

1. **Use Webmail.** Always try to use Webmail through a web page i.e. Google mail, which most can give you full guard against unwanted messages. Check your web-based mail regularly to see spam you've blocked and ensure nothing has been incorrectly classified as spam.
2. **Keep your address safe.** Your email address is a valuable thing, so valuable in fact that spammer will pay good money for 'live' email addresses of real people. So take care of your address and do not give your details to anyone you don't know.
3. **Turn off all images.** Spammers can tell if you view a mail with images in, which lets them know if it's a live one. If you want an extra level of protection you can block all images in every mail.
4. **Never respond.** Don't reply to spam – this tells the senders your address is live. They will use tricks such as a line saying 'If this email reached you by mistake, please reply', suggesting that it is an official message. But it's not so don't reply, and don't even click on any unsubscribe links, unless you know that the email is genuine.
5. **Don't forward chain letters.** Many of us receive email chain letters asking us to forward the message to a friend. They often include claims such as you'll get 5 pence for every email of face bad luck if you send it to fewer than 5 people. These are hoaxes mostly to promote spam. Never forward these emails thinking that you will receive money for that you forward on, you don't. In fact you'll be doing the spammers job for them, and forwarding their email to your friends. They wont even thank you for it.
6. **Never click on a web link.** Unless you know its source. Spam emails contain web links that are supposed to take you to an unbelievable offer. This alerts the sender that your email is valid. It could result in a virus or Trojan being downloaded to your PC. Your should be protected from these kinds of programs.
7. **Don't reveal your details.** You may receive email that look as if they are from legitimate companies, such as Amazon, Ebay or a bank, asking you to click on a link in their mail and update your details on your website. Most companies never ask for your personal details, such as account information. So if it does it is a fake, it is some form of spam called PHISHING, that aims to get you to go to their site and give them some of your personal details. If you are ever unsure about the email, use your browser to go to their main page and follow its instructions, so your know your are on the right site.
8. **Protect you address.** Do not post your email address in public places – treat it as if it is your phone number. If your email address appears on a message board, in a chat room or any public place, others can use automated robots or 'bots' to search the internet and grab your email address. Resulting in you getting inundated with spam.
9. **Beware of email spoofing.** This is a fake email address to make you think that the message has come from your address or a credible source. Spammers use spoofing to get you to open and respond to their mail. Remember, you should never respond to unsolicited mail – instead report it.