Experts say spam e-mail grows because it works

January 4 2010, By Tim Barker

It was Ben Franklin who made the famous comment about death and taxes being the only things certain in life.

Of course, old Ben didn't have Internet access. Otherwise, he would have added spam to the mix.

No matter how many laws or brilliant minds we throw at the scourge of electronic communication, spam always finds a way.

It finds a way because -- well, it works.

"The things that wind up in your in-box: They are there because people buy them," said Brandon Phillips, chief executive of Lashback, a St. Louis-based firm that monitors and rates bulk e-mailers based on their compliance with federal anti-spam laws.

Strange as it may sound, there are people out there willing to spend money on deals most people consider absurd. More than just a few, actually, according to a study released over the summer by the Messaging Anti-Abuse Working Group, a consortium of Internet and technology providers. The study found that half of Internet users have opened e-mail they thought was spam. Of those, 12 percent did it because they were interested in the product.

Exactly how much spam is out there is a source of some debate. Some studies have suggested it's around 85 percent of all e-mail. Some say it's

90 percent. Microsoft recently pegged it at 97 percent. Pick whichever number you'd like to believe. All that matters is that the vast majority of e-mail coursing through the Internet's veins is worthless, unwanted and sometimes dangerous.

Worse, most experts agree there's little hope you'll ever escape those unsolicited offers of free money, larger male members and secret weight loss techniques. Unless, that is, you unplug yourself from the net.

"People are sort of resigned to the fact they're going to get spam. It's just a question of how much," said Lorrie Cranor, an associate professor of computer science at Carnegie Mellon University in Pittsburgh.

It really comes down to money, and the fact that there is so much of it to be made by spammers, who need only a tiny investment to set up shop.

Generally speaking, all you need is an Internet connection ($20), an e-mail account (free), a list of e-mail addresses (about $50 for a million addresses) and a message to send. It takes just a few successful hits for the spammer to recoup expenses and turn a profit. The good ones can make thousands of dollars a day.

But there's also a more legitimate side of the business. And those are the ones who occupy the minds of the folks at Lashback. Phillips is quick to point out that reputable bulk e-mailers don't particularly like being called spammers.

Often, they're doing marketing work on behalf of companies like NewEgg, Match.com and eHarmony. And they generally adhere to rules set forth in the so-called CAN-SPAM act of 2003.

That's the law that, among other things, requires unsolicited commercial e-mail to include an "unsubscribe" feature that's supposed to take you

off the mailing list.

Lashback offers a monitoring service that rates bulk e-mailers based on how well they comply with law. That information helps retailers and service providers decide who to use for their e-mail marketing efforts.

Just how well those unsubscribe buttons work has long been a matter of debate among security experts. Some advise you to never click the unsubscribe link, since it effectively tells the spammer that yours is a valid e-mail address.

"What we found out is that sometimes "unsubscribe" works. And sometimes it gets you on a list to be sent more mail," Phillips said.

Still, of the companies monitored by Lashback, he said the unsubscribe feature works at least 95 percent of the time.

Of course, legions of spammers out there make no effort at legitimacy. They are little more than pirates of the online world, pitching scams and spreading malicious programs.

You might even be helping them.

Much of the truly bad spam is essentially untraceable. Or, at least, it can't be traced back to the real senders, who often hide from authorities by using loose configurations of hijacked computers called "bot nets." It's a bit sobering to think that while you sleep tonight, your computer -- hijacked because it's infected with a virus -- could be sending out hundreds of thousands of spam e-mails.

On any given day, there are some 400,000 active bots in the world, according to Project Honey Pot, a group of developers and IT professionals who track spammer activities. The number has quadrupled

every year since 2004.

Naturally, one of the ways spammers gain control of others' computers is through spam. A common ploy is an e-mail warning that a computer has become infected with a virus. The e-mail urges the user to click a link for a quick scan and repair. It fixes nothing, and instead installs a virus allowing the computer to be used as a bot.

"Spammers have gotten really smart. They are very good at social engineering," said Suzanne Magee, chief executive officer of TechGuard Security in Chesterfield, Mo. "They know how to play on your fears."

They are also in a constant state of war with security experts and anti-virus firms who try to block spam before it ever gets to you. A common filtering technique looks for, and blocks, all e-mail that appears identical, figuring it must be spam, said Cranor, of Carnegie Mellon.

Spammers counter with programs that insert random spaces or words into the text, making each message slightly different.

"It's sort of an arms race," Cranor said.