world summit on the information society
Geneva 2003 - Tunis 2005

Global SPAM – Global Problem

It used to be the case that the world only had two certain things to worry about — death and taxes. Now a four-letter nuisance has cropped up in that category.

SPAM, or the annoying, relentless and indiscriminate sending of unsolicited, commercial email is an irrefutable fact of life. Volumes may drop on new Spam-blocking filters and laws, offensive mailings may shrink but, like junk mail, those electronic pests are here to stay.

Indeed, exploding handset growth — and many handsets are newly Internet-enabled — and always-on broadband connections could even ease entry for infiltrators.

With less secure mobile phones now the primary way most low-income country residents communicate and will, ultimately, access the Internet, SPAM, electronic security and data protection are also headaches emerging economies.

For those reasons, the World Summit on the Information Society (Geneva, December 10-12) will focus on those, among other, issues. The UN-Summit, being organized by the International Telecommunication Union, its specialized agency for telecommunications, brings together over fifty heads of state and thousands of regulators, NGO reps and business leaders to bring the latest technologies to underserved areas, address the human implications of technologies, and use them to shape a better world.

Spam and data protection problems are no longer only relegated to wealthy economies. The borderless boundaries of the Internet require collaboration. International agreements on security protocols, standardization and, possibly, the harmonization of laws will make today's systems more secure.

Today, over half of all email falls in the Spam bin, with far over $20 billion in lost productivity and costs to boost bandwidth and storage, as users wade through their ever-flowing inboxes. Many of these e-mails are offensive or misleading.

Viral Spam

What's more, the boundaries between viruses and Spam are blurring. With the Sobig virus, the "Love Bug" last summer, infectors joined forces with spammers, and bombarded computers across the world. The debilitating injection made headlines and crippled communication at smaller companies. Though software developers raced to decode and block malicious code through updated filters, mutation makes them likely to emerge again. The damage wrought underscored the vulnerability of our most important communications systems.

Indeed, the importance of secure systems that increasingly span the globe and interoperate with others' infrastructure is growing, as governments and corporations use the Internet as their primary mode of communication and transactions. Organizations need to continue to operate when hackers attack and keep infiltrators out. More security incidents were reported in 2002 than in the prior two years combined.

And with most systems going wireless, security is paramount. Between palm pilots, mobile phones and laptops, data on our bank accounts, homes, families and future plans are at our very fingertips wherever we go. That's a huge time-saver and helps keep us all connected, all the time. But if misused, that information can prove profitable for credit card fraud, customer leads and, in some cases, corporate espionage; spammers following us on-the go is annoying, as well.

"The world is fed up with Spam," says Robert Shaw, Internet Strategy and Policy Advisor at the International Telecommunication Union. "Spam is especially a problem for mobile users because it is so intrusive and personal."

Wireless systems need to be more secure since their mobility makes it easier for sensitive information about our call history and whereabouts to leak if it falls into the wrong hands. Moreover, cellular carriers keep location and call data about their users for at least a year, sometimes up to five years.

Global Markets Mean Global Concerns

The fact that our data now crosses borders and that on-the-run spammers can relocate to safe havens — where privacy laws vary widely — is also a concern.

That's why stopping SPAM and the protection of data has emerged as a top concern of Internet and handset users across the world today. The personal intrusion that could follow a company obtaining such data through invasive emails, calls or personal visits are worrisome, too.

"Companies have data scattered in so many places," says Walter Janowski, a research director at Gartner. "The more information propagated, the more potential there is for a hole in security."

There is, however, good news. Governments are talking cross-border agreements that ban spamming across countries; global regulatory bodies are hammering out legislation to fence off personal data for unapproved use (Australia, Republic of Korea and many European countries already have such laws) and major blue-chip companies are forging customer privacy rules.

This year's EU Directive for the Protection of Personal Data and Privacy in E-Communications, for example, requires mass marketers to get a green light from new targets well before Spam starts, or "opt in". It takes effect in October. Japan and Australia have anti-Spam laws, too.

While not all marketers welcome these developments that they feel could limit their search for more buyers, they realize customer loyalty rests largely on trust from those they are trying to win over.

But notorious spammers are difficult to track down, and when the forces close, they often adopt new techniques to again slip through filters using misspellings or forged mail origins, or shift operations offshore. Most Spam originates from several hundred mega-spammers in the US and is increasingly sent via servers in Asia, or even Latin America to evade the law.

Multilateral Solutions Emerging

Countries are reacting, albeit slowly: Servers suspected of spamming get shut down after surfers complain about voluminous unsolicited emails clogging their in-boxes. For early adopters in emerging economies, the initially low number of Internet users are likely to be swamped with unwanted marketing messages — many originating abroad.

And the Council of the Europe's Convention on Cyber crime proposes harmonizing national laws and offences and a rapid and effective international co-operation system.

Other ideas include a global clearinghouse of information on cybercrime; perhaps overseen by an unbiased international body since governments might be reticent to share such sensitive information for fear that its release would undermine public confidence or expose failures.

Global cooperation is particularly important since solutions may even involve revisiting standards that are more vulnerable to break-ins.

Interesting business models are emerging too, though many Spam-busters are dubious about the long-term efficacy (and ethics) behind such projects.

One notable idea originates in the US, where Stanford Business School professor Lawrence Lessig has proposed "bounties" for tracking down elusive cyber-bandits on the run. E-sleuths, which will likely draw from the ranks of yesterday's washed up Web entrepreneurs — would chase a cut of hefty fines imposed upon spammers after capture.

Ultimately, a workable but imperfect solution may span several sectors and multiple stakeholders. If today's whingeing grows to a roar and laws have teeth, companies using Spam or otherwise questionable techniques for customer data, potential customers may boycott such companies, drying up lucrative opportunities for the spammers and those providing personal information by eliminating the economics (spamming is the cheapest way to blanket potential customers). Australia's National Office for the

Information Economy, for example, found in April that close to one in five spammed email messages came from blue chip companies.

"People do bad things in the real world and every communications medium has been abused," says ITU's Shaw. "Wild west bank thefts were thwarted through alarms, vaults, security guards, laws, bounties and penalties. Spam will be solved by a combination of defences, not just one."

The World Summit on the Information Society provides an opportunity for the global community to take stock of these measures and commit themselves to building a more secure on-line future that respects our freedom but protects our privacy.