It's the scourge of the Internet: flooding the globe's email servers night and day; billions of messages stalking inboxes, frustrating users, swallowing up bandwidth. Spam is sabotaging the world's email system but what's being done to fight it?

Based on 'Inbox Insanity' broadcast on Radio National's Background Briefing, 3 Aug 2003

Two years ago spam was a relatively small problem, representing about 10% of all email. Now it's everywhere, and it's doubling in volume every six months. On any given day, the world generates 20-billion email messages. It's estimated half of all this traffic is now unsolicited junk mail, or spam.

All this junk comes at a cost. There's lost productivity, calls to the help desk, damage to brands through fake emails and a huge strain on the network. Secretaries are refusing to sort their bosses' email because the amount of pornographic and offensive material is bordering on sexual harassment.

In the United States, spam will cost business $10 billion this year. That's the estimate from IT consultancy, Ferris Research. It says junk mail costs $10 per worker per month.

This increase in spam is threatening the future of email. If 50% of your email is spam, then you've got to start asking the question, Is this an effective use of my time?

The war on Spam

The war on spam is a technology race between the spammers sending the junk and the anti-spammers, the people blocking it and chasing the offenders. But because the spammers got going first, it's still a game of catch-up.

It's an irony that it's impossible to get in touch with either the spammers or the anti-spammers by email. On the frontline, the medium has been abandoned.
SpamHaus

Leading the global battle against spam is the London-based organisation, SpamHaus. It's been aggressively tracking the worst offenders since 1997 and is under constant cyberspace attack.

SpamHaus compiles evidence records on spammers to track who they are, what names they're using, what addresses they're using, and what domains they're using. Then they block the IP addresses.

These lists are powerful weapons against spammers because instead of filtering the mail, they actually jam it before it can be sent. It's like nailing a postbox shut. It annoys the spammers no end.

But just as there are many post boxes in the world, so too are there many email servers. Spammers are constantly on the lookout for servers which will accept and deliver their bulk mail without asking too many questions. These are called open relays or open proxies.

Anti-spam groups like SpamHaus also identify hardcore spammers and name them on ROKSO, the Registry of Known Spam Operators. To make the list, a person has to be thrown off three different ISPs for spam behaviour.

Who are the spammers?
Meet Scott Richter, a spammer who has made it onto the ROKSO list. He's 31, lives in Colorado and runs a business called Opt In Real Big. Every day he sends 80-million emails, mostly for other companies. Less than 1% of the people he emails respond. But it's enough. In four years the business has made him rich. His turnover is $20-million a year.

"The majority of the emails we send out are a variety of different products, some mortgage and debt leads, a lot of information about websites, information about new products that are coming out, health and beauty products. Just the whole gamut, a lot of ink-jet cartridges, credit card offers, it's a whole wide variety" says Scott.

Scott says he's a legitimate email marketer.

"We don't use false names, we don't encode our emails. We don't do those illegal activities and stuff as your hardcore basement spammer does. We just send high volumes of email, but all our IP space is registered to us, our domain names come to us, we have two to three ways in every email we send to be removed, we honour opt out requests, we honour the domain name's ban requests, we work with the large ISPs to be whitelisted so the mail can be delivered."

For a spammer, being blacklisted by SpamHaus can help rather than hinder business according to Scott.

"In the old days it used to affect us a little bit, but actually lately, stuff like SpamHaus actually helps our business, because people know there's a reason they're talking about us" he says.

---

**Spam terms**

**What is Spam?** - Unsolicited email that is commercial in nature. Spam takes its name from the canned ham satirised in a Monty Python skit.

**First spam** - The first known spam was sent in America in 1978. It advertised a new computer and was sent to several hundred users on what was then called Apranet.

**Opt in** - Users consent to receiving commercial email. If you sign up to a newsletter then you have opted in.

**Opt out** - Places the onus on the user to tell the company to go away, to remove you from their mailing list. The problem with this is that the user still has a major spam problem. Also, when a user replies and asks to be taken off the list this often serves instead to validate that the email belongs to a real person - making it more valuable.

**Big fry** - Eddie Marin, of Florida is one of the largest spammers in the US and he's responsible for about 200-million to 250-million spams a day.

**Profits** - It only takes one purchase in every million messages for a spammer to be in profit.

---

**Who opts in?**

According to Scott, of the millions of people he emails every day have all opted in. In other words, given permission to receive the message.
Anti-spam fighter Steve Linford says Scott Richter is just like the other people on the RIKSO list. They constantly blur the lines between what is permission-based email and what isn't.

"Scott Richter sends on average about 80-million spams a day and he will tell you that all of those 80-million people all opted in" says Steve Linford.

It's something very hard to verify, either way. All it takes to prove that spam recipients have opted in is provide an Excel spreadsheet with IP addresses and dates!

**Fighting with filters**

After blocking IP addresses, the best protection on offer for dealing with spam is email filtering. Filters often use heuristics, an artificial intelligence system using predictive technology to say that an email that exhibits the characteristics associated with previous emails is potentially spam.

The Internet Industry Association offered the chance to road test spam filtering products for free until the end of August 2003. One of the companies involved was MessageCare, a small Sydney business that opened in March. MessageCare offers a filtering product aimed at home users, the people with the least spam protection. It's cheap, there's no software to download and it promises an 85% success rate. It intercepts emails from the ISP or Internet Service Provider, checks the content and then passes it on to the end user. But mistakes can happen.

Many users and ISPs dismiss filtering technology because it's not 100% accurate. People are also paranoid about missing an email. To get around this problem some filter companies allow users to check their junk mail at the end of the month, in a case a wanted email has been caught by accident.

---

**Spammers fight back**

To beat the filters, the spammers are simply turning up the volume and cranking out more spam. Rather than sending one message to millions of people, they now send multiple variations to fool the filtering system. This is one reason why the amount of spam is skyrocketing.
If you're wondering why a lot of subject headers in junk mail contain typos, are spelt wrong, or look strange, it's because they're trying to outsmart the filters by disguising words or phrases.

**The Nigerian Spam**

A perfect example of this is the good old Nigerian Banking Scam. The typical Nigerian spam identifies an account in the bank, and asks for assistance in removing the money from it. "I want to transfer this money into a safe foreign account, but I don't know any foreigners. I'm contacting you as a foreigner because this money cannot be approved to any local bank here but can only be approved to any foreign account.'

All of these are random paragraphs in random order that essentially say the same thing every time.

It's this random use of words that makes the Nigerian spam hard for filters to detect. For this reason, Andrew Kent, Chief Executive of MessageCare says it's one of the smartest spams ever designed.

**Spoofing**

The innocent victims of the growth of spam are individuals and companies who've been 'spoofed'.

Spoofing (or masquerading) is when a spammer uses your Internet email identity to send spam. Companies and individuals with their own domain name have this name hijacked and used illegally as a cover to send millions of spam messages.

The ones that don't reach their target bounce back into inboxes - up to 1000 messages a day.

The most effective way to kill the spam is to delist the domain name, but these days a domain name is an essential part of a business identity. There is almost nothing that can be done about it legally.

---

**A new law for Australia**

The Australian Federal government is drafting Opt In legislation to be in place by the end of the year. This means commercial email could only be sent to people who give permission to receive it, or have a pre-existing business relationship.

Where the Opt In concept gets tricky is in the business-to-business market. Jodie

**Spam Trap**

A spam trap is a fake email address set up by the anti-spammers to harvest spam.

Emails to the fake address are checked against emails to other fake addresses. If there's a match then they've caught a possible spam.
Sangster, Australian Direct Marketing Association's Legal Affairs Manager is concerned about the impact of a strict Opt in law on small business, which relies heavily on email as a cheap marketing tool.

"By requiring companies to opt in to receive emails from another company, what you're effectively going to do is make it so that companies only request from the companies that they actually know about, which are generally the big companies" she says.

The Federal government doesn't want to stifle legitimate e-business but to curtail spam it's got to walk a tightrope.

To navigate the problem it says a 'cold call' approach will be acceptable if a business advertises its email address in the yellow pages or online, and as long as the approach is directly relevant to the business at hand.

Either way, imagine trying to police email, it's complex. Definitions are crucial. What is a pre-existing business relationship? What's a commercial email? And what is actually meant by consent?

The Internet Industry Association wanted criminal charges for the worst spam offence, but the government says civil laws are easier to enforce and require a lower standard of proof. The fines will be around the million dollar mark.

The legislation will also ban the sale of email lists and the software that collects them. Fraudulent email headers that disguise the origin of emails will also be illegal. It's up to the Australian Communications Authority to try and enforce the rules.

### Spam is a global disease

But outlawing spam in Australia won't solve the problem. The volume of spam originating from Australia is about 2% of the world total. Even if spam was made a hanging offence tomorrow, our inboxes would still attract junk because spam comes from overseas.

Britain has just held its first spam summit and will follow EU countries with Opt In rules by the end of October. America, however, is taking the Opt Out approach.

"They want you in America to opt out of receiving" says Derek Wyatt, Chairman of the British Parliamentary Internet Committee. Like many, he's deeply concerned about the direction the United States is heading.
"We think that's not the way to go. We think that the American politicians simply don't understand how serious an issue this is."

To argue their point, Derek Wyatt and his British committee headed to Washington in October 2003 to lobby Congress to outlaw spam. As far as they know, it's the first time British MPs have ever gone to lobby on anything.

**What's the solution?**

Derek Wyatt says the ultimate solution is a global spam regulator, especially as we head towards a wireless world.

"As the Internet matures you'll get some sort of world governance " he says.

In the meantime, get yourself a good email filter and just keep hitting the delete button!

**More email spam?**

If you'd like to receive regular updates of what's new in ABC Science TV, Radio and Online then you can sign up for the Lab's Science Updates - we promise to take your email address off the list if you opt out, and never to sell on your email address!

---

**More about Spam from ABC Science**

*Junk email gets smarter:* Junk email is getting intelligent, as spammers find better techniques to find inboxes. - Jun 24, 2003

*Computer experts to discuss spam concerns:* Computer experts and politicians are meeting in Canberra this week to discuss ways to curb growing number of unwanted emails, or spam. - Jun 23, 2003

*That's a Lot of Spam:* More than 40% of emails are spam. Spam clogs our inboxes and chews up our time. It slows down our email systems, uses up storage space and costs billions - it's a massive worldwide problem. But there are grounds for hope. - May 26, 2003

*Spam Catcher:* Statistical spam filters use Bayesian analysis to eliminate 99% of the problem. They work by examining every word in an incoming email and assigning a probability that it is involved in spam. Then they add up all the probabilities and designate the email as spam or non-spam. - May 26, 2003
AOL takes spam fight to court: America Online has taken its battle with junk e-mailers to court. - Apr 16, 2003

If you enjoyed this feature you might like...

Tech Talk: A forum for everyone with an interest in (or a problem with) digital technology. This is the place to ask your curly computer questions or let us know of some groovy new trick you've discovered.

E-media III - Let's Talk Science: Ian Allen on "portal sites" and science communication over the web. - Mar 9, 2000

E-media II - Can the Empires fight back?: Ian Allen on the changing media environment. - Mar 2, 2000

E-media I - The Decline of TV: Ian Allen on our changing relationship with T.V. - Jan 24, 2000

Information Poverty: Why the Internet isn't helping the 3rd world as much as originally hoped. - Jun 3, 1999

Cyberwarfare: Feature includes synchronised audio. Is our dependance upon computers posing a potential threat to national security? - May 13, 1999


Published October 23, 2003