

STOPPING UNWANTED E-MAIL AND SPAM

Do you feel like you are getting more and more e-mail from unwanted sources everyday? Unwanted commercial e-mail (UCE), otherwise known as spam, can be an annoying, costly and time-consuming problem for many consumers

1. Use a unique e-mail address - Pick an address that is hard for spammers to guess and easy for you to remember. Also, if chatting online, use a unique screen name that is not associated with your e-mail address

An e-mail address containing both numbers and letters can help prevent spam. Many spammers use "dictionary attacks" to e-mail many possible name combinations at large Internet Service Providers (ex: Verizon, AT&T, Earthlink...) or e-mail services (ex: Hotmail, Yahoo, Lycos...), hoping to find a valid address.

Also, use a unique screen name that is not associated with your e-mail address if you chat online. Screen names are accessible to spammers so don't make it too easy for them to guess your e-mail address.

2. Use multiple e-mail addresses - Consider creating separate addresses or accounts that can be used for online purchases, chat rooms and other public postings. You can also use a free forwarding address

Consider creating multiple e-mail addresses or accounts. Use one address for family and friends only. Do not post this address online or give it to merchants. Your second address can be used online and for purchases. If you begin to receive unwanted e-mail at this address you can delete that account while not affecting your primary address.

Check with your Internet Service Provider. They may offer additional addresses for little or no fee.

Another solution is to set up a free forwarding address. By using a forwarding address you do not have to give your primary address to merchants or post it online. If you begin to receive unwanted e-mails you can change your forwarding address while not affecting your primary address. Forwarding addresses are available from Bigfoot.com or NetAddress.com. Yahoo! Plus users can create disposable addresses with Yahoo!'s AddressGuard. Messages sent to Yahoo! disposable email addresses will be delivered to your inbox or to any personal folder you select. If a disposable email address begins receiving spam, you can delete it - without affecting your primary address.

3. "Mask" your e-mail address - If you post your e-mail address online consider masking your address. There are several ways to correctly mask your address and thwart spammers.

If you need to post your e-mail address on a publicly available Web site, you can mask your address. Masking is also called "munging" your address. What this does is make it difficult for spammers' computers to automatically collect your e-mail address, but fairly simple for other people to be able to use your e-mail address.

Simple masking

Add a phrase, or a character, that is obviously not a part of your e-mail address. Then users simply remove that part of your address to contact you. So if your e-mail address is "jsmith@example.com," you could mask it as "jsmith@nosпам.example.com." This technique can be used on Web pages, in UseNet newsgroup postings, and in some mailing lists. But, if you need to get an automated response, this will not work. So you would still sign up for a mailing list with your regular address, but remember to change the signature that goes out with your e-mail messages.

Web Site Masking

If you operate a Web site, you may want to go one step further. A study reported in March 2003 by the Center for Democracy & Technology shows that using character entities to represent your e-mail address is currently very effective at preventing spammers' computers from recognizing e-mail addresses posted on a Web page.

4. Check the privacy policy when you submit your address to a Web site -

Always be familiar with a Web site's privacy policy before submitting any information

The cornerstone of good privacy protection is a Web site's privacy policy - a statement of how and why a company collects information, what it does with that information, what choices you have about how the information is used, whether you can access the information, and what the site does to assure that the information is secure. On the basis of this information, you should be able to decide whether or not to give information about yourself to the site.

Ideally, a privacy policy is a brief, easy-to-read, comprehensive statement of how a site collects, uses, retains and secures your information. To make the policy easier for consumers to read and understand, sites will sometimes post a simplified version of the policy and provide links to more specific information (e.g. descriptions of the site's relationships with other businesses, links to governing laws). This approach to posting a policy enables a user to get a general idea of the policy without having to read through legalese and technical language.

Checklist for Reading a Privacy Policy

- What information is being collected? Is the information personally identifiable?
- Why is it necessary to collect this information? Is the data collection appropriate to the activity or transaction? If not, why does the site need it?
- How is the data being collected? Does the site set cookies? Does the site maintain Web logs?
- How is personal information used once it is collected? Is it ever used for purposes other than those for which a visitor has provided it? (If so, the visitor should be informed of the use.) Has the visitor consented to it? Does the visitor have the option to prohibit such secondary use? Can a visitor prohibit it and still enjoy the site?
- Does the site offer different kinds of service depending on user privacy preferences? Does a user have a choice regarding the type and quantity of personal information that the site collects? Does the site disadvantage users who

exercise data collection choices?

- Can users access information that has been collected about them? Are users able to correct inaccurate data?
- How long is personal information stored? Is it kept any longer than necessary for the task at hand?
- What is the complaint and redress process? Whom can users contact?
- What laws govern the collection? Is it a federal government site regulated by the Privacy Act?
- Is the entity collecting information regulated by another privacy law?
- When reviewing the policy, be careful to distinguish information about information collection and privacy from language included to market to you or to encourage you to reveal information.

6. If it sounds too good to be true - it probably is. Fraudsters, scammers, and crooks take advantage of people via unwanted e-mail.

Don't Be a Victim

Don't let spammers get the best of you. Don't fall for their tricks. If someone came up to you on the street and offered you a million dollars if you simply gave them \$10,000, would you do it?

Be on the lookout for urgent or time sensitive requests. Truly sensitive financial transactions should not be handled through e-mail.

Also, friendly or casual messages (such as "Re: meeting yesterday" or "the information you requested") can be designed to entice you. Did you have a meeting yesterday? Have you recently requested information via e-mail? Your gut reaction is usually correct. Be careful of false subject lines.

7. Learn more about "pop up spam"- recently a new form of spam has developed via the Microsoft Windows operating system feature Messenger Service. It is a stream of "pop up" messages that stop you from using your home computer until you close them. If this is a common problem that you are experiencing learn how to make it stop.

Recently a new form of spam has been invading computers. This new form is called "pop up spam." This type of spam occurs when spammers exploit a feature of the Microsoft Windows operating system known as Messenger Service. The Messenger Service is designed to provide users on a local- or wide-area network with messages from the network administrator. Instead outside organizations are taking advantage of this opening into your computer and are sending "pop up spam" including advertisements, new programs or worse.

Disabling the messenger service will prevent the possibility of "pop up spam." To disable the messenger service:

- Click **Start**, and then click **Control Panel** (or point to **Settings**, and then click **Control Panel**.)
- Double-click **Administrative Tools**. Double-click **Services**. Double-click

Messenger. In the **Startup** type list, click **Disabled**. Click **Stop**, and then click **OK**.

You can also cut off "pop up spam" by using a **firewall**. We strongly recommend the use of firewalls for this and many other security related reasons. Free [Firewall](#) software is included in IPositif CD

[8. Use tools to help prevent spam](#) - Learn about tools that can filter or tag spam before it fills your e-mail inbox.

Spam-Fighting Tools

- **Reports Spam**

These tools help you to report spam to the proper authorities. This is a key step to preventing further spam from the same culprit. By reporting spam you can help yourself and the entire online community.

- **Filters or blocks unwanted email**

These tools prevent suspected spam from entering your inbox. The potential spam may be identified based on blacklists, whitelists, key-word/character criteria, etc. Please note that not all spam may be identified as such and that some wanted mail may be mistakenly categorized as spam. Many filters send the suspected spam to a separate folder so that you can look through the mail to see if any non-spam has been inadvertently filtered out.

- **Provides multiple, tagged email addresses**

These tools provide you with multiple email addresses to use when your email address is requested by businesses or others online. Typically, these email addresses will forward to your regular email account and the individual email addresses can be turned off if they are abused. Because the email addresses are tagged, you may also be able to determine which companies have sold or disclosed your email address.

- **Gives a challenge-response to incoming email**

These tools are designed to ensure that a human is sending you mail. When you receive mail from an address not on your list, the system requests a response from the sender. If the sender does not reply, the mail is handled as spam. Please be aware that a challenge response may be categorized as spam and that some humans may not be able to respond for that reason. Also, some companies use the challenge-response email to market their product to the people who are trying to email you.