amount of firewall protection can protect this kind of internal threat. But the article also counsels remedies such as employee education, legal protections, setting up classification systems, smart encryption systems and other remedies.

For the threats posed by hackers and crackers, I have noticed that there are a number of “alliance” sites set up to help businesses openly discuss and provide relevant information on the problem. A site dubbing itself Commercial Business Intelligence (2006) urges visitors to: “minimize the risk… maximize the opportunity.” Like others, this ultimately describes a “holistic” approach as the remedy for the problem including using encryption, firewalls and intrusion protection software along with continuing vigilance. All these are probably ideal solutions from a businesses standpoint. However, looking up the cost of some of this software I see that some of it costs as much as $10,000, (Simomds, 2005). As a small business owner myself (as well as an employee of a larger company) I often have a hard time with software purchase and upgrade costs for things like Microsoft Office. The idea of laying out that kind of money for intrusion protection is something that would definitely have it on the backburner for me. As with other technology, I suppose I can wait for market forces and further innovations to force prices down a bit. Then more of us can sleep easier. But for now, I’ll focus on the less technical things I can do—like putting a password on my home wireless system.

Viruses. Curing of the darkest afflictions of the Internet.

The world of computer viruses has come a long way since the 1986 computer virus called “Brain” made its way into the computer world and traveled via shared floppy disks from computer to computer. “Brain” ultimately proved little more than

a curiosity in the end but it was the first of one of computing's darkest, most destructive aspects.

Today, among other damaging effects, computer viruses cost businesses millions per year. They sap the productivity that could be better-spent delivering products and services. And they damage important intellectual that resides as data on the world's hard drives. In 2003, viruses wreaked incredible havoc, causing 55-billion in damages, double the previous year and nearly four times as bad as 2001 (SecurityStats.com, 2006). Microsoft had a particularly bad year in 2003, with the *Sasser* and *Blaster* viruses attacking Windows PCs worldwide. Today, as Microsoft scurries to remedy all the flaws in its operating system, virus makers have turned their attention to other manufacturers products (Metz, 2006).

According to recent information from the FBI, 84% of American companies fell victim to viruses, spy ware and other malicious programs last year. Clearly the virus has moved beyond a curiosity to become one of the most destructive daily threats we face as computer users. "The most significant change has been the evolution of virus writing hobbyists into criminally operated gangs bent on financial gain," said Mikko Hypponen, chief research officer at Finnish anti-virus firm F-Secure, (BBC News Online, 2006).

Small businesses can easily be ruined by the problem, too, particularly considering that many operate on small margins and have smaller customer bases. All it takes is a few days downtime caused by a virus, corrupted files and poor or non-existent back-up procedures. The problem of computer viruses is of course something that can and should be blamed primarily on those of malicious

intent who create and propagate them. However, the online world—from computer manufacturers, to ISPs, to consumers bear some of the responsibility for the viruses that victimize us. According to PCMagazine a great number of us either don't have security software installed or the software is way out of date. It adds however, that hardware and software vendors bear just some of the blame and that ISPs and PC makers could have alleviated much of the problem if they made security more integral to what they sell. Ultimately, PCMagazine says that software developers deserve the brunt of the blame—particularly the anti-virus software makers. It seems they are more intent on protecting other parts of the computer and often fail to recognize their own vulnerabilities. (Metz, 2006).

The problem of viruses has affected me recently, although moderately. Three or four weeks ago, I heard my office computer hard drive spinning persistently, and unnaturally. I called our IT guy and before I could say anything he said "you got a virus". It's great to know that people are looking out for me and others when it comes to our computer and ongoing security. But looked at another way, if the IT man where I work wasn't using his remote tools to take care of viruses, he could probably be working on new productivity-boosting ideas for the company. This may ultimately be the biggest cost of viruses.

Spam—Working to can it.

I have two different perspectives on small business spam. That's because I both own my own small consulting/freelance writing business and work as a contract employee for another larger firm that also would still be considered a small

business by most standards (under 60 people). In the case of my own business email, I am continually deluged by spam. But at the company I work for I have probably received less than a handful of “junk” emails in the past year.

And for small businesses as a whole, the numbers do not look good. According to a 2005 article small businesses employees receive four times as many spam emails in a day as those in large companies. And with a daily average of 50 spams per day, they are seeing the trend continue upward, given that the daily average in 2004 was just 36. (Small Business Pipeline, 2006).

There are a couple of reasons why small businesses get the brunt of the spammer’s onslaught, according to the Small Business Pipeline article. One is that law, advertising, real estate and publishing are spammer’s most frequent targets and these generally fall within the “small business” category. What’s more as small businesses, they are less likely to employ spam-filtering tools.

In 2003 spam accounted for almost 50% of all Internet traffic, according to Business Wire, (2003). But beyond the traffic, estimates from 2003 showed the total cost of spam to be approximately $20 billion worldwide when lost productivity, anti-spam software and other spam-related costs were taken into account.

Designed to answer, at least partially, the deluge, the CAN-SPAM Act of 2003, CAN-SPAM created a uniform standard for e-mail marketers while also enumerating civil and criminal penalties many questionable spam tactics. Another economic cost is that spam makes it more difficult for legitimate

companies to conduct email operations. A recent FTC paper summarized the feeling of legitimate businessman:

> Spam negatively affects legitimate marketers' response rates, and long term, it will drive their marketing dollars towards other media down the road, and impact our business. This is why it's important for those of us who want to provide services to legitimate opt-in email marketers to help get rid of the porn, get-rich-quick, penis enlargement, Viagra and mortgage offers, (Federal Trade Commission Site, 2006).

In the case of my independent business, I chalk up the unwanted email to the fact that I have used the same address for years and have given it to numerous vendors, survey takers, and business associates. My other job however, is one where only a small circle of people outside my company even knows that email address. The cost of spam is significant to me as an independent businessman, but negligible as an employee of a slightly larger small business. For example I spend several minutes a day highlighting and deleting the email that comes into my business through my Earthlink account. Occasionally, a spammer will use a subject or a sender ID that confuses me into thinking it might be from a genuine acquaintance or business contact from the past. That too wastes time. And when you consider that as a result of all the spam, 95 percent of my email just gets deleted—yet it is still something that used networks, server space and other resources. I think it would be ideal if there were devices that automatically returned unwanted spam to the servers that delivered them, creating a sort of DNS effect. However, that would also mean more network traffic, and slower networks.

While lawmakers' efforts could certainly benefit those of us who object to spam, even small businesses have a tremendous ally in some of the software that is available. Dixon Schwabl Advertising's Bob Hotchkiss, quickly dispelled my notion that the reason I wasn't getting much spam at work was the relatively limited way in which I have shared that email address. Showing me statistics generated by the Agency implementation of Barracuda Networks Spam and Spyware Firewall, he pointed out that the software has stopped nearly a million spam messages since late October—an average of 20,000 per employee.

In my opinion, spam should be described as the *artery plaque* of the Internet. Because of the preponderance of spam, email servers have to process far more volume than necessary. That is something that requires extra hardware, thus increasing costs. Combine that with the lost productivity and it is easy to see how costly it becomes in the long run. Barracuda Networks solution is an ideal solution for making spam less troublesome for businesses and less rewarding for spammers.

Chain Letters. Go Ahead, Break The Chain!

I can say honestly that I don't think I have ever participated in an Internet chain letter, due in part to the heartbreak of a snail mail chain letter I participated in the 1960s as a 6- or 7-year old child six or seven-year-old child. Someone at my school had gotten my address and put me on their chain letter list. The request was simply that I mail a post card to the person at the top of the list and then send the letter to six new people with the person at the top of the list removed

and my name added to the bottom. My mom, who read and explained the thing to me tried to discourage my participation but I persisted, enticed no doubt by the promise of hundreds, perhaps thousands of beautiful, colorful postcards from all over the world. Postcards would certainly fall under the minor value description within the postal lottery statute (U.S Postal Service, 2006), which is probably why my mother ultimately agreed to let me participate and learn the little object lesson that I did.

I can still see her typing away to create six, new neat lists to send to the list of six I compiled. And for weeks after we mailed the letters, I went to the mailbox eager for the deluge to begin. One week, nothing. Two weeks, nothing. Three weeks, nothing. And, so after a period it became clear that I probably wouldn't get a single chain letter. "No fair", I thought. The person at the top of the list got the post card from me. Being disappointed as a hopeful little boy is something that never really leaves you. And so those people who put me on their lists may not realize it, but the chain gets broken fairly early. Because I simply don't play.

For the rest of the world however, chain letters are the gift that keeps on giving. Unfortunately, what they give seems to be bogged down network systems and a treasure trove of email addresses for spammers and other cyber miscreants downstream. Not only do they clog networks, they waste bandwidth and disk space. Ultimately they hurt everyone who sends, receives or otherwise relies on legitimate email. Chain letters are illegal if they contain any requests for money or items of value, (University of Arkansas Department of Computing

Services, 2003). Multiply the geometric power of a chain letter and combine it with anything that is libelous, false or fraudulent and it is easy to see that chain letters can, in many ways be considered just as bad or worse than viruses and spam.

Today's chain letters have a natural advantage over the chain letters of yesterday. Before computers, all chain letters were sent by U.S. mail and required a stamp. And because sending them involved a real, up front cost in time to type the letters and money for stamps, chain letters faced an uphill battle (as my childhood example probably demonstrates) for survival. Today however, participating in a chain letter is easy—whether it's a hoax or driven by someone of misguided sincerity, (University of Oklahoma Police Department, 2006). All it takes is a few mouse clicks and you can move a letter to 6 or 10 select names on your own email list. The U.S Postal Services urges recipients of chain letters to write a note indicating a possible chain letter and return it to their office for possible follow-up by postal authorities (U.S Postal Service, 2006). It is too bad this can't be done for email chain letters (as it would probably swamp their servers). Still the Post Office has some kind of jurisdiction over email chain letter scams whenever mails are used.

But in the spirit of "if you can't beat 'em, join em", I wonder if the best way to kill chain letters might be to create a chain letter that defines the problem, tells people how they clog networks, perpetuate frauds and ultimately end in disappointment. This letter could remind people of all the disappointing returns they received and ask them to think about all the spam they get in their inboxes,

perhaps from spammers who get their names from chain letters. If I sent that "down with chain letters" message to six people and asked them to send it to six, and so on, the letter could conceivable go to millions of people in just a few days—and to every conceivable computer user on the planet in a few more. The only problem is that the letter doesn't hold out the promise of something for virtually nothing. And it just isn't a whole lot of fun. Plus, the pragmatic people who receive this email would probably, like me, decline to pass the letter on.

Identity Theft—Shredding The Practice

There have been as many as 10 Million American victims a year. And at a cost of more than $53 Billion, (UIUC Library, 2006). Identity theft is something that is a fear that my father in law—now an Alzheimer's sufferer—has long had. His concern about raising the flag on the mailbox was something I remember him harping about for at least the past 20 years. And his obsession about burning or otherwise destroying every unnecessary document that had account information on it made him seem like a bit of a kook to a lot of us. When my wife's brother bought him a shredder about 10 years ago, he began imagining all the ways a thief could piece the shreds back together.

But with all this, there appears to be some headway in the battle to counter identity fraud and theft. According to the Better Business Bureau. In a recent article on the Bureau's website, the number of annual victims has actually declined from slightly over 10 million in 2003 to 8.9 million (Better Business Bureau, 2006). The BBB points out however that even with numbers declining,

the cost to the economy has held constant due to the fact that the average fraud per victim has increased from over $5,200 to $6,300 and the average amount of time to resolve the problem has increased to 40 hours, from 32 a couple of years ago.

Identity theft is clearly a significant problem. But it is one area where the consumer has a great deal of control—and the ability to prevent victimization. In addition, only a small amount of identity theft occurs online. The Bureau says, for example, that the vast majority of identity theft comes through those old fashioned methods my father-in-law used to obsess over—stolen mail, trash cans, co-worker swiping a wallet from a desktop, etc.

But the online world, with its large centralized databases and easy hemisphere-to-hemisphere commerce hold out the potential for cataclysmic losses for individual and the economy as a whole. It takes just a few clicks of the mouse for a person of ill intent to gather key fragments of personal information. Corporate data bases are also within easy reach, particularly if there are people of less than honorable persuasion within the IT sphere.

> Nearly all security consultants, including Ed Neumann at Javelin Strategies, say the weakest link in protecting personal data is a bad employee at a company that uses these databases. "We've found that very few companies are safeguarding it against employees. They've done a fair amount of erecting 'firewalls' and other safety mechanisms from outsiders 'hacking' in. But they're not doing enough to safeguard employee access," (Young, 2005).

There is a lot of merit to the statement above. Numerous times—either in setting up a company computer, establishing network access or setting up an email account—I have been told to just use “password” as my password. And even

though this is something that is easily changed, I have a feeling that many people continue to use these defaults. That alone is a huge point of vulnerability. And I can imagine that if people would be willing to walk into my office and grab a wallet or look for a checkbook stub in my drawer, they might be just as willing sign onto my computer if they knew that “PASSWORD” could get them it.

It is curious though, that the recommendations of the BBB point to gradual and slight improvements in the problem over the years while noting that computer identity theft is only a small part of the problem. And their recommendations contain many my father in law would applaud:

- Retrieve paper mail promptly and place outgoing checks or other sensitive documents in a U.S. Postal Service mailbox.
- Sign up for automatic payroll deposits.
- Replace paper bills, statements and checks with online (paperless) versions.
- Keep passwords hidden (even in your own home) and change them frequently.
- Use and regularly update firewall and anti-virus software.
- Do not respond to suspicious e-mails. Delete them, and if there is any doubt contact the company to determine if the e-mail is real.

And the BBB has one recommendation that really catches my attention:

- Don't discard a computer without completely destroying the data on the hard drive.

Having owned a dozen or so computers in the last 18 years, this item is one I have to admit total failure on. Sure I have deleted files but I've never wiped a hard drive clean. Gulp.

Cyber terrorism and cyber stalking—Evaluating the dangers, far and near. The scenarios are frightening. The banking system being taken down overnight. A hacker uses computers to take over a food processing or food production line to create poisoned consumer food products. An air traffic control system paralyzed by a uniform attack against the networks and computers it depends on.

All of these possibilities haunt those concerned with the cyber terrorism phenomenon. But despite the real possibilities of these eventualities, most systems in which computers play a vital role ultimately maintain a component of human override. Air traffic control systems are, as of this point, not computers on the ground talking to computers in the sky. Rather, humans still do the communicating and the flying of the planes. Similar human safeguards ease the fears of cyber terrorism in other areas, (Pollit, 2006).

While a popular topic and one that certainly merits attention in the face of well-known hacker and cracker escapades, cyber-terrorism is believed to be an overrated threat. A U.S Institute of Peace website sums it up "# The potential threat is, indeed, very alarming. And yet, despite all the gloomy predictions, no single instance of real cyber terrorism has been recorded," (Green, 2002).

As some experts point out, the real danger of terrorists remains bombs and guns. Computers have yet to kill people. Of more concern are those areas

where worms, virus, and other afflictions cause real damage to networks and computers, (Green, 2002). Cyber terrorism however looks like it might be more terrifying phenomenon if the skills of malevolent computer whizzes ever combined with the criminal actions of bad guys gifted in explosives, poisons or other forms of mass destructions.

The issue of terrorizing via the Internet is a lot more significant on an individual level. Cyber stalking, as it is known, has been defined as: “an extension of the physical form of stalking… where the electronic mediums such as the Internet are used to pursue, harass or contact another in an unsolicited fashion,” (Petherick, 2006). While typically thought of as a crime of deceitful anti-social middle age males, cyber stalking is something perpetrated by a surprisingly wide age and socioeconomic range—and a third of stalkers are women (ZDNet, 200).

The resources of reach, data, and the characteristic of invisibility enable stalkers to victimize their prey from afar if they choose. The effects of cyber stalking have and do end with genuine contact between stalker and victim. According to CyberAngels.org, “When a stalker takes it "offline" they are far more likely to pose a physical threat to the individual being stalked,” (Cyberangels.org, 2006). The organization counsels contacting the FBI or local law enforcement officials immediately. Cyber stalking can occur when the stalker happens to develop a particular interest in a victim and uses the power of the internet to these ends and sometimes it can begin with the internet itself and encounters in chat rooms or other methods of online contact. And sometimes this ends very

badly, particularly when those bent on stalking are given the easy access to victims that is afforded by sites like MySpace.com

Two current murder investigations, the death of 14-year-old Judy Cajuste found strangled and naked in a Newark, New Jersey, garbage bin and 15-year-old Kayla Reed who was found dead in a canal in Livermore, California, may be related to cyber-stalking according to what authorities are saying, (Apuzzo, 2006).

With all the frightening scenarios playing out daily and throughout the world, wiredkids.org (2006) makes it clear that unlike the physical world, so much control over the situation remains in the hands of the victim. As the site—which bills itself the largest online safety and help group—points out, 100% of all victims go willingly to meet their victims. In the case of older victims there is a significant, commonsense advice to guide personal behavior including guarding private identity.

An Australian site counsels that parents take a broad view of the problem in three potential problem areas for kids:

- Content (what they may view online)
- Contact (someone trying to meet them in person after initial online contact is made)
- Commercialism (being exposed to inappropriate advertising and marketing messages), (NetAlert, 2004)

For parents, there are numerous guides (including common sense) that urge parents to recognize behavior indicative of a problem, encourage proper but monitored use of the internet and to watch for sudden appearances of new friends outside what would be considered normal. Wiredsafety.org has an

“Online Parent Guide” that offers a wealth of advice relevant to adults and children alike including:

> Don't tell people personal things about yourself. You never really know who you're talking to online. And even if you think you know who you are talking to, there could be strangers lurking and reading your posts without letting you know that they are there. Don't let your children put personal information on profiles. It's like writing your personal diary on a billboard, (WiredKids, 2006).

Stalkers are not always anonymous either. In some cases, they can be as close as co-workers. One story of a spurned IT employee’s obsession with an attractive female clerk illustrates. When the worker’s on-the-job harassment of the worker got him fired, he was still able to use his knowledge of his company’s system to harass her by email, play tricks on her by misuse of databases and create numerous other problems. Though he may have been suspected, he was clever enough so that his new stalking was un-provable, to a point. His one mistake occurred when he mistakenly used his new employers company email system to engage in his harassment. That not only got him fired from the new job but had him facing indictment as well, (ZDNet News, 2001).

When a significant new force becomes part of daily life, societies have to adjust. I believe this is the case with much of Internet security, particularly as it relates to cyber crime. Stalkers will always be there, but the next generation of parents will themselves have greater commonsense and awareness of the dangers. Ideally, the power of technology itself will result in new tools that make it easier to track and identify stalkers. With these, a better educated society and coordinated government or public/private cooperative effort, cyber stalking and

other types of online crime will result in a safer online community for everyone.

Urban Legends, Hoaxes: You Can't Believe Everything—But Can You Believe Anything?

I have to admit that there is a certain quaintness or charm to some of the urban legends that I have come across in past years as well as those sampled or previewed at snopes.com. I think perhaps that this is because these rumors, half-truths, fantasies and examples of tomfoolery somehow take the predictable edge off of something that should be very predictable and rule bound. And, in some cases, they appeal to the masses casual belief that the fix is in…and a great deal is to be had out there for anyone who knows the secret. I believe they also succeed because as far-fetched as some of them sound, there is a corps of people who will believe them. And in some cases they have some genuine truth to them. For example, there is the boy who was suffering from terminal cancer and wanted to get into the Guinness Book Of Records for receiving the most cards from well wishers. The boy was suffering from the disease and did get into the Book. But his cancer has been in complete remission and he is still receiving cards—even though his story began circulating in 1991 (Imler et al, 1998).

But in another way, urban legends illustrate the destructive power that can occur when misinformation meets information technology. The Applebee's example is just one area example of how a widely and rapidly disseminated falsehood can cost business plenty. But they also cost us all plenty in wasted time and lost productivity. The Oliver North / Osama Bin Laden is one I have

heard discussed by co-workers, clients and numerous others over the past three years. And despite remembering the Oliver North Testimony in the late 80s, plenty of people are willing to argue that they remember exactly who North was warning the world about 18 or 19 years ago. But the fact is, it was Abu Nidal, a menacing and well-known Palestinian terrorist (North, 2004) . Here, the legend had a sliver of truth to it in that Oliver North did warn the world. But how the person who started this one could confuse the names Osama Bin Laden and Abu Nidal is a mystery—unless all middle eastern names just sound the same to him. Then the power of the Internet magnified this misunderstanding many times over. The same can be said for many of the 911 Urban Legends including:

- There were more than 4 terrorists
- England was also attacked
- One of the planes was shot down
- People in the Towers had advance warning

(Emery, 2006)

In a lot of ways, urban legends have an effect similar to chain letters. People want to believe certain things and they want to be among the first to tell their friends, family and co-workers. While often of relatively benign consequence, it is easy to see how human nature can be easily exploited into believing them. What strikes me about some of the best-known hoaxes is that there is a degree of believability to them. And they prey on human nature's desire to believe.

On one level some people who didn't think about it very deeply might be able to see logic in Applebee's trying to boost their local image through a "viral marketing" campaign like the free dinner hoax. And I think that for some businesses, the cost of an urban legend is real but almost unbeatable. For

example, the idea that a tooth will dissolve in Coke (Snopes.com, 2006), in a day is so widely disseminated that I have heard a hygienist at my dental office repeat it—and she is someone who should know better. But it is not too far from the long held notion that “candy will rot your teeth.”

I think that Snopes, Scambusters and other sites are also valuable to these efforts. Ideally some kind of site that links fact-checking resources of the mass media with those of the business world would be ideal aids in the fight to discern what is true, what is false and what is only partially true. Coke (or any soft drink maker) just has to be ready in instances like these to combat the falsehood with relevant believable facts that are easily attainable on their website. It is noteworthy that although it has moved the response to the free dinner hoax off of its front page anyone without their “pop-ups” turned off gets that message immediately, (Applebees, 2006). And I am not sure to what degree Applebee’s forthrightness mitigated their losses in the “free dinner” hoax, but it had to help some. And whether or not it did help, it was the right thing to do.

Phishing For Fraud Opportunities

The term “Phishing” seems far too gentle and good-natured for the crime it describes. It conjures up fun-loving band imagery or the colorful entrepreneurs, Ben & Jerry selling Phishhead Ice Cream. Instead, Phishing is something that costs individuals significant money in time and lost productivity and directly in the money they are defrauded out of, endure risks to their credit and privacy. Perpetrators are becoming more aggressive, too. Using the familiar email

methods and praying on people's trust of certain domain entities, they have developed spear-phishing techniques which mimic the sender address of a person's company IT department, (Terdeman, 2005).

I was first a victim myself a number of years ago when what appeared to be an AOL email requested an update of account information from me. Forgetting temporarily about AOL's often repeated caveat that it would never ask for my password, I took the *phisher*man's bait and gave up the goods he or she was looking for. Shortly thereafter I noticed that my name and password wasn't working and contacted AOL to learn that my account had been shut down because as they said, literally thousands of emails were going out from my address. After a brief period with the AOL rep, I was back up and using my account. However I noticed that once I was in my account, I was myself deluged with hateful emails from irate people who'd apparently received some kind of lewd, licentious or otherwise disgusting email from me.

And yet one would think that someone who's well educated, Internet savvy and reasonably wary by nature would learn. Not necessarily. In November, shortly after purchasing something on EBAY, I received an account verification notice from eBay—or so I thought. Like my experience with AOL, this phishing expedition succeeded in getting me to give them my eBay password. This time, however, I realized my mistake the instant I clicked my mouse. I got onto eBay and quickly changed my password myself. I never had a problem either, but it served as a wake-up call.

According to PCMagazine, the eBay fishing scam is apparently one that is wide ranging, as PC magazine has given coverage to the exact scam that hooked me.

> Looking at the eBay phishing message in figure 1 , it appears to be a legitimate message, sent from aw-confirm@ebay.com, the standard e-mail address for eBay announcements. The logos are linked directly back to eBay's site, and you can even click on the links on the bottom to get to eBay's own help and forums. (Rupley, 2003)

Apparently it is hard to get a close handle on the actual costs of phishing. Banks and financial institutions are reluctant to reveal the impact of the practice on their operations for fear that their online business might be negatively affected. In mid-2003 an Australian bank announced that it had several million dollars on reserve to cover losses from phishing (Rupley, 2003).

There are, of course, a number of resources to combat phishing. The first and most basic being well educated computer-using public. The greater the vigilance on the part of businesses and consumers, the more the practice can be made less-rewarding to perpetrators. American Express recently notified me of a phising scam that it is facing and so I will be continuously careful with anything that appears to be from them. Their notice describes all the tricks that phishing victims have become familiar with:

> Techniques such as a false "from" address, the use of seemingly authentic logos from financial institutions, or Web links and graphics may be used to mislead consumers into believing that they are dealing with a legitimate request for personal information, (American Express, 2006).

Thanks to this information, I will look very carefully at everything that I get in email that appears to be from American Express. But, this also means I may

consider even their legitimate attempts to contact me as “phishing.” And one danger of the practice is that I might ignore or delete an email that is really worthy of my attention—just another one of the subtle, indirect costs created when the phish hooks get to us.

Conclusion

This exercise strikes me as a good news/bad news scenario. On one hand, looking into the “dark side of the internet” reveals problems deeper and more pervasive than the typical user is likely to consider while surfing the web, typing away in Microsoft word or emailing friends. Yet there is something empowering in knowing that much of our victimization can be prevented or remedied—from proper spam filtering to simple vigilance to prevent identity theft. Still, I would like to see the matter addressed through some kind of industry-government consortium specifically established to combat misuse through a combination of education and information, but also with some kind of enforcement powers. After all, we have coast guards to protect our shores, the FBI to investigate federal crime and Drug Enforcement Agencies to deal with the problem of illegal narcotics. So why not create an organization that combines the best and brightest in business and government to literally police the online world? Such an organization may not solve every problem (particularly those with off-shore origin), but it would certainly make the Internet less hospitable world for hackers, virus builders, cyber stalking predators and others. Naturally creating such an entity would also require negotiating myriad trade issues, international

considerations and free speech considerations. But like anything in democratic societies, the momentum of public opinion can be a powerful motivator.

But even in the absence of such a policing organization, the fact that consumers vote with their dollars could spur software makers, hardware sellers and service providers to become more innovative in combating the dark side.

# # # #

References

Commercial Business Intelligence (2006). Minimize the loss. Maximize the opportunity. Commercial Business Intelligence Website. Retrieved February 9, 2006, from, http://www.cbintel.com/cihackerdanger.htm

American Express (2006). About email fraud. American Express Website. Retrieved February 17, 2006 from, http://www10.americanexpress.com/sif/cda/page/0,1641,21372,00.asp

Applebees (2006). Applebees gift certificate hoax. Applebees Corporate Website. Retrieved February 10, 2006, from, http://www.applebees.com/popup.html

Apuzzo, M (2006). Teens Putting Themselves at Risk Online. Netscape Gadgets & Tech Website. Retrieved February 19, 2006, from, http://channels.netscape.com/tech/story.jsp?idq=/ff/story/0001%2F20060204%2F0725235218.htm&sc=1333&ewp=ewp_news_0206teens_online_risk

BBC News (2006). Limited damage from Nyxem virus. BBC News Website. Retrieved February 18, 2006, from, http://news.bbc.co.uk/2/hi/technology/4677022.stm

BBC News Online (2006). PC viruses hit 20 year milestone. BBC News Online Website. Retrieved February 18, 2006, from, http://news.bbc.co.uk/2/hi/technology/4630910.stm

Better Business Bureau (2006). New research shows identity fraud growth is contained and consumers have more control than they think. Better Business Bureau Website. Retrieved February 14, 2006, from, http://www.bbb.org/alerts/article.asp?ID=651

Business Wire (2003). Basex names spam its product-of-the-year; spam's impact on it spending and productivity major factor in selection. Business Wire Website. Retrieved February 14, 2006, from http://www.findarticles.com/p/articles/mi_m0EIN/is_2003_Dec_22/ai_111500758

Chubb Insurance (2006). CyberSecurity by Chubb. Chub Insurance Website. Retrieved February 15, 2006, from, http://www.chubb.com/businesses/csi/chubb822.html

Crowley, M. (2003). Computer security: Searching for the full truth. Las Vegas Review Journal Website. Retrieved February 14, 2003, from, http://www.defcon.org/html/links/dc_press/archives/11/reviewjournal-compsec.htm

CyberAngels (2005). Responding to Cyberstalking. CyberAngels.com Website Retrieved February 19, 2006, from http://www.cyberangels.org/stalking.html

Emery, D. (2006). Rumor Watch: 9/11 Terrorist Attack on U.S. About.com Website. Retrieved February 18, 2006, from, http://urbanlegends.about.com/library/weekly/aa091101a.htm

Federal Trade Commission (2003). Spam forum. FTC Website. Retrieved February 11, 2006, from, www.ftc.gov/bcp/workshops/spam/Supplements/smith.pdf

Green, J. (2002). The myth of cyberterrorism. Washington Monthly Website. Retrieved February 15, 2006, from, http://www.washingtonmonthly.com/features/2001/0211.green.html

Imler, D., et all (1998). Folklore on the Internet. Miami University Psybersite. Retrieved February 17, 2006 from http://www.units.muohio.edu/psybersite/cyberspace/folklore/legends.shtml

Small Business Pipeline (2006). Small Businesses Get Four Times The Spam Of Larger Enterprises. InternetWeek Website. Retrieved February 14, 2006, from, http://internetweek.cmp.com/177105435;jsessionid=A15TR3HAKA134QSNDBECKHSCJUMEKJVN%20)

Metz, C. (February 21, 2006) The sorry state of security. *PC Magazine.* 25, 78-83.

NetAlert (2004). Parental concerns addressed. NetAlert Safety Newsletter Website. Retrieved February 17, 2006, from, http://www.netalert.net.au/print.asp?file=/01533-August.asp

North, O., (2004). Feeling the draft. Townhall.com Website. Retrieved February 18, 2006, from, http://urbanlegends.about.com/gi/dynamic/offsite.htm?site=http://www.townhall.com/opinion/columns/ollienorth/2004/10/22/13417.html

PCMagazine, (2003). Lets go phishing. PC Magazine.com Website. Retrieved February 18, 2006 from, http://www.pcmag.com/article2/0,1759,1838798,00.asp

Petherick, W. (2005). Cyber-stalking: obsessional pursuit and the digital criminal. Crime Library Website. Retrieved February 15, 2006, from http://www.crimelibrary.com/criminology/cyberstalking/

Pollit, M. (2006). Cyberterrorism – fact or fancy? Georgetown Department of Computer Science Website. Retrieved February 14, 2006, from, http://www.cs.georgetown.edu/~denning/infosec/pollitt.html

Rupley, S. (2003) Fighting phishing. PC Magazine.com Website. Retrieved February 17, 2006 from, http://www.pcmag.com/article2/0,1759,1407048,00.asp

Rupley, S. (2003) Warning: Look out for the Ebay Scam. PC Magazine.com Website. Retrieved February 17, 2006 from, http://www.pcmag.com/article2/0,4149,1402431,00.asp

SecurityStats.com (2006). Virus related statistics. Security Stats Website. Retrieved February 18, 2006 from, http://www.securitystats.com/virusstats.html

Simonds, L. (2005). Intruder alert: Arxceo aims to guard the gateway. SmallBusinessComputing.com website Retrieved February 11, 2006, from, http://www.smallbusinesscomputing.com/testdrive/article.php/3570541

Snopes.com Website (2006). Cokelore. Retrieved February 10, 2006, from, http://www.snopes.com/cokelore/cokelore.asp

Syracuse University Website (2006). Adversaries. Retrieved February 12, 2006, from, www.hpdc.syr.edu/~chapin/cis583/Adversaries.pdf

Terdeman, S. (2005). Spear-phishing on the rise. PC Magazine.com Website. Retrieved February 18, 2006 from, http://www.pcmag.com/article2/0,1759,1863470,00.asp

Totty, M. (February 13, 2006). The Dangers Within. *The Wall Street Journal.* 247, R1-R-4.

UIUC Library (2006). Identity Theft. University Of Illinois-Urbana Champaign Website. Retrieved February 17, 2006, from, http://www.library.uiuc.edu/ugl/subjects/identitytheft.html

University of Arkansas Department of Computing Services (2003). Chain email and spam. University of Arkansas Website. Retrieved February, 15, 2006, from, http://compserv.uark.edu/policies/chainspam.htm

University of Oklahoma Police Department (2006). Chain Letters. University of Oklahoma Website. Retrieved February 14, 2006, from http://www.ou.edu/oupd/ichain.htm

U.S Postal Service (2006). Chain Letters. U.S Postal Service Website. Retrieved February 14, 2006, from http://www.usps.com/postalinspectors/fraud/chainlet.htm

Weimann, G. (2004). Cyberterrorism: how real is the threat? U.S. Institute of Peace Website. Retrieved February 17, 2006, from, http://www.usip.org/pubs/specialreports/sr119.html

WiredKids (2006). Parenting online. WiredKids.Org Website. Retrieved February 16, 2006, from, http://www.wiredkids.org/parents/parentingonline/parentingonline.pdf

Young, J (2005). Identity theft now global problem. Politics Ol.com Website. Retrieved February 18, 2006, from http://www.politicsol.com/news/2005/04-27-identity-theft-now-global-problem.html

ZDNet (2006). Cyberstalking rears its head in the workplace. ZDNet News. Retrieved February 15, 2006, from, http://news.zdnet.com/2100-9595_22-529416.html