

Spam Education

What is spam?

Spam is unsolicited commercial email (UCE) or unsolicited bulk email (UBE).

How much does it cost to produce spam?

Currently, the cost of acquiring an email address list, creating a spam message, and delivering it to a million email addresses can cost less than \$50. That's less than \$.00005/email recipient. Compared to the cost of Sending bulk "junk" mail, this is relatively free. With less than 1 in every 100,000 recipients responding, a "spammer" can turn a nice profit.

How do "spammers" get my address?

Spammers have many ways of finding your email. Some of the more popular tools are:

- "Viruses" – stealing address books and contact lists
- MX server extractors – Ping email servers until a valid email is returned
- Various spy-ware tools – Extract email addresses from stationary and transient emails
- Opt-in/Opt-out lists – Regardless of what the web site/email says, you are probably added to an address list
- Automated email spiders – continuously search websites, forums, and newsgroups for individual email addresses and email lists (same technology that creates most web databases)

How can I combat spam personally?

No one method is fool-proof, but every little bit helps. Here are nine ways to minimize your "spam exposure".

1. Never give your email address to someone/some-site you don't trust (treat it like a credit card number, not like a phone number).
2. If you don't know the sender of an unsolicited email, delete it (sometimes just viewing it can let spammers know that you are a "live customer" and a future target).
3. Never make a purchase from a spam message (if UCE or UBE became economically infeasible, then it would go away).
4. Never respond to a spam (even clicking on "please remove me from your mailing list" links may result in even more spam).
5. Never click on a link within a commercial email (even if you trust the company it is safer to go to their website another way).
6. Never use the preview function on email clients (this is basically like opening all of your email – see above).
7. Always use the "BCC" field for addressing large groups (the exposed "TO" field is much easier for spammers to harvest email addresses from).
8. Never provide your email in a public forum (like on public web sites, forums, and newsgroups).
9. Have a "placebo" or "dummy" email address (I use Hotmail.com) for use when filling out public surveys, forum registrations, commercial account registrations, etc... (Secondary accounts are always easier to discontinue or replace than a primary account).

How can the University combat spam?

Again, no one technique is fool-proof, but here are 7 common "tools of the trade". Most of these techniques require specific software to run on the email server, email client, web or a combination.

1. Pattern matching – looking for specific patterns in the emails (header, body, or attachments). Usually several different or separate test are combined to create an overall pattern match or "spam score". Pattern matching can find stuff like:
 - HTML forms in the message body
 - Common keywords and phrases (casino, limited offer, get paid, XXX, amazing, credit card)
2. Malformed/Suspicious headers – looking for header information that is either incorrect or suspicious. This would find stuff like:
 - Forged header information
 - Lists sent to many people with similar addresses (esmith, dsmith, fsmith, etc...)
 - Invalid dates

3. Local whitelists - A list of IP addresses, domains, and email addresses that are allowed to pass through the filter unchecked (this can happen locally on the server or at the client). Administrators update a group white list and individual users update personal white lists.
4. Local blacklists - A list of IP addresses, domains, and email addresses that are not allowed to pass through a filter. Local blacklists may result in the email being deleted automatically or just tagged and dealt with by the user. Administrators update a group blacklist and individual users update personal blacklists.
5. Realtime Blackhole Lists (RBLs) - A commercial list of networks that either allow spammers to use their systems to send spam, or have not taken action to prevent spammers from abusing their systems. There are many RBLs, but frequent changes and multiple "false positives" make this method problematic.
6. Reverse DNS checks – Checking incoming e-mail's originating IP address to see if it resolves to a valid domain name or Web address. Spammers often use false IP information. This method is also problematic due to such things as servers having multiple domain names and changing architectures.
7. Signature Lists – Similar to virus signature lists, several spam signature lists exist which allow anyone to add a spam sender to the published list. Other members are then able to block the spam. The public nature of this technique also provides both false positives and false negatives.