Spam, Spyware, Viruses and Spam

How the Internet has become an unfriendly place

Michael Sofka
Communications & Collaborative Technologies
Rensselaer Polytechnic Institute
sofkam@rpi.edu
Gary Schwartz, Director C&CT
Pat Valiquette, ARC, Manager Help Desk Services
Nigel Westlake, NeTel, NOC Specialist
Graham Doig, NeTel, Associate Director
Frank Hill, ARC, Sr. System Administrator
Ed Seeger, ARC, Manager Educ Tech Svcs
Dennis Milkiewicz, IACS, Manager Desktop Services
Gail Kaiser, C&CT, Academic Computing Analyst
George Biggar, RRL, Sr. Systems Administrator
Brenden Conte, C&CT, Systems Programmer
Arthur Hyun, C&CT, Systems Programmer
Colleen Morrissey, NeTel, Network Engineer
Kenneth Dupre, IT Ops, Sr. A/V Technician
Nelson Brownell, IT Ops, Manger Computer Operations
Otis Williams, IT Ops, Sr. Computer Operator
Jim Evans, Director IT Operations
What is Spam, and Why is it called “spam?”

What is Spyware?

What are computer Viruses, Worms, Trojans?

The dark side of Spam and Viruses

Why doesn’t somebody do something!?!?

Protecting yourself
Waitress: Well, there’s egg and bacon; egg sausage and bacon; egg and spam; egg bacon and spam; egg bacon sausage and spam; spam bacon sausage and spam; spam egg spam spam bacon and spam; spam sausage spam spam bacon spam tomato and spam; spam spam spam egg and spam; spam spam spam spam spam baked beans spam spam spam; or Lobster Thermidor a Crevette with a mornay sauce served in a Provencal manner with shallots and aubergines garnished with truffle pate, brandy and with a fried egg on top and spam.

Customer: Have you got anything without spam?

Waitress: Well, there’s spam egg sausage and spam, that’s not got much spam in it.

—Phython, Monty, 1970.
Pre-history of Spam:
Jon Postel, RFC 706 “On the Junk Mail Problem,” 1975

Chain letters
Good Times virus hoax

Cantor & Siegal, Usenet “Green Card” Lottery, April, 1994

Usenet Spam:
Jeff Slaton, Spam King; Sanford Wallace, Cyber Promotions.

Now Spam Means:
Unsolicited Bulk Email:
Alan Ralsky, Scott Richter, . . . and a host of others
- Viagra, Body Enhancement, Pornography
- Pyramid Marketing, Ponzi, Nigerian 419
- Commercial Email
- Unwanted Email

Uppercase “SPAM” is a trademark of Hormel
More than 50% of email is spam (Brightmail)

Approximately 50% of email to RPI is spam

Up from 30% one year ago, 20% two years ago

Spam is profitable in the short run (Leung, 2003)
- Spam has a 0.005% response rate
- For every 50 responses 999,950 people annoyed
- Cost of sending spam is near zero
- (Only because spammers steal services, Shein, 2003)

Easy for spammers to hide:
- Forge sender address
- Use “Open” mail relays
- Compromised home machines

Harder for average user to hide
- Web-page harvesters
- Open database harvesting
- Web bugs (8/10 in survey)
Cost of Spam

Financial Cost
$9 billion, US; $2.5 billion, EU (Ferris Research).
  – Productivity: email management and distraction
  – Connectivity: slower servers and networks
  – Storage: It costs money to store email
  – Support: Anti-spam products, training, complaints

Nortel estimates average $1.00 per spam message
AOL $5.00 per user per month
$500,000 would not surprise me for RPI (higher with Viruses)

Social Cost
Email has become an unfriendly place (Pew Internet)
Personal spam load varies from zero to 100s/day
People less trusting of email, e-business
Women bothered more than men, older more than younger
Harassment lawsuits a looming concern
Programs that spy
Usually with the users “permission” (click-through license)
Spyware Cookies (Doubleclick)
—Not all cookies are spyware, or bad
Spyware-Virus-Spam cross: FriendGreet, Buddylist
Anti-Spyware industry: Ad-Aware and Spybot Search and Destroy.
False Anti-Adware industry: SpyBan
Read the license agreement (especially for free software)
Viruses, Worms and Trojans, oh my!

Programs you did not buy or install on your computer, and which do things (usually to other people) you wouldn’t do and don’t want done.

**Viruses:**
- Latch on to other programs (traditional, e.g. Michelangelo)
- Require human intervention (modern, e.g. MyDoom)

**Worms:** Self propagating (Morris worm, MSBlaster, Welchai)

**Trojans:**
- Programs that entice people to run them (traditional)
- Programs that provide a back door to a computer (modern)

Many programs combine elements of all of three

**Anti-virus worms** (Welchia/Nachi)

Modern viruses and worms minimally impact infected host

Use host to infect and annoy others (covering their tracks)

The Press almost always uses “virus,” sometimes uses “worm”
The Cost of Viruses

Financial:
- Estimate $55 billion in 2003 (Trend Micro)
- Up from $20–$30 billion in 2002
- Lost productivity, Connectivity and Support
- Easily 6 figure at RPI

Social:
- Social confusion (Viruses forge sender)
- Co-workers are less tolerant
- Company reputation damaged
- People become less trusting of email
- Personal and company secrets exposed

Technical: A virus infected machine is compromised—nothing from it can be trusted (Not a new problem)
The Dark Side of Spam and Viruses

Spam is often used to further a crime
- Organized Crime
- Nigerian 419 scams
- Pyramid marketing (often for spam services)
- Ponzi schemes
- Stock Market pump-n-dump
- Phishing
- Identity theft

Spammers often engage in crime to distribute spam
- Viruses installing back door (Sobig-F)
- Hackers going “pro” and selling services
- Conditions of Use/License violation
- Violations of CAN-SPAM act since January 1, 2004
- Theft of service by using open relays
Legal Responses

Federal Trade Commission (most spam already illegal)
State Anti-spam Laws
CAN-SPAM: Controlling Abusive Non-Solicited Pornography and Marketing act
USA-PATRIOT act
ECPA: Electronic Communications Privacy Act
CFAA: Computer Fraud and Abuse Act
Lawsuits against spammers are usually successful—but recover no money after legal costs
Technical Responses

The delete key
Black Lists
Filters: SpamAssassin, RESPITE
SpyBot, Ad-Aware
Anti-Virus programs
Anti-virus viruses: They are a technical response, but not a good one
Protecting your email address

Do not give email to marketers!
Use “throw-away” address to order on-line
Use alt-address for untrustworthy associates
Don’t put email address on web page

Hiveware Encoder

Don’t respond to spam
Don’t opt-out of spam – controversial

Opting out of “legitimate” mailing lists ok
Apply Patches Frequently
Run Anti-Virus software and update patterns frequently
Run a firewall or NAT (Firewall lite)
Anti Spyware programs: Ad-aware, Spybot

Common sense:
– Don’t open strange attachments (or wait before you open them)
– Don’t open attachments from strangers
– Read license agreements: If you don’t agree, don’t install

Don’t be a spammer: Operation Secure Your Server
Resources

Ad-Aware: http://www.lavasoftusa.com/
Spybot: http://www.safer-networking.org/
Hiveware E-mail Encoder:
   http://hiveware.com/enkoder_form.php
Spamhaus: http://www.spamhaus.org/
SpamCop: http://www.spamcop.com/
Sophos: http://www.sophos.com/virusinfo/
Symantec: http://securityresponse.symantec.com/
MIT Spam Conferences:
   http://www.spamconference.org/
ARC Helpdesk: http://j2ee.rpi.edu/helpdesk
Hormel Spam Museum: “For the love of SPAM”:
   http://www.spam.com/