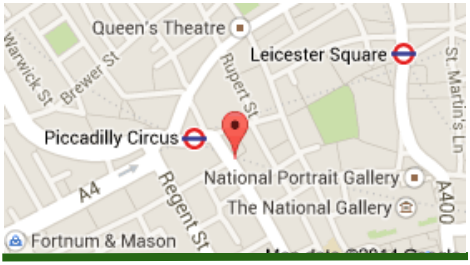
LMUG SoundByte
London Mac User Group
Number 241 March 2015

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

29 Haymarket, London SW1Y 4SP.



On Monday 9th March 2015

Apple Watch Keynote LMUG Special Event

March 9th @ 17:00 - 19:00
£5 (refunded on the night for members)
We would like to invite you to an exclusive showing of the Apple Watch keynote on March 9th.

March 9th 2015, 5pm at Tiger Tiger: Come watch the Apple keynote in an amazing BIG central party venue at Piccadilly Circus with the London Mac User Group.

Our last event had amazing feedback, but this TIME we are making it special.
We will be giving LMUG members a chance to win an Apple Watch.

So make Time for the keynote:

In room bar
Happy hour prices with bottled beer £3 and wine £9 a bottle.
Keynote bingo with prizes
State of the art sound system!
Hard Wired Internet
Food to your seat
Due to demand we have increased the venue size to fit in around 160, with seating in front of the screen for 60, with additional seating booths around the room.

Please note that in order to accomodate for this special event, our AGM has been rescheduled to April 13th 2015 at 7pm, at Tiger Tiger.

To help cover the event costs and to keep track of numbers and we will be asking for £5 with each RSVP. This will be refunded to all existing LMUG members. Anyone who upgrades on the night to full LMUG membership will be entered into the Apple Watch Raffle. Existing LMUG members can also join the raffle.

#keynotelondon

Please RSVP at this link

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'.

PLEASE NOTE

The AGM is rescheduled to our next meeting on April 13th 2015 at 7pm at Tiger Tiger.

Apple Opens iWork Web-only Access to All

Apple has opened up its iCloud Web site to anyone who signs up for a free Apple ID, providing access to Apple's iWork Web apps — Pages, Numbers, and Keynote — plus 1 GB of iCloud storage. The iWork Web apps, which remain labeled as "beta" since their debut in October 2013, are less fully featured than their sibling apps on iOS and OS X. Nonetheless, the Web apps produce documents that are completely compatible with the Mac and iOS apps — and vice-versa.

Anyone who wishes to use the iWork Web apps can sign up for a free account by browsing to icloud.com and clicking Create Apple ID. The signup process requires you to supply an email address, a strong password, and the answers to a set of security questions. Apple then sends a six-digit code to the email address you supplied; you enter that code on the iCloud site to complete the signup process.

After that, you can log in to iCloud on any supported browser — the iCloud site and its Web apps require a recent version of Safari, Google Chrome, Firefox, or Internet Explorer — and use the Web versions of Pages, Numbers, and Keynote.

Web-only users cannot upgrade their iCloud accounts to get more than 1 GB of iCloud storage or access any other iCloud features; owning a Mac or iOS device is required to do that (Mac and iOS device owners get 5 GB of storage for free automatically). An Apple support document provides more information about Web-only iCloud Access.

Keeping Up with the Snoops 8: Snoop Harder

To be honest, I thought "Keeping Up with the Snoops 7: Too Many Snoops" (21 November 2014), might have been the last in this series. The release of Snowden's documents seemed to be finished, the USA Freedom Act has been defeated, and the battle between the CIA and Senate over hacking has been quietly swept aside.

But as we approach the two-year anniversary of the first Snowden revelations of government mass surveillance, it turns out that the topic still has legs. Here's the latest in the saga.

Iron Patriot Act -- Like many "temporary" measures, the USA PATRIOT Act, signed into law quickly after the 11 September 2001 attacks, isn't going away anytime soon.

On 25 February 2015, the Patriot Act was extended for yet another year, with all attempts at adding civil liberty protections defeated.

The Patriot Act has often been used to enable or justify NSA mass surveillance. However, its author, Representative Jim Sensenbrenner, has accused the NSA of abusing the law by attempting to collect records of all phone calls in the United States.

Have You Been Spied On? -- Since I began this series, I've heard a common complaint from critics: "No one is spying on YOU," a statement that no one could prove or disprove with certainty.

Now, thanks to a UK court ruling, we may be able to find out. The Investigatory Powers Tribunal (IPT) found that secret intelligence sharing between America's National Security Agency (NSA) and Britain's Government Communications Headquarters (GCHQ) violated human rights laws. The ruling was especially interesting, given that in its 15-year history, the IPT has never before ruled against intelligence agencies.

So how does this ruling affect you if you live in the United States? Anyone whose data was shared illegally with or by the GCHQ can ask if his or her communications were included. While the IPT will not divulge details, it will give a simple "yes" or "no" determination (which is more like a maybe than a plain "no").

To make this process easy, Privacy International, one of the plaintiffs in the suit, has set up a Web page where it's collecting data to make the appropriate requests to the IPT, and also to request that the GCHQ destroy its illegally collected data.

Be aware that it could be a long time before action is taken. Privacy International says that nothing like this has ever happened before, especially not at this scale. It could take years before things are sorted out.

What's Hiding in Your Hard Drive? -- According to a report from Kaspersky Lab, your hard drive might have malware hiding in its firmware.

The work of the so-called Equation Group of malware authors has been traced all the way back to 2001. One piece of the Equation Group's malware is able to hijack the hard drive itself, preventing users from deleting data, or even enabling attackers to create hidden partitions that can be used to bypass encryption or collect data.

Some malware from the Equation Group bears several similarities to the Stuxnet worm that destroyed many of Iran's nuclear centrifuges between 2009 and 2010. Stuxnet is largely attributed to a collaboration between the United States and Israel.

Indeed, malware linked to the Equation Group is prolific and highly sophisticated, leading many to believe that the Equation Group is linked to, or even part of, the NSA.

Should you worry about your hard drive being hijacked by government snoops? Probably not. Despite the furor this story has sparked, the victims that Kaspersky has discovered so far have been highly targeted, either individually or through Web sites linked to religious radicals.

Still, the work of the Equation Group goes to show just how inherently insecure computers can be — even down to the bare metal.

Continued on page 4

iPhone 6 Plus: The two things Apple got wrong with the big phone

The iPhone plus has been a revelation and I am a huge fan. For me, it has become the only device I carry around every day. No longer do I feel the need for an iPad mini to supplement the phone. It is truly a one-stop shop. There is just one major aspect of the design that niggles—the placing of the lock (or on/off) button on the right of the handset, directly opposite the volume controls. Many times I have inadvertently locked the phone just by picking it up or when attempting to alter the volume. The top-placed button on the iPhone 5 was much more sensible in my view.

I am glad to see, therefore, that I am not alone. Writing for TekRevue, Jim Tanous highlights this feature as a major design flaw of the 6 Plus. However, as he says, it really wouldn't have been a good idea to leave that button on the top of the phone:

Both new iPhones are larger than their predecessors, too big to keep the lock button (a.k.a. on/off or sleep/wake button) in its traditional location on the top edge of the device. Leaving it there would make it nearly impossible for most users to reach it while holding the phone with one hand, especially those using the iPhone 6 Plus. Therefore, Apple decided to move the lock button to the right side of the phone. But he believes that the decision to place it exactly where it is, opposite the volume controls, is the worst possible option.

While he is at it, Jim also complains about the inability selectively to disable home-screen rotation. Many users prefer to keep the home screen in portrait mode—for instance, to stop auto rotate when lying in bed—while allowing landscape in applications. But with the iPhone 6 and 6 Plus the rotation lock is a system-wide setting. I confess I hadn't gathered my thoughts on this. Now I've read Jim's comments I realise this has been bugging me all along and it will bug even more now I realise the cause.

As Jim points out, "these are first-world problems". He goes on to say that Apple created a great phone, but they didn't create a perfect phone.

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

Tim Cook: The Apple Watch will likely require daily charging

Shock, horror. Tim Cook says we might need to charge our Apple Watch every day? What is the world coming to? But just who, with anything but the most tenuous grasp of physics, expected that the Apple Watch would not require daily charging? All those naysayers haven't got a clue. I will be happy if the Apple Watch lasts a day on a full charge, just like the iPhone and iPad.

Nightly charging is a good discipline and a good routine. I don't really like devices, such as the Kindle Paperwhite, that last days or even weeks between top-ups. At some stage you are going to be left high and dry without power unless you are meticulous in checking and breaking your routine to plug in the charger. Better to plug in nightly. Think of it like brushing your teeth.

Desktop Clutter: How Hazel can clean things up automatically

I've been using Hazel's automated features for years but I am the first to admit that I merely scratch the surface of this deeply capable application. So I was all eyes when I saw that Harry Guinness at Tutsplus has produced a detailed guide to getting Hazel to tidy up the desktop of my Mac. As he says:

Hazel is a great app for automating file management in OS X. You can assign certain folders for Hazel to watch and then perform specific actions if the files within meet set criteria. Hazel can automatically put videos in the Movies folder and audio tracks in the Music folder. It can also, as you'll see, do a whole lot more. In this tutorial I'll demonstrate how to create the ultimate workflow for keeping a Mac clutter free—or at the very least, keeping the clutter organised—using Hazel and a dedicated Inbox.

Armed with Harry's step-by-step instructions I shall be commanding Hazel over the Christmas holidays and hope to start 2015 with a pristine, uncluttered desktop. I plan to make just one tweak to Harry's sage advice. Instead of putting the Inbox in my computer's user folder I will place it in Dropbox. I keep all my current data on Dropbox so that it is available wherever I am and on either of my two Macs (MacBook Pro and MacBook Air).

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

continued from page2

The focus of the summit was an executive order, signed by President Obama at the event, that encourages greater sharing of security information between tech companies and the federal government. The order, which is advisory and not prescriptive, calls for central clearinghouses for information between the government and private enterprise.

The president also agreed to a few interviews, mostly notably with Re/code's Kara Swisher.

In the interview, Obama admitted to a strained relationship with Silicon Valley, mostly pinning the blame on Edward Snowden's revelations of NSA spying. Indeed, revelations about mass surveillance have caused the Chinese government to drop many American technology brands, including Apple. However, the president did acknowledge that the NSA had gone too far in its intelligence gathering efforts. "There have been abuses on U.S. soil," the president said.

One of the main tussles between the government and the tech sector has been over encryption. The NSA has been caught weakening encryption standards, and law enforcement has complained about stronger encryption measures in consumer products. Swisher asked the president about this, but his response was something of a waffle.

But the intelligence agencies' biggest win over encryption had yet to be revealed…

The Great SIM Heist -- Just when the Snowden revelations seemed to be fading away, The Intercept dropped another bombshell.

Britain's GCHQ, with help from the NSA, infiltrated Gemalto, the world's leading producer of SIM cards. Gemalto produces 2 billion SIM cards a year for AT&T, Sprint, T-Mobile, Verizon, and others. Intelligence operatives mined the private communications of engineers to steal SIM encryption keys.

In effect, the NSA and GCHQ may have the capability to decrypt voice and data from almost any cell phone in the world. "Once you have the keys, decrypting traffic is trivial," Christopher Soghoian of the American Civil Liberties Union told The Intercept. "The news of this key theft will send a shockwave through the security community," he said.

In fact, the ramifications for cellular security could be significant. Matthew Green, a cryptographer at Johns Hopkins University, called it, "bad news for phone security. Really bad news." He continued, "Gaining access to a database of keys is pretty much game over for cellular encryption."

Gemalto has admitted that it was hacked, but has downplayed the severity of the intrusion. The company said that the infiltrators gained few, if any, SIM card keys, and that the ones that might have been stolen were outdated anyway. However, many are skeptical that Gemalto could have performed a thorough security audit in such a short amount of time.

The Gemalto story has caused even more tension between the federal government and security experts. At a New America Foundation conference on cybersecurity on 23 February 2015, things got heated when NSA Director Mike Rogers was grilled by Yahoo's chief information security officer, Alex Stamos, about the NSA's desire for encryption backdoors (a term Rogers rejected). Rogers dismissed concerns that foreign nations could also demand their own encryption backdoors with, "I think we can work our way through this." (As an aside, this picture of Admiral Rogers does not inspire confidence.)

The silver lining in this cloud is that this may have finally alerted technology companies to the stark reality that many of the technologies we rely on every day are inherently insecure. Let's hope it causes the tech world to focus more on fundamental security practices.