

## E-Mail in the Age of Spam

By Holly Moskerintz, Online Services Manager,  
Reid Trautz, Practice Resources Associate,  
and Robert P. Deasy, Director of Liaison and Information

E-mail, praised by many as the Internet's killer application, is also the one that people love to hate. It's not uncommon to hear complaints about e-mail such as I get too much junk or unsolicited e-mail; I got a virus via an email message I opened, etc. Spam, viruses, identity-theft schemes, and hoaxes are just some of the threats to e-mail users today.

### Common Email problems

**Spam:** Spam is junk email that is unwanted or unsolicited and is mostly advertising, like junk mail you receive in your mailbox everyday. Spam is more of a nuisance than a threat, but some spam can transmit viruses, adware or spyware on to your computer and cause problems. Every day, spammers find new routes to try to get into your email inbox. When you receive an e-mail and you are suspicious of its origins, the best practice is not to open it, but to delete it entirely from your system.

**Spoofing:** "Spoofing" is a form of spam where the "header" of an email address is falsified to appear as if it came from a different sender's address. This type of activity is commonly used to circumvent spam filters and deliver spam email to end-users. In fact, you may have received emails that appear to be from AILA, or other organization, but which in fact are not. It is almost impossible to stop these deceptive email messages.

**Phishing:** A form of spoofing which takes criminal activity to the next degree. It is a play on the word "fishing", i.e. to throw out bait or lures in the hopes of getting a few bites. Phishing involves sending an email and making it appear as if it comes from a legitimate corporation or organization. The purpose of the email is to scam the user into providing private information for the purpose of fraud, identity theft, and so forth.

### Solutions to Common Problems

Tools have been developed to prevent some of these problems from happening, including spam filters, phishing filters, antivirus and antispyware software, and Sender ID software.

**Spam Filters:** Spam filters are software that blocks unwanted spam. Features include the ability to set rules about which email you want to receive in your inbox, reject or delete, or divert to be put in a certain folder. You should be able to set up blacklists (also called blocklists these are lists of IP addresses, domain names and email addresses to be blocked from private networks) and whitelists (a record of senders that have explicit permission to e-mail an individual).

**Phishing Filters:** Phishing filters include several technologies designed to warn or block you from potentially harmful Web sites.

**Antivirus Software:** Antivirus software are programs that either come installed on your computer or that you purchase and install yourself. It helps protect your computer against most viruses, worms, Trojan horses, and other unwanted invaders that can make your computer "sick." Viruses, worms, and the like often perform

malicious acts, such as deleting files, accessing personal data, or using your computer to attack other computers.

**Antispyware Software:** Antispyware software helps to protect your computer from known programs that can track your Web browsing habits or make changes to your computer settings without your consent or control.

**Sender ID:** Sender ID checks and validates the sender's e-mail address against the actual sending address and Sender Policy Framework (SPF), and provides a way of authenticating an e-mail sender's IP address and blocking e-mails with false sender information.

## **Problems With the Solutions**

Unfortunately, Spam blocking software is far from perfect and you may not be getting important email messages that you need or want. Although we all complain that the software still lets some spam through, the bigger concern is that it blocks legitimate and important emails from getting to your Inbox.

Spam blocking programs create a folder (i.e. "Junk Email", "Spam", etc.) in the email client (Outlook, Hotmail, etc.) to place the emails the software characterizes as "spam." In truth, the folder should be labeled "Suspected Spam" because the software can often mischaracterize a legitimate email. When that email is a message from a client or an agency on an important matter, letting it be filtered as spam can be a fast way to a malpractice claim.

In addition, some anti-spam filters require senders of the e-mails to go through an "approval" process so that their emails can be approved by the recipient. If they are not approved, the email message will be "blocked" and will never reach the recipient. It should not be expected that all senders, whether government or non-government, will go through these extra steps to get their email address approved and accordingly, you will not receive their message. Moreover, automatic notification systems, such as the USCIS Premium Processing e-mail notification system and the DOL e-mail PERM filing notification system, are not set up to respond to these "authentication" requests. Therefore, you will not receive an e-mail notification or receipt from government agencies if you have this type of spam filter enabled.

In any environment where you are expecting an e-mail to an address that is protected with an authentication application, the benefits and risks of disabling the feature should be considered.

## **Email From The Government**

With increasing frequency, government agencies are relying on e-mail to notify applicants and attorneys of important events on pending cases. For example, USCIS uses e-mail notification in its Premium Processing service. The Department of Labor uses e-mail notification at several stages in PERM processing, and many of the State Workforce Agency (SWA) offices use e-mail notification. (The Colorado SWA has this message on its job order page: "\*\*\*7/2006 Due to recent changes at Yahoo, job notifications will no longer be sent to Yahoo email. You will need to use a different email address to receive scout emails from this site.\*\*" See: [http://www.connectingcolorado.com/.](http://www.connectingcolorado.com/)) E-mails from the DOL's PERM system containing your Password and PIN may be blocked by your Internet Service Provider's (ISP)

spam blocking features. If you want to receive email messages from the government, you need to follow the instructions below to include government-related domains on your whitelists and approved list of senders to ensure that email messages from the Government are not blocked.

## **Email From AILA**

As you may know, AILA relies on email to communicate and disseminate information to our members. These emails include messages from our listserves, AILA e-newsletters, all-member announcements, and InfoNet Recent Posting Alerts. Additionally, AILA's case-specific liaison assistance system relies on e-mail communication from member volunteers on liaison committees to members who submit requests to the liaison committees. Unfortunately, we, too, are finding that some anti-spam and other protection software blocks these e-mails from reaching you and you may not be getting important news, updates, and information from AILA.

In order to receive mail from AILA and AILA members, make the same kinds of adjustments to your spam blockers and whitelists that are suggested for receipt of government e-mail.

## **Ensuring You Receive the Emails You Want/Need**

- Make sure AILA and others have your most up-to-date email address. For AILA, confirm your email address on the "My Profile" page on InfoNet (<http://www.aila.org/user/>).
- Include AILA and others, such as the government, on your whitelist in your email server Spam Filter. For AILA, add aila.org and lists.aila.org to your whitelist, or if you want them to unblock individual addresses, use conferences@aila.org, membership@aila.org, ailanews@aila.org, aila\_e-news@aila.org, webmaster@aila.org, teleconferences@aila.org, advocacy@aila.org, etc.

When seeking case-specific liaison assistance, add the related service center email alias (vscliaison@aila.org, nscliaison@aila.org, cscliaison@aila.org, tscliaison@aila.org, nbcliaison@aila.org,) to your whitelist so that you can receive a receipt for the inquiry. Once you receive email notification from AILA informing you of the liaison committee member to whom your case is assigned, "whitelist" or otherwise unblock that committee member's address.

- Check the "Spam" folders in your email application for legitimate emails each day. Important emails may be going there and you may miss them. Your practice may depend on it.
- Adjust your email software spam blocker options to allow the aila.org and other domain emails to be on the list of approved senders. If you cannot correct this problem yourself, it is recommended that you contact your ISP to ensure the AILA addresses, and other approved sender addresses, are not blocked. Here are suggestions for those who use EarthLink, AOL, or Hotmail e-mail services:

-- EarthLink's ScamBlocker: change settings at Your Support Center/Fraud-Spam Protection. Unblock a Blocked Email Address in SpamBlocker for EarthLink Web Mail

-- AOL Customizable Spam Controls: change settings at: Spam Controls Settings. Unblock Sender with AOL® and AIM® Mail Controls

-- Hotmail's Junk E-Mail Protection: change settings on the Safe List page. Messages from addresses (or domains) on your Safe List are never filtered to Junk E-Mail.

## **Conclusion**

Increased reliance on e-mail for critical communication is truly a double-edged sword. For every step that has to be taken to guard against harmful e-mail there is erected a corresponding hurdle to the receipt of legitimate e-mail that has a direct bearing on the outcome of cases and the lives of our clients. We hope these insights and suggestions are helpful as you try to balance these competing concerns.