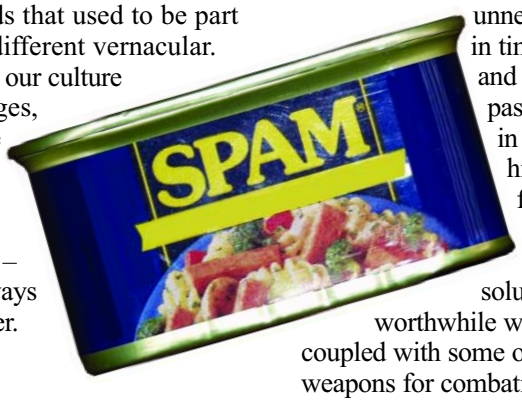
by Jen Sharp
JenSharp.com

The language of Internet danger

The Internet spawns new meaning for words that used to be part of a different vernacular. But as our culture changes, so does the technology that gives rise to new definitions – and not always for the better.



Spam and Filters

Today spam is not primarily the harmless yet repugnant brick of chopped meat product. It is now the scourge of the e-mail inbox. By December 2006 spam accounted for 90% of all e-mails. And there's more bad news on the horizon – it is predicted to get worse. Specialists at the California based global IT security firm, Secure Computing, predict that the volume will increase to 97% by December 2007!

Jen Sharp
JenSharp.com

Like the oil filter on a car, spam filters work similarly, but they are not a stand alone solution. There is simply too much spam! Filtering means the end user, the Internet Service Provider (ISP), and the computer system all have to work together and work harder. Yet, spam still gets through as spammers incessantly find new ways around filters. For example, spammers are now using image files for messages that include a random text to confuse filters. The unnecessary costs in time, money, and resources are passed on to users in the form of higher access fees. Using filters is only a temporary solution, and only worthwhile when they are coupled with some of the other weapons for combating spam.

Spoofing

A "spoof" used refer to a satire or parody. The Internet version of a spoof is not as innocuous. One of the dangerous things about spammers is an ability to "steal an identity." They can do this even if no personal information is given out. Let's say a user has an e-mail address on a Web site, on a contact page for a water system, recreational activity or club. Spammer robots are created that automatically detect an e-mail address format from Web pages much like search engines "crawl" sites to index them. Then, the fraudster spoofs your e-mail address and uses it as the "Return-Path" for their spam e-mails. Any return path can be used by simply changing a user's e-mail account settings. It doesn't even have to be a valid e-mail address. It can appear that *any* innocent Internet user is sending out spam, even if it did not originate from their computer!

A somewhat effective solution for this is a Javascript snippet that is placed directly into the html document exactly where the e-mail address will be displayed (see at left.) Another solution is to use an e-mail address separate

```
<script
language="JavaScript"
type="text/javascript">
<!-- Begin
user = "krwa";
site = "krwa.net";
document.write('<a
href=\"mailto:' + user +
'@' + site + '\">');
document.write(user + '@'
+ site + '</a>');
// End -->
</script>
```

Where did using the term "spam" to mean unsolicited e-mail originate?

The prevailing theory is that it is from the song in Monty Python's famous spam-loving vikings sketch that goes, roughly, "Spam spam spam spam, spam spam spam spam, spam spam spam spam..." The vikings, who were sitting in a restaraunt whose menu only included dishes made with spam, would sing this refrain over and over, rising in volume until it was impossible for the other characters in the sketch to converse (which was, of course, a large part of the joke.)
– *from* www.cybernothing.org

The Internet spawns new meaning for words that used to be part of a different vernacular. But as our culture changes, so does the technology that gives rise to new definitions — and not always for the better.

from one's personal address for public use. Yahoo and Hotmail are two providers of free e-mail services.

Headers

Not the All-American double header baseball game, e-mail headers are a sort of "envelope" that traces the path of an e-mail from its sender to its recipient. In the sidebar at right shows an example of an e-mail header. The number following the Originating IP is usually the sender's *IP address* (the yellow hi-lited line)**.** An IP address is a specially assigned number, like a serial number, assigned to the user's exact computer. Although the user can assign their own IP address to their hard drive, many Internet service providers dynamically assign a number to the user as they log onto their service. The IP addresses following *Received: from* tells the story from top to bottom, the path that e-mail took to reach the user's computer. Online databases can be used to look up information about suspect IP addresses.

Internet numbers are assigned by region. Anyone can look up a specific IP address using any one of these Regional Internet Registries (RIR) and find information about where that IP originated (see chart on the next page.) It may not known immediately what region the IP address is in, but these IP databases will redirect to the appropriate region. Most of the time, one will find the IP address as part of a range of numbers assigned to a company. However, by looking at the range of IP addresses, an investigator can narrow down what company a particular spammer uses as their ISP. E-mail addresses can be found along with physical addresses, and phone numbers to contact these companies. Since in most cases, individuals will have a different IP number each time they log on, a sleuth will need to report the IP number *and* time of the abuse to the network administrators, who should be able to use log files to contact the individual involved. ISPs will not give out detailed information about the exact user. If that company receives multiple and frequent abuse complaints about a particular IP address, they can take action on that spammer, such as a refusal to continue providing service.

Obviously, looking up an IP address for every spam e-mail would be time consuming and nearly impossible. However, if there is a particular repetitive problem, complaining to the ISP of a spammer can get results. There are also services and shareware available that do this automatically, such as SpamCop, Spam!Alert, and Spam Control. Other resources can be found at http://spam.abuse.net/userhelp/#report.

E-mail header – complete from sender to recipient

From KRWA Wed Jan 10 06:24:34 2007
X-Apparently-To: skydivekansas@sbcglobal.net via 192.168.12.711; Wed, 10 Jan 2007 06:27:16 -0800
X-Originating-IP: [192.168.12.711]
Return-Path: <krwa@krwa.net>
Authentication-Results: mta129.sbc.mail.mud.yahoo.com from=krwa.net; domainkeys=neutral (no sig)
Received: from 192.168.18.408 (EHLO flpi136.sbcis.sbc.com) (192.168.189.408) by mta129.sbc.mail.mud.yahoo.com with SMTP; Wed, 10 Jan 2007 06:27:16 -0800
X-Originating-IP: [192.168.12.711]
Received: from vision.worldhosted.com (vision.worldhosted.com [192.168.12.711])
by flpi136.sbcis.sbc.com (8.13.8 inb/8.13.8) with ESMTP id l0AER40W007437
for <skydivekansas@sbcglobal.net>; Wed, 10 Jan 2007 06:27:05 -0800
Received: from SMTP32-FWD by jensharp.com (SMTP32) id A037032D0; Wed, 10 Jan 2007 09:22:59 -0500
Received: from server.haugcomm.com [12.40.38.9] by vision.worldhosted.com with ESMTP (SMTPD32-8.05) id A65E2DE4007C; Wed, 10 Jan 2007 09:21:18 -0500
Received: from 12.40.38.196.haugcomm.com ([12.40.38.196] helo=[192.168.0.5])
by server.haugcomm.com with esmtpa (Exim 4.60)
(envelope-from <krwa@krwa.net>)
id 1H4eNR-0006cx-Tg
for jen@jensharp.com; Wed, 10 Jan 2007 08:25:12 -0600
Message-ID: <45A4F722.2020300@krwa.net>
Date: Wed, 10 Jan 2007 08:24:34 -0600
From: KRWA <krwa@krwa.net>
User-Agent: Mozilla Thunderbird 1.0.7 (Windows/20050923)
X-Accept-Language: en-us, en
MIME-Version: 1.0
To: Jen Sharp <jen@jensharp.com>
Subject: Re: Web Update
References: <45A2A8D7.4070907@krwa.net>
In-Reply-To: <45A2A8D7.4070907@krwa.net>
Content-Type: multipart/alternative; boundary="----------070708090509090601050300"
Content-Length: 422056

How do I view a header in my e-mail program?

With Outlook Express – Select a message, under main menu: File, Properties, Details tab

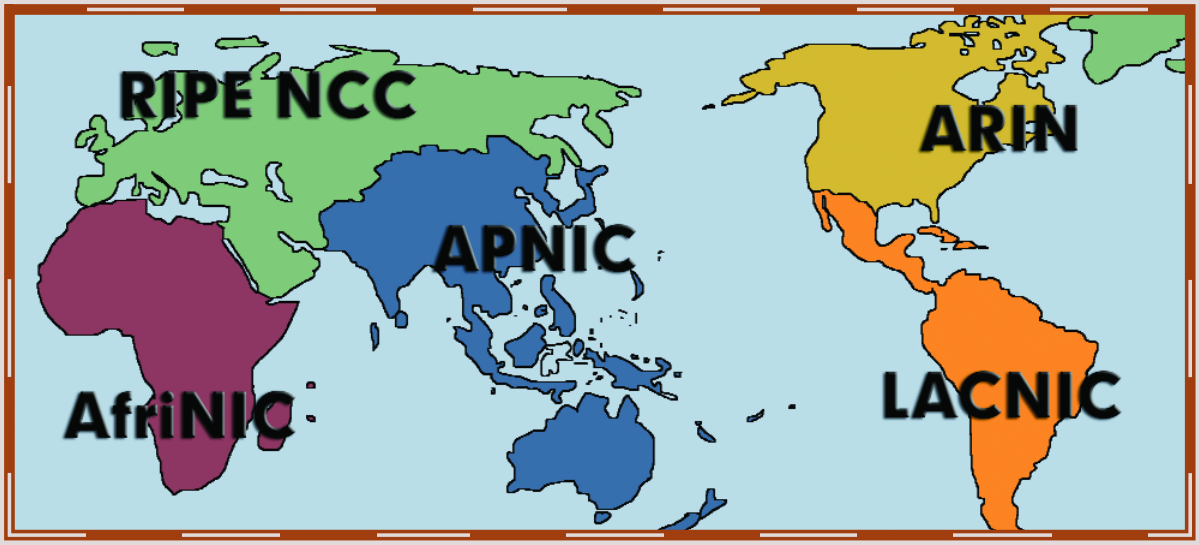
With MS Office – Select a message, under main menu: View, Options: Internet Headers at bottom of window

With Yahoo – click on Full Headers at the top right of the message

With Hotmail – on top menu bar at right: Options, Mail Display Settings, under Message Headers select Full or Advanced

With Thunderbird – under the main menu: View, Headers, All

World Regional Internet Registries



APNIC – Asia Pacific Network Information Centre	**www.apnic.net/apnic-bin/whois.pl**	Asia/Pacific Region
RIPE NCC – Réseaux IP Européens Network Coordination Centre	**www.ripe.net/perl/whois**	Europe, the Middle East, Central Asia, and African countries located north of the equator
ARIN – American Registry for Internet Numbers	**www.arin.net/whois**	Canada, the United States, and several islands in the Caribbean Sea and North Atlantic Ocean
AfriNIC – African Regional Network Information Centre	**www.apnic.net/apnic-bin/whois.pl**	Africa Region
LACNIC – Latin American and Caribbean Internet Addresses Registry	**http://lacnic.net/cgi-bin/lacnic/whois**	Latin America and some Caribbean Islands
ICANN – Internet Corporation for Assigned Names and Numbers	**www.icann.org & www.internic.net**	Global non-profit organization that oversees distribution of IP addresses to RIRs

In general, these databases contain details of the networks that are using address space, not the individual users. There are two major types of whois databases. One type contains records on domain names and the other contains IP address (the numerical sequence that serves as an identifier for an Internet server) records .These are IP address databases.

Blog Posters

"Poster" used to mean a large colorful picture or advertisement – now it's someone who posts on a *blog.* More and more Internet users are posting to guest books, forums, newsgroups, and the increasingly popular chronological "diary" called a blog. This means, more opportunities for spammers to flood resources and lock up a site, or simply to post annoying or advertising content.

If a Web site is maintained with a contact form, forum, guestbook, newsgroup, or blog, be sure to include as part of the information gathered from posters their IP address, or remote name as it is sometimes called. This will allow the ability to look up their origination information, or even block their IP address from your site.

Phishing

No, it's not something to do at the lake on a lazy Sunday afternoon—Internet criminals set up fraudulent Web sites or solicitations by e-mail that invite users to give them personal data. They set the bait and hook and wait as they *phish* for unsuspecting users to believe their scam. Phishers need user cooperation for this to work: their schemes to get your sensitive private information include lottery winners, free Web space, soliciting donations for a cause, make money fast claims, and chain letters. This is the "Information Age" where data is gold. Protecting personal information is as imperative as keeping valuables in a safe.

Users are becoming educated and more cautious to fraudulent e-mails claiming to be a well-known company asking for sensitive information. So, fraudsters take it up a notch: a new extension to phishing is *vishing,* where criminals use the Internet to call users on the phone, leaving them an automated

Who to complain to:

America Online: abuse@aol.com
Compuserve: ecgintern@csi.compuserve.com
Prodigy: mailadm@prodigy.com
AT&T WorldNet: abuse@worldnet.att.net
Earthlink: spam@earthlink.net
abuse@earthlink.net
Netcom: abuse@netcom.com
For others: postmaster@<the provider's site>
(according to internet standard RFC822 (STD 11), all sites are supposed to have such a mailbox)

message that warns them some "account" is in jeopardy. They are told a call is needed to update account information, which of course includes a credit card number.

Herders and Zombies

Many think that "Night of the Living Dead" defined zombies? And many have thought the worst thing a virus could do was to cause a cough and fever? In the past, a hacker goal was to write a virus that would be the most destructive. Today, viruses are being written specifically to create a robot network or *botnet*. The botnet goal is to elude detection by anti-virus software, to "lay low" and quietly take over the user's computer. The botnet collection of compromised machines runs programs (worms, Trojan horses, and viruses) under a common command that controls the network. The *bot herder*, or originator, controls the group, much like herding cows, only it is done remotely without the user's knowledge or permission. Any user could be an involuntary spammer, a *Zombie*, and not know it! It is estimated that more than 450,000 unique zombies appear every day!

Sample complaint letter:

Hello. The spammer below is either using your resources to send out bulk unsolicited commercial e-mail (spam) or is deceptively trying to make it look like he/she is. In either case, a legitimate company like yours probably would not approve. The information below should be all you need.

--begin full headers--

(from abuse.net)

What to do and what not to do.

Do's

- Subscribe to a blocking list or ask your ISP to do so.
- Install spam-reporting software or use an automatic spam reporting service.
- Report spam abuse to sites like abuse.net that are dedicated to fighting spam.
- Complain to ISPs that originate and forward the spam.
- Things change all the time. Keep up-to-date, educated and watch for suspicious activity.
- Consider using a separate e-mail address for some public activities such as chat rooms or contact list on your Web site, in order to protect your main address from spammers.
- If possible, consider setting up a filter to block all e-mail unless its address is on the approved list.
- Write legislators and let them know this is an important issue to you. Suggest they promote an "opt-in" approach vs. the current "opt-out" view.

Don'ts

- Give your e-mail address or other personal information when filling in forms online unless you are confident in the reputation of the company and confident it's not an imitation Web site.
- Give any private sensitive data such as credit card numbers or social security numbers unless you are confident you are dealing with a reputable company and not an imitator.
- Never reply to spam, even if it is to send a "remove" request. Most spammers ignore such responses, or worse, add you to their list of validated e-mail addresses that they sell.
- "Spam the spammer" – this doesn't help, wastes time, and can validate the user's address e-mail to the spammer.
- Just rely on your filter, or use a manual filter. This means even more time is wasted. Filters don't work that well, and spammers continue to find ways around them. You also must act in other ways.

Additional online resources

Check these Web sites for additional help:

- http://spam.abuse.net/
- http://spam.abuse.net/userhelp/howtocomplain.shtml
  How to complain!
- www.cauce.org
  Coalition Against Unsolicited Commercial E-mail
- www.spamcop.net
  List of Resources
- www.windweaver.com/nospam2.htm
  How to Report Spam
- www.abuse.net
  Network Abuse Clearinghouse
- www.mynetwatchman.com
  Monitoring and reporting worm/hacking activity
- www.cybernothing.org/faqs/net-abuse-faq.html
  Spam FAQs
- www.elsop.com/wrc/nospam.htm
  List of Links
- www.ecofuture.org/jme-mail.html
  List of Links