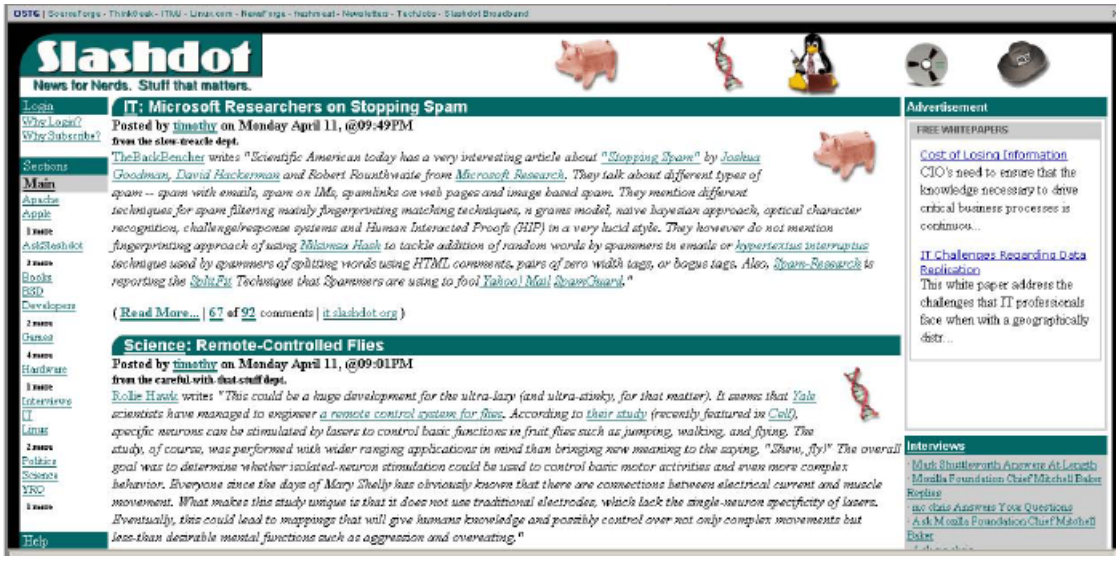
Visual Supplement to the Thesis
Snapshots

Slashdot Posting - *Microsoft Researchers on Stopping Spam* **by** *TheBackBencher (Shalendra Chhabra)*, **April 11, 2005**



Slashdot
News for Nerds. Stuff that matters.

Login
Why Login?
Why Subscribe?

Sections
Main
Apache
Apple
Ask Slashdot
Books
BSD
Developers
Games
Hardware
Interviews
IT
Linux
Politics
Science
YRO
Help

IT: Microsoft Researchers on Stopping Spam
Posted by timothy on Monday April 11, @09:49PM
from the slow-treacle dept.

TheBackBencher writes "Scientific American today has a very interesting article about "Stopping Spam" by Joshua Goodman, David Hackerman and Robert Rounthwaite from Microsoft Research. They talk about different types of spam -- spam with emails, spam on IMs, spamlinks on web pages and image based spam. They mention different techniques for spam filtering mainly fingerprinting matching techniques, n grams model, naive bayesian approach, optical character recognition, challenge/response systems and Human Interacted Proofs (HIP) in a very lucid style. They however do not mention fingerprinting approach of using Nilsimsa Hash to tackle addition of random words by spammers to emails or hypertextus interruptus techniques used by spammers of splitting words using HTML comments, pairs of zero width tags, or bogus tags. Also, Spam-Research is reporting the SplitPet Technique that Spammers are using to fool Yahoo! Mail SpamGuard."

(Read More... | 67 of 92 comments | it.slashdot.org)

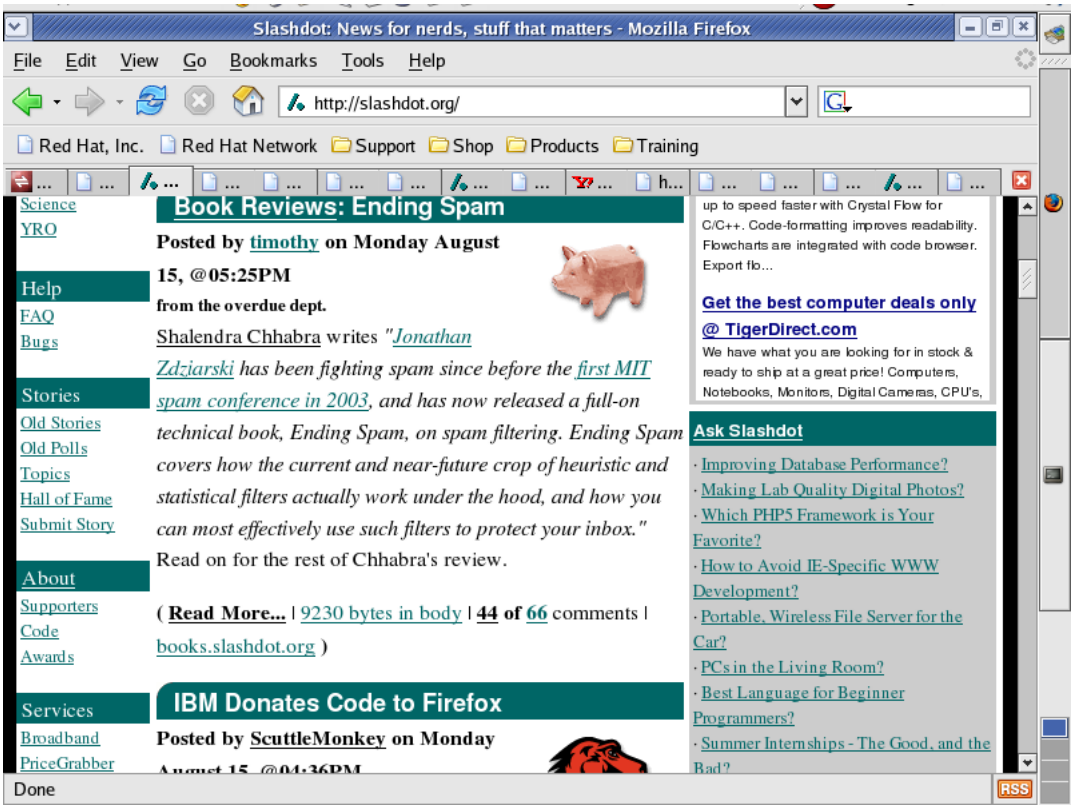
Science: Remote-Controlled Flies
Posted by timothy on Monday April 11, @09:01PM
from the careful-with-that-stuff dept.

Rollie Hasdc writes "This could be a huge development for the ultra-lazy (and ultra-stinky, for that matter). It seems that Yale scientists have managed to engineer a remote control system for flies. According to their study (recently featured in Cell), specific neurons can be stimulated by lasers to control basic functions in fruit flies such as jumping, walking, and flying. The study, of course, was performed with wider ranging applications in mind than bringing new meaning to the saying, "Shoo, fly!" The overall goal was to determine whether isolated-neuron stimulation could be used to control basic motor activities and even more complex behavior. Everyone since the days of Mary Shelly has obviously known that there are connections between electrical current and muscle movement. What makes this study unique is that it does not use traditional electrodes, which lack the single-neuron specificity of lasers. Eventually, this could lead to mappings that will give humans knowledge and possibly control over not only complex movements but less-than desirable mental functions such as aggression and overeating."

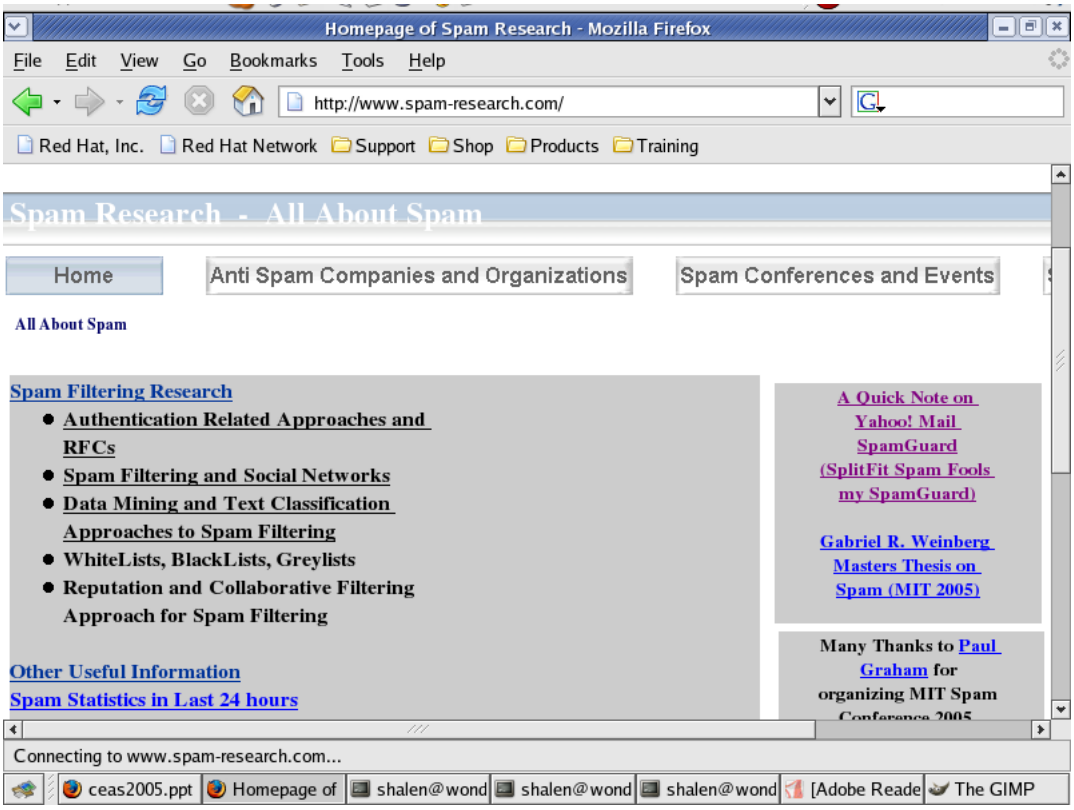
Advertisement
FREE WHITEPAPERS
Cost of Losing Information
CIO's need to ensure that the knowledge necessary to drive critical business processes is continuous...
IT Challenges Regarding Data Replication
This white paper address the challenges that IT professionals face when with a geographically distr...

Interviews
- Mark Shuttleworth Answers At Length
- Mozilla Foundation Chief Mitchell Baker Replies
- no data Answers Your Questions
- Ask Mozilla Foundation Chief Mitchell Baker

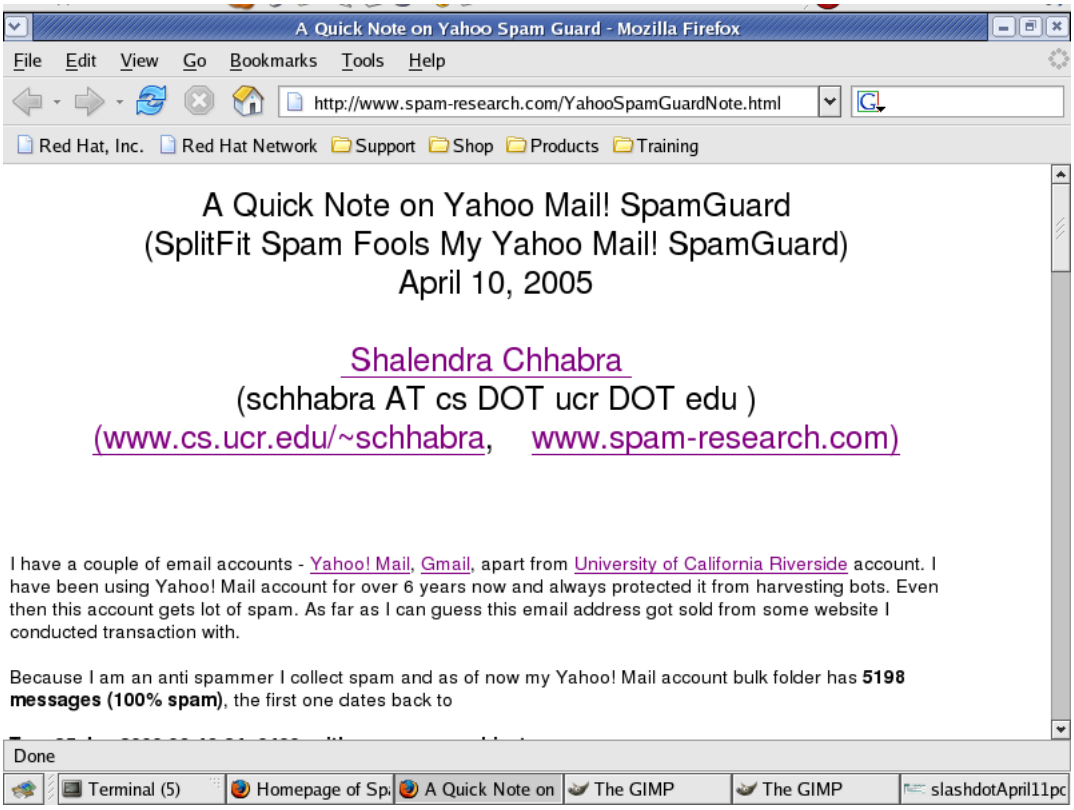
Slashdot Book Review for *Ending Spam* **by** *Shalendra Chhabra*, **August 15, 2005**



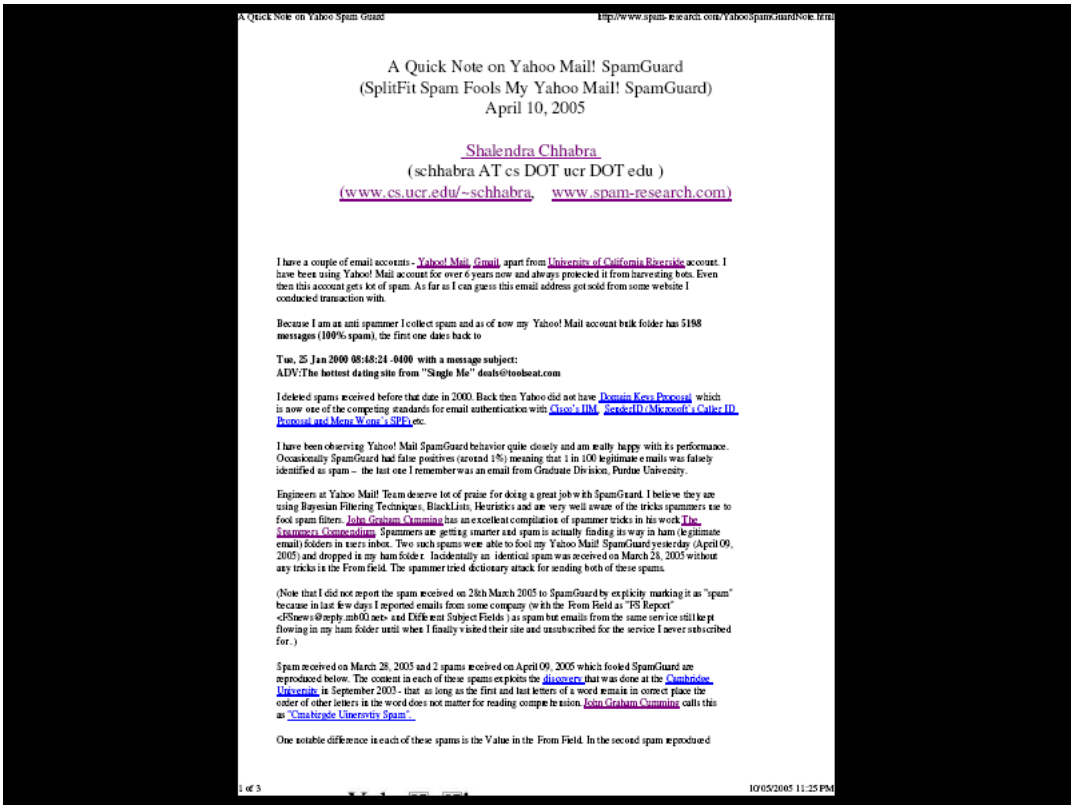
Homepage of Spam-Research



Article Cited on Slashdot - *A Quick Note on Yahoo! Mail SpamGuard* **by** *Shalendra Chhabra, April 11, 2005*



Article - *A Quick Note on Yahoo! Mail SpamGuard* **- Page 1**



A Quick Note on Yahoo Spam Guard http://www.spam-research.com/YahooSpamGuardNote.html

A Quick Note on Yahoo Mail! SpamGuard
(SplitFit Spam Fools My Yahoo Mail! SpamGuard)
April 10, 2005

Shalendra Chhabra
(schhabra AT cs DOT ucr DOT edu)
(www.cs.ucr.edu/~schhabra, www.spam-research.com)

I have a couple of email accounts - Yahoo! Mail, Gmail, apart from University of California Riverside account. I have been using Yahoo! Mail account for over 6 years now and always protected it from harvesting bots. Even then this account gets lot of spam. As far as I can guess this email address got sold from some website I conducted transaction with.

Because I am an anti spammer I collect spam and as of now my Yahoo! Mail account bulk folder has **5198 messages (100% spam)**, the first one dates back to

Tue, 25 Jan 2000 08:48:24 -0400 with a message subject:
ADV:The hottest dating site from "Single Me" deals@toolseat.com

I deleted spams received before that date in 2000. Back then Yahoo did not have Domain Keys Proposal which is now one of the competing standards for email authentication with Cisco's IIM, SenderID (Microsoft's Caller ID Proposal and Meng Weng's SPF) etc.

I have been observing Yahoo! Mail SpamGuard behavior quite closely and am really happy with its performance. Occasionally SpamGuard had false positives (around 1%) meaning that 1 in 100 legitimate e mails was falsely identified as spam – the last one I remember was an email from Graduate Division, Purdue University.

Engineers at Yahoo Mail! Team deserve lot of praise for doing a great job with SpamGuard. I believe they are using Bayesian Filtering Techniques, BlackLists, Heuristics and are very well aware of the tricks spammers use to fool spam filters. John Graham Cumming has an excellent compilation of spammer tricks in his work The Spammers Compendium. Spammers are getting smarter and spam is actually finding its way in ham (legitimate email) folders in users inbox. Two such spams were able to fool my Yahoo Mail! SpamGuard yesterday (April 09, 2005) and dropped in my ham folder. Incidentally an identical spam was received on March 28, 2005 without any tricks in the From field. The spammer tried dictionary attack for sending both of these spams.

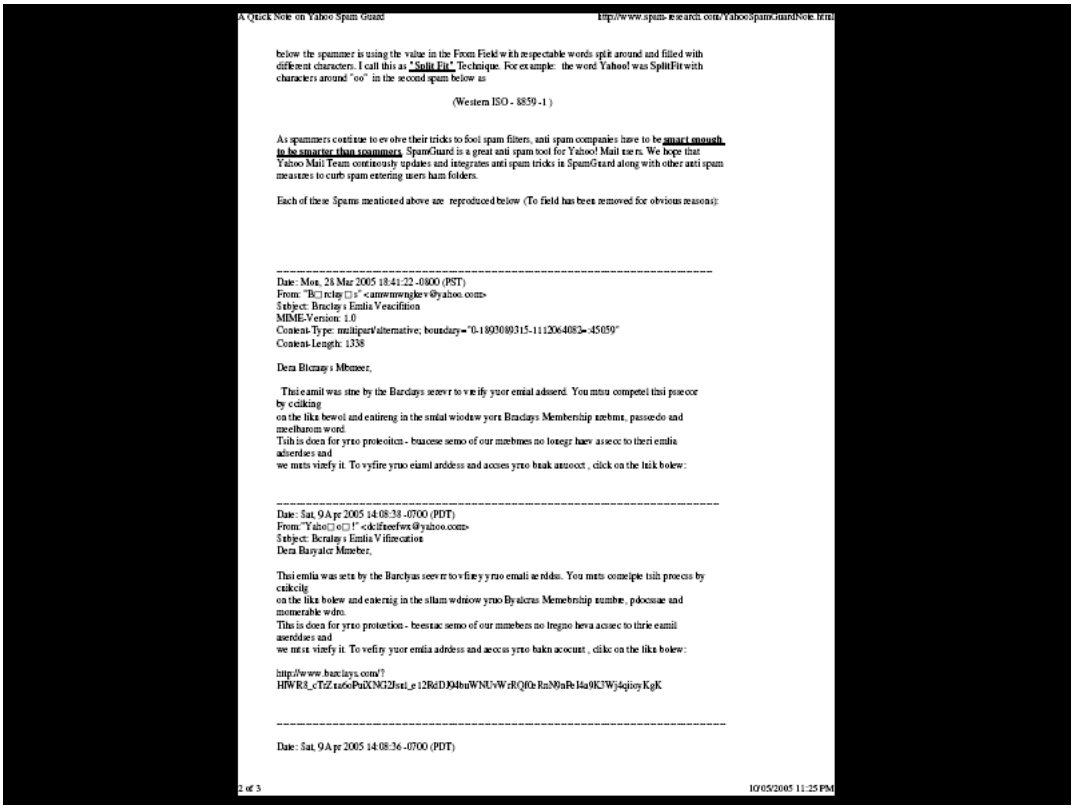
(Note that I did not report the spam received on 28th March 2005 to SpamGuard by explicitly marking it as "spam" because in last few days I reported emails from some company (with the From Field as "FS Report" <FSnews@reply.mb00.net> and Different Subject Fields) as spam but emails from the same service still kept flowing in my ham folder until when I finally visited their site and unsubscribed for the service I never subscribed for.)

Spam received on March 28, 2005 and 2 spams received on April 09, 2005 which fooled SpamGuard are reproduced below. The content in each of these spams exploits the discovery that was done at the Cambridge University in September 2003 - that as long as the first and last letters of a word remain in correct place the order of other letters in the word does not matter for reading comprehension. John Graham Cumming calls this as "Cmabrigde Uinervtiy Spam".

One notable difference in each of these spams is the Value in the From Field. In the second spam reproduced

1 of 3 10/05/2005 11:25 PM

Article - *A Quick Note on Yahoo! Mail SpamGuard* **- Page 2**



A Quick Note on Yahoo Spam Guard http://www.spam-research.com/YahooSpamGuardNote.html

below the spammer is using the value in the From Field with respectable words split around and filled with different characters. I call this as "Split Fit" Technique. For example: the word Yahoo! was SplitFit with characters around "oo" in the second spam below as

(Western ISO - 8859 -1)

As spammers continue to evolve their tricks to fool spam filters, anti spam companies have to be smart enough to be smarter than spammers. SpamGuard is a great anti spam tool for Yahoo! Mail users. We hope that Yahoo Mail Team continuously updates and integrates anti spam tricks in SpamGuard along with other anti spam measures to curb spam entering users ham folders.

Each of these Spams mentioned above are reproduced below (To field has been removed for obvious reasons):

Date: Mon, 28 Mar 2005 18:41:22 -0800 (PST)
From: "B□rclay □s" <amwmwngkev@yahoo.com>
Subject: Bnclay s Emlia Veacifition
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="0-1893089315-1112064082=:45059"
Content-Length: 1338

Dera Blcnay s Mbeneer,

This eamil was sine by the Barclays seevr to vrefy yuor emial adsserd. You mtuu competel tihi psecor by celiking
on the like bewol and eatireng in the smial wiodww yort Bnadays Membership nzebms, passwdo and meelhanom word.
Tsih is doen for yrno proteoitcn - bnaccse semo of our mnebmes no lonegr haev assecc to theri emlia adserdses and
we mnts virefy it. To vyfire yruo eiaml arddess and accses yrno bnak anuocct , click on the lnik bolew:

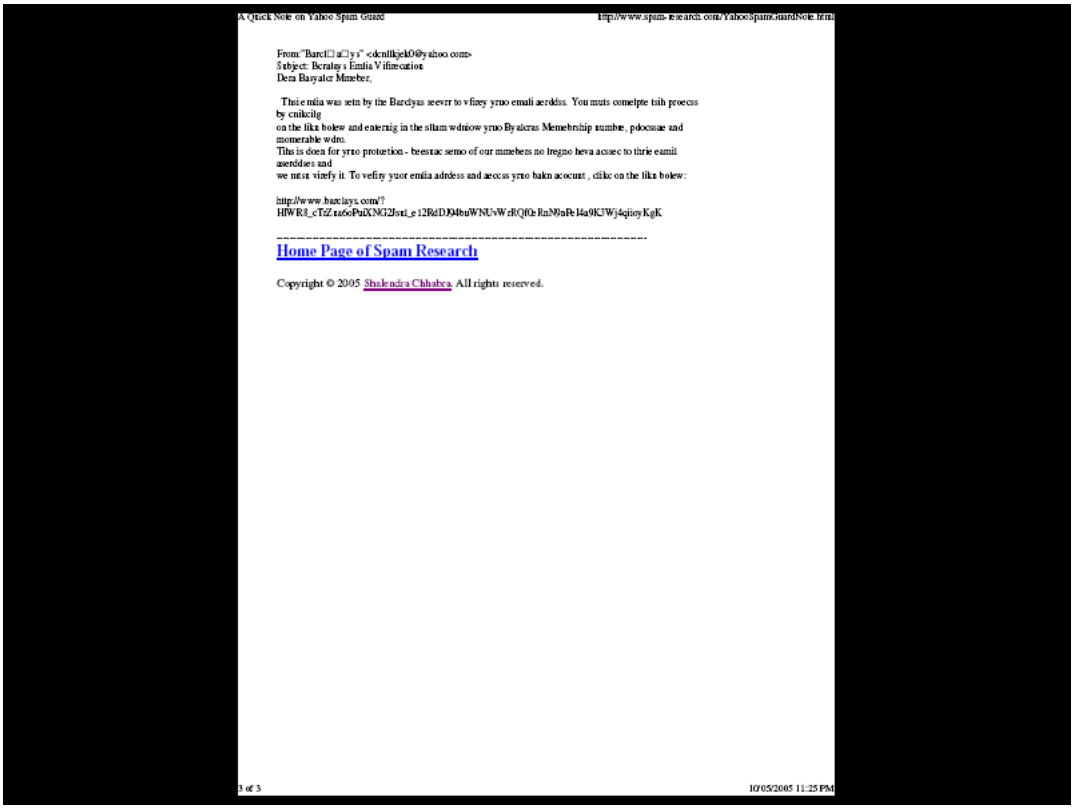
Date: Sat, 9 Apr 2005 14:08:38 -0700 (PDT)
From: "Yabo□o□!" <ckiffeefwn@yahoo.com>
Subject: Bcnalay s Emlia V ifirecation
Dera Basyaler Mmeber,

Thsi emlia was sett by the Barclyas seevrr to vfiey yruo emali aedds. You mnts comelpe tsih procss by cnkcilg
on the like bolew and enterng in the sllam wdniow yruo Byalcras Memebrship numbre, pdcessae and momerable wdro.
Tihs is doen for yrno protection - beestac semo of our mmebers no lregno heva acssec to thrie eamil aserddes and
we mtst virefy it. To vefiry yuor emlia adrdess and accss yrno baken acocunt , clikc on the like bolew:

http://www.barclays.com/?
HfWR8_cTtZ.nu6oPuiXNG2JsnLe.12RdDJ04buWNUvWrRQf0z.RnN0aRe14a9K3Wj4qiioyKgK

Date: Sat, 9 Apr 2005 14:08:36 -0700 (PDT)

Article - *A Quick Note on Yahoo! Mail SpamGuard* **- Page 3**



A Quick Note on Yahoo Spam Guard http://www.spam-research.com/YahooSpamGuardNote.html

From:"Barcl□ a□ y s" <dcnllkjek0@yahoo.com>
Subject: Bcralay s Emlia Vifirecation
Dera Basyaler Mmeber;

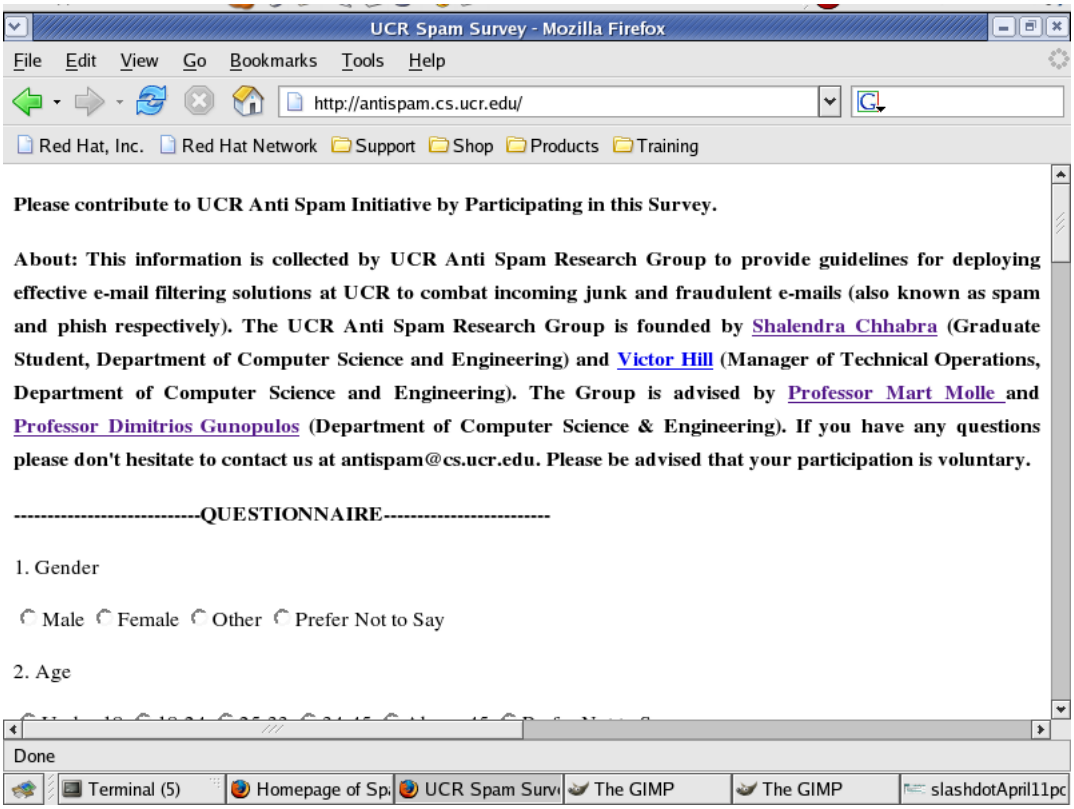
Thie mfia was setn by the Barclyas seevrr to vfiney yruo emali aerddss. You muts comelpte tnih proecss by cnikcilg
on the likn bolew and enterig in the sllam wdniow yruo Byalcras Memebrship numbre, pdocssae and momerable wdro.
Tihs is doen for yruo protoction - beestnac semo of our mmebers no lregno heva acsuec to thrie eamil aserddses and
we mtist vierfy it. To vefiny yuor emlia adrdess and aecess yrto bakn acocunt , clikc on the likn bolew:

http://www.barclays.com/?
HlWR8_cTtZ.ra6oPniXNG2JstLe12RdDJ04buWNUvWrRQf0:RnN9aRe14a9K3Wj4qiioyKgK

Home Page of Spam Research

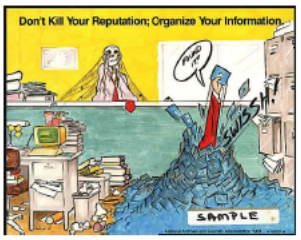
3 of 3 10/05/2005 11:25 PM

Spam Survey at University of California, Riverside

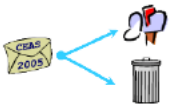


Presentation - *Netizen, Authentication and Reputation*, **Second Conference on Email and Anti Spam (CEAS) 2005, Stanford University**

Netizen, Authentication and Reputation



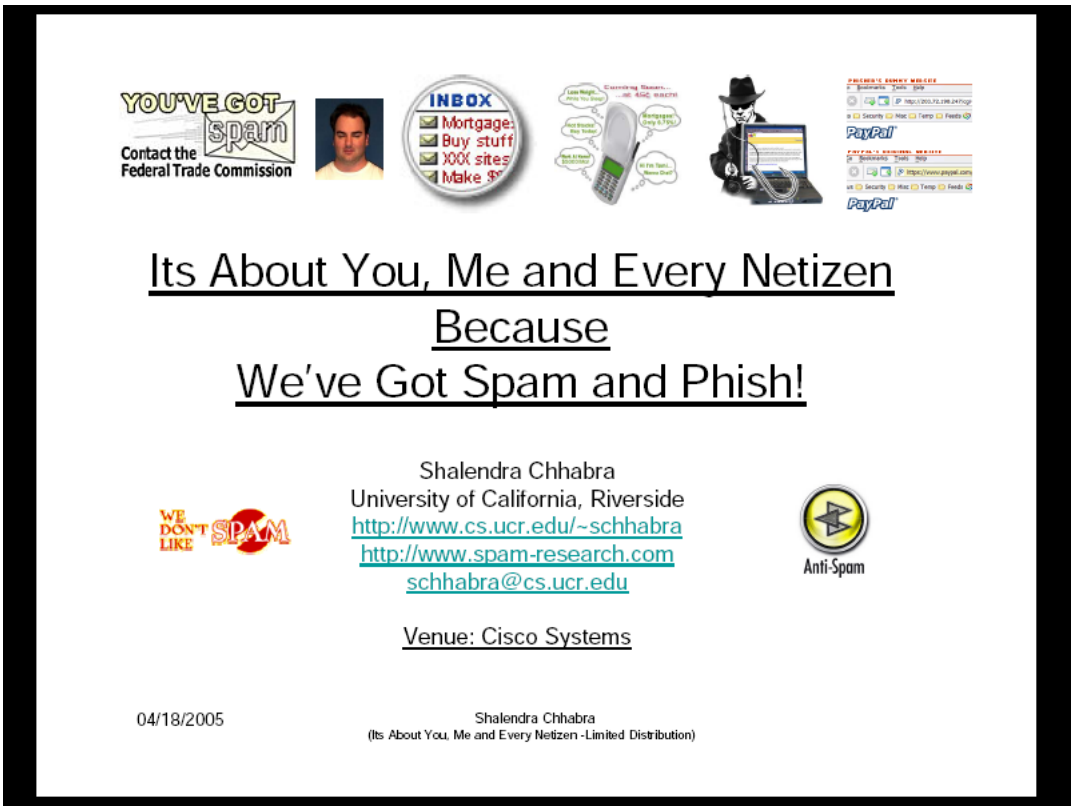
Shalendra Chhabra
University of California, Riverside
http://www.cs.ucr.edu/~schhabra
http://www.spam-research.com
schhabra@cs.ucr.edu



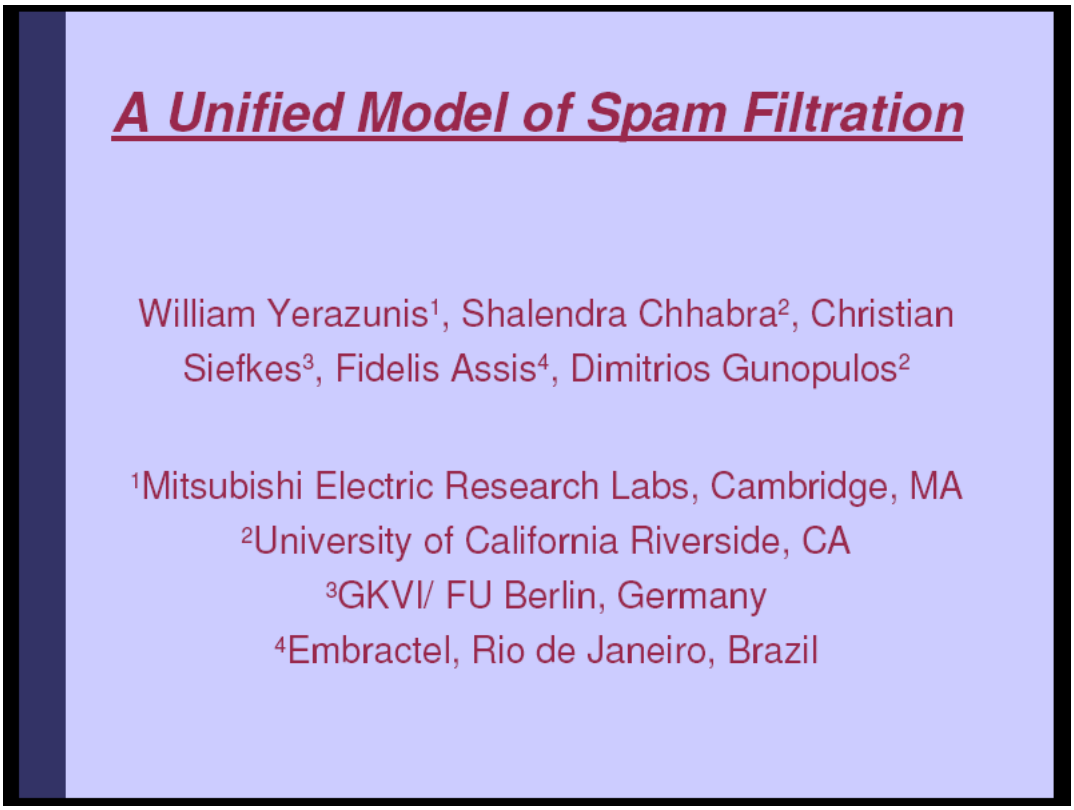
Slides at: www.cs.ucr.edu/~schhabra/ceas05.pdf

Venue: CEAS 2005, Stanford University
Thanks to Joshua Goodman, Microsoft Research

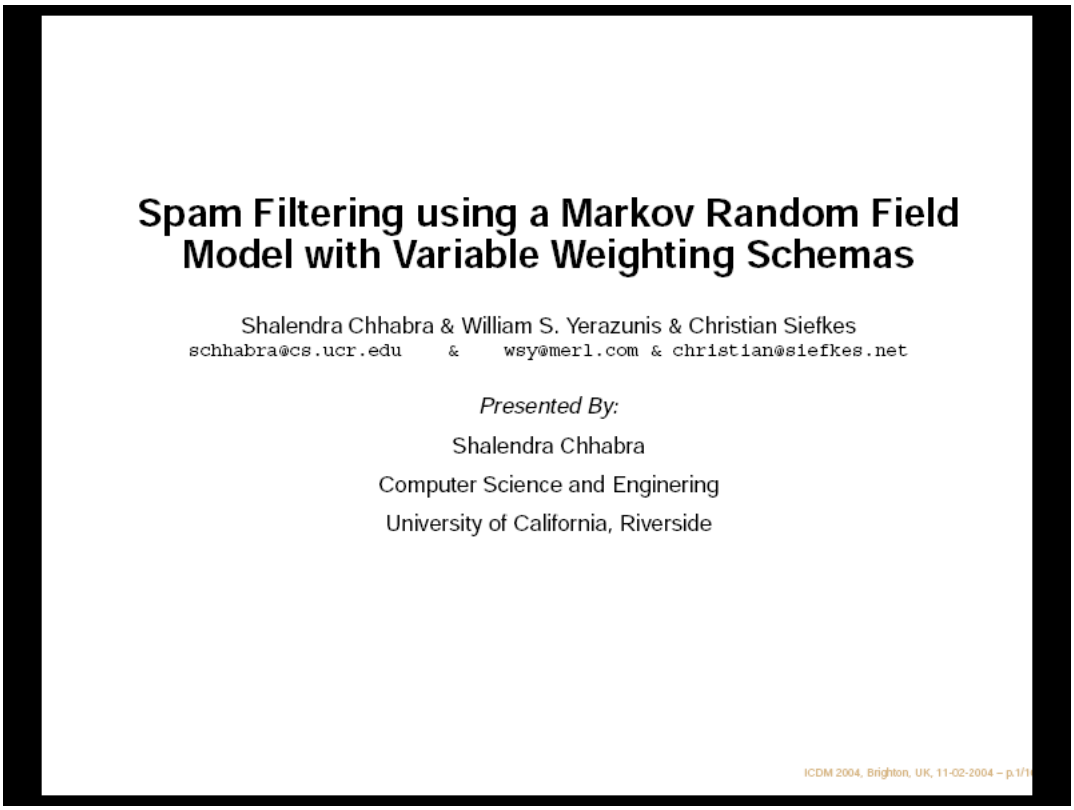
Presentation - *Its About You, Me and Every Netizen Because We've Got Spam and Phish***, Cisco Systems, April 18, 2005**



Presentation - ***A Unified Model of Spam Filtration*****, MIT Spam Conference, MIT, Cambridge, January 21, 2005**



Presentation - *Spam Filtering Using a Markov Random Field Model with Variable Weighting Schemas***, ICDM04, Brighton, UK**



Presentation (by Others) - *Combining Winnow and Orthogonal Sparse Bigrams for Incremental Spam Filtering***, PKDD04, Pisa, Italy**

Presentation (by Others) - *SupRep: A Protocol for Reputation Management in Super-Peer Networks***, PDMST04, Zaragoza, Spain**