



# Understanding Email Services: What are they and what do you need?

by Erik Kangas, President, Lux Scientiae

You *thought* email was a simple concept, but you are confronted with a plethora of acronyms and jargon like POP, IMAP, WebMail, Aliases, Forwards, SMTP, Quota, SPAM, TLS, SSL, and more! This article will describe the ins and outs of email, explain these terms, and help you figure out what services and features you need from your personal or business email service provider.

Every email provider supplies you with three fundamental services:

- A way to send email
- A way to receive email
- A way to store received email, at least temporarily

The difference between email providers, and their cost, comes down to the versatility, security, and extent of each of these services. In the next sections, we discuss each of these services in detail and consider many of the possible and/or desired features that could come with them. First, we will define a few concepts central to email — the types of programs used for email.

**Email Clients.** Email clients are computer programs that run on your local computer which enable you to perform actions such as composing and sending email messages, retrieving your new email messages, and looking at your old email messages. Examples of email clients include: Microsoft Outlook, Microsoft Outlook Express, Eudora, Pine, Netscape Communicator, and Entourage.

Email clients are characterized by being installed on your local machine and requiring you to configure them with details of your email provider so that they can send and receive your email.

**WebMail.** WebMail is like an email client in that it allows you to compose and send email messages, view new and old email messages, and perform other email activities. However, unlike an email client, WebMail programs run on your email provider's web servers and are accessible via any computer connected to the Internet that has a compatible web browser, such as a recent version of Internet Explorer or Netscape Navigator.

WebMail programs do not require configuration, you simply login and they work. You may, however, be able to customize them to match your operational preferences.



## Sending Email: SMTP

Any email message that you send is passed along from your computer across any number of intermediate email servers to the server on which the recipient of your message receives his or her email. All of these email servers talk to each other via a language called **SMTP**, which stands for *Simple Mail Transport Protocol*. Thus, your *outgoing email server*, the server through which you send email messages, is also known as your *SMTP server*.

Every email provider has one or more SMTP servers for your use. Some providers allow you to connect to these servers directly so that you can send email directly from your Email Client; other providers do not permit you to connect to their SMTP servers directly, requiring you to send all email via their WebMail applications.

Why would an email service provider not want his clients to connect directly to its SMTP servers? Using an Email Client, you may be able to easily send lots of email messages, whereas with WebMail it is difficult to send many messages in a short period of time. Allowing you to send lots of email messages in a short time exposes your email provider to the risk that you may 1. load down his servers with excessive amounts email, and 2. send SPAM.

If your email provider does provide you with access to his SMTP servers, he may or may not support **SMTP Relaying**. Support for “SMTP Relaying” means that your provider allows you to use his SMTP server to send email to people whose email is not managed by your provider. For example, if you are using the SMTP servers of Lux Scientiae to send email to bob@luxsci.net, this would not require SMTP relaying because LuxSci’s servers handle Bob’s email, and thus they **HAVE** to let you connect to them to send him email (or else Bob would have the misfortune to never receive any email). However, if you are using LuxSci’s servers to send email to bob@hotmail.com, this would require SMTP Relaying because Lux Scientiae does not manage the email for addresses at hotmail.com.

What’s wrong with SMTP Relaying? Nothing, as long as your email provider restricts who can use his server for sending email. If he doesn’t, then *anyone* could send email through his servers to anyone else, making his servers ideal tools for hackers desiring to send SPAM. For this reason, most email providers require you to **Authenticate** yourself when using their SMTP servers for sending email. This often means that you need to send your correct username and password to their server *before* it will allow you to send your email. This process is commonly called **SMTP Authentication**. Some email providers go a step further and also provide you with **Secure SMTP**. Secure SMTP (along with other secure services described below) encrypts the communication between your computer and the server such that no one can eavesdrop and detect your username, password, or message contents – the communication channel is *secure*.

**What is right for you?** If you wish to use an email client for sending and reading your email, your email provider must provide you with SMTP Relaying services. If you are very security-conscious, you should ask if they support Secure SMTP. LuxSci provides both SMTP Relaying (with authentication) and Secure SMTP.



## Receiving Email

If someone sends you an email message, how do you obtain it and read it? There are basic three ways to do this which differ in usefulness depending on your needs.

**WebMail.** WebMail applications have several advantages:

- **Read It Anywhere** – They allow you to read (and send) email from any computer that is connected to the Internet and which has a modern web browser.
- **No Special Software** – Beyond a modern web browser, which comes with most computers, no special software is required to use WebMail, and no time needs to be spent configuring software.
- **Can Be Secure** – Some WebMail applications run over a secure connection between your browser and the email provider's servers (an SSL – Secure Socket Layer – connection) so that all of your email messages, passwords and other data cannot be eavesdropped upon. Many WebMail services do not provide this, however.
- **Backed-up & Safe** – Your email service provider is responsible for backing up your email messages. Your email is stored on your service providers servers, so if your personal computer crashes, none of this email is affected!

The disadvantages of WebMail include:

- **Internet Required** – You cannot view any of your email unless you are connected to the Internet. The speed by which you can manage your email is related to your Internet connection speed — it can be slow or fast!
- **Disk Space** – Since your email messages are stored on your email provider's servers, they take up his disk space. Your email provider may limit the amount of disk space you can use, or charge you a premium for additional disk space. If you exceed your allotted disk space, you could be charged a fine or your services could be suspended! Most free email services give you very little disk space, and are very strict about disabling your account if you exceed your quota.
- **Features** – Your provider's WebMail program may not provide you with as many features as you would have if you used an Email Client for reading your email. The features provided by different providers' WebMail clients vary greatly — make sure yours provides those features that you need! I.e., some features include: sending attachments, viewing attachments online, viewing messages written in particular languages, address books, personalities, spell checking, read receipts, SPAM filtering, auto responders, email aliases, etc.

A good email provider will supply you with WebMail services *and* one or both of IMAP or POP (see below) for use with Email Clients.



**IMAP** is a *protocol*, i.e. a language used by an Email Client program to talk to your email provider's servers. It stands for *Internet Mail Access Protocol*. IMAP is one of the two major protocols that can be used by Email Clients to allow you to access your email messages. IMAP allows you to keep some or all of your email messages stored on your service provider's servers, thus sharing many of the pros and cons of WebMail. Your service provider may offer **Secure IMAP** (a.k.a. **IMAPS**) which makes sure that the data sent back and forth between your Email Client and the server cannot be eavesdropped upon. Secure IMAP connections are encrypted via the same technology that encrypts secure WebMail — SSL (or TLS). Use of IMAP provides the following advantages:

- **Read It Anywhere** – Read email from any computer that is connected to the Internet and which has an Email Client supporting IMAP installed.
- **Backed up & Safe** – Your email service provider is responsible for backing up your email messages. Your email is stored on your service providers servers, so if your personal computer crashes, none of this email is affected!
- **Features** – You can use any modern Email Client which provides you with all of the email management features that you require.
- **Download** – Most Email Clients allow you to download some or all of your email messages from the server to your local computer for viewing while you are not connected to the Internet, or for archiving without taking up disk space on your provider's servers.
- **View only Headers** – Your IMAP client can download and display only the headers of the messages in your eail folders, thus requiring little bandwidth until you need to actually view the body of a message.
- **Server Side** – many operations such as sorting messages, and moving messages between folders can be done by the server without requiring you to download the messages involved, thus requiring little bandwidth.
- **WebMail Compatible** – All of the email that you keep on the server (even if it is sorted into multiple folders) can be viewed by either WebMail or an Email Client using IMAP. This is great for people who travel.

The disadvantages of IMAP include:

- **Internet Required** – You cannot view any of your email unless you are connected to the Internet. The speed by which you can view your email is related to your Internet connection speed — it can be slow or fast!
- **Disk Space** – Since your email messages are stored on your email provider's servers, they take up his disk space. Your email provider may limit the amount of disk space you can use. If you exceed the allotted disk space, you could be charged a fine or your services could be suspended!
- **Software** – You must obtain, install and configure your Email Client software on each computer that will be used for checking your email via IMAP.



**POP** is also a *protocol*. It stands for *Post Office Protocol*. Sometimes you will see it written as **POP3** which implies *Version 3 of the Post Office Protocol*. POP is the other of the two major protocols that can be used by Email Clients to access your email messages. POP enables you to automatically download your messages from your email server to your local computer (and usually to then remove them from the server). This is intrinsically different from IMAP and WebMail, where the email always stays on the email server. Your service provider may also offer **Secure POP** (a.k.a. **POPS**) which makes sure that the data sent back and forth between your Email Client and the servers cannot be eavesdropped upon. Use of POP provides the following advantages:

- **Disk Space** – Because POP usually downloads all messages to your local computer and automatically deletes them from your email provider’s server, you minimize the amount of disk space that you use on the servers, possibly lowering the cost of your account.
- **Speed** – Once your email messages are downloaded on your local computer, you can read them very easily and quickly, even if your computer is no longer connected to the Internet.

The disadvantages of POP include:

- **Not Anywhere** – Since your email is downloaded to your local computer, you cannot view this email from any other machine. If you travel or go home from work, you lose access to your downloaded email (unless you copy it to a disk and take it with you!)
- **Software Required** – You must obtain, install and configure your Email Client software on each computer that will be used for checking your email via POP.
- **You Manage Backups** – As your email is on your local computer, you take all responsibility for ensuring that you have backups of your email messages in the event that something goes wrong with your computer.

Email providers like to offer POP email boxes because you download all the email from their servers, minimizing the impact of your email usage on their servers. They dislike providing IMAP services, as IMAP users can leave gigabytes of email on their servers and exert much more of a computational load on their servers. Email providers offering IMAP services are usually more expensive than those that do not for exactly these reasons — and these are good reasons!



Compare Features			
	WebMail	IMAP	POP
<b>Access Email From Anywhere?</b>	Yes	Yes	No
<b>Large Server Disk Usage?</b>	Yes, unless you use POP as well	Yes	Minimal
<b>Dependence on Internet Connectivity</b>	Strong	Very Strong	Moderate
<b>Special Software Needed?</b>	No	Yes	Yes
<b>Data Backup Responsibility</b>	Service Provider's	Service Provider's	Yours
<b>Security</b>	Depends on Provider	Depends on Provider	Depends on Provider

**What is right for you?** If you wish to use an email client for sending and reading your email, your email provider must provide you with POP and/or IMAP services. If you wish to access your email from multiple computers (i.e. when traveling), then WebMail and/or IMAP services are essential. WebMail is *always* a plus as it generally works in conjunction with IMAP and can be used even with POP to view new messages that have not yet been downloaded by your Email Client. If you are looking for the least expensive solution, use WebMail in conjunction with POP. IMAP adds a lot of flexibility and power, but also requires that you purchase more disk space with your email provider and have a reliable and speedy Internet connection. If you are very security-conscious, you should ask for Secure versions of any of the services that you need.

## Important Email Concepts

**Security.** Email is an inherently insecure communication medium. Learn why this is so and what you can do about it in this article "[The Case For Email Security.](#)"

**SPAM.** Sending a message, especially an advertisement, to more than five recipients, can by itself be considered spamming unless the individuals have specifically requested to be added to a mailing list on that topic. This includes commercial advertisements and informational messages sent to recipients via electronic mail. Email is a person-to-person medium, not a broadcast medium.

While there are currently no laws against the sending of unsolicited email or SPAM, most email providers and Internet service providers have strict policies against the use of their services for such purposes. Sending of SPAM is very bad Net-Etiquette.



What is the problem with SPAM? Unlike postal mail, email is virtually cost free to the sender, so advertisers have no problem sending unlimited quantities of email in the hope that some small percentage will result in sales, or responses. The result is that an ever growing proportion of email is SPAM — current projections indicate that in several years, more than 90% of email will be SPAM, greatly diminishing the use of email as an effective means of communication.

Sending SPAM, unsolicited commercial email (UCE) or any unsolicited email to multiple people is considered an abuse of your email provider's services and may subject your account to immediate cancellation.

What about that list of 100,000 opt-in email addresses I purchased? Any opt-in email list is going to have people on it that will complain if you send them email, and the burden of proof is upon you, the sender, not on them! So if you sent 100,000 emails and %0.1 of the people complain, you just got 100 complaints! That's enough to get your account terminated with almost any email provider! The only safe way to use opt-in email lists is to create the lists yourself via your own web site – not by buying it from anyone, no matter how "reputable," and certainly **NOT** by scanning or spidering the Internet and grabbing people's email addresses from their web pages!

To help with the proliferation of Internet SPAM, many email providers offer **SPAM Filtering** software. This is software built into your provider's servers that can detect a large proportion of the SPAM being sent to your email address(es). Detected SPAM emails can then be deleted, stored in alternate email folders, bounced back to the sender, or simply marked as potential SPAM. Be careful with such software as, incorrectly configured, it can result in the *loss of important non-SPAM email!*

**Email Aliases and Email Boxes.** Both email aliases and email boxes are email addresses, like bob@luxsci.net, to which email can be sent. An email box is the address of an *actual user* on the email provider's server. I.e. if bob@luxsci.net is an email box, then bob is an actual username on the luxsci.net servers and "bob" can be used as a login to the IMAP, POP, or WebMail services. An alias, however, is *not* an actual user, but rather a *rule* that indicates who should receive the email addressed to the email alias' email address.

For example, let's say that fred@luxsci.net is an email alias. We then also have to say where email to fred@luxsci.net goes. One possibility is that we configure the email alias such that email for fred@luxsci.net goes to bob@luxsci.net. In this case any email sent to either bob@luxsci.net or fred@luxsci.net gets deposited in bob's email box.

Thus, email aliases allow you, or Bob, to receive email sent to lots of different email addresses in the same email box.



One special kind of email alias is called a Catch-All Alias. If you have a catch-all alias for your domain then all email addressed to addresses that don't correspond to email boxes or other email aliases will be delivered to the recipient of the catch-all alias. These are often used to make sure that you get any email sent to any address at your domain. However, using a catch-all alias subjects you to the receipt of more SPAM — SPAM sent to any address caught by the catch-all alias!

Typically, email providers allow you to set up any number of email aliases to help you better manage your email. Some email providers allow you to specify more than one recipient to an email alias. I.e. fred@luxsci.net could be configured to go to *both* bob@luxsci.net and joe@hotmail.com. In this case, the alias is also an **Email Forward** and one or more of its recipients is an email address not located on the email provider's servers — the hotmail.com address in this case. Thus, aliases and forwards are really very similar concepts.

**Email Personalities.** Your Email Personality is applied to the email messages that you send. It consists of who the messages is "From" and who replies to the message should be sent to. Most simply, your email personality consists of your Name and Email Address; however, you may wish to use "multiple personalities" — one for your "Sales" department email, one for your "Support" email, one for your "Personal" email, one for your "Academic" email, etc. Each personality might use a different email address and name.

Some WebMail clients allow you to configure them with multiple personalities and choose the personality of your outgoing email message when you are composing the message. This is very convenient, especially if you would like to manage all of your email in one place and you wear "multiple hats" in your business, or have different email addresses for different purposes. Note that any WebMail program that allows you to specify arbitrary personalities will include information in your email messages indicating from where they were sent, allowing them to be **tracked back to you** — this protects your email provider from possible use of this service for illegal purposes. So, be careful to use only personalities that you rightfully own or to which you are authorized.

**Autoresponders.** Also known as an out-of-office response, an autoresponder automatically sends an email message back to the senders of messages that you receive. You can usually customize these automatic responses to have any fixed subject and body that you desire. Autoresponders are often used to inform senders that you are, for some reason, not checking your email for a time, that your email address is changing, that the email arrived in your email box, or of other important information.