

## Junk Mail

Junk mail, also known as spam, accounts for 76% of global email traffic and 86% of US corporate email, according to Business Wire magazine in October of 2005. It's a safe bet that spam levels have gone up since then. Junk mail is now nearly unavoidable, so junk mail filters are mandatory.

There are many varieties and flavors of spam. Most of the spam I personally receive (in my junk mail folder, discussed later) is advertising penny stocks and pharmaceuticals, but there are many more varieties. *"Why do advertisers send out so much junk mail? Nobody actually buys this stuff..."* This is a valid question. However, by the numbers, junk mail is the cheapest advertising there is. Sending out a million emails would only cost the spammer something like \$150 (for a high-speed internet line for a month, and a list of email addresses). If .0001% of the spam recipients bought the product, that would be 100 people. If the product costs \$1.50, the spammer would break even. If the product costs \$50 (much more common), the spammer makes nearly \$5,000. Compared to the cost of Web banner-ad advertising, TV or radio commercials, or even traditional postal junk mail, Email spam is by far the cheapest type of advertising. However, not all email spam is advertising a product. This brings us to Stock Spam.

## Stock Spam

The financial fraud known as pump and dump (aka "Stock Dump" or "Hype and Dump Manipulation") involves artificially inflating the price of a stock or other security through promotion, in order to sell at the inflated price (creating artificial demand). This practice is illegal under securities law, yet it is particularly common (Taken from Wikipedia).

Fraudsters artificially inflate the price of a stock (usually a "penny stock") by sending out massive email spam advertising the stock, frequently including false information (forged press releases, etc...) making the company look much better than it is. Unwitting investors buy the stock in heaps (since it's so cheap anyway), driving the price up. When the persons behind the scam think the price has reached it's peak, they sell all their stock at the inflated price, and stop advertising. This causes the stock to dramatically decrease in price, and all the unwitting investors loose money. Organized crime groups (particularly the Mafia) are frequently involved with stock manipulation schemes.

Pump-and-dump spam now accounts for about 15% of all spam.

Now that we've covered what spam is and why we all receive it, let's talk about preventing it.

## Spam Filters

There are several types of spam filters. The less-obtrusive, ruleset-type filters use a set of rules to decide, message by message, if an email should be let through. These filters look for certain words or combinations of words, check to see if the email was mass-distributed or sent directly to you, and look for other signs of spam. The filter then puts the suspected junk mail into a separate junk mail folder. You should check your junk mail folder once a week or so to check for any legitimate email that might have slipped through, and then delete the rest.

The more-obtrusive kind of filter uses a "whitelist" (which is based on your address book). All email from people not on your whitelist is rejected. An email is automatically sent to the sender, briefly and politely asking them to confirm their identity. Spammers won't go through this process, but your friends can do so easily.

AOL, MSN, EarthLink, and Outlook all include a ruleset-type spam filter. You can adjust the "level" (or sensitivity) of the filter through the Options menu. AOL, MSN, and EarthLink automatically update their spam filters, however, with Outlook, you should manually update your junk mail filter by visiting <http://officeupdate.microsoft.com> (must be done from Internet Explorer).

One good free whitelist-type filter is called ChoiceMail. You can get it from [www.download.com](http://www.download.com), just type ChoiceMail into the Search box. It's the first result.

If you have Outlook Express (which has no junk mail filter capability), I highly recommend switching to Mozilla's Thunderbird email client. It's free, and will automatically import your account and email from Outlook Express (you don't have to set up Thunderbird; it automatically copies your settings and email from Outlook Express). Thunderbird has a very good filter-type junk mail filter that, in addition to the usual filter, actually "learns" what's spam and what's not, based on what you mark as spam. Thunderbird also filters out most phishing and stock spam, and is automatically updated. You can get Thunderbird at [www.mozilla.com/thunderbird](http://www.mozilla.com/thunderbird) .

## Phishing

Phishing scams take junk mail to the next level, combining massive spam with fraud and/or identity theft. For one example, "Phishers" would create an exact duplicate of a major bank's website. In appearance, the website looks identical to a major financial institution's website, but when you enter your account number and PIN to access the site, instead of displaying your account information, the fraudulent site sends your private information to the phishers so that they can steal your money. Phishers frequently duplicate websites such as PayPal, Washington Mutual, Bank of America, etc... and then send out millions of emails. They may try to convince you that your account has been illegitimately accessed, and you need to login to "confirm" your information, or something else. They'll provide you a link to click that goes to the fraudster's site; this site will look EXACTLY like your bank's site, but it's not. When you enter your account information to "log in", instead of logging in, you've just handed your info over to the fraudster's.

There is one very simple measure you can take to avoid being a victim of phishing.

If you ever receive an email that you suspect may be a phishing scam, **DO NOT CLICK THE LINK IN THE EMAIL!** Instead, open your web browser and type in the address manually (for instance, [www.washingtonmutual.com](http://www.washingtonmutual.com) ). Log into the site as you normally would. If there's really a problem or question about your account, you'll see it when you log in.

Another tip for identifying phishing scams is that most banks and financial services automatically insert your real name at the top of the email. If the email says "Dear Customer" or something similar, it's almost definitely a phishing scam.

Obviously, if you get an email pretending to be from a company that you don't do business with, it's a phishing scam.

If you've fallen victim to a phishing scam, you must act quickly. Here are the steps to take:

1. Contact the institution that was being imitated by the phisher and tell them exactly what's happened. Have them freeze or cancel your account(s) as required.
2. Change your PIN number(s) and/or password(s) that you've given to the phisher.
3. If you gave the phishers your credit card number, contact the credit card company immediately. Also consider using one of the major credit bureaus (Equifax, Experian, Trans Union) for their credit monitoring service, which will tell you whenever any of your cards are used.
4. If you gave the phisher any information that could be used for identity theft (mothers maiden name, social security number, date or place of birth, bank account #s), you have some serious work to do. You'll need to contact every organization you have an account with and make the appropriate arrangements. The best thing to do would be to close all your accounts and open new ones with new numbers, and a new pin/password.
5. Visit the FTC's Identity Theft center at <http://www.consumer.gov/idtheft> .