A few weeks ago, a new Google Labs feature for their Gmail system made some news. They called it “mail goggles” and the tag line was “Stop sending mail you later regret” (http://gmailblog.blogspot.com/2008/10/new-in-labs-stop-sending-mail-you-later.html).

The announcement said that one of their engineers wanted to keep from sending pleas to his ex-girlfriend when he wasn’t thinking straight, so he came up with a simple test. I checked my calendar — no, it wasn’t April 1st — but I still couldn’t help thinking this was an odd joke. Nope! Sure enough, if I go to the Labs page from my Gmail account, I see that the feature exists, with examples of simple — but not too simple — math problems it might pose.

Wow. I would love to know how many people have adopted this by now, and how many continue to use it. I’d especially like to know how many times people have failed to send mail because they flunked the test and whether they feel this actually saved them from a mistake.

I don’t think I’m particularly prone to saying things in late-night emails that I wouldn’t say otherwise, but I have other email vulnerabilities. In particular, I have to confess to a profound need to set the record straight or get the last word in email exchanges, a trait that can result in longer and more heated debates than would be desirable. Perhaps the next Google goggle can add even more checks to protect us from ourselves:

- “You’re sending the 10th message in this thread in the past hour. Take a break!”
- “You have a lot of exclamation points in your message. Want to tone it down?”
- “You and Jon have exchanged lots of messages on this, but the 20 other recipients of these notes haven’t said a peep. Take it private?”
- “Are you sure you want to take that tone with your upper management?”

I could go on, but you get the idea. In fact, as machine understanding continues to improve, I can imagine the analysis of such things moving from mechanical checks (any mail sent at 2 a.m. Sunday morning requires a sanity check, or flow analysis shows that many messages went out over a short period) to a deeper understanding. After all, if the mailer could distinguish between the drunken appeal to the ex-girlfriend and “normal” exchanges, it wouldn’t have to encumber sending normal email with the extra process. And if it could analyze intent, it could sense tone, examine what it knows about a recipient, and raise the red flag suggested in my last bullet item.

Not Just Email

Of course, email is just one way in which our computer systems and, in fact, other mechanisms are increasingly protecting us from our own mistakes.

One example is navigation systems. Cheap GPS technologies have made such systems almost as ubiquitous as mobile phones. The ability to get live updates on traffic status is a relatively recent addition to the technology, and a welcome one to anyone who drives a lot. But navigation systems (both handheld and online) could do other things better, such as factoring the time of a drive into the directions to avoid known, predictable bottlenecks.

Navigation systems should also be reliable. That is, their directions must be trustworthy. I’m on my second GPS, and it’s occasionally given me some strange directions — such as telling me to get off at one part of an exit and make a u-turn rather than get off the exit going in the right direction in the first place. But this is nothing compared to some of the odd directions I received from my first GPS (circa 2002), which became the “GPS that cried wolf.” It was so unbelievable that when it tried to offer a shortcut one time, I went miles out of my way before I realized that it wanted me to cut across a peninsula rather than traverse its perimeter.
Protecting the Vulnerable

Several utilities, such as gas, electricity, and phone companies, let customers specify in advance whom to notify in the event of nonpayment. The idea is that if a senior citizen or other vulnerable customer becomes forgetful or has other issues, a family member can take countermeasures before disconnecting a vital service.

Online services such as banks and credit cards have similar features: email alerts for late payments, unusual activity, low balances, and so on. Identity-theft defense mechanisms will notify you when new activity appears on your credit report. When someone is deemed especially vulnerable, such as when a hacker steals personal information from a company or government agency, extra countermeasures such as credit report freezes can deter abuse. (In fact, you can now freeze access even without an actual explicit fraud threat; see www.aarp.org/money/wise_consumer/scams/block_your_credit_reports_to_prevent_id_theft.html).

The catch is that, over time, it becomes easier and easier to become complacent. The first time I was notified that a thief had gained access to my US Social-Security number, I raced to block my credit files. The second time, I reactivated the freeze, perhaps after a few more days. More recently, I’ve just given up. But I ask myself, why is it that the default is to allow access to my report, without my explicit permission, in the first place? These days, everyone is vulnerable; just like the utility companies informing a relative when a problem occurs, each consumer should be entitled to free notification of anything affecting their credit report.

A Cautionary Tale

I recently saw an item on Slashdot about a woman who fell victim to a “Nigerian 419 scheme” (see http://tech.slashdot.org/article.pl?id=08/11/13/1659214, which refers to the original article at www.katu.com/news/34292654.html). I imagine that every reader is by now well familiar with the 419 schemes, named for an article in the Nigerian criminal code (see http://en.wikipedia.org/wiki/419_Advanced_Fee_Schemes for a history), and of course these scams aren’t limited to Nigerians.

The woman was suckered in part by the scammers’ email, which used her grandfather’s name and claimed he had left behind millions of dollars. As with all these scams, she was asked for a little money, then some more, and then still more. This particular article was interesting because the woman reportedly lost US$400,000 by mortgaging her (fully paid for) house, borrowing against her (paid for) car, and so on, and during this process she ignored many people’s advice to give up and stop throwing good money after bad.

What does this have to do with IEEE Internet Computing? Well, the victim here was taken in by a bo-

IC Welcomes New Board Members

Virgilio A.F. Almeida is a professor in the Computer Science Department at the Federal University of Minas Gerais (UFMG), Brazil. His research interests include large-scale distributed systems, Internet computing, autonomic computing, and performance modeling and analysis. Almeida has a BSEE from UFMG, an MS in computer science from the Pontifical Catholic University in Rio de Janeiro, and a PhD in computer science from Vanderbilt University. He has published more than 100 technical papers and coauthored five books on performance modeling, including Performance By Design (2004), Capacity Planning for Web Services (2002), and Scaling for E-Business” (2000), all published by Prentice Hall.

Stephen Farrell is a research fellow in the Department of Computer Science at Trinity College Dublin, where he teaches and researches security and delay/disruption-tolerant networking (DTN). He is also chief technologist with NewBay Software (www.newbay.com), a provider of digital lifestyle solutions for mobile network operators. He has a PhD in computer science from Trinity College Dublin. Farrell has been involved in Internet standards for more than a decade and currently cochairs the IETF Domain-Keys Identified Mail Working Group, is an invited expert in the W3C Web Security Context group, and cochairs the IRTF Delay Tolerant Networking Research Group. He coauthored Delay and Disruption Tolerant Networking (Artech House, 2006).
Editor in Chief
Fred Douglas • f.douglas@computer.org

Associate Editors in Chief
Siobhán Clarke • siobhan.clarke@cs.tcd.ie
Doug Lea • d@cs.oswego.edu
Michael Rabinovich • misha@eeecs.cwru.edu

Editorial Board
Virgilio Almeida • virgilio@dcc.ufmg.br
Helen Ashman • helen.ashman@unisa.edu.au
Elisa Bertino • bertino@ceriased.purdue.edu
Azer Bestavros • a@cs.harvard.edu
M. Brian Blake • blakeb@cs.georgetown.edu
Vinton G. Cerf • vint@google.com
Stephen Farrell • stephen Farrell@cs.tcd.ie
Robert E. Filman* • filman@computer.org
Carole Goble • c@cs.man.ac.uk
Michael N. Huhs • huhs@sc.edu
Barry Leiba • leiba@watson.ibm.com
Samuel Madden • madden@csail.mit.edu
Mark Manasse • manasse@microsight.com
Cecilia Mascolo • c.mascolo@cs.ucl.ac.uk
Pankaj Mehra • pankaj.mehra@hp.com
Chris Metz • chmetz@cs.com
Dejan Milojicic • dejan@hp.lhp.com
Jason Nieh • nieh@cs.columbia.edu
Charles J. Petrie* • petrie@stanford.edu
Krithi Ramamritham • krithi@cs.ibt.ac.in
Benno Schneidewind • hgs@cs.columbia.edu
Amit Sheth • amit.sheth@wright.edu
Munindar P. Singh* • singh@ncsu.edu
Oliver Spatscheck • oliver@spatscheck.com
Torsten Suel • suel@poly.edu
Craig W. Thompson • cwt@uark.edu
Shenggu Tu • shenggu@cs.uno.edu
Maarten van Steen • steen@cs.vu.nl
Steve Vinoski • vinoski@iiee.org

IEEE Computer Society Publications Office
10662 Los Vaqueros Circle
Los Alamitos, CA 90720 USA

Technical cosponsor:
IEEE Communications Society Liaison
G.S. Kuo • gskuo@mail.com

CS Magazine Operations Committee
David A. Grier (chair), David Albonesi, Isabel Beichl, Arnold (Jay) Brand, Carl Chang, Kwang-Ting (Tim) Cheng, Fred Douglass, Hakan Erdoganus, Carl E. Landwehr, Dejan Milojicic, Sethuraman (Panch) Panchanathan, Crystal R. Shif, Maureen Stone, Fei-Yue Wang, Roy Want, Jeff Yost

CS Publications Board
Sorel Reisman (chair), Alain April, Angela Burgess, Alan Clements, Frank E. Ferrante, David A. Grier, Audrey Kremer, Phillip A. Laplante, Paolo Montuschi, Jon Rokne, R. Sampath, Steve Seidman, Linda I. Shafer, Roy Sterritt, Steven L. Tanimoto

Sorel Reisman (chair), Alain April, Angela Burgess, Alan Clements, Frank E. Ferrante, David A. Grier, Audrey Kremer, Phillip A. Laplante, Paolo Montuschi, Jon Rokne, R. Sampath, Steve Seidman, Linda I. Shafer, Roy Sterritt, Steven L. Tanimoto

Writers: Access www.computer.org/internet/author.htm. Articles are peer reviewed for technical merit and copy edited for clarity, neatness, and space. Unless otherwise stated, bylined articles and departments, as well as product and service descriptions, reflect the authors’ or firms’ opinion; inclusion in this publication does not necessarily constitute endorsement by the IEEE or the IEEE Computer Society.

Letters to the Editors: Send letters to lead editor Rebecca L. Deuel at rdeuel@computer.org.


Subscribe: Visit www.computer.org/subscribe/.

Subscription Change of Address: Send requests to address.change@ieee.org.

Missing or Damaged Copies: Contact help@computer.org.

To Order Article Reprints: Email internet@computer.org or fax +1 714 821 4010.