White and Black listing email senders

The problem

You may discover that emails that you may have sent to someone have not been received.

Or, you may discover that emails being sent to you from someone you trust are dumped into your spam folder or not even shown in your inbox. Here are some explanations and solutions that may apply.

Introduction and some possibly useful definitions

Email is accessed using an app or program that is referred to as an **email client**. Many users of email use a **browser** - such as Chrome, Firefox, Safari, Opera &c, - to access their email and the email client is effectively that of their email service provider such as Google, Yahoo, or their broadband service provider. You may use more than one app or method to access email; each chosen for convenience or features.

Email service providers include, Google(gmail), Microsoft (OutLook, hotmail), Proton (Proton, very secure and end to end encrypted), BTinternet (Yahoo, btinternet.com), your domain hosting service provider[1]. Your company may operate a corporate email system. Examples of email clients include OutLook, ThunderBird, K-9 (good on Android), apple's email app; many of these are free to use. If you are using an Android device - a tablet or mobile phone - you may encounter a wide range of email clients some cost, some are free and some carry adverts.

The browser is how you access content from the internet. Don't confuse the browser with the **search engine**; the software, or app, that you use with the browser to find things or places on the internet. Search engines include DuckDuckGo[2], Wikipedia, Bing!, Google &c.

Email clients - whatever they be - require you to **login** -usually with your **email address** such as rolling_stone@startmeup.co.uk - and a password. This is your **email account**. Your email app may have been set up so that the key information items of your email account are managed by the *Remember Me* option which may be provided by your browser, operating system or your email client; let's hope that you keep a written record of it as retrieval can be tricky.

There are two **protocol**s[3] that are used in email. A protocol is the collection of rules that your email client uses to manage your email service and the presence and deletion of emails on *all* of your machines that

---

1 For example oilbuying@lockerley.org.uk is an email that uses the **domain name** of lockerley.org.uk. The lockerley.org.uk website domain is **hosted** by ionos.co.uk and ionos.co.uk is also the email service provider for this domain.

2 Try DuckDuckGo at duckduckgo.com. Theis is a search engine that does not track you and which does its best to keep your results pages free of adverts.

3   There are two protocols in use PoP3 and IMAP and which to use, if you are setting up a new email account, is a topic in its own right. IMAP is commonly recommended.

use the same email account.

Email service providers, and many email clients, provide options for managing *junk* or *spam* emails. Your email client may place these in the obviously named folder of your inbox. These will often include emails from senders which your email service provider has recognised as being from an *untrusted* source; quite often a sender who is using a random, often temporary, *spoofed*[4] domain identity or one who has a record of sending bulk emails which have been identified as junk.

Email clients will usually have a way to indicate an email whose source you consider to be a source of junk. Your email client will usually place such email into your junk folder. Usually your junk folder is emptied regularly - you may be able to set this period.

How you recognise whether an email is from a *trusted* source depends on the features of the email client app that you are using. One of the features of a spoofed email source is that it may look like the email is coming from someone you know. If you are concerned then you should look at the full *header* of the email as this will show information of the originator and the route it has taken to reach you. It seems that few email clients on mobile devices make this an easy, or even possible, thing to do. Email security and the avoidance of scams and so on are yet further topics.

Typically

A typical view of a web browser email client …
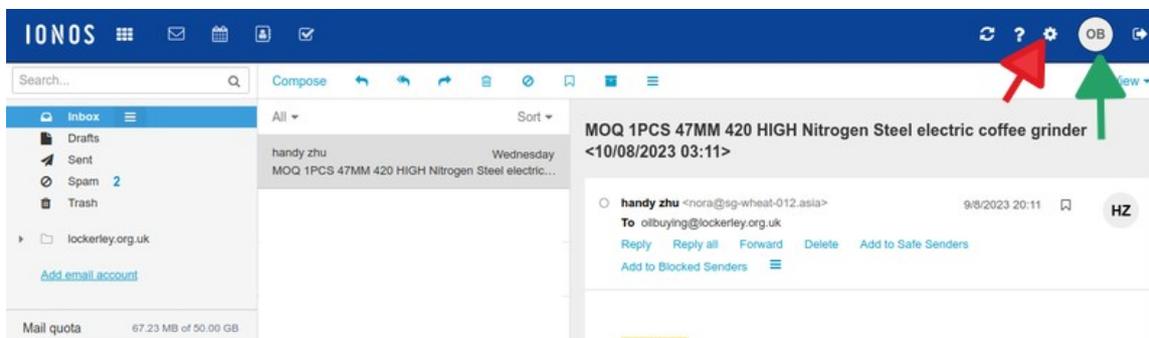
This shows a spam email which has just been captured and which I will move to the spam folder.

Select the email in the inbox list of emails. Then right click and select "mark as spam". Subsequent email from this source will automatically be placed there and will be deleted after a month. It is useful to review the content of the spam folder in case there is an email from a source you are expecting. You can then drag'n'drop it into your in box and mark it as not junk.

Email client apps will usually provide a similar facility.

---

4 A spoofed address is one which is false. Such emails may appear to come from someone you might trust but the true sender is often only revealed when you inspect the email *header*. The header is the usually hidden information that details the sender, the email client, and the principal servers in the internet world that the email has taken to reach your inbox.

So what to do about emails that your email provider has recognised as spam and has deleted before it reaches your in box. You need to access the settings for your account. Some web-based , or browser, clients use the gear wheel symbol (red arrow) others use an option in a drop down menu that appears when you click on your account symbol (green arrow). What you do next depends on the provider and the browser but in general … Follow the available menu options and you should have something like this:

In the example above if "Show" is selected then the list of good, or bad, senders is shown and the option to Add or Remove will appear. You will be asked to enter the email address that should be blocked, or

unblocked. If someone tells you they are not receiving your emails this note may help them too.

A full email client will likely provide similar features … just look for the terms of good or bad, *safe* or *blocked*, *trusted* or *untrusted*, *whitelist* or *blacklist* &c.

There are, of course, many other ways in which email systems appear to misbehave but this too is another topic.