

THE ACADEMY OF PLUMBING – LOCATION E-MAIL

Those of you who frequent the AOP E-mail Forum will probably know me by now as a bit of a Macintosh nerd. I know it's sad, but someone has to be. Consequently, I've been persuaded by the estimable Janet Ibbotson to write a column in IMAGE, all about the fascinating world of the Apple Macintosh, the Internet, digital storage, e-mail and the collected foibles thereof. As I'm a Mac tech, this column will be rather Mac-centric, but much of the underlying methodology is equally applicable to Windows, or even Linux. Not knowing at this stage whether I've just been handed a poisoned chalice, I'll press on anyway and we'll see where we end up. This month, I'll mostly be blathering about the exciting world of location e-mail.

Ah, Easter. A nowt-nor-summat holiday: finally the days are getting longer, the kids are off school, we're all sick of winter and want to go away somewhere, so we do, but the weather's unreliable (as indeed it was this year) and we get stuck in cars with bored kids looking out through steamy glass at grey skies, on our way to somewhere which isn't home. And therein lies the problem. Being hunter-gatherers we take our laptops with us because we daren't be out of e-mail contact: just in case, y'know. The hotel brochure said 'Wireless Access'; the PowerBook has an AirPort card installed, so we're ready to rock, right? Mmm. Depends...

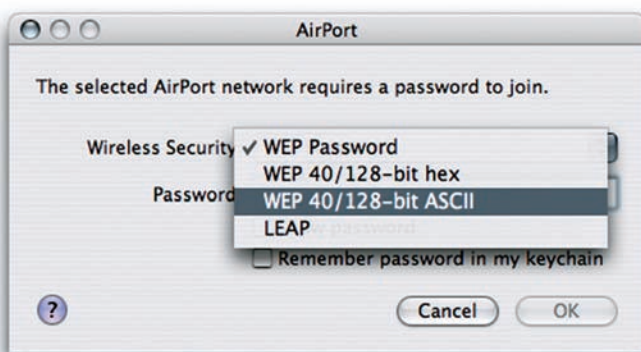
GETTING CONNECTED

The first problem is actually getting connected, which for a PowerBook user can be a painful experience. Commercial wireless access points are set up in a variety of ways, the two most common being WEP or WPA encrypted/password-protected, or via a browser portal. A browser portal will usually require a username and password; a WEP/WPA access point will be password-only.

Make sure AirPort is turned on. Click on the AirPort icon: the drop-down menu should display the names of all wireless access points within range. Select the network name you've been given by the hotel staff. One of two things is likely to happen:

- you're presented with a dialogue box asking you to enter a WEP or WPA key;
- you seem to be connected immediately with no further ado.

If a WEP/WPA dialogue box appears on your screen, there's a field in it in which to enter the password you've been given. Blithely, you type it in. Nothing happens. Duh? It transpires that PC wireless connections default to the password being entered in plain text, also known as ASCII, whereas Apple connections by default use a different coding format. The trick is to set the password field to accept **plain text**, as shown here:



Then, with luck and a fair wind behind you, you're connected and free to experience the next pitfall, of which more below.

If, on the other hand, nothing appears to happen and the previously-grey AirPort menu-bar icon turns black, or at least partly-black, the access point uses a browser-based portal for connection. Launch a browser (Safari, Firefox, Camino, OmniWeb, Opera, Internet Explorer as a last resort) and try to go somewhere. With luck, you'll be taken to the hotel's portal in which there will be fields to enter the username and password you've been given. Enter them, and suddenly the Web is yours to surf... Or not.

Some hotels (including many in France, it seems) use a browser portal coded using Microsoft-specific JavaScript, Java or ActiveX, which only runs in Internet Explorer 6. Which only runs on Windows. In which case you've lucked out, except for the very rare instance in which the portal for some reason is only checking to see if you're running IE6 and doesn't actually require it. In this case, using any one of several shareware add-ons to Safari (I like PithHelmet: <http://snipurl.com/pf06>), you can enable Safari's Debug menu and change its browser ID to make it pretend to be IE6 running on Windows, and barge in. It might work...

AND WE'RE OFF!

Right, let's say you've made it this far and established a working connection. You go to get your e-mail. You launch Microsoft Entourage or Apple Mail, click the Get button and: Bingo! A torrent of job offers pours in. Naturally you wish to gracefully accept these fabulous, generous, respectful offers without delay, and set about composing replies. Satisfied with your literary style, tone and eloquence you hit the Send button and, unless you are very lucky, are immediately confronted with a message telling you in one of many unhelpful ways that you are not allowed to send mail. Eh?

Here are the reasons why. The mailboxes from which you receive e-mail and through which you send it are two entirely different entities, which is why in your e-mail settings they're referred to as POP3 or IMAP for receiving and SMTP for sending. When you contact your POP3 or IMAP mailbox to get your e-mail, your e-mail client sends your e-mail username and password to the mail server. If they correspond to the list of valid usernames and passwords it maintains, you're allowed in and can get your mail. This almost always works from anywhere.

Sending e-mail is different, because of the spam problem. In order to prevent spammers sending mail through their servers, ISPs only allow in trusted people. These are defined in one of two ways:

- You're sending from an IP address which has been given to you by your ISP. This is the case when you're at home or in the office and using the SMTP server provided by your ISP. Because your IP address is one from the ISP's pool of addresses, the ISP assumes it knows who you are and lets you through. If you turn out to be a spammer the ISP can see from its mail logs that you were the source of spam and turn you off.
- You authenticate to the SMTP mail server. Usually, this process is similar to that for getting your mail in that your e-mail username and password is again sent to the mail server. If they correspond to the list of valid usernames and passwords it maintains, you're allowed in and can send your mail through it.

Sadly, a surprising number of ISPs don't support **authentication** and of those that do, some insist on you using a different, authenticated account to your usual one. Dump them without delay and get a proper services provider. If you have your own domain

I said be prepared...

So, of course, you have an up-to-date clone of your PowerBook's internal hard drive at home, don't you?

If you do, should your PowerBook get nicked/destroyed/blown up, all of your data is safe at home. Is it? Yes, I thought so, because you used SuperDuper! (<http://www.shirt-pocket.com/>) or Carbon Copy Cloner (<http://www.bombich.com/software/cccl.html>) to clone your internal drive to a FireWire drive before you departed.

If you're working on location you cloned to two drives: one you left at home as a backup, and one (of the powered variety) you brought with you, just in case, because should a calamity befall your PowerBook you can boot any other Macintosh from it (except Intel Macs, about which more next month, if I'm still invited) and are instantly back in business with all of your software and data running as you left it. Oh, except for CS2, which will need re-authorising. As might Capture One. Still, it's better than nothing, eh?

And what might have befallen your PowerBook in the blowing-up department? The most likely is the hard drive failing on you. Laptop drives are quite delicate and can fail without apparent warning, unless you install the wonderful, free SMARTReporter (<http://homepage.mac.com/julianmayer/>), which will check your hard drive hourly and warn you if the drive thinks it's about to fail.

If you do get such a warning, copy your important data onto another drive immediately as the warning won't be messing about. If you keep all of your important data within your Home folder, even on the desktop, then simply copying this folder will preserve all your data, preferences, passwords, e-mail, contacts and addresses, and so on and is by far the best and easiest way to manage things.

Also, keep your ears open. If the drive starts making a repeated clicking noise, a.k.a The Click Of Death, close the PowerBook immediately and get help as the drive is about to destroy itself.

name, this is usually hosted by a provider which does support authentication, in which case you should be in business. Even then, I've heard of exceptions.

I recommend you get your e-mail hosted by a provider which properly understands the modern world and the spam problem. For pure e-mail I can thoroughly recommend Ultradesign Internet (<http://www.ultradesign.com>) who not only support proper authentication but are also closely allied to Spamhaus.org and run very effective spam filters. I've been with them for years and get an average of less than one spam e-mail per month.

BUT I STILL CAN'T SEND EMAIL!

What? I'm a smart-aleck, have a proper, authenticated e-mail account and still can't send? Some ISPs, notably Wanadoo, insist that all outgoing e-mail from their pool of assigned IP addresses goes through their own **SMTP servers**. Quite why, when authentication is sufficient security against spam, I'm not sure. They do this by intercepting and re-routing all of your outgoing traffic on TCP Port 25 (the SMTP port) through their servers. So you're stuffed, because of course you don't have an account with them. In this instance your only recourse is **Webmail**, if your ISP provides it, or to use an SMTP server which will accept e-mail on a different port to

25. These beasts exist and I'm in the process of setting one up; if you wish to know more, make contact.

YES, BE PREPARED...

Before you travel, arm yourself with at least some of the following:

- A list of **wireless access points** in your destination area, courtesy of <http://www.hotspot-locations.co.uk/>
- Access point **sniffer software**. The process of looking for open access points is called stumbling and can be done with MacStumbler (<http://www.macstumbler.com/>), iStumbler (<http://www.istumbler.net/>) or, for those running Tiger and who prefer widgets, AirTrafficControl (<http://www.spintriplet.com/atc/>) or AirPort Radar (<http://snipurl.com/fktj>). Using this software it's often possible to pick up access points which AirPort can't, and see which are password-protected and which are not. Handy.
- Your **e-mail username and password**.
- The **URL** of your ISP's Webmail portal, if they provide this service (Ultradesign do). *If you end up using Webmail, remember to c.c. all sent e-mails to yourself, otherwise you'll have no record of what you wrote.*
- An **authenticated SMTP e-mail account**. Your ISP's portal or helpline will tell you if they offer this service and, if so, how to set up the authentication. The best kind is one that uses an alternative port for sending, to avoid port-blocking ISPs such as Wanadoo.
- A Yahoo/Hotmail/Gmail account so that, if all else fails, you can still send mail to clients from internet cafés and the like.
- An **Ethernet cable**. Sometimes you can bypass the whole wireless palaver by just plugging in.
- A modem cable, kit of international adapters for same (from the Apple Store) and your **ISP's international dial-in** number so that you can at least make an expensive dial-up phone call in order to get and send your mail. Don't get or send pictures this way, though, unless you want to re-mortgage your house to pay the phone bill.
- A tri-band **Bluetooth** mobile phone on a roaming account, or GPRS PC card adapter, so that you can connect via the local mobile operator and enjoy somewhat higher speeds than ordinary dial-up. You'll have to sell the kids to pay the bill, though.
- The contact details of someone who can help you out if the going gets tough. These individuals are often known as Digital Plumbers...

There we are, then. Those of you still awake can keep up with this exciting world by periodically checking my blog at <http://www.thedigitalplumber.co.uk>, where you'll also find my contact details. Pass the monkey, wrench.