

The Multi-Billion Dollar Spam Threat

Stephen Cobb, CISSP
Chey Cobb, CISSP

(An earlier version of this article first appeared in our weekly column, Safe & Sound in the Cyberage, in the electronic newsletter Newsscan and at www.newsscan.com)

We'd be very surprised if any reader of this article could find even one good word to say about spam, that seemingly endless stream of unsolicited email, stuffed with offers to sell you things you don't want to buy and enlarge parts of the human anatomy you may not even possess. But as unsavory as most folks find this subject, we need to bring it up, because spam has now gone way beyond annoying, right pass disgusting, to downright costly. According to Ferris Research, spam set U.S. organizations back \$8.9 billion in 2002, based on lost productivity and the consumption of IT resources and help-desk time. A more recent study by analysts at Radicati Group put the worldwide cost to companies at \$20.5 billion in 2003. They predicted that figure reach \$198 billion by 2007.

It Gets Worse

Unfortunately, those figures are not, in our opinion, an exaggeration. Even worse, we don't think they reflect the full measure of spam's economic impact, not by a long way. Even as companies invest in spam filtering software to screen it out of their networks, and ISPs invest in more and more storage and bandwidth to cope with the rising tide of spam messages (which now make up half of all email traffic), the bigger cost may be the effect on companies of the spam that their customers get.

We are not talking about the negative effect that sending spam has on the company that sends it. Respectable companies gave up sending spam some time ago; the negative consumer backlash is just too great for any sane executive to sanction unsolicited commercial emailings. What we are talking about are the messages that spammers send in the name of your company, what we call "bogus email." This is spam that attempts to pass for legitimate email by making unauthorized use of established brand names and logos.

A classic example is the mortgage offer spam that uses the brand name and logo of a respected bank or real estate firm to persuade people to supply personal data to the spammer's web site (under the pretense of confirming a pre-qualified mortgage). Such data can then be sold by the spammer. If phone numbers and physical addresses are obtained, these can be sold as sucker lists for bottom-feeding boiler-room peddlers of things like "limited edition" coins. Any email addresses harvested this way can also be sold—as "confirmed" lists used to send more spam.

A variation of this spam-scam leverages the good name of established software brands, such as Adobe and Symantec, to harvest data that includes your credit card number. Ever wonder why Symantec would authorize those email marketing offers that knock 90 percent off the price of its products? Well it doesn't. Those messages—often featuring a product that people tend to buy in a state of panic, such as Norton Antivirus—are either looking to grab your credit card or sell you pirated software.

The Multi-Billion Dollar Spam Threat

It is a sad fact of Internet life that consumers receive millions of emails every day that use hijacked brand names and corporate logos to further the—often illegal—profiteering goals of the sender. This unauthorized use of valuable corporate assets ranges from the merely sneaky to the blatant theft of corporate identity, perpetrated for the sole purpose of defrauding consumers. Some of those consumers lose money.ⁱ Exactly how much is lost by consumers is not known, but we do know that the cost to companies who rely on email is significant.

The cost to companies like Symantec begins with the need to divert staff and resources to try and stop this dilution of their brand. But that may just be the tip of the iceberg compared to the effect that brand dilution has on revenues. The combined annual revenues of the Fortune 1000 are roughly \$7 trillion. If top brand names account for just 10 percent of that figure, and those names suffer a 10 percent reduction in revenue due to people's association of them with unpleasant email experiences, we are looking at \$70 billion in lost value, per year.ⁱⁱ

Hand Wringing

You know spam is a problem when you turn on the news and see a reporter talking to you from the Federal Trade Commission's Spam Forum in Washington, D.C. That is what we saw on April 30 this year, along with a lot of hand-wringing about what a menace spam has become. The focus of most reporters was the pain that spam causes the consumers who find it in their inbox. A close second was the billions of dollars companies pay to prevent spam from flooding their networks. We heard very little about the tendency of fraudulent email to undermine brand value. So let us present a scenario to make it a little more real. Imagine you run a company that has a thriving online retail operation. One day several thousand customers get email that says:

“As part of our continuing commitment to protect your account and to reduce the instance of fraud on our website, we are undertaking a periodic review of our member accounts.”

The message displays your corporate logo and the “From” address is at your company's domain. However, your company did not send the message. Even worse, the message goes on to say:

“You are requested to visit our site by following the link given below. Please fill in the required information. This is required for us to continue to offer you a safe and risk free online shopping environment.”

The link contains your site's domain name, so it looks legitimate, but the link leads to a different site, that looks a lot like yours, but actually harvests your customers' account numbers, user names, passwords, and possibly credit card numbers. This is not an imaginary scenario. These quotes come from a fraudulent email that we, and millions of other consumers received recently.

Another Threat Surfaces

If consumers continue to get this type of email, the effects are going to be very serious for some companies. Apart from the erosion of brand value that we talked about earlier, there is the possibility of legal action by consumers who have been duped, cheated, or had their identity stolen due as a result of such messages. The perpetrators of these scams are hard to find and harder to prosecute. So lawyers for the plaintiffs are going to look to those they can find, the same

The Multi-Billion Dollar Spam Threat

companies whose names and logos are being misappropriated. Right now some product liability lawyers are bound to be asking themselves these questions:

- Could Company X have done more to prevent dilution of its brand by bogus email?
- Could said company have done a better job of protecting consumers from those who are perpetrating email fraud in the company's name.

Class action lawsuits along these lines, from shareholders and consumers, are not hard to imagine. Without a miraculous end to the flood of spam, the likelihood of such lawsuits will only increase over time, especially if companies fail to take stronger action in defense of their good names. How and when companies respond to this threat will determine the extent to which they are exposed to accusations of negligence with respect to both brand dilution and customer protection.

But is there anything companies can do, apart from encourage the large Internet Service Providers to get their act together to put an end to spam? The challenge can seem daunting when you look at the low cost of entry into mass emailing and the relative ease with which their digital assets can be ripped off. After all, these days anyone can make a pixel-perfect, zero-cost copy of whatever logos, trademarks, and signage appears on your company's official web site.

With HTML email it is easy to make official-looking messages and hide hijacked links. A screen shot of a real world example, the recent Bank of America "technical update" spoof, is included at the end of the article to illustrate this point. When you view the message it certainly appears to be from Bank of America and the link looks like it leads to Bank of America.

Even when the spoofed email is just a text message, the links are hard for the average consumer to decipher as false. Consider this one:

```
http://cgi3.BigBrand.com:aw-cgiBigBrand
ISAPI.dllSignInRegisterEnterInfo&siteid=0co_partnerid
=2@210.103.121.131/BigBrandcgi/>http://cgi3.BigBrand.com:
aw-cgiBigBrandISAPI.dllSignInRegisterEnterInfo&siteid=
0co_partnerid=2@210.103.121.131/BigBrandcgi/
```

What would the average consumer make of this? It sure looks like this link takes you to BigBrand.com, right? But this convoluted link actually takes you somewhere else, a server with no name, just an IP address of 210.103.121.131.

This example was pasted directly from a fraudulent email we received, except we have changed the name of the targeted company—a household name you would recognize—to BigBrand, out of respect (and fear of lawyers). We also changed one or two characters to prevent obvious reengineering. The point is, something that looks a lot like the above was in a message that millions of consumers received. If clicked, it led the hapless consumer one step closer to becoming a fraud victim.ⁱⁱⁱ

The Two-Pronged Strategy

In some ways it might be tempting for some companies to conclude there's nothing they can do to stop this sort of thing, apart from launch the occasional token prosecution and put up a consumer

The Multi-Billion Dollar Spam Threat

help line. However, this view is not supported by the facts. Remember those questions that the imaginary lawyers were asking earlier? If we were called to testify today, we would probably have to answer “Yes” to both of them. The plaintiff’s lawyer might have to ask the court to treat us as hostile witnesses—we don’t believe suing victimized companies is the answer to the spam problem—but we cannot tell a lie: The problem can be addressed.

How? With a strategy that combines two proven tactics: positive discriminators and a preponderance of discouragement (if we wanted to be cute, we could call this strategy PD² or PD-squared). A wide range of businesses have faced analogous challenges in recent years. Consider counterfeit goods, fake credit cards, and pirated software. There is no way to stop people trying to make counterfeits. But that does not mean nothing can be done. The answer is to first adopt positive discriminators, for example, inform consumers that all products which lack X are inferior rip-offs, where X is a hard-to-counterfeit mark, like a hologram, embedded logo, and such like. This is then backed up by a preponderance of discouragement, a framework of technical and economic obstacles, legal penalties, and enforcement actions.

Bogus email can be tackled in the same way. The positive discriminator can be something you place in all company email. Today, the technology exists to generate a unique, cryptographically protected, spoof-proof seal or “trust stamp” in each outbound email (this technology is in use and millions of stamped messages have been sent by consumer companies). The mere presence of this seal will satisfy most recipients that the email is official, but they can also verify the fact using a simple client-server interaction).^{iv}

You then put everyone on the planet on notice, via your web site and all the other branding channels you use, that only those messages which contain the official trust stamp are official messages and any message that purports to be from your company but lacks a verifiable trust stamp is bogus, illegal, and should be reported.

Having deployed the required positive discriminator in your email, you will find the preponderance of discouragement falls neatly into place. There are plenty of laws under which to prosecute bogus email (trademark and copyright infringement for a start, plus deceptive business practices, which the FTC is eager to enforce against spam). But even more importantly, you have, through the adoption of a positive discriminator, significantly increased the economic obstacles to fraudsters seeking to profit from abuse of your good name.

We say “significantly” because of the proven equation that says anything which raises the bar for successful counterfeiting also raises the profile of counterfeiters, making them easier to catch. For example, if your currency includes \$50 bills of which credible copies can be made on Xerox paper with a \$99 inkjet printer, the profile of the counterfeiter is very low. The profile is much higher if you alter the design of the \$50 bill so that credible copies require a \$500,000 dye-sublimation printer and a supply of paper that can only be had from two sources. Note that altering the design did not prevent counterfeiting, but it did three very useful things:

1. Reduced the number of people who are likely to try counterfeiting \$50 bills,
2. Made people who counterfeit \$50 bills easier to catch
3. Made it less likely that the public will be fooled by fake \$50 bills.

Due Diligence

Amazingly, we have heard, as an argument for not making the effort to place trust stamps in consumer email: “spammers will just fake the trust stamps.” This strikes us as a fairly preposterous lack of due diligence. Yes, spammers will try to fake the trust stamps. But “try” is the operative word. To succeed in any plausible way is non-trivial, and you have raised the bar for imposters. You have made a good faith effort to employ a remedy that is at your disposal.

About ten years ago, the Royal Bank of Scotland introduced debit cards that had the account holder’s photograph and signature printed on them. Almost immediately, debit card fraud dropped by 70 percent. About five years after that we were telling some friends in America about this and got the following response: “That wouldn’t work here, store clerks wouldn’t bother to check the photo.” But guess what? Several American banks now offer this feature anyway.

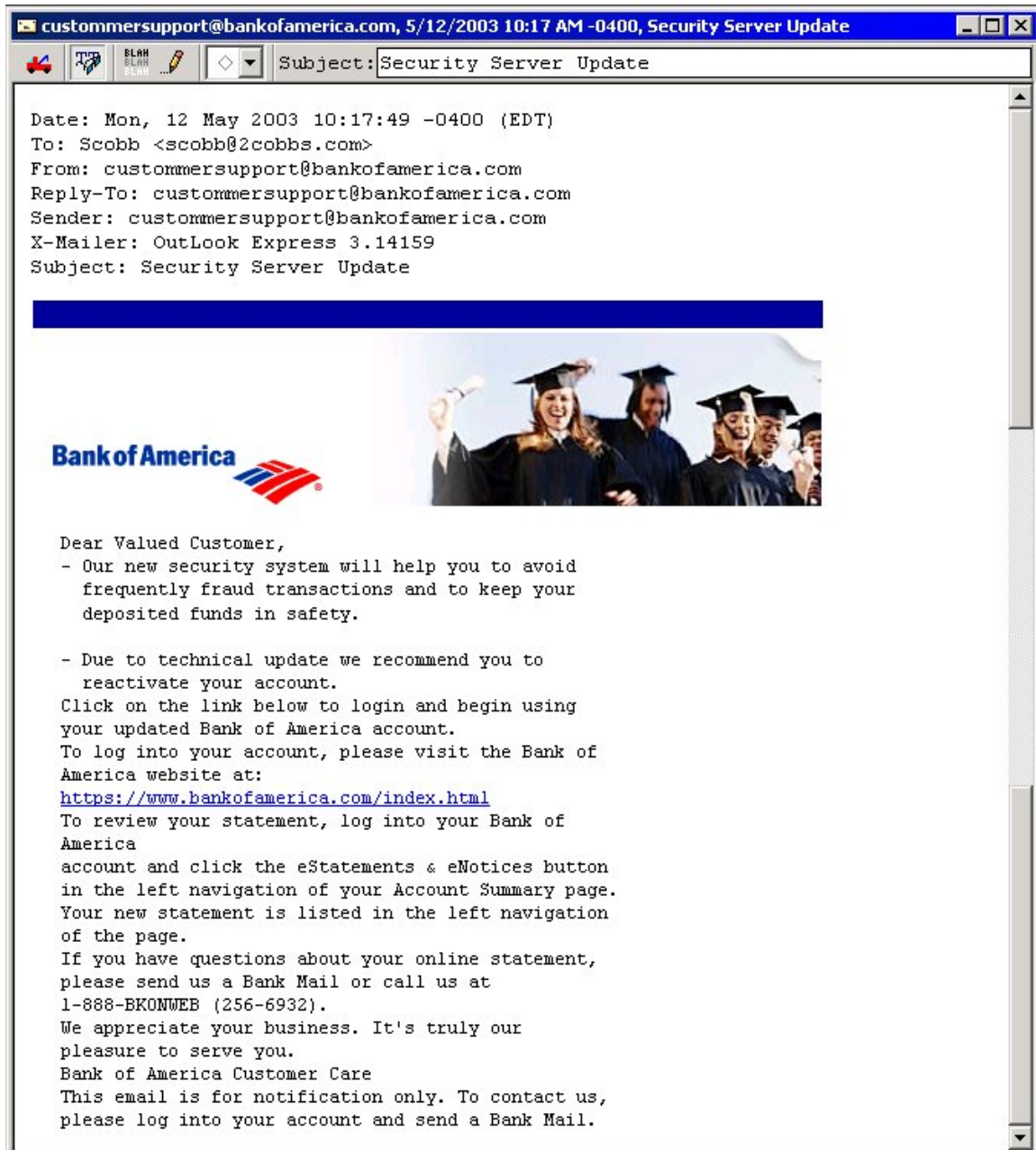
If your company uses the Internet to communicate with customers you need to realize that right now the average consumer has no way to consistently and immediately distinguish between bogus email (fraudulently purporting to be from your company) and genuine email that really is from your company. Not only is this a major source of frustration and risk for consumers, it is the main reason why fraudsters continue to send bogus email in your company’s name. If you give consumers a positive, non-spoofable means of identifying genuine email, then the fraudster’s ratio of return-on-effort plummets. At the same time, you greatly increase your ability to claim due diligence in the areas of trademark defense and customer protection. Not to mention the fact that your consumers will likely thank you for making an effort to reassure them.

Big Picture

Beyond the possibility of lawsuits against companies that don’t do more to prevent consumers from being confused and ripped off by bogus email, beyond the erosion of brand value, there is an even bigger picture. For years now, spam has surged like a flood-swollen river through the Internet infrastructure, eroding people’s faith in what they see and read, both online and offline. Sound implausible? Imagine how you would feel about network television advertisements today if, for the last ten years, they had featured nothing but blatant rip-offs and sick pornography. Imagine if everyone in middle America knew at least one person who had suffered fraud or identity theft because of a primetime TV ad. That’s where spam has taken email and it threatens to drag other forms of marketing down with it.

This is not just an opinion. A recent PlanetFeedback study found that the more spam and pop-up ads consumers encounter, the angrier they are about all forms of advertising, even event sponsorships and radio/TV advertising. These consumers are “willing to take drastic action to control or outlaw unsolicited emails.” In fact, more than one-third support ‘do-not-email’ regulations, 27 percent support taxes and fines on spam, and nearly 25 percent support outlawing spam. The bottom line for companies, even ones who don’t use email much at all, is that spam is eating away at your ability to mount successful ad campaigns. For those who believe that advertising and marketing create jobs and profits and drive the U.S. economy, this is very bad news indeed.

The Multi-Billion Dollar Spam Threat



Notes:

ⁱ Total dollar loss from Internet fraud in 2002, as reported to the Internet Fraud Complaint Center, run by the FBI and the National White Collar Crime Center: \$54 million. Over 48,000 separate consumer complaints were referred for prosecution. In many cases, losses were over \$1,000 per consumer.

ⁱⁱ You could argue that the value is not lost because demand is not reduced, just shifted to competing products; but negative experiences in a product category can actually reduce demand for competing products. Also, if it is your company's revenue that is being eroded, you will surely see it as a loss.

ⁱⁱⁱ You can buy software to "obscure" URLs so recipients can't see where links leads before they click them.

^{iv} One such technology is Trusted Sender™ from ePrivacy Group (Disclaimer: Stephen helped developed Trusted Sender).