LMUG SoundByte
London Mac User Group
Number 240 February 2015

The meeting on Monday 9th February 2015 will be at Tiger Tiger

29 Haymarket, London SW1Y 4SP.

On Monday 9th February 2015

7pm Newbyte—Paul Foster

7.15 Software Snapshot—Yosemite and continuity including taking calls, text messages and handoff

Announcements—AGM March-its next month

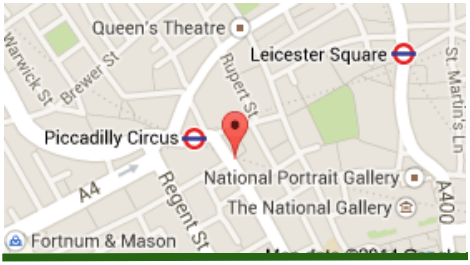
Main Topic— Show Us Your Apps Members show us their favourite apps.

Raffle Prize— Bluetooth Headphones

Buying Through Amazon? Think LMUG

LMUG is part of the Amazon Associates programme. This means that we receive a small commision (~5%) on purchases made through Amazon using a URL with our code in it.

Find the item you want through the Amazon web site, scroll down to 'Product Details' and locate the ASIN code (or ISBN number for books) and copy it. Then go to <http://www.lmug.org.uk/amazon-associates/> and paste the code into the slot waiting to receive it. Then press 'Submit' not 'Enter'.



The AGM of LMUG will be on Monday 9th March

The following nominations have been received for the new committee that will need to be confirmed at the meeting:

Post	*Nomination*
Chairman	Steve Naybour
Secretary	Tina Jacobs
Treasurer	Pietro Falcone
Membership Secretary	**Vacant**
Webmaster	**Vacant**
Newsletter	Maurice Baker
Technical Officer	**Vacant**
Communications	Martin Kelly
Committee member	Paul Foster
Committee member and support for secretary	Chris Mahon

Please come to the AGM meeting so that you can form and shape LMUG for the future.

LMUG is run by a small dedicated team of people who are great, but we need more, we need your help to keep this going.

We are after your input, drive and ideas to help shape LMUG into an even better club.

Please consider offering a little of your time to help in one of the vacant roles.

The committee are busy but great people and it would be great to have you as part of the team.

Please consider joining the committee.

Audio Hijack 3 Bumps Up the Volume

On the Mac, Apple has long made it relatively easy to plug in and immediately use audio inputs, like microphones and headsets. But Mac OS X has almost no built-in support for mixing different audio sources, which provided a perfect opening for Audio Hijack from Rogue Amoeba. It's a workflow tool for audio inputs and outputs that enables you to combine and separate sources, set timers to record audio at specific times or at recurring intervals, and add effects and filters.

The just-released Audio Hijack 3 extends and improves the software, including a radical overhaul of its interface and methods of pulling together different audio elements. It also adds new options for manipulating settings and listening to audio as it's being captured.

Rogue Amoeba has decided on a single edition release, which is now called simply "Audio Hijack" — it offers no fewer features than its former "Pro" version, but the name is no longer suffixed with that word. A fully functional version can be downloaded and used for recording up to 10 minutes of audio, after which noise is overlaid. A new copy costs $49 (with a 20 percent discount for TidBITS members), but Rogue Amoeba is offering a $25 upgrade to owners of any previous version. Note that Audio Hijack 3 requires OS X 10.9 Mavericks or later.

You can turn to Audio Hijack any time you need to capture audio. This could be for a recording session, whether live or for a podcast; to grab a broadcast Internet radio session to time-shift; or for recording the outputs of DVDs, webinars, other real-time events, or digital-rights managed media.

Users of previous versions will need to wrap their heads around the new approach because of how distinctly different it is. Veteran hijackers may miss the left-hand navigation bar that compactly listed all of the available input-source workflows; the new display uses spatial and iconographic displays, which may take getting used to.

The Basics of Hijacking -- Audio Hijack's name comes from its basic function: "hijacking," or taking over, audio streams on a Mac. In previous releases, the input source was the commanding factor. You would set Audio Hijack Pro to grab the sound from a microphone, an app, or a virtual device. Each of these inputs was a separate entry, and could be scheduled, saved to a file, and passed through effects.

This was useful for simple situations, but at one point I had four different input items configured for recording Skype calls, in which I routed multiple sources to a single virtual input, and from there to a file. It was tweaky to use, requiring that I start four separate "hijacking" sessions but record only one.

In Audio Hijack 3's new conceptual scheme, a session lets you combine multiple inputs, multiple recordings, and multiple outputs in a drag-and-drop layout. Each item has its own controls. This makes typical activities dramatically easier, while also revealing much more of what's going on at a glance.

"The just-released Audio Hijack 3 extends and improves the software, including a radical overhaul of its interface"

This revision also builds in live interaction, allowing changes to many parameters of an active session. One significant new feature lets you pause, rewind, and step through live audio without interrupting the recording.

Audio Hijack still divvies up inputs into Application, Input Device, and System Audio. Any USB-connected or other available audio source appears as an option for Input Device. With Instant On installed (choose Audio Hijack > Install Extras), applications can have their audio re-routed without being relaunched, which is otherwise required. (Installing the free Soundflower virtual audio device lets you collect and route outputs from multiple sources, too, though it's not as necessary in this new release.)

Outputs include devices like speakers, Soundflower, headphones, and Recorder — the last of which lets you capture the resulting audio to a file. What's fantastic in Audio Hijack 3 is that you can have multiple recorders in the same session, recording in different ways, while also having multiple sessions operating at once.

There's also the option to insert effects along the way, which can include boosting the volume, equalizing bands of sound frequencies, and cleaning up audio. While recording, animation lights up all active audio paths, letting you see precisely the flow of audio from and to devices.

For the full story go to *tidbits.com*

Amazon Prime: Even more of a rip-off for services you don't want

Over the past year I've written several times about my dissatisfaction with Amazon's arbitrary decision to offer "free" video steaming while at the same time increasing the cost of the Prime service to £79 a year. I've argued, quite rightly I think, that the original Prime service should have remained at £49 while anyone wanting video services or book lending should have paid extra. I also think it is intrusive the way Amazon deluges Prime users with spam-like reminders to watch videos they may not want.

We're sending you this email because you're a Prime member who is not using the video benefits that you're eligible for.
You don't have to sign up for anything new -- unlimited instant video streaming is included in your Prime membership.

Now comes insult added to injury. According to press reports, we in the UK are being well and truly milked in comparison with even with US subscribers who pay £14 less, at £65 a year. That, though, is only the start: In Italy, Amazon Prime costs only £7.50, while in Spain it is £11.25 and still only £36 a year in France and Germany.

"It isn't a question of how much the service is actually worth, it is how much Amazon can get."

Unlike Apple, which strives to have broadly comparable pricing throughout the world, Amazon appears to decide how much they can get in any particular locality. It isn't a question of how much the service is actually worth, it is how much Amazon can get.

It is about time Amazon accepted that not everyone wants to have a compulsory video-streaming service (after all, many choose to pay Netflix or other providers according to choice) and the subscription to Prime should be structured according to the services required. And they should charge broadly the same in all countries.

All the articles on this page come from Michael Evans www.macfilos.com. These and many others are well worth reading.

Mac Security: Making life harder for those with evil intent

It is nearly ten years since I abandoned Windows and bought my first Mac. Better security that came with Apple's computers was one of the most compelling reasons for the change and I took some comfort in the fact that in 2005 Macs were still a niche product. There were so few of them out there, relatively speaking, that most of us believed hackers and malware artists were less likely to target us rather than the soft underbelly of the PC world. This could have been so But, even then, OS X was inherently more secure, requiring a password before the installation of any application for instance.

A lot has changed in those ten years. Mac sales are booming, there is no longer an "Apple premium" and Macs are now reasonably priced, albeit at the higher end of the market. With this success has come more danger as criminals find it lucrative to target OS X as well as Windows. Despite this, many Mac users still do not use virus-protection software because it is intrusive and can undoubtedly cause unpredictable problems.

"Topher Kessler, writing in Macworld, highlights four security options that we should all know and implement."

That said, Mac users tend to be more technically aware and take other steps to operate in as safe an environment as possible. There are some things that every Mac user should do to protect themselves and their computer; they are simply implemented and should be high on everyone's list.

Topher Kessler, writing in Macworld, highlights four security options that we should all know and implement:

While OS X is relatively secure by default, there are some additional steps you can take to ensure the data on your Mac is only accessible by you, even if your Mac is stolen..... Overall, while Apple can do very little to prevent your computer from being stolen, OS X does its best to protect the data it holds as well as offers a chance that you can pinpoint its location. With these options enabled, you can be sure your

continued on page 4

SoundByte is the newsletter of the London Mac User Group.
It is produced solely by, and for, LMUG members.
LMUG Committee 2013/14

Chairman	Steve Naybour(chairman@lmug.org.uk)
Treasurer	Georgina Chui (treasurer@lmug.org.uk)
Secretary	Tina Jacobs (secretary@lmug.org.uk)
Assistant Secretary	Chris Mahon
Editor	Maurice Baker (soundbyte@lmug.org.uk)
Webmaster	
Membership Officer	Pietro Falcone (membership@lmug.org.uk)
Technical Officer	Andy Leigh (technical@lmug.org.uk)
Communications Officer	Martin Kelly (communications@lmug.orguk)
Committee Members	Gareth Mills & Eoin O'Cléirigh

Ideas & Suggestions suggestions@lmug.org.uk. **Website**: http://www.lmug.org.uk

Enquiries:

If you need to contact LMUG by post, email secretary@lmug.org.uk with a reason and a postal address will be emailed by return **Phone:** 07919 968075

continued from page3

Mac's data is as safe as possible, with little to no inconvenience for you

You can read the full article here. But Toby's four points are all absolutely essential to your computer's wellbeing and your protection from identity theft or worse:

Enable the OS X firewall

Enable FileVault

Manage your passwords effectively and securely

Lock your computer and enable Find My Mac

Most readers will already have taken these steps, as I have. In particular, FileVault, which encrypts your internal disk (or connected external disks) is an essential protection. It means that even if your computer is stolen and the disk removed for inspection (to circumvent the login lock), data cannot be viewed. I've been using FileVault for many years and have not had the slightest problem. It just works, silently and efficiently.

Similarly, password management is vital. I employ 1Password, as do most savvy Mac users. Not only does it encourage you to create really secure and unmemorable passwords, it manages the whole kit and caboodle brilliantly. All you need to unlock this potential is, as the name says, one password. This should be secure but something you can remember and it should under no circumstances be used elsewhere.

In addition to Topher's four cardinal precautions, you need to be aware of the security risk that comes with using your Mac in public, particularly on free wifi networks. "Free" often means unmanaged and, if you leave the door of your computer ajar, nasty people could gain access to your data while you are sipping your latte.

Christopher Breen addresses this problem in another Macworld article. He discusses ways to exclude intruders, particularly by turning off sharing that you might have enabled for a specific reason in the past, and the nuclear option of paying for a VPN (virtual private network) account.

These days, though, I tend not to use public wifi because of the various security scares. With fast 4G cellular networks available in larger cities, it now makes more sense to stick with your phone or iPad's mobile service and enable a hotspot to feed your Mac. In most cases, 4G is actually faster than most public wifi services. Christopher also recommends this and you can read all his advice here. *Christopher Breen*