

SPAM:

More than just a nuisance.

SPAM is a real cost burden on business. Reports estimate that US businesses spend close to \$4 billion annually to remediate the aftereffects of SPAM. This figure does not count the endless number of undocumented hours of lost employee productivity.

What defines SPAM?

SPAM covers many forms of fraudulent email. Much of it attempts to appear legitimate by using the look and feel of well-known organizations such as eBay, Citibank, Amazon, etc. The contents of SPAM messages can span from offering software and diet pills to “phishing” and distributing “badware”. (The term badware is a new word encompassing viruses, spyware, malware, and other malicious software into a single term.)

Why is spam so prolific?

SPAM is a business, and sadly it works. On average, spammers send between 50 and 70 million emails per day. Given only a .05% response rate that still accounts for 25,000 to 35,000 leads. It is estimated that one quarter of those responders have acted upon the emails revealing personal and financial information. In comparison to direct mail campaigns, spammers enjoy a much higher return for a much lower investment.

So what does this all mean?

Unlike the real world, interacting with spammers and thieves can seem as professional as connecting with legitimate businesses. In several recent cases, so-called anti-spyware and anti-SPAM programs were circulated

that did nothing to stop SPAM, but rather turns your unsuspecting PC into a distribution point for SPAM. Those free tools or deceptive forms could be out to steal your bank account codes or your company’s credit identity. And in business this can compromise your customers and ruin your reputation.

How can I prevent from being the victim?

Technology is getting better at cleaning out spam, but as smart as the software gets, the spammers are finding ways around these systems. This is why a two-phased approach involving both software and people is key to success.

1. Anyone who represents your company needs to be aware of the dangers of SPAM. Make sure your staff knows who your vendors and representatives are. If you are suspicious, call the vendor or rep back and make sure it was their request. Never give confidential account numbers, passwords, or instructions over email.

2. Use a hosted SPAM filtering service. This way you won’t be caught needing to constantly update your software as methods change, and you can rely on your vendor’s system to provide backup in case your system faces downtime.

With better tools and better knowledge, you can help safeguard your business from the virtual theft of your reputation.