The past decade has witnessed a radical transformation of international communications. Thanks to the digital revolution, people on different continents can interact as easily as if they were across town, and thanks to mobile devices and wireless access, they can do so from nearly anywhere. At the core of this increasingly “flat world” is the networked computer, which has revolutionized the ways in which we work, obtain information, communicate, shop, manage our finances, pay our bills and taxes, and spend our leisure time.

However, the digital revolution is a two-edged sword. Computers and the Internet offer unparalleled opportunities not only to those who use them, but also to those who abuse them. Consequently, our increasing reliance on computers and information technologies in both our professional and personal lives represents a potentially significant source of cyber risks. If we fail to identify, understand, and mitigate these risks, we leave ourselves vulnerable to a variety of online threats whose consequences can range from annoyance and inconvenience to devastating disasters such as identity theft, credit card fraud, and catastrophic data loss.

In order to mitigate cyber risks, it is necessary to identify and understand both the threats and the vulnerabilities. This sounds straightforward enough in the abstract. However, the Internet differs in fundamental ways from traditional large-scale distributed services, such as gas, water, or electricity. As Scott McNealy, chairman of the board of Sun Microsystems, has observed: “In the past we’ve had all kinds of utilities—water, electricity, dial tone—that have been distributed through large servicing and client models. A large water reservoir connected with pipes to a water tap. It’s a very easy on/off kind of use at the client’s site. You don’t need a manual to take a shower. Or you have a large telephone switch connected to wires or wireless and connected to a very easy to use device called a telephone. Do you know how you boot a telephone? You pick it up and you’ve now booted the most incredible system on the planet—dial tone. The same is true with electricity. You have this huge nuclear power plant or Hoover Dam connected with wires to a thin client. That thin client is a hairdryer or a light switch. Do you have manuals for light switches? It’s up or down, on or off.”

The relationship of users to the Internet is fundamentally different, and therein lies a conundrum: the responsibility for cyber security rests largely on the shoulders of the individual, but most individuals are not in a position to address information technology issues of this scope, scale, and complexity. Because ignorance is most certainly not bliss where cyber security is concerned, this will be the first in a series of articles in The ATA Chronicle that will explore some of the most prevalent online threats facing users today, namely spam, phishing, spyware, adware, viruses, and survival time. Examining each in turn, we will discuss the nature of these threats as well as tools and strategies for detecting and preventing them. This first article will focus...
on spam. Although spam is not a security problem per se, it is a common vector for phishing activities, which represent very serious threats indeed. Phishing will be the subject of the next article.

**Spam: From Processed Meat Product to Electronic Annoyance**

Spam® is a canned processed meat product made by the Hormel Foods Corporation. Until recently, such was the primary—and for most people, the only—meaning of the word. However, over the past decade or so, “spam” has also come to connote a scourge of modern life—unsolicited bulk electronic communications. Although there are many different types of electronic spam, we will confine our discussion to e-mail spam, i.e., “unsolicited commercial e-mail from someone without a pre-existing business relationship.” A given spam message is typically sent *en masse* to hundreds of thousands or even millions of e-mail addresses. Typical e-mail spam includes offers for discounted medications, mortgages, and software or watches; invitations to fill prescriptions online; announcements of job opportunities; and hot stock tips (to cite just a few examples).

Spam is first and foremost an annoyance. A recent Pew Internet study of spam and e-mail habits found that:

- 67% of e-mail users say spam has made being online unpleasant or annoying.
- 53% of e-mail users say spam has made them less trusting of e-mail.
- 52% of Internet users consider spam a big problem.

In order to mitigate cyber risks, it is necessary to identify and understand both the threats and the vulnerabilities.

According to Postini, spam currently accounts for a whopping 90.9% of e-mails. The prevalence of spam translates into an enormous waste of bandwidth, disk space, and time. The problem is one of such magnitude that ignoring spam is not a viable option for most people. Indeed, if left undeleted, incoming spam can rapidly cause e-mail account quotas to be reached or exceeded, at which point all new incoming messages will be rejected. If left undeleted, incoming spam will also bump legitimate e-mail down the list of incoming messages in one’s inbox. Depending on the user’s page settings and the volume of spam received, legitimate messages may be quickly displaced from the first page of new messages onto subsequent pages where they run the risk of remaining unseen. Consequently, the more quickly spam accumulates, the more often it must be deleted.

**How Did They Get My Address?**

Such problems lead us to ask where spam comes from and what we can do to minimize it. To answer these questions, we must begin by examining how

---

**Figure 1**

```html
<TR>
<TD><STRONG>Contact Me:</STRONG></TD>
<TD><a href="mailto:translator@company.com">Click here to contact me</a></TD>
</TR>
```

**Figure 2**

```html
<a href="mailto:user@domain.com">Hyperlink text</a>
```
spammers get our e-mail addresses in the first place. One of the main ways that spammers compile mailing lists is to harvest publicly available e-mail addresses from the web. Spammers create special programs called “spam bots” (short for “spam robots”) to scour the web looking for e-mail addresses, which they harvest and compile for future spam mailings. One of the easiest ways for spam bots to harvest e-mail addresses is to pull them from e-mail hyperlinks within webpages.

For example, let us imagine that we create a website to advertise our translation services. As part of our site, we author a “Contact” page with an e-mail hyperlink that prospective clients can use to contact us. Let us imagine that our imaginary contact page includes an e-mail link as shown here in bold:

**Contact Me: Click here to contact me**

The underlined text is a hyperlink that points to our e-mail address. If someone clicks on the hyperlink, his or her e-mail program will open a new message addressed to “translator@company.com.” The HTML source code of our e-mail link is shown in Figure 1.

The snippet of code in bold specifies a hyperlink to an e-mail address. E-mail hyperlinks take the generic form shown in Figure 2. In an e-mail hyperlink, the syntax, “mailto:user@domain.com” means “clicking on this link will open an e-mail message to user@domain.com.” The text that is enclosed within tags (i.e., located inside angle brackets) remains hidden from users and is only used behind the scenes, as it were, to specify the recipient of the new e-mail message that will open when a visitor clicks on the link. In an e-mail hyperlink, the browser only displays text that is located between or outside pairs of tags—in this case, the phrase “Hyperlink text,” or in the case of our imaginary “Contact” page, the phrase “Click here to contact me.”

Although it remains hidden from humans who browse the page, the e-mail address inside the hyperlink is clearly visible in the code—and thus entirely exposed—to anyone who wants to look for it. Consequently, spam bots can locate e-mail addresses automatically by scanning webpages until they find an occurrence of the syntax “mailto:” that characterizes an e-mail hyperlink. Once the spam bot has found an e-mail link, harvesting the address is a relatively simple matter of reading from “mailto:” until it reaches either the closing quotation mark (“”), or a question mark (?), ampersand (&), or any other character that is illegal within an e-mail address, as shown in Figure 3. In this example, the spam bot would read from “mailto:” until the question mark, thus identifying “user@domain.com” as the e-mail address, which it would store for later use.

**Encryption, Please**

Because spam bots regularly visit webpages looking for “mailto:” links, it is imperative that we encrypt or otherwise obfuscate our e-mail hyperlink so as to render the address invisible to spam bots. If we do not, we...
might as well invite the world to spam us. A few days after we publish the page containing the e-mail link, we will notice a dramatic increase in the number of spam messages that we are receiving. Once our e-mail address has been added to a spam list, there is a good chance that it will be bought and sold as part of that list (and/or other spam lists), which will in turn further increase the volume of spam that we receive.

This imaginary scenario need not become reality. If we author web materials, or even if we contract with a designer or developer to have such materials authored for us, we can encrypt or otherwise “hide” our e-mail address so that spam bots cannot find and harvest it. We can use Automatic Labs’ free Enkoder or some other encryption tool to obfuscate the source code of the hyperlink. Here’s how:

• First, we copy the source code:
  
  &lt;a href="mailto:translator@company.com">Click here to contact me&lt;/a&gt;

• We then paste the source code into the Advanced Form textbox on the Enkoder page and click the "Enkode it >>" button. The Enkoder converts our hyperlink code into what appears to be gibberish.

• We copy and paste the results back into the source code of our webpage, overwriting the original hyperlink source code. After doing so, the code of our e-mail link looks like Figure 4.

At this point, our e-mail link has been effectively obfuscated. Henceforth, the e-mail address will be invisible to spam bots looking at the code, but not to people who browse the page. Like a disguise, the Enkoder changes the appearance of the code, but not the information it contains.

Unfortunately, spam bots are not the only means by which our e-mail addresses can be compromised. Spammers are extremely clever, and they also compile mailing lists by means of algorithms that combine large numbers of common first names, last names, and/or digits to randomly generate massive numbers of e-mail user IDs. These user IDs are then tacked on to the names of popular e-mail providers such as Gmail.com, Hotmail.com, and Yahoo.com. In this way, the first name “John” and the last name “Doe” might give rise to the following e-mail addresses (among many others):

  john.doe@gmail.com,
  john.doe@hotmail.com,
  john.doe@yahoo.com,
  jdoe@gmail.com,
  jdoe@hotmail.com,
  jdoe@yahoo.com,
  jdoe1@gmail.com,
  jdoe1@hotmail.com,
  jdoe1@yahoo.com, etc.

This technique is known as a “dictionary attack.” The more common the first and last names, the greater the chances that some of these randomly generated addresses will actually be in use.

### Practical Strategies for Limiting Exposure to Spam

The spam/anti-spam battle is a large-scale game of cat and mouse. Given the profit motive—“some 6% of e-mail users say they have ordered a product or service offered in an unsolicited email”—experts predict that “[spam] will be with us in one form or another for the foreseeable future.”

All is not lost, however. Consistently following a few simple rules can help reduce and prevent spam:

• Never post your personal or work e-mail address on the Internet. Spam bots search every possible online source of e-mail addresses, including webpages, blogs, forums, guest books, chat rooms, and news groups to name just a few. If the publication of your address is unavoidable for one reason or another, obfuscate your e-mail address as described above, if possible; otherwise, create a new e-mail account specifically for this purpose using a free e-mail provider.

• Another cardinal rule of spam mitigation is that you should

Depending on the user’s page settings and the volume of spam received, legitimate messages may be quickly displaced from the first page of new messages onto subsequent pages where they run the risk of remaining unseen.
never reply to spam messages. Doing so identifies you as someone who reads spam, and only serves to guarantee that you will receive even more of it.

• Likewise, it is critical to never open spam if your e-mail client displays images by default. If possible, configure your e-mail client to turn off images or to allow you to decide on a per-message basis whether to display images. Spam often includes links to graphics and images. These graphics and images are not sent as part of the message, but are stored on the spammer’s server. In order to display the images, your e-mail client must “request” them from the spammer’s server, which will be only too happy to comply. The transfer of the graphic files to your machine will be noted, and you will be identified as someone who reads spam, thereby ensuring that you will receive more of it.

• Follow e-mail Netiquette. If you send e-mail to multiple recipients, either send the message individually to each recipient, or enter the addresses of the multiple recipients in the “BCC:” (blind carbon copy) field. Never enter multiple addresses in the “CC:” (carbon copy) field. If a forwarded copy of your message falls into the wrong hands or your e-mail address book is compromised by a virus, those contacts will likely be added to a spam list.

• Given the sheer volume of spam, which as noted above comprises over 90% of all e-mail messages, it is essential to use a spam filter to diminish the volume of unsolicited and undesired junk e-mail that ends up in your inbox. Many Internet service providers offer spam filtering as part of their packages, as do commercial e-mail providers such as Gmail, Hotmail, and Yahoo!. Stand-alone anti-spam software is also available from companies such as Firetrust and Cloudmark. Although this article is written for a target audience of e-mail end-users, it is important to note that spam can have serious unintended consequences for server administrators as well. Today, e-mail servers must be configured properly so that they do not act as anonymous “open relays” that will allow anyone on the Internet to forward e-mail. Spammers open relays, which help them avoid detection. If spam is relayed through your server, it is your server that will be identified as the source of the spam and added to spam block lists compiled by Brightmail, SpamCop, Spamhaus, and others. If your server is blacklisted, the messages you send will be rejected by anyone whose e-mail is filtered using such lists.

• A final technique that can help reduce spam is to create dedicated e-mail accounts for public use and/or any application that places your e-mail address at risk of being harvested by spammers, and then configure these accounts to forward incoming mail to your personal, non-public e-mail address. The advantage to forwarding e-mail in this way is that spam will be stripped at each step of the journey.

Conclusion

Spam is a bane of modern life by which unscrupulous individuals and companies send vast quantities of unsolicited and unwanted e-mail to unsuspecting innocent victims, most of whom have no idea why they receive spam or what they can do to prevent it. Indeed, a 2005 Pew Internet study of e-mail habits noted that “e-mail users have changed their spam avoidance behavior very little in the last year and a half. If anything, they have been a little less likely to practice good habits.” The study concluded that when it comes to spam, “users are not helping themselves.” It is hoped that the information in this article will help ATA members reduce their exposure to spam. While no single tool or technique can guarantee total immunity from the sophisticated and ever-evolving methods employed by spammers, following a few simple steps can help reduce vulnerability to spam, and thus limit the volume of junk e-mail received. It is incumbent upon individual users to take every possible precaution to protect themselves and others against spam, because when all is said and done, you can ignore spam, but it will not ignore you.

Notes


3. This connotation can ultimately be traced to a 1970 Monty Python sketch, “set in a café where nearly every item on the menu includes SPAM luncheon meat. As the server recites the SPAM-filled menu, a chorus of Viking patrons drowns out all conversations with a

4. Forms of electronic spam include blog spam (“blam” or “splogs”), instant messaging spam (“spim”), short message service (SMS) and text-messaging spam (“SpaSMS”), search engine index spam (“spam-dexing”), plus their venerable predecessor, junk mail faxes. Some of these media suffer an even higher proportion of spam than e-mail. Real-time statistics published by Askimet, for example, indicate that no less than 94% of all blog comments are spam. Askimet. “Live Spam Zeitgeist.” *Askimet Frequently Asked Questions.* http://akismet.com/faq (February 20, 2007).


6. See, for example, the October 20, 2006 SecuriTeam blog posting in which an anonymous information technology security professional announces his recent inadvertent acquisition of a spam list containing 23.5 million addresses. Prozpagod. “Very Big Spam List.” *SecuriTeam Blogs* (October 20, 2006). http://blogs.securiteam.com/index.php/archives/691 (February 28, 2007).


9. One can view the source code of a webpage by choosing View → Source in Internet Explorer, for example.


14. Because legitimate mail is occasionally misidentified as spam, it is important to periodically check your spam folder to ensure that it contains no legitimate messages.
