Keir Thomas-Bryant
Portfolio
May 2017

Over a two-decade career I've written countless pieces for countless properties under my "maiden name" of Keir Thomas, which I continue to use for my professional work. I've long since stopped keeping clippings of my work but here's a selection of excerpts that aim to be as representative as possible – please click on each entry listed below to jump straight to that excerpt.

Note that links in blue take you straight to an online property displaying my work.

Online content

I have written for *PCWorld* (US), *Macworld*, *Cult of Mac*, *OS X Daily*, *Mac Kung Fu*.

"How To Get An Old Mac Working": A recent post taken from many at *Mac Kung Fu*, the blog I created and run single-handedly, including turning it into a brand that across 2016 attracted over 600,000 page impressions.

"Sony PlayStation Hack": One of many posts written for IDG's online properties in the US. I worked across different sections of *PCWorld*, including breaking two stories each day for their business/SME BizFeed section.

"How To Remove Mac Ransomware": Recently written for *Macworld* in response to the NHS ransomware attacks; 2,000+ words written and researched in four hours. I've worked freelance for Macworld over many years, including when it was also a print publication.

Print journalism

I have written for *Computer Buyer* (staff member), *PC Direct* (staff member), *Information Week*, *Mobile Computing*, *PC Explorer* (staff member), *PC Utilities* (editor), *PC Utilities Gold* (originator and editor), *PC Tools* (originator and editor), *Linux User & Developer* (editor), *PC Extreme* (editor), *Digital Photography Buyer & User*, *Macworld*, *Micro Mart*, *iCreate*, various Imagine Publishing bookazines, *Writers' Forum*, *Writing Magazine*, *The People's Friend*, *Viz* comic, and others.

"Alternative Operating Systems": One of many features I wrote for *Micro Mart* magazine before its closure last year (following the pattern of nearly all UK computer magazines, sadly).

"The World's Greatest Viruses": A feature I wrote for *PC Extreme* magazine, which I also edited. While editing magazines I also wrote significant amounts of copy each month for my own and other titles.

"Broadband Revolution": A feature I wrote for *PC Utilities*, a magazine I also edited. Included in this excerpt is the magazine's cover, plus the editorial/copyright page.

"Install Multiple Operating Systems On Your Mac": One of many tutorials I have written for Imagine Publishing bookazines.

"Light Bulb Moments": I am *The People Friend*'s go-to source for articles about technology and write for it regularly. This piece is about energy-efficient light bulbs.

Technophobia column: For the past four years I've written a regular column for *Writers' Forum*, explaining how technology can benefit writers. Older pieces can be found at a basic blog I created: http://writer.support.

"Getting Good Publicity": An interview with the book publicist Louise Rhind-Tutt for *Writers' Forum* magazine.

"I Wish I'd Known": One of an interview series written for *Writing Magazine*, in which I questioned three successful authors each month.

Books

I'm the author of *Beginning SUSE Linux* (several editions), *Beginning Ubuntu Linux* (several editions), *Beginning Fedora*, *Ubuntu Kung Fu*, *Mac Kung Fu* (several editions), *iPad and iPhone Kung Fu*, *Ubuntu Pocket Guide & Reference*, *Working at the Ubuntu Command-Line Prompt*, *Managing The Ubuntu Software System*.

Beginning Ubuntu Linux: An excerpt from one of the first IT textbooks I wrote.

Mac Kung Fu: An excerpt from another of my books.

Ubuntu Pocket Guide: An excerpt from another of my books, this time one that I self-published after seeing a decline in the traditional IT publishing industry. Read by over 1,000,000 people worldwide.

Publisher

I have created two small presses: Macfreda publishes IT books I've written, while Puppywolf publishes mainly poetry originating in Manchester.

iPhone / iPad / Mac / Watch / TV ... and more
MACKUNGFU
Get the latest tips & tricks at TWITTER or FACEBOOK

How to get working an old Mac you've received

7 March 2017, 10:27

Somebody is either given a dirty old Mac, or buys one from a thrift store, and they have absolutely no information about it. It might be bootable. Sometimes the disk has been wiped, or all you see is a **scary boot time icon**. In most cases the urge is to start again with a clean installation of the operating system. Complicating the situation is that this new Mac owner has little experience of them. A vital fact is that Macs just don't work like Windows PCs when it comes to installing the OS.

Does this sound familiar? Then read on.

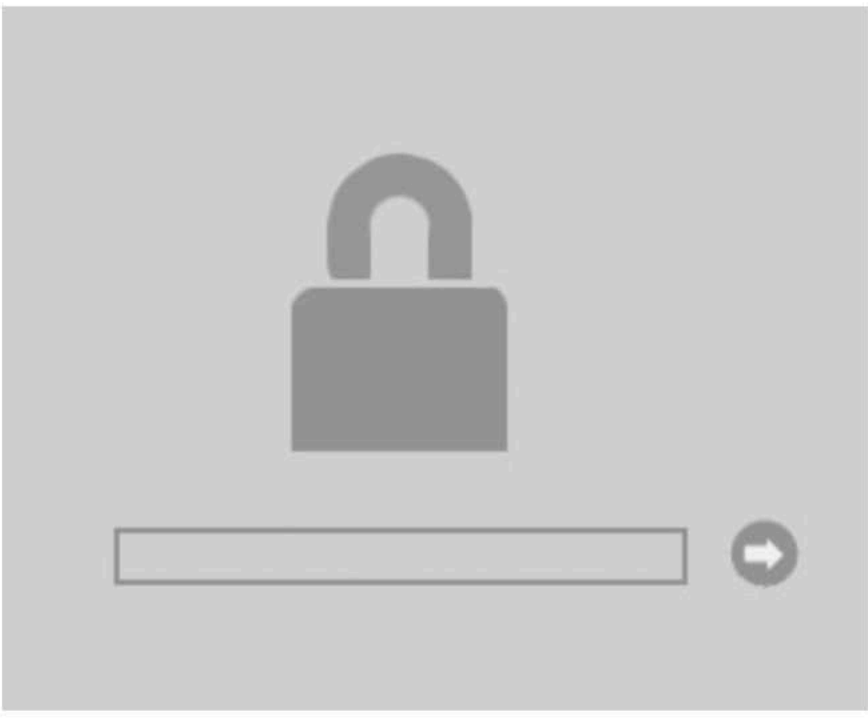
Using Internet Recovery

Most Macs since around 2010 have featured Internet Recovery and this is the most direct route to getting a fresh installation of the operating system on the computer. There's also something called Recovery Mode, but if the disk has been wiped then this might not be present, so I advise Internet Recovery. Notably, Internet Recovery will install the version of the OS X/macOS that the computer came with when first purchased, and often this is optimised for that machine (and you can always upgrade later). It's also one of the only ways to actually install that particular operating system version because Apple typically only makes available the latest versions for upgrade purposes.

Obviously, for Internet Recovery to work you'll need to be within range of a standard internet-connected Wi-Fi signal, and also know the Wi-Fi password. Apple **lists all the computers** that are compatible with Internet Recovery but, of course, you might not know the make and model of your Mac, so this could be moot. Just give a try and see what happens.

To boot into Internet Recovery mode, boot the computer and, before the Apple logo appears or you hear the chime, hold down the Cmd+Option+R keys (in some countries this will be Cmd+Alt+R).

If you see the following padlock image on the boot-time screen...



... then I'm sorry but it's game over at this point because this means Mac has a firmware password. If you don't know this password then you can't do much apart from boot the computer to its existing operating system. You might try **creating a bootable USB stick** to install an operating system while the computer's booted-up, but that's outside the scope of this article.

Note that, to my knowledge, it's impossible to crack a Mac's firmware password. That doesn't stop many scammers saying they can, however, so be careful should you google this issue.

UPDATE: It transpires there might be a way of **resetting the firmware password on Macs manufactured before 2009**. It involves disassembly of the computer, however.

If you don't see the firmware password request then you should find yourself prompted to join a Wi-Fi network, and following this the operating system recovery partition will be downloaded. This might take a while.

Formatting the disk

After this you should see a menu offering various options, including installing OS X/macOS, but don't jump into that just yet! Instead, click to start the Disk Utility app. Once that's up and running, select the main partition on the left of the Disk Utility window – the one that's slightly indented from the header showing the name of the disk drive – and click the Erase button. You'll then be prompted to give the new partition you're creating a name, and ensure you select "Mac OS X Extended (Journaled)" from the dropdown list beneath. If there's a third drop down menu beneath this ensure you select "GUID Partition Table" (or "GUID Partition Map") and not MBR, as you might with Windows or Linux.

Once your new partition is created, close Disk Utility (click Disk Utility > Quit) and this will return you to the previous menu. Select to install Mac OS X/macOS. At this point you might be prompted for an Apple ID and password. If you have an existing one that you use, such as one used on your iPhone or iPad, then use that rather than creating a fresh one. This is important because not all Apple IDs are equal and those already in use – and that have already downloaded apps, for example – have superpowers that are useful here. However, if you don't have an Apple ID then you'll need to **sign-up for one**.

Installation from this point should be straightforward. If you run into any issues, post them below ensuring you complete the email address field too, and I'll attempt to get to back to you.

Installing Windows or Linux

You might be tempted to forgo the OS X/macOS experience and just install Windows or Linux. After all, a modern Intel Mac is just a PC in other clothing... right? Surely you can just jam in a bootable Windows/Linux USB stick? Sadly, no. You might be able to boot from the USB stick (hold down Option/Alt at boot to see the boot-time menu), but the EFI boot ROM in a Mac is different compared to a PC, and you can't simply install Windows or Linux without first **using the Boot Camp utility**, which is built-in to OS X/macOS. This means you'll need to have a working OS X/macOS installation.

Really old Macs

If you end-up with a really old Mac – like the fruit-colored iMacs or clamshell iBooks – then Internet Recovery won't work. The best bet for these computers is to source the original installation CDs/DVDs, which you might be able to do via eBay. Alternatively, you might find in one of the many online Mac communities that somebody will create disks for you. There's a **lot of excellent resources** out there if you do end-up with a vintage Mac, and they can be surprisingly usable.

Leave a comment...

NEWS

Sony Makes it Official: PlayStation Network Hacked

By Keir Thomas

PCWorld | APR 23, 2011 7:35 AM PT

When Sony's PlayStation Network was taken offline three days ago, all eyes fell on the Anonymous group, who've taken a dislike to Sony over its treatment of hardware hacker George Hotz. The network allows online play between PlayStation 3 consoles and boasts 70 million users, so this is no small inconvenience.

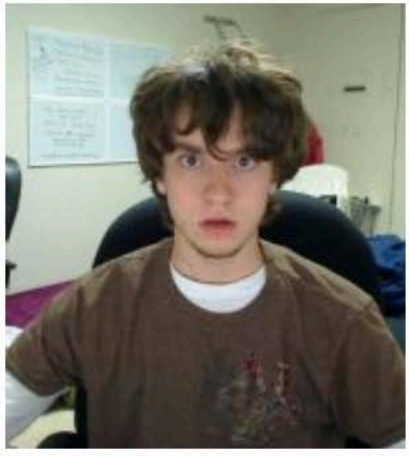
[Further reading: Best NAS boxes for media streaming and backup]

Last night Sony confessed that an "external intrusion" caused the company to take-down the PlayStation Network and also Sony's Qriocity service in order "to verify the smooth and secure operation of our network services going forward". However, they're not saying anything more, or giving a time scale as to when gamers will be able to resume playing online.

What makes it strange is that Anonymous has denied being involved, claiming "for once we didn't do it" and suggesting Sony was using rumors of an Anonymous attack as cover for an internal problem with

their servers. As yet Anonymous hasn't responded to the latest update from Sony.

However, the decentralized nature of Anonymous means that individuals act alone with no governance, and Anonymous admitted that "it could be the case that other Anons have acted by themselves."


George Hotz

The phrasing Sony used--talking of an "external intrusion"--indicates that this wasn't a Distributed Denial of Service (DDoS) attack, which is one of Anonymous' most popular modus operandi. Instead, this seems to be an individual breaking into the network and this is probably why it's taking so long to clean-up--Sony has to trace every corner of their systems affected by the hacker and repair it or restore files. It's like removing a rodent infestation from a house--there's no quick and easy fix.

The break-in might even be coincidental to the recent Anonymous actions, or could be a hack attack from some time ago that has until now remained undiscovered. However, the timing is certainly suspicious, with several of 2011's most anticipated game titles launching this week, including Mortal Kombat, Portal 2 and SOCOM 4.

To comment on this article and other PCWorld content, visit our Facebook page or our Twitter feed.

How to remove Mac ransomware

Worried about WannaCry? Don't get caught out by Mac ransomware. Here's how to fight back and avoid being caught by scams in the future

by Keir Thomas | 16 May 17

With the outbreak of WannaCry crippling the world's computers, Mac users might be wondering what they can do to protect themselves from ransomware, and how to fix things if they get hit. Here's everything you need to know about detecting, avoiding and removing ransomware on Macs.

This is one of several in-depth Macworld articles dealing with Mac security. If you're looking for AV buying advice, read our roundup of the Best Mac antivirus and Do Macs get viruses?; general advice can be found in our Mac security tips; and those who have been hit by a virus should try How to remove Mac viruses.

What is ransomware?

Ransomware is a type of malware attack where your personal files are encrypted against your wishes, before a 'ransom demand' tells you to pay a fee if you want to get the files decrypted again.

Although at the time of writing there hasn't been a serious ransomware outbreak on the Mac (or any Apple hardware), security researchers reckon it's a real possibility. For example, security researchers have found Mac-specific lines of code within Windows ransomware, which indicates that the bad guys are at least considering the possibility.

Speaking on CNBC's 'Squawk Box' programme in the wake of the famous WannaCry ransomware attack, Aleksandr Yampolskiy, CEO of SecurityScorecard, insisted that Apple users are vulnerable to WannaCry-type attacks, even if that specific event affected Windows systems only.

"It happens that this attack is targeting the Windows computers," he said. "But Apple is absolutely vulnerable to similar types of attacks."

Help! My Mac been infected by ransomware!

Very well: let's hypothetically assume you've been infected. What should you do?

Don't panic

Take your time and avoid kneejerk reactions.

Clean up

Use a malware scanner like the free Bitdefender Virus Scanner to search for the ransomware and remove it.

It's unlikely you'll be the only person affected by the ransomware so keep an eye on sites like Macworld to learn more about the nature of the ransomware infection. You'll very likely find specific instructions on how to clean up the infection, if a virus scanner isn't able to do so.

You might find that a security researcher has found a way to decrypt your files for free, something that happened with the most recent example from the handful of ransomware infections that have been identified on a Mac.

Don't pay

As you'll see later when we examine the handful of existing ransomware outbreaks affecting the Mac, there's a good chance paying up won't actually recover your files!

Unplug and disconnect storage

The one example of effective ransomware seen on a Mac so far - KeRanger - also attempted to encrypt Time Machine backups, to try to make it impossible for the user to simply restore files from a backup.

Therefore, upon discovering your Mac has been infected by ransomware you should minimise the possibility of backups becoming encrypted too by immediately unplugging any removable storage like external hard disks, and disconnecting from any network shares by clicking the eject icon alongside their entries in the sidebar of Finder.

Are Macs affected by WannaCry?

Put simply, no. WannaCry takes advantage of a bug in Microsoft Windows' network file sharing system, a technology called SMB. Once WannaCry gets onto a single computer on the network - usually because an individual opened a rogue email attachment - it then uses a bug in SMB to inject itself into all other computers on the network that haven't been patched.

Macs also use SMB as the default network file sharing technology, so you might initially think Macs could be affected too. However, Apple uses its own bespoke implementation of SMB. While this is fully compatible with Microsoft's version, it doesn't suffer from the same bugs or security holes, so isn't affected by WannaCry - or at least not in WannaCry's current manifestation.

The iPhone, iPad, Apple TV and even the Apple Watch don't use SMB file sharing, so aren't even theoretically at risk from WannaCry.

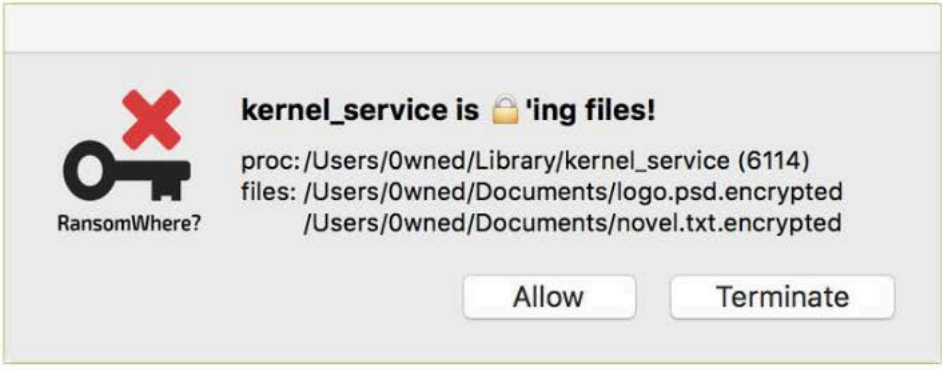
Content continues below

How do I protect my Mac against ransomware?

There are several things you can do to protect your Mac against ransomware:

Install RansomWhere?

Consider installing the RansomWhere? app. This free app runs in the background and watches for any activity that resembles the rampant encrypting of files, such as that which takes place during a ransomware attack. It then halts the process and tells you what's happening. Okay, so some of your files may end up being encrypted, but hopefully not very many.



Basic phishing protection

As with many examples of ransomware and malware, WannaCry initially infects computer networks via a phishing attack. Never open an email attachment you weren't expecting, even if it appears to come from somebody you know, and no matter how important, interesting or scurrilous it appears to be.

Don't use dodgy software

The most recent Mac ransomware attempts to spread via "cracked" or patcher apps designed to let you use commercial software for free. Therefore, avoid all dodgy software like this.

Always ensure your system and apps are updated

On a Mac you can configure automatic updates by opening the System Preferences app, which you'll find in the Applications list of Finder, and selecting the App Store icon. Then put a tick alongside Automatically Check for Updates, and putting a tick in all the boxes directly beneath this heading.

Install only from official websites

If you suddenly see a pop-up saying one of your browser plugins is out of date, for example, then be sure only to update from the official webpage for that plugin - such as Adobe's website if it's the Flash plugin. Never trust the link provided in a pop-up window! Hackers make frequent use of such pop-ups and fake websites to spread ransomware and other malware.

Back up frequently

If you have a backup of your files then it matters less if ransomware strikes because you can simply restore. However, the KeRanger ransomware outbreak attempted to also encrypt Time Machine backups, so you might choose to use a third-party app like Carbon Copy Cloner instead to backup your files. Read more: How to back up a Mac

How do I protect my iPhone or iPad against ransomware?

iOS devices like iPhones and iPads were built from the ground-up to be much more secure than Macs, and true ransomware via some kind of malware infection would be extremely difficult to pull-off. There certainly haven't been any examples so far, or at least on iOS devices that haven't been jailbroken.

However, iPhones, iPads and even Macs are subject to iCloud hijacking, a type of ransom attack whereby a hacker reuses passwords discovered through one of the many large-scale security breaches in order to log into and take control of a user's iCloud account. They then change the password and use the Find my iPhone service to remotely lock the iOS device or Mac, sending the user demands for ransom money in order to restore control.

Often they threaten to remote wipe the device or Mac in addition to this. The first such attack of this nature was the Oleg Pliss attack back in 2014.

iCloud hijacking is easily thwarted by setting up two-factor authentication, and you should do so now!

However, regardless of whether an actual ransomware infection is possible, it certainly makes sense to ensure you keep your iPhone or iPad fully updated (read How to update iOS on iPhone or iPad) so as to have the best possible protection against any potential threat. When a new iOS update becomes available a notification will appear alongside the Settings app, and you'll be able to update by opening Settings then tapping General > Software Update. (Note that there's no way to configure automatic system updates on iOS.)

Any app claiming to provide antivirus scanning for iOS devices is likely to be dubious at best because all iOS apps are sandboxed, so are unable to scan the system or other apps for malware.

Have Macs ever been affected by ransomware?

With the exception of the FBI web page scam described below, which is more of an annoyance than a serious threat, the handful of Mac ransomware examples identified by security researchers to date have not led to serious outbreaks and few if any Macs have been affected. However, the list makes interesting reading to learn how a future ransomware outbreak might spread and how it might operate.

FBI scam (July 2013)

For over a decade, website-based ransomware has attempted to extort money from gullible Windows users by "locking" the web browser to a purported law enforcement website. This was always mere smoke and mirrors, however, and could be overcome easily.

But in July 2013 security researchers discovered a similar scam specifically targeting the Mac's Safari browser. The user was locked to a fake "FBI" webpage via a dialog box that wouldn't let them leave the site, and a $300 "fine" was demanded to unlock the system.

Quitting the browser was made impossible. If the user force-quit Safari, the ransomware page simply reloaded itself next time Safari started.

Apple has since fixed Safari on both Mac and iPhone/iPad so that it's less easy for browser-based ransomware like this to operate. However, you might still encounter less virulent examples.

How to clean up FBI scam and its variations

Force-quit Safari by right-clicking its Dock icon, holding down Alt (Option on some keyboards) and selecting the force quit menu option. Then start Safari while holding down the Shift key. This will stop Safari loading the last page it had open, which escapes the annoying reboot loop of the ransomware.

FileCoder (June 2014)

Security researchers found and identified FileCoder via the Virus Total virus-scanning website, although by that point FileCoder was already old, having been first detected by the site's malware scanner two years earlier.

Specifically targeting OS X/macOS, FileCoder is unfinished and not a threat, in that it doesn't actually encrypt the user's data. It does display an app window demanding a ransom of €30 (rather cheekily, this is discounted to €20 if a credit card is used instead of PayPal or Western Union).

It's not known where FileCoder originated, or how it was intended to spread.

How to clean up FileCoder

Because FileCoder has only been spotted a single time in the wild, we have hardly any information about how it operates and therefore how to clean it up. However, because of this it should not be considered an active threat.

Gopher (September 2015) and Mabouia (November 2015)

Two security researchers, working independently, separately create Gopher and Mabouia, two examples of ransomware specifically targeted at Macs. However, both are only proof-of-concept demonstrations, intended to show that fully fledged ransomware on the Mac is entirely possible.

Aside from copies shared with security researchers for them to learn from, neither ever leaves the researchers' computers, so cannot spread.

How to clean up Gopher or Mabouia

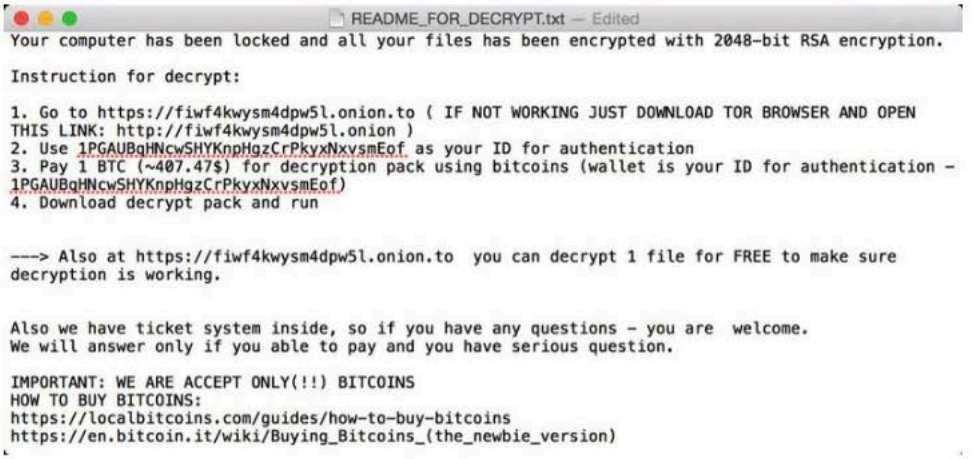
Because both are merely proofs of concept, and have never been actually deployed in the wild, it's impossible to say how any ransomware infections created Gopher or Mabouia could be cleared up.

KeRanger (March 2016)

Security researchers find and identify KeRanger ransomware within an authorised update for the Transmission BitTorrent client. The first real example of Mac ransomware, this time the ransomware creators have clearly made an effort to create a genuine threat.

KeRanger is signed with an authorised security certificate, so isn't blocked by the macOS Gatekeeper security system, for example. KeRanger encrypts files and then leaves a README_FOR_DECRYPT.txt file in the directory, in which the ransom demand is made (one BitCoin; around £1,338.62 at the time of writing in May 2017).

However, thanks to fast action by the researchers and also Apple, who immediately revoke the security certificate, KeRanger is halted before it becomes a serious threat. If both agencies hadn't been quite so quick off the mark, however, it could've been a very different story.



How to clean up KeRanger

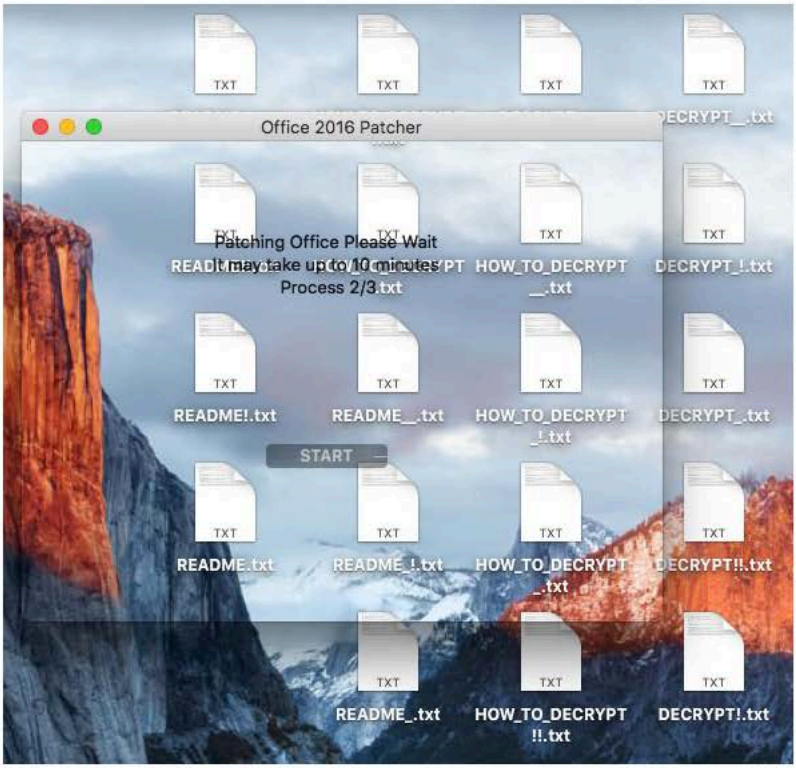
Our understanding is that you will not be able to decrypt the files. However, if you're worried that KeRanger ransomware may have infected your Mac, here is how the security researchers who identified it - Palo Alto - suggest you clean it up:

1. Using either Terminal or Finder, check whether /Applications/Transmission.app/Contents/Resources/ General.rtf or /Volumes/Transmission/Transmission.app/Contents/Resources/ General.rtf exist. If any of these exist, the Transmission application is infected, and we suggest deleting this version of Transmission.
2. Using 'Activity Monitor' preinstalled in OS X, check whether any process named 'kernel_service' is running. If so, double-check the process, choose Open Files and Ports and check whether there is a file name like "/Users//Library/kernel_service". If so, the process is KeRanger's main process. We suggest terminating it with Quit > Force Quit.
3. After these steps, we also recommend users check whether the files .kernel_pid, .kernel_time, .kernel_complete or kernel_service exist in ~/Library directory. If so, you should delete them.

Filezip (February 2017)

Security researchers find and identify Filezip ransomware masquerading as "patcher" apps that can be downloaded from piracy sites. Patcher apps are designed to illegally modify popular commercial software like Adobe Photoshop or Microsoft Office so they can be used without purchase and/or a license code.

When the user attempts to use the patcher app, Filezip instead encrypts the user's files and then places a "README!.txt", "DECRYPT.txt" or "HOW_TO_DECRYPT.txt" file in each folder listing the ransom demands (0.25 BitCoin; around £335 at the time of writing in May 2017). Notably, like many Windows-based examples of ransomware, Filezip is unable to actually decrypt any files, so paying the ransom is pointless.



How to clean up Filezip

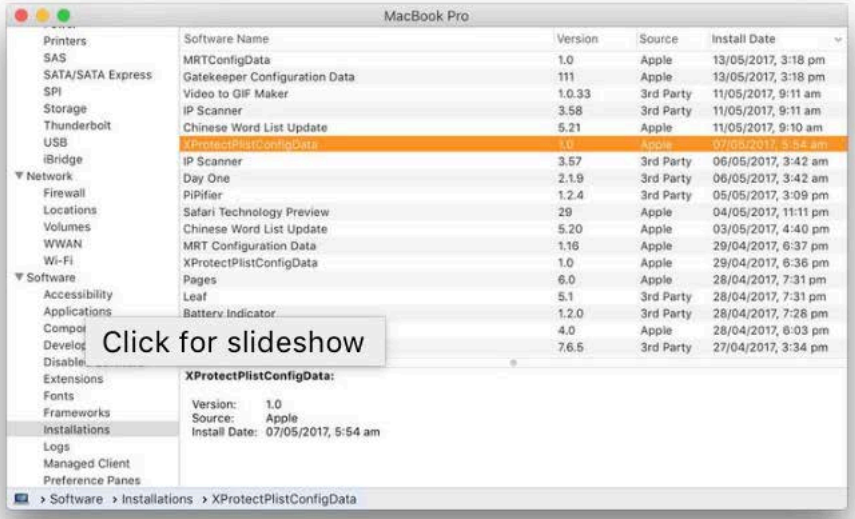
Simply delete the patcher file from your hard disk. Security firm Malwarebytes has since discovered how to decrypt any affected files affected by Filezip for free, although the process is a bit complicated.

Should I run an antimalware app all the time?

It might surprise you but Macs already have antimalware built in, courtesy of Apple.

XProtect runs invisibly in the background and scans any files you download as part of the standard file quarantining process. XProtect is updated regularly by Apple with new malware definitions and you can see the frequency of updates by following these steps:

1. Open the System Information app by clicking Apple > About This Mac, then clicking the System Report button.
2. Select the Software heading in the list at the left, and then the Installations heading beneath this.
3. Click the Install Date column heading to sort the list by most recent and look for entries that read XProtectPlistConfigData.



XProtect was how Apple was able to defeat KeRanger, perhaps the most serious Mac-based ransomware threat so far, before it had a chance to become endemic. Additionally, the most recent Mac ransomware, Filezip, has been added to XProtect too.

Combined with other built-in safeguards such as file quarantining and Gatekeeper - both of which stop the user blithely running apps or opening docs they download from strange websites - the Mac is better guarded against ransomware than you might think.

However, there's certainly no harm in occasionally running an on-demand virus scanner such as Bitdefender Virus Scanner, even if this may well find many false positives in the form of Windows viruses in things like mail attachments. Windows viruses are harmless for Mac users. Read about the best Mac antivirus software here.

Tags: Mac ,Mac Software

Share this article

Alternative Operating Systems

Keir Thomas takes a walk on the wild side of desktop operating systems that offer an alternative to Windows and Linux

The desktop wars are over and the surprise result is that we don't care who won. It's all about what you can do online nowadays, and Microsoft's even giving away the latest update of Windows.

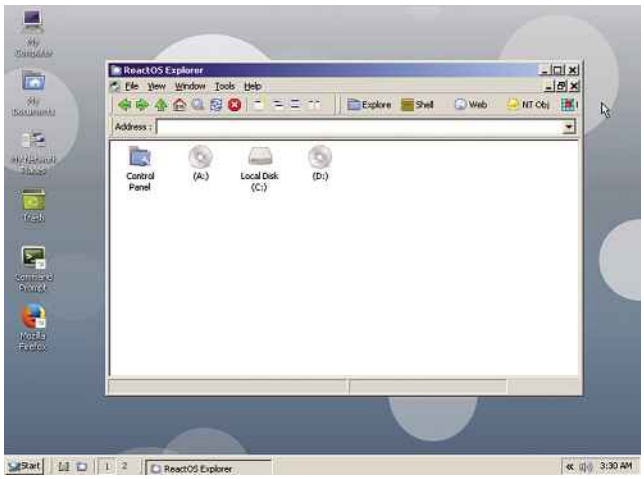
That said, the desktop is still the jumping off point for PC users, and those who find Linux as irksome as Windows might be wondering if there's a third choice – something that's neither, yet provides the basic capabilities we've all come to expect.

Below we look at four candidates. Bearing in mind the tremendous time and expense that's gone into creating Microsoft's product, along with most Linux distros, we simply can't say the operating systems are a straight swap-in. However, for the user who isn't afraid to get their hands dirty, they offer more than you might think.

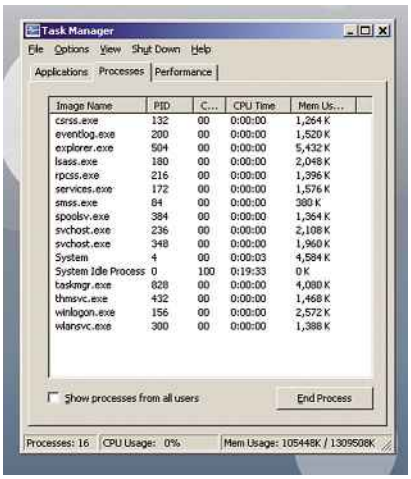
ReactOS

ReactOS (**www.reactos.com**) was a child of the mid-1990s desktop war. The project's goal back then, as now, was to provide an open source and free clone of Windows. That's an actual, binary-compatible swap-in and not a version of Linux/Unix that merely apes the look and feel. The goal has since mutated into an attempt to recreate the Windows NT architecture and APIs, which means binary compatibility with not just software but also device drivers. In other words, you should not only be able to install the latest Microsoft Office direct from DVD/download, with no additional hacks, but also the latest Nvidia 3D drivers.

Well, you'll be able to do that at some point in the future. Since its inception in 1998 the project has been in pre-release stage (alpha) because, as strange as it might sound, a group of enthusiastic volunteers struggle to keep up with a million-billion-dollar corporation that's constantly redefining its product. That ReactOS has come so



▲ *ReactOS looks, feels and works like classic Windows mode under XP, and most built-in apps look identical*



▲ *Look familiar? This isn't a Microsoft product! ReactOS's wizards and windows mirror Windows almost exactly*

far is laudable, and it works via a combination of original code created by the project members (including an NT kernel), along with some bolt-on bits from the Wine project (**winehq.org**), which creates a Windows emulation layer on Unix/Linux.

What you get when ReactOS boots is a desktop that looks spookily similar to Windows XP in classic mode (and the ReactOS team have promised never to embrace Metro design concepts). This includes everything from the Start button to Windows Explorer, and basic apps like Calc, Notepad, WordPad and Paint. Pop-up windows like driver installation wizards or the task manager are essentially identical to Windows.

One of the biggest and most welcome non-standard features is the Application Manager, which links straight to freeware, shareware and open source Windows apps that are known to work with ReactOS. Examples include Firefox, Thunderbird, OpenOffice.org, 7-Zip and more. Most seemed to work just about okay in our tests but, to be honest, freezes and crashes weren't hard to bring about.

The ReactOS YouTube channel shows somebody installing and using Microsoft Office 2007, which is pretty impressive. We wanted to install Office XP but couldn't find a way to get the installation files into our virtual machine. We couldn't get Windows file sharing (that is, Samba) to work, for example, and an attempt to access a home-made web server resulted in a web page with distorted text.

With its potential for the fuss-free recreation of Windows, which surely is a desire of many business users, and its ability to be compiled for ARM hardware, it's a small mystery why ReactOS has never picked up corporate custom in the way eComStation has (see below). That said, ever keen to avoid imperialistic American influence, the Russian government has shown interest in ReactOS, and even Vladimir Putin has pushed a cursor around its desktop. Indeed, despite its longevity and the fact that right now ReactOS isn't ready for primetime use, its story is still being written.

eComStation

OS/2 provides a fascinating chapter in the history of computing that features once typical Microsoft treachery versus the striving of IBM to be relevant for desktop computer users.

IBM failed, of course, but not before garnering significant corporate clients including a chunk of the worldwide banking and manufacturing industries. Most Westerners are heavy users of OS/2 without knowing it, because it continues to run older cash and ticketing machines, while companies like Siemens use it to run industrial machinery. This is at least partially because OS/2 scratched multitasking and security itches that were mere pipe dreams for Microsoft of the era.

Of course, this being the world of computing, there's also a community of die-hard OS/2 fans out there, so when IBM decided to finally step away from it in the late 1990s a handful of third-parties continued development via the eComStation project. The latest release – 2.2 Beta II – came out in December of 2013 but the project is still very much alive.

It's important to note that although eComStation is a proprietary, commercially oriented project that has the original OS/2 at its core, it isn't an open-source hobbyist recreation or an emulation. You can download a live CD/ISO demo from **www.ecomstation.com**, but if you want to run eComStation full time you'll have to pay an $82 yearly subscription fee if you're a business or $41 if you're a home or student user. Bearing in mind Windows 10 will soon be free for most people, this is a bit tough to swallow.

Don't release the moths from your wallet just yet, though, because eComStation is an operating system that has fallen badly behind the technical times. It's 32-bit only, for example, so can only address up to 4GB of RAM, and it simply won't work on modern UEFI-based computers. Very limited hardware driver support means there's no USB 3.0. On the other hand, eComStation will install and run just as sweetly as OS/2 ever did on older hardware,

eComStation picks up the dying embers of OS/2 and, well, keeps them glowing just that little bit longer so corporate users don't have to scrap old systems

An old-ish version of Firefox is provided with eComStation and provides an acceptable if ugly contemporary browsing experience

and it works well as a virtual machine (which was how we tested it and how many corporations now make use of it).

Booting eComStation is pure 1990s nostalgia, with a variety of desktop tools and widgets that give a feel of Linux of that same era (or perhaps Amiga OS?). Who doesn't want a six-screen virtual desktop tool or a CPU usage graph built right into the taskbar?

It's hard to overemphasise how dated eComStation feels. We're not even sure on-screen fonts are anti-aliased, for example. A concession to the modern times is the Firefox web browser, which is the extended support release (ESR) version 10 that's pretty ancient now but still offers basic HTML5 support. A lack of web fonts like Arial and Tahoma makes browsing a little strange, but it can be done, and while there's no Adobe Flash support, this is less of an issue than it used to be. Some HTML5-based video playback is possible, and YouTube should therefore be a possibility, but it choked on the old version of Firefox.

eComStation also involves a pretty solid DOS platform (and an authentic one, thanks to Microsoft's input back in the day). Despite eComStation's bravado in attempting to remain relevant to modern users, it's blindly obvious that its purpose is to act as a roll of virtual duct tape for systems that shouldn't exist any longer. For the rest of us eComStation is an interesting curio, and it should be remembered that the subscription fee includes tech support to get it up and running. You really can use it on your desktop PC, if you're that way inclined.

Haiku

Talking of history lessons, BeOS was the little engine that could – and then didn't. Developed from the ground up in the 1990s as a multimedia operating system, it also introduced user interface design concepts that meant it was genuinely easy to use – compared to alternatives at the time, at least. Most importantly, audio and video playback and manipulation was blazingly fast in an era when watching a 352x240 resolution music video from the Windows 95 installation CD made us feel sci-fi.

The fact that BeOS was not sold to Apple in 1999, as many expected, heralded the Steve Jobs era when he sold them his NextSTEP operating system instead. Deflated like a leaky balloon, BeOS would be sold off to Palm (remember them?) and within a few years had a headstone in the crowded operating system graveyard.

Fans of BeOS weren't about to let it go, however, and Haiku (**www.haiku-os.org**) is an attempt to recreate the magic. In an age when even your gran's crappy mobile can play 1080p video, Haiku has dropped the multimedia boasts and instead focuses on "targeting

Haiku is brave enough to continue BeOS's innovative user interface that relies on right-clicking to bring up app menus

VLC Media Player support in Haiku pushes it beyond a mere curiosity and makes it a real prospect for an alternative desktop OS

personal computing" via a "fast, efficient, simple to use, easy to learn, and yet very powerful system."

Once again this is a complete ground-up recreation of an older operating system rather than a skinned version of Linux/Unix. That said, Haiku is itself open source, and the folks behind it aren't afraid to judiciously borrow here and there – the network drivers come via FreeBSD, for example, which means Haiku should support the majority of wi-fi hardware. Compared even to Windows, that's an extraordinary boast. Some components even come from the original BeOS, which was partially open-sourced before pallbearers arrived.

Using Haiku is almost identical to using BeOS back in the day, and it retains the characteristic yellow 'stacked' menubar system that was a precursor to modern tabbed interfaces. Right-clicking on the desktop shows a menu by which apps can be accessed, alongside configuration options, and open windows are minimised to the Deskbar at the top of the desktop. A full and very readable user guide is provided by which you can learn tricks and terminology that can make Haiku very productive.

New software can be installed via the HaikuDepot package manager, based on the same principle as most Linux package managers. We simply couldn't find this on the myriad app menus provided by Haiku, however, but we did find its website catalogue (**depot.haiku-os.org**) and it shows a healthy list of apps such as VLC Media Player, BeZilla (a Firefox derivative), MailNews (a Thunderbird derivative) and Caya (an IM app). The only tool missing is an office suite, although the Haiku developers point out ThinkFree Office (**www.thinkfree.com**) works fine because it runs on top of Java, which Haiku supports. You could also use any online office suite, of course, thanks to BeZilla being HTML5-compatible.

Of all the alternative OSs reviewed here, Haiku is perhaps the best contender for everyday desktop use, thanks to the HaikuDepot apps and broad wi-fi support. Don't expect it to be optimised for modern hardware (the Nvidia graphics driver doesn't even support 2D acceleration, never mind 3D or modern compositing techniques), and Adobe Flash support is again missing. However, Haiku's a competent effort that despite its alpha testing status was stable and speedy during our time with it.

Syllable

Syllable (**web.syllable.org**) is something of a Heinz 57 operating system. It grew from the ashes of AtheOS, which was apparently abandoned because its creator wanted to learn how to fly (in an airplane, not by jumping off buildings). Begun in 1994, AtheOS had been an attempt to build on the Amiga OS legacy, although it would end up borrowing a little from BeOS for its file system and program interfaces, and pursuing a path independent of both Amiga OS and BeOS in any case (and not being binary compatible with either to boot, meaning you couldn't run Amiga or BeOS software).

AtheOS raised eyebrows for what at the time were technical triumphs such as support for symmetric multiprocessing, pre-emptive multitasking and multithreading. Some anticipated AtheOS one day providing a third man to the duelling partnership of Windows and Linux.

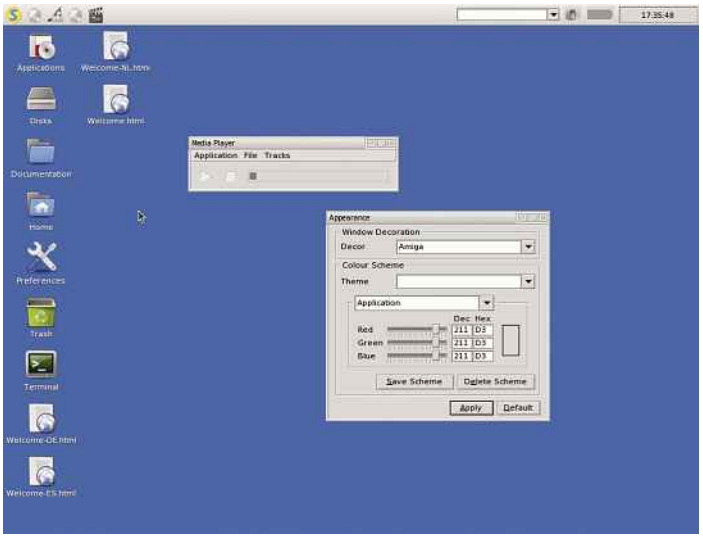
Because time and technology have since moved on, the folks behind Syllable no longer make such boasts and instead talk of it being an easy-to-use operating system for the common man. Booting Syllable shows a desktop styled a little like Amiga OS of old, but borrowing much from the classic Windows XP-style taskbar and Start button arrangement – except here the taskbar is at the top of the screen by default. Desktop icons should be familiar from most Linux users because they're borrowed from the popular Tango set.

A handful of core apps are provided out of the box, including a WebKit-based browser, basic email client and media player. Support for typical video formats is provided by FFMPEG inclusion, as you might find in Linux or Unix, and graphical configuration tools are provided for most system requirements.

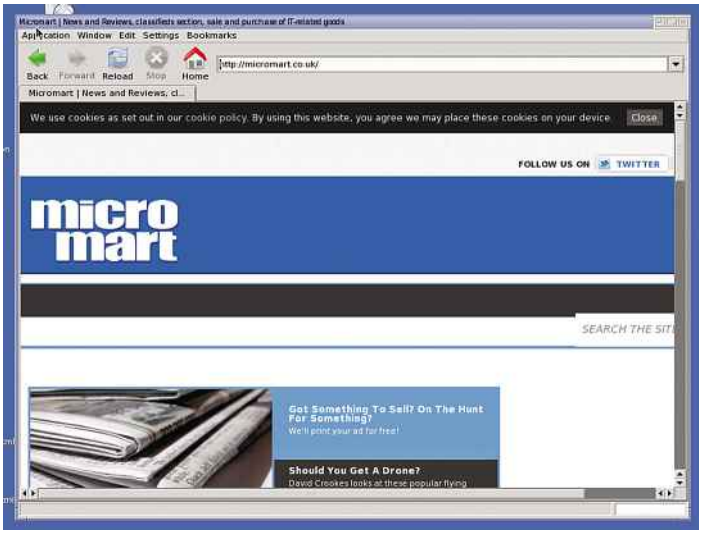
What you get, then, is a capable operating system for basic everyday tasks if you're a truly undemanding user. What you don't get, sadly, is the ability to add your own choice of apps. There simply aren't any beyond those preinstalled. Because of this there's not been any need to create the likes of a package manager. Also missing is support for wireless networking, and although we tested Syllable inside a virtual machine, we'd guess that hardware driver support for other PC components is basic at best.

What struck us most about Syllable is that it looks and feels like a Linux desktop such as Xfce. And if that's the case, then you might as well just use a Linux distro and get a wider range of hardware support to boot, as well as a bigger range of software. At least Haiku, mentioned above, is distinct and unusual in its look and feel, as well as its aims.

None of this should diminish the achievement that is Syllable in its current state. It's just that it lacks anything to make it genuinely appealing or to make it stand out from the crowd. **mm**



Syllable benefits from Amiga OS inspirations, as well as bits of BeOS, but mostly it looks and feels like a basic Linux desktop



Like all the operating systems included in this feature Syllable includes a basic web browser that's based on the evergreen WebKit engine

The world's greatest computer viruses

Keir Thomas takes a look at some of the dirtiest tricks employed by virus writers

> *"Viruses are pieces of software with a unique twist – they're designed to recreate themselves. They're designed to survive and even thrive"*

They say that if a nuclear bomb was dropped tomorrow, the only creatures to survive would be cockroaches. The future of the Earth's ecosystem would be invested in those horrid little blighters that scuttle under the cooker when you flip the kitchen light on.

In a similar way, one suspects that if the world's computers simultaneously combusted and we had to start again, the very first user booting the very first computer would be hit by a virus.

Viruses are pieces of software with a unique twist – they're designed to recreate themselves. They're designed to survive and even thrive. They hide away within computer systems and in the majority of cases the user isn't even aware they're there.

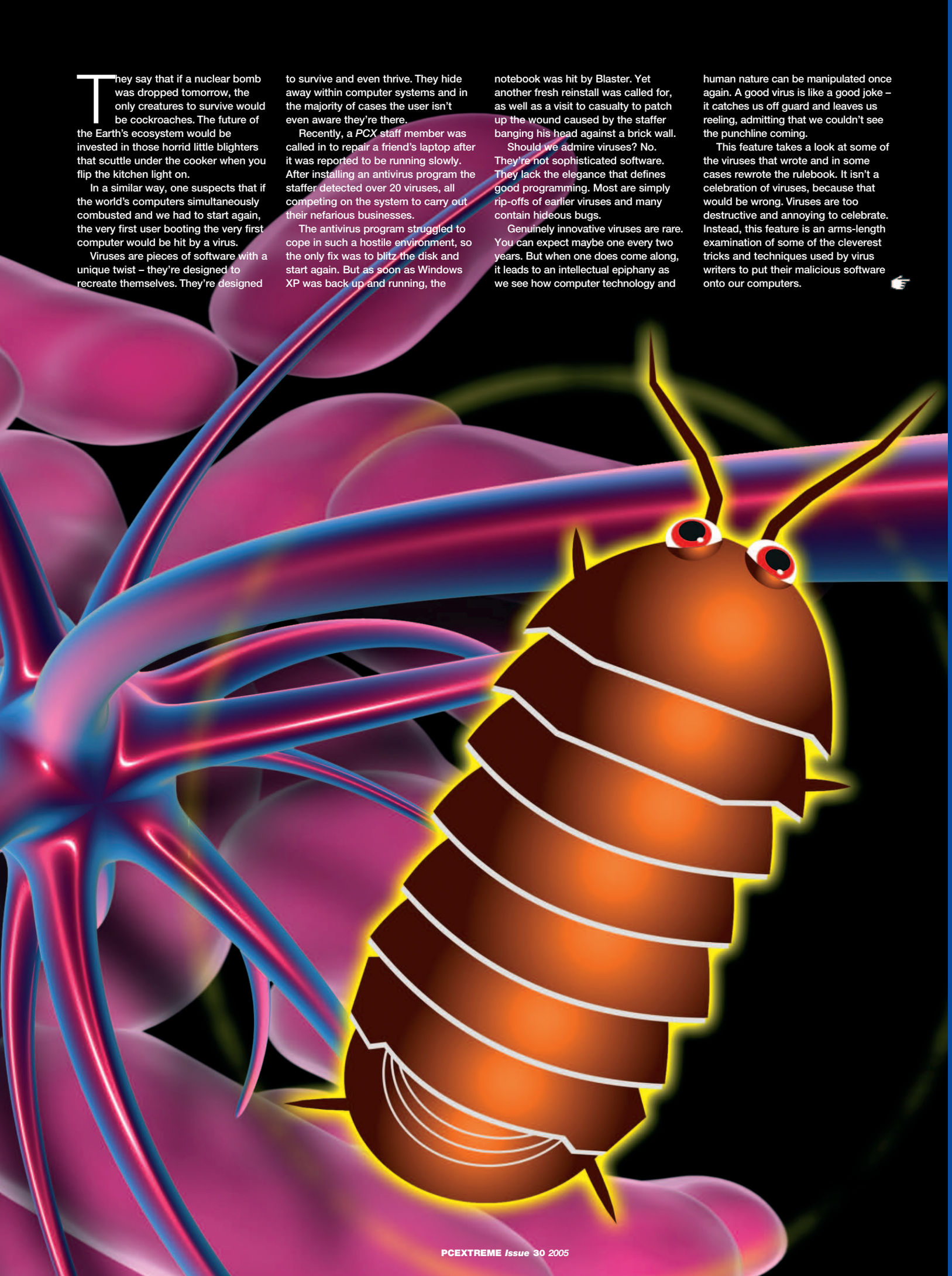
Recently, a *PCX* staff member was called in to repair a friend's laptop after it was reported to be running slowly. After installing an antivirus program the staffer detected over 20 viruses, all competing on the system to carry out their nefarious businesses.

The antivirus program struggled to cope in such a hostile environment, so the only fix was to blitz the disk and start again. But as soon as Windows XP was back up and running, the notebook was hit by Blaster. Yet another fresh reinstall was called for, as well as a visit to casualty to patch up the wound caused by the staffer banging his head against a brick wall.

Should we admire viruses? No. They're not sophisticated software. They lack the elegance that defines good programming. Most are simply rip-offs of earlier viruses and many contain hideous bugs.

Genuinely innovative viruses are rare. You can expect maybe one every two years. But when one does come along, it leads to an intellectual epiphany as we see how computer technology and human nature can be manipulated once again. A good virus is like a good joke – it catches us off guard and leaves us reeling, admitting that we couldn't see the punchline coming.

This feature takes a look at some of the viruses that wrote and in some cases rewrote the rulebook. It isn't a celebration of viruses, because that would be wrong. Viruses are too destructive and annoying to celebrate. Instead, this feature is an arms-length examination of some of the cleverest tricks and techniques used by virus writers to put their malicious software onto our computers.



Virus creation toolkits

If you've taken a peek at our Rogue's Gallery section, you'll have noticed that a lot of virus writers – known in the Net underworld as VXers – are usually both male and teenagers. Often their computing knowledge is pretty limited, leading to many bugs in the viruses they create. Their level of ability can be so low that many VXers aren't actually able to create a virus from scratch, and instead they'll use toolkits designed for the purpose.

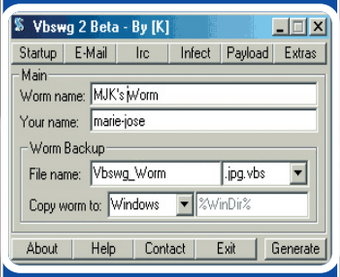
Virus creation kits have been around since the early days of the PC and 16-bit home micros. The Smeg Virus Construction Kit on the Amiga and the Virus Construction Lab on the PC are just two examples.

But perhaps the most famous toolkit is the VBSWormGenerator, created by the hacker [K]aLaMar. This is what Jan de Wit used to create the Kournikova virus. After the virus tore through the world's email servers, causing major chaos, [K]aLaMar apparently pulled the program from his website under pressure from concerned friends.

But VBSWormGenerator is a drop in the ocean and experts believe there might be hundreds of similar kits freely available for download on the Internet.

NOTE: *PCX is bought by a diverse readership and some of you might be thinking about downloading and trying out such toolkits. Don't. We're serious. Just don't. They are genuinely dangerous pieces of software that can cause disruption and destruction even by accident. Playing with such programs is a little like cleaning a fully-primed flame-thrower with a blowtorch – there's a strong possibility you'll do much more than singe your eyebrows.*

If nothing else, delving into the Net underworld to uncover such software is also a first-rate way of having your computer hacked and/or compromised, even if you think you're smart enough to enact defences.



The VBSWormGenerator was used to create the Anna Kournikova virus

In the early days, viruses often had humorous and entertaining payloads – such as Fear, shown here

Worms and viruses

You might think you already understand what a virus is, but the chances are you don't know the half of it. There are many different kinds of viruses.

Like their biological counterparts, computer viruses are defined by the simple fact they covertly spread from one computer to another. To stop a virus spreading, the user needs to take special measures. This might mean killing it by erasing it from memory, or becoming immunised prior to infection by giving the computer knowledge of the virus (which is to say, installing an antivirus program that contains a profile of the virus within its definition file).

At their most basic, viruses are small computer programs. The programmers' main goal is to ensure that the program can propagate itself. If the program can't spread, it can't be called a virus.

In addition to the ability to spread, most viruses have what's described as a payload – a chunk of the program code given to some kind of undesirable action. This might be as simple as displaying a message, or it could be something as drastic as wiping the hard disk. Often payloads are constructed around humorous or ironic premises – files are deleted only at certain times, for example, or upon certain user actions. There are even computer viruses designed to spread political propaganda.

Nowadays, antivirus experts prefer the term 'malware' to describe viruses as well as a host of other unwanted software that covertly installs itself on a system. But traditionally there were three different categories of unwanted software: viruses, worms and Trojans. The distinctions between the three are blurry.

Viruses usually attach themselves to other programs or documents on the system and rely upon the popularity of that program or document to spread. If the program is executed (or the file accessed), so is the virus, which is to say the virus is activated and looks for other files to infect.

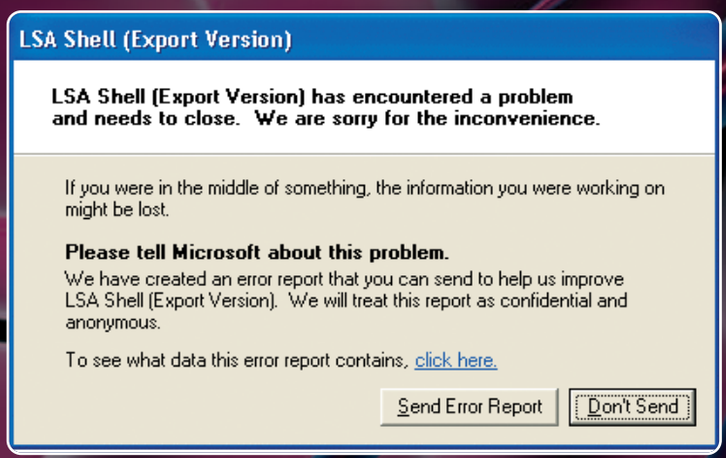
Viruses can spread using any means possible. In the early days they spread via floppy disks, but more recently Microsoft Office documents have also been used to spread viruses – when the document is opened, macro code is run automatically that causes the virus to spread. Nowadays, email is the preferred vehicle for spreading viruses.

Worms tend to target an entire operating system and, although they usually rely on pieces of software that are running in the background, don't aim to infect any particular file. They are independent programs that install themselves on a system.

Worms normally aim to spread across network connections (including the Internet as well as smaller affairs such as LANs), leaping from computer to computer. Worms sometimes – though not always – consume the entire resources of the host computer in order to spread.

Trojan Horses aren't designed to propagate themselves but instead usually rely upon humans to spread them. This is done via social engineering tricks.

At its most basic, a Trojan is simply a malicious program disguised as something else. You might download a program from the Internet that claims to be a piece of shareware, for example, but is actually designed to give hackers



Viruses like Sasser and Blaster drove users mad by infecting computers via Internet connections

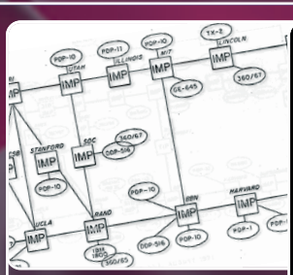
Rogue's gallery

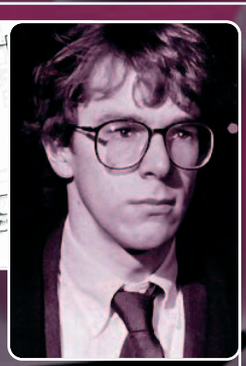
Law enforcement agencies have had moderate success in catching and prosecuting virus writers, though their task isn't an easy one – computers are particularly good at allowing people to become anonymous.

Any breakthroughs usually come about because the author boasts about his/her achievements in Internet chat rooms. Sometimes the author posts the source code for the virus on a newsgroup so that others can see and adapt it. Occasionally they're stupid enough to leave significant clues in the code itself, or even their email address.

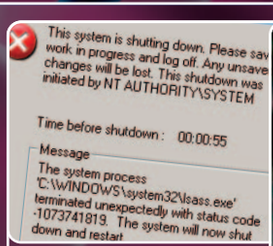
It's usually postings online that let the police track down the author. Authorities then subpoena the records of the ISPs concerned and track the IP address to a geographical location.

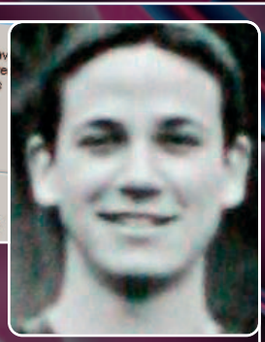
Here are the authors of some notorious viruses (including worms and Trojans), as well as the sentences they received – if any – after they were tried.



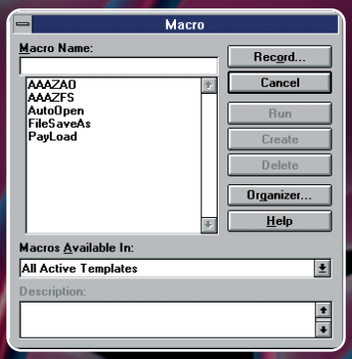


Virus: Morris Worm
Author: Robert Morris
Location: USA
Occupaton: Student
Details: Back in 1988, Morris single-handledly brought the Internet to a standstill by unleashing a buggy worm onto the network. It infected DEC VAX systems.
Sentence: Despite sneakily launching the worm from a university other than his own, Morris was fingered and received three years' probation plus 400 hours' community service. In addition, he had to pay a fine of US$10,050.





Virus: Sasser
Author: Sven Jaschan
Location: Germany
Occupation: Student
Details: Hailing from Waffensen in Germany, Jaschan created both the Sasser worm and the NetSky worm in 2004. Jaschen was turned in by his schoolmates, who went on to collect a chunk of the US$250,000 reward offered by Microsoft.
Sentence: Because he was 17 when he wrote and propagated Sasser, Jaschen escaped a prison sentence. After pleading guilty, he ended up with 21 months' probation and community service.



The Concept virus infected Word documents with a handful of macro scripts

backdoor access to your system. Alternatively you might be emailed a file that claims to be a naked picture of a tennis star but in fact is a piece of code designed to wipe your hard disk. More often than not, Trojans are the payloads of viruses or worms.

Nowadays, Trojans are most associated with remote-access programs designed to provide backdoor access into systems, and give hackers the ability to either control the system or plunder it of personal information (such as online banking passwords and details). To say somebody is infected with a Trojan is to imply that their system has been compromised by a hacker.

Worm in the Apple

As the home micro revolution came about in the 1980s, it didn't take people long to realise that the metaphor of human viruses could very easily be applied to computing. In an edition of *Scientific American* from March 1985, Roberto Cerruti and Marco Morocutti proposed the concept of small programs propagating themselves across floppies. They envisioned this happening on the premier home computer of the era, the Apple II.

The concept was simple. The program would fit onto the boot sector of Apple's Disk Operating System and thereby be loaded into memory whenever a floppy disk was inserted into the computer. Then, when a different disk was inserted, the program would write itself to that disk's boot sector too. Claiming not to be malicious, Cerruti and Morocutti stated that their theoretical virus would wipe itself after 16 infections had taken place, thus limiting the rate of infection.

Alarmed by the clear destructive potential of what they had dreamed up, Cerruti and Morocutti didn't actually create such a virus. They even agreed not to discuss their idea with others, though writing into *Scientific American* meant they immediately broke their own agreement.

But they needn't have worried. In the same edition of the magazine, a virus created by teenager Richard Skrenta Jr was described. Created as a joke (as with the Morris Worm, mentioned later), Skrenta's virus was designed to subtly alter operating system files to introduce irritating bugs. But it clearly demonstrated the ability of viruses to spread uncontrollably. Soon Skrenta's virus had overrun his systems and those of his friends, and was making inroads into his high school computer systems. Eventually, Skrenta created his own antivirus program to kill off the virus.

What Skrenta didn't mention was that he'd also created Elk Cloner some years earlier. This was probably the very first computer virus and spread from floppy to floppy on the Apple II. It didn't have a malicious payload and was practically invisible, except for the fact that on the 50th boot after infection the virus would display a poem:

Elk Cloner:
The program with a personality

It will get on all your disks
It will infiltrate your chips
Yes it's Cloner!

It will stick to you like glue
It will modify RAM too
Send in the Cloner!

Cloner was actually a worm rather than a virus because it was a independent program that didn't attach itself to any other file. Part of the problem with Elk Cloner was that although it wasn't malicious, it had to be removed manually. Back then, there weren't any antivirus programs! The user had to use a disk-editing program to alter the contents of the boot sector.

Although annoying, it wasn't until 1988 that the full potential of worms to cause chaos was demonstrated. The Morris Worm, named after its author, Robert Morris Jr, spread like wildfire across the fledgling Internet. Morris was a student at Cornell University in the US and launched the worm from Massachusetts Institute of Technology in order to disguise its origins.

The worm was designed to exploit bugs in several programs on DEC computers running Unix. Like Skrenta's worm, it didn't carry a malicious payload – but it did have a bug that meant it executed multiple instances of itself, chewing up both memory and bandwidth. The Internet was slowed to a standstill.

The Morris Worm demonstrated the work required to clear up after a virus. The US government put the cost of the clean-up effort at up to US$100 million. Morris was convicted under the Computer Fraud and Abuse Act and given three years' probation, plus fines.

But it's not all bad. The Morris Worm lead to the setting up of the Computer Emergency Response Team (CERT), an organisation designed to monitor and report on threats to the Internet. This is still around today and acts as an early-warning system when trouble is brewing.

Nor did Morris find his life or career blighted by his escapades. Nowadays, he's an associate professor at the Massachusetts Institute of Technology (in a further ironic twist, it should be noted that Morris is also the son of the one-time Chief Scientist at the US National Computer Security Center).

Richard Skrenta has also gone onto great things and is now the CEO of Topix.net, a company that produces news aggregator software.

Shooting blanks

There were a few more notable floppy-based viruses in the late 80s and early 90s, including Brain, probably the first virus to infect IBM PCs. Brain apparently started life in 1986 as an advert for a Pakistani computer shop. The creators of the virus had a brainwave – the virus would contain a message suggesting that the infected user comes to their shop:

On your mobile

The next big thing in the world of viruses is mobile phones – or so say many experts, despite the fact there have been almost no examples so far.

Computer viruses need a handful of prerequisites in order to be effective. For starters, they have to have an operating system to operate within. Viruses are little more than pieces of software, so they need a system to run on. Then they need some kind of organised file system in which to hide themselves. This should be semi-permanent, otherwise the virus would die out too quickly. Finally, they need some way of moving from one system to another.

At the present time, mobile phones are deficient in many of these regards. They contain operating systems but lack any kind of coherent file system. Prerequisite number three, of providing a means to spread, is also missing on many phones. Theoretically viruses could spread via the phone network, though it's hard to imagine how this could work in an efficient manner.

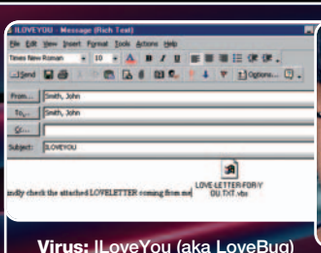
But the very latest 'smart' phones provide an excellent means of virus propagation. Usually they're based around a computer-like operating system, complete with a browsable and permanent file system. Examples of smart phone OSes include Symbian OS or Microsoft's Pocket PC OS (yes, Microsoft, that bastion of security – starting to be worried yet?). These phones really are miniature computers that happen to have phone functionality tacked on.

Bluetooth looks like the best means of virus propagation. Although theoretically secure, Bluetooth was compromised several times over 2003/4. Often the particular implementation of Bluetooth on various phones was to blame, but there exists a flaw in the PIN system of the current generation of Bluetooth phones.

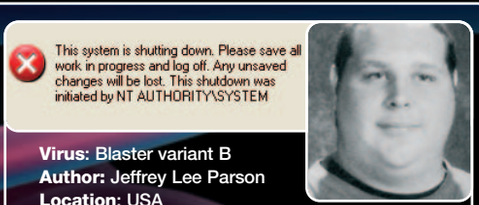
Anybody using an infected Bluetooth phone could theoretically infect anybody else within a 30-metre radius. It's possible that an infected user could walk into a café and instantly infect anybody else there, for example.

Bluetooth is useful for sharing data between phones, but might also allow mobile phone viruses to spread

Virus: Melissa
Author: David L Smith
Location: USA
Occupation: Computer programmer
Details: A resident of New Jersey in the US, Smith named the Melissa virus after his favourite nightclub stripper. He was traced via a posting of the virus he made to the alt.sex newsgroup. The virus started spreading in 1999.
Sentence: Originally facing up to 40 years after pleading guilty, Smith spent 20 months in jail after it was revealed he was helping the FBI track down other virus authors. He was also handed a US$5,000 fine.



Virus: ILoveYou (aka LoveBug)
Author (alleged): Onel de Guzman
Location: Philippines
Occupation: Student
Details: Manila resident de Guzman admitted he might have accidentally released the mass-mailing virus while playing around on a computer in 2000. But he denied writing it.
Sentence: Although arrested and interrogated, de Guzman walked free after it was found there wasn't a law that covered his alleged crime in the Philippines (there is now). His flatmate Reomel Lamores was implicated as well but also walked free.



Virus: Blaster variant B
Author: Jeffrey Lee Parson
Location: USA
Occupation: High school student
Details: Minneapolis resident Parson wasn't charged with creating the original Blaster worm, for which the author remains at large. Instead Parson was charged with modifying Blaster – creating one of many variations – then releasing it in 2003. He was caught because the virus created a file called 'teekids.exe'. Parson's online handle at the time was 'teekid'.
Sentence: Parson was sentenced to 18 months in prison plus 100 hours' community service. In addition he was ordered to pay a US$500,000 fine to Microsoft (shurely shome mishtake?). Microsoft let him off in return for an additional 225 hours of community service.

Norton was one of the first companies to produce an antivirus product, which ran under DO

Avoiding viruses

Put simply, the best way to avoid viruses is to stop using Windows. Microsoft's product is undoubtedly the most virus-prone computer operating system that has ever existed – thousands of new viruses are released every month that target it. In fact, when we talk of viruses, we're implying the involvement of Windows because other computer platforms and operating systems simply don't have such problems.

Why is this? There are perhaps a number of reasons. The first is that Windows is set up by default so that all users have administrator powers. Even the most basic user can wipe or modify vital system files. This means that the task facing a virus – of penetrating a computer system – is made easy.

Secondly, Windows has had some pretty appalling security holes. The two most annoying viruses of recent times, Blaster and Sasser, infect any computer that's on the Internet by connecting to port 445 and causing a buffer overflow. Some viruses took advantage of a bug in Outlook Express that meant simply viewing an email was enough to become infected!

Thirdly, and most damningly, Windows is ubiquitous. Everybody uses it. Virus writers want notoriety and there's little point in writing a virus for an unknown computer platform.

Fourthly, nobody likes Microsoft. The company has been accused of various dirty tricks and this has turned much of the computing underworld against it. Many virus writers see their virus-creating actions as justifiable punishment for Microsoft.

Avoiding viruses is therefore a matter of finding a way around these four clauses. The solution many choose is Linux. By default it sets up limited user accounts, making virus propagation much more difficult. And while it doesn't necessarily have fewer bugs than any rival Microsoft product, it's less popular than Windows – virus writers simply don't target it. Additionally, in the eyes of many virus writers, Linux is cool and therefore approved of, unlike Microsoft.

But Linux is arcane and complicated, and in recent times many users have switched to the Apple Mac and OS X, its operating system. OS X is rather like Linux on steroids – it's built on a secure Unix base and, more importantly, there are practically no viruses targeting it. Perhaps most crucially, it's not as popular as Windows – so there's little if any reason for publicity-seeking virus writers to target it.

Security through obscurity – switching to the Apple Mac means you won't be hit by viruses

(c) 1986 Basit & Amjad (pvt) Ltd.
BRAIN COMPUTER SERVICES
LAHORE-PAKISTAN
Beware of this VIRUS....
Contact us for vaccination

All viruses need a method of travelling from computer to computer, and any home computers that relied upon floppies became viable targets, including the popular Atari ST and Commodore Amiga computers.

More dangerous than actual viruses at the time was the hysteria over viruses. Hoaxes were commonplace and the newspapers had a field day inspiring panic in the users of what were then newfangled devices.

During this period, viruses also began to become more malicious in terms of their payloads. On IBM PCs, viruses started to wipe the first tracks and sectors on a hard disk, destroying vital file information. Recovery, though possible, was difficult and involved. Usually it was simpler to wipe the hard disk and start afresh.

In 1990 the first antivirus programs hit the market, and included titles such as Norton and McAfee. As the 90s rolled on, floppies fell out of use as hard disks became more and more common. Virus writers needed a better method to spread their work and turned to Microsoft Office files to spread viruses. As the most popular component, Microsoft Word was the obvious vehicle for virus propagation.

Here the viruses were coded using Microsoft Visual Basic for Applications (VBA), a macro language included within the Microsoft Office suite. This gave the viruses their title: macro viruses.

The trick was to hide the code within the template document that's loaded every time Microsoft Word starts. Once in memory, the code then writes itself to any document that's opened or created. Once *that* document is then opened on a different machine, the template file on that computer is also infected.

At the time, VBA was trusted enough to have access to the entire hard disk file system, so the viruses had free run of the system. Files could be deleted or modified, and often were.

The first macro virus was Concept. Because antivirus programs were oblivious to the threat, it also became one of the most popular. Concept had no payload. In fact, although there's a component of the virus named 'payload', it contains a harmless remark:

Sub MAIN
REM That's enough to prove my point
End Sub

This is how the virus got its name – it was designed to show the potential for macro viruses and the concepts behind them, but not to cause damage. It allowed the antivirus companies to be turned onto the threat before somebody with more malicious interests discovered the potential.

Despite the good intentions of the author, variations of Concept appeared that performed tasks such as password protecting random documents. In fact, in the late 90s and beyond, macro viruses would become by far the most popular type of virus around. When mixed with the then all-new Internet, they became practically unstoppable.

Oh Melissa!

The Melissa virus used an explosive combination of macro virus, email and social engineering to further the virus writer's cause. It became one of the fastest spreading viruses ever, and even Microsoft had to switch off its email system to stop the virus spreading.

Melissa was blissfully simple. It arrived on a computer via an email, seemingly from a friend. The message body contained the message:

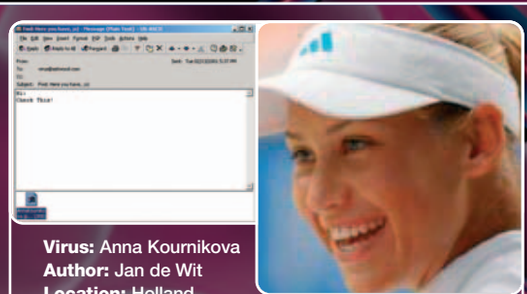
Here is that document you asked for ... don't show anyone else ;-)

Attached to the email was a Word document. Believing that the email had come from a friend or colleague, most people then opened the document. This activated the macro virus, causing it to plunder the user's email address book and email itself to all that person's friends, colleagues and even loose acquaintances. The virus simply picked Word documents at random from the user's hard disk and emailed them out, attaching the virus code.

The virus had a payload of sorts but it wasn't destructive – whenever the minutes past the hour of the system clock matched the date of the month, the virus would add the following text

DEC VAX systems were infected with the Morris Worm in 1988, thus proving how dangerous viruses could be

Virus: CIH (aka Chernobyl)
Author: Cheng Ing-Hau
Location: Taiwan
Occupation: Soldier
Details: It's not clear how Sergeant Ing-Hau was caught, but the fact he named the virus after his own initials – CIH – might have provided a big clue. CIH was one of the nastiest and most prolific viruses of all time, wiping countless hard disks and causing massive disruption back in 1997/8. Variations of it are still around nowadays.
Sentence: Ing-Hau was arrested but never charged because, as strange as it sounds, no Taiwanese company was prepared to admit it had been hit by his virus. So Sgt Ing-Hau walked free.



Virus: Anna Kournikova
Author: Jan de Wit
Location: Holland
Occupation: Sales assistant
Details: Described as a "collector of viruses", de Wit created the Kournikova virus using a simple virus-creation toolkit in 2001. He was so shocked at the impact that he handed himself into his local police station. (The picture above is, of course, of Ms Kournikova. We couldn't find one of de Wit.)
Sentence: During his trial, de Wit was offered the option of 150 hours' community service or 75 days in prison. He took the community service. The court also confiscated his virus collection, which filled a CD-ROM.

Elk Cloner was one of the first viruses and spread using Apple II floppies

into any Word document being worked on at the time:

Twenty-two points, plus triple-word-score, plus fifty points for using all my letters. Game's over. I'm outta here

This is a quote from an episode of *The Simpsons*.

As was common within the virus-writing world, variations of Melissa appeared that were more destructive. Some deleted vital system files. Most altered the message that appeared to the end user, meaning that people who had been educated to immediately delete messages containing the text above were still being caught out.

Variations of macro viruses were made easy because the source code was always open to inspection. Additionally, VBA was based on BASIC and this meant that even schoolchildren were able to understand and adapt the code. Prior to this, viruses had been written in traditional programming languages such as C, then compiled before being released. Although virus writers often shared the source code via the Internet, it was impossible to significantly adapt an already-compiled virus without a high skill level.

The I Love You virus, also known as VBS/loveletter, followed a year later. It adopted the same social technique of spreading via the user's email address book, this time spicing up proceedings by claiming to be a love letter. The message of the body stated:

kindly check the attached LOVELETTER coming from me

Attached to the file was LOVE-LETTER-FOR-YOU.TXT.VBS. Note the use of dual file extensions. The theory was that most people would only read the .txt part of the filename and assume that the attachment was a simple text file (though it's open to debate how many users know what a .txt file is).

The file was designed to be run by a little-known Windows component called the Windows Scripting Host (WSH). In a typical fashion for a Microsoft operating system, WSH was designed to run arbitrary code at the whim of the user and had system-wide access.

I Love You had a significant payload in the form of a Trojan that attempted to steal the users' passwords. These were then emailed to *mailme@super.net.ph*. In addition, I Love You went to painstaking lengths to infect the user's machines. MP3s and pictures were deleted then replaced with dummy files containing the virus code. The virus added itself to the registry so that it booted with Windows, and wrote itself several times to the Windows subsystem directories.

I Love You was followed by a great many variations, not only viruses based on the original code but others using similar techniques. The Anna Kournikova virus pretended to be a picture of the tennis star and used a similar dual-filename approach, for example.

The macro virus SirCam added a twist whereby it would also spread by non-passworded network shares. It simply connected to shared folders on other computers and secreted a innocent-looking file. The user would then stumble across the file and run it in order to find out what it was.

SirCam's code contained a number of messages that *should* have appeared in the message body. But a bug meant that only one appeared. Anybody using email at the time became extremely familiar with it:

I send you this file in order to have your advice

Next generation

Once the world had recovered from the flood of macro and email viruses, the buffer overflow invasion began. These are worms that exploit security holes within the default install of Microsoft operating systems. Perhaps the most famous was Code Red, which infected Web servers running Microsoft's Internet Information Server (IIS) software. This didn't impact desktop users directly but brought the Internet to a standstill and took many websites offline.

Like all viruses, Code Red was very simple in its execution. It worked by connecting to a port on machines running IIS and causing a buffer overflow, which is to say the software was overloaded with data in a bid to take control.

Then the virus checked to see if it was running on a machine set to US English. If so, the website's homepage was changed to display the message:

HELLO! Welcome to http://www.worm.com! Hacked By Chinese!

> *"Unfortunately, as with many viruses, there appeared to be a bug in the code. It meant the random addresses weren't actually very random"*

Unless wiped off by the system administrator, this message stayed on the infected computer's homepage for 10 hours, after which it disappeared. By that point, the virus would have pinged millions of random IP addresses in order to find other machines to infect. Once each machine was infected, it too would search for other machines to infect. The sheer bandwidth consumed increased logarithmically, causing problems for Internet hardware such as routers.

Unfortunately, as with many viruses, there appeared to be a bug in the code. It meant the random addresses weren't actually very random. The result of this was that certain machines were attacked on a regular basis. A user might clean the machine of the virus, only to find it infected seconds later.

The virus had one additional trick up its sleeve. If the date was beyond the 20th of the month, it would launch a flood of data against the webserver located at the **www.whitehouse.gov** address. Bearing in mind that all the infected machines undertook this action, the virus's effective payload was a DoS (Denial of Service) attack against the Whitehouse webserver.

Code Red was followed by Slammer, which gained notoriety as being the fastest-spreading worm ever. It managed to infect 75,000 computers in just 10 minutes and became the first example of a 'Warhol' worm, as theorised by computer scientist Nicholas C Weaver (ie it was famous for five minutes). Slammer took advantage of a buffer overrun security hole in Microsoft's SQL server.

Blaster was the first worm to affect ordinary Windows users and exploited a hole in the Windows Remote Procedure Call (RPC) component. Once Blaster had infected a computer, it would then generate random IP addresses and attempt to infect the computers using them.

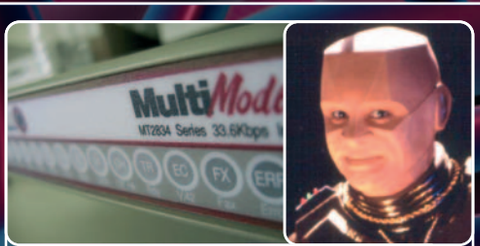
Blaster's payload was to attack Microsoft's Windows Update servers on 15 August 2003. To avoid the threat, Microsoft deactivated the relevant servers during that period.

Blaster's code contained a few messages, including the following:

billy gates why do you make this possible ? Stop making money and fix your software!!

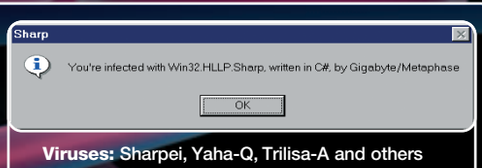
Cynical readers might endorse that statement. Because of Blaster and the Sasser worm that followed, an unprotected Windows XP machine is now compromised within 12 minutes of going online. This makes installing Windows XP very difficult.

In the case of worms that attack home-user Windows machines, most users are unaware they're infected. It's likely they'll notice that their machine slows down and their Internet bandwidth is reduced as the worm bites, but this is considered standard fare under Microsoft operating systems. For this reason, Blaster and Sasser remain very potent threats even now.



Viruses: Pathogen, Queeg and Smeg
Author: Christopher Pile
Location: UK
Occupation: Unemployed
Details: Under the pseudonym Black Barron, Pile was traced on the back of his phone line, which in 1995 he used to illegally access various computer systems and upload his *Red Dwarf*-inspired viruses.
Sentence: One of the first people to be convicted of virus authorship anywhere in the world, Pile ended up with a one-and-a-half-year sentence.

Viruses: Gokar, Redesi and Admirer
Author: Simon Vallor
Location: UK
Occupation: Website designer
Details: It's not clear how Vallor was tracked down, but somehow the FBI came across his exploits in 2002 and tipped off Scotland Yard. Vallor's viruses aren't well known, though they infected 27,000 computers around the world.
Sentence: Although the two years in prison Vallor received sounds weak, it is in fact one of the strongest sentences ever handed down for virus creation. Vallor also had his computer equipment seized.



Viruses: Sharpei, Yaha-Q, Trilisa-A and others
Author (alleged): Kim Vanvaeck
Location: Belgium
Occupation: Student
Details: Kim Vanvaeck allegedly created clever viruses involving simple games, as well as the first virus ever to infect Microsoft's .Net technology. Which isn't bad considering she's a girl! Her female charms have made her something of a heroine in the virus-writing underworld, with hormonally challenged boys crying out for photos of her (we couldn't find one either).
Sentence: Although arrested in 2004, Vanvaeck is still awaiting her day in court. She has claimed she never propagated viruses but merely sent them to antivirus companies to increase her notoriety.

www.pc-utilities.co.uk

PC Utilities

Broadband Revolution

Get the most from your high-speed connection with our in-depth guide and essential software

PARAGON DRIVE BACKUP

FULL VERSION as sold for £30

883 TOP PROGRAMS!

Including 271 Windows tools, 201 Internet apps, 68 email essentials, 62 graphic greats, 68 audio and video aids —plus 44 essentials that will save you bags of money!

1.3Gb

INCLUDING Essential broadband toolkit!

More than 50 incredible broadband tools

Dr Fix It
ON THE CD – complete fix it toolkit, plus guide in the mag

Summer fun
FREE holiday software to keep kids (and parents) happy

How to
- Create eyecatching 3D text
- Mail merge in MS Word
- Build a PC family tree
- Upgrade to USB 2.0
- Switch to Linux

Expert advice
11 pages of problems solved

www.livepublishing.co.uk
ISSUE 37
£4.99
LIVE
9 771469 042009
37

Welcome!

Summer's here at last – and it's about time! The days are long and the holidays are looming, but that's no good reason to go turning your back on your PC pal. There's a lot of fun to be had even when the sun shines and we're back with a bumper bundle of just such goodies, enforced by masses more technical support and knowledge to keep the dark days far, far away.

That's why this month we're featuring Summertime Fun, a unique feature packed full of super FREE leisure and educational software that will keep you and your kids entertained and save you from a lolly meltdown!

You'll have already seen from the cover that this month's lead feature is an in-depth probe into the broadband revolution now sweeping Britain and the world. You might have got broadband (or be planning to) but do you have the must-have toolkit of programs to get the most from it?

> "...There's a staggering double-disc bonanza that gives you over 880 top programs"

Our third feature is a bit less jolly but no less necessary. In Dr Fix It, the PCU medical officer will call round to dispense some vital PC pills, from his little brown bag. We're tried to put together our very own Symantec SystemWorks wannabe – there are some cures for current woes, and a lot of preventative medicines too.

There's also a superb 11 pages of readers' problems solved, covering everything from PCs that won't boot to finding you the program of your dreams. We've got the lot, as usual.

Add to this eclectic mix our monthly foray into can-do tutorials, in the form of How tos and Mini manuals, and you'll see we're really buzzing with advice once more. Then there's the news, and the reviews...

There's so much in the mag that we almost forgot the staggering double-disc bonanza that gives you a thousand and one top programs, including the great FULL program, Paragon Drive Backup. This really is a great little package that set the PCU office alight when we used it. It will backup your entire hard drive or individual partitions and can even be used to create bootable CDs.

Enjoy the magazine.

Keir Thomas
Editor
keir.thomas@livepublishing.co.uk

Our promise

- **Not everybody wants to pay lots of money for software** and our coverdisc reflects that. Each month we present a selection of the finest free programs available, with a selection of the best shareware. **We discuss the best of the best** of this selection within our coverdisc review pages, and present a catalogue of every single utility on the disc afterwards in our listings pages.
- **Your PC is not just for business** so we also promise to provide the best projects for you to undertake, whether this is to increase your knowledge or simply provide fun and entertaining ways to use your PC. **Wherever possible we provide all the programs you need on our coverdisc**. We also respond to your requests so if there's something you'd like to know about, just **let us know**.
- **No PC is without problems** so each month we will try and **answer as many of your technical queries** as we can fit into our Professional Help pages. No question is too complex and no subject too trivial.

That's our promise to you. If you have any comments, please contact us by emailing **letters@pc-utilities.co.uk** or writing to PC Utilities magazine, Live Publishing International Limited, Europa House, Adlington Park, Macclesfield, Cheshire, SK10 4NP.

Get in touch

Letters for publication
letters@pc-utilities.co.uk
Coverdisc submissions
coverdisc@pc-utilities.co.uk
Technical help
professionalhelp@pc-utilities.co.uk
Coverdisc problems
techsupport@livepublishing.co.uk
Subscriptions
iain.anderson@livepublishing.co.uk
01625 850565
Web site www.pc-utilities.co.uk
Postal address Live Publishing International Limited, Europa House, Adlington Park, Macclesfield, Cheshire, SK10 4NP
Phone 01625 855086
Fax 01625 855071

Editorial
Editor Keir Thomas
Deputy Editor Jim Oldfield
Reviews Editor Aaron Birch
Staff Writers David Nield, Dave Mycroft
CD compilation Iain Warde
Contributors
Roland Waddilove

Production and administration
Design Advanced Design
Subscriptions and Marketing Manager Iain Anderson
01625 850565,
iain.anderson@livepublishing.co.uk
Production Controller Debbie Whitham
Financial Controller Karen Battrick
Editorial Director Wayne Williams
Publisher Robin Wilkinson

Advertising and licensing
Sales Executive Kenny Leslie
01625 855113
kenny.leslie@livepublishing.co.uk

Subscribe
12 issue subscription
UK: £59.88
Europe: £73
Rest of world: £91

Distribution Comag - 01895 444055
Printed by Polestar Chantry
ISSN 1469-042x

Broadband revolution

The broadband revolution has started, so take to the streets with our selection of cool utilities

The next stage in the evolution of the Internet is here and it goes by the name of broadband. You get the same email and Web access as old-fashioned dial-up Internet connections. It's just that broadband is fast. Very fast. At least 10 times faster than a standard dial-up modem, in fact, and often much more when real world figures are taken into account.

This increased speed allows you to do a great many things, including watching online media, chatting to family and friends via your webcam, or just downloading files much more quickly than you could previously.

You can get a broadband connection in a number of ways. The principal method in the UK is via Asymmetrical Digital Subscriber Line (ADSL). This is a complicated way of saying that the Net is provided via your phone line, which is converted at the telephone exchange into a high-speed Net connection (although the user doesn't notice this – you still get telephone and fax calls, and you don't lose your phone number)

The second way to get broadband connectivity is by means of cable TV. This works only in areas that have digital cable TV services, but functions in a similar way to ADSL Net connections – the Net signal is combined with the existing TV and phone data travelling through the cables and wires.

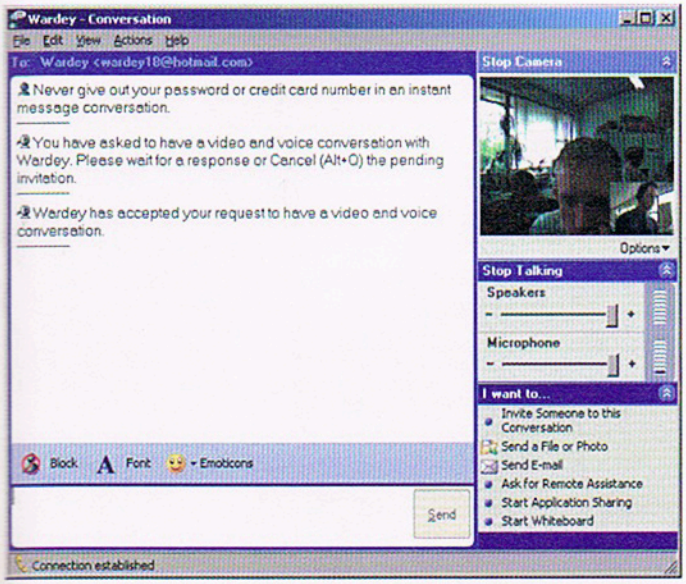
The trouble is that both methods are limited to certain areas, with built-up urban areas being particularly well served. If you live in rural areas then you'll most likely find yourself high and dry, although this will change slowly over time.

There is another option which can serve more remote areas – satellite broadband. Older versions of this technology were clumsy – a standard modem had to be used for the uplink, and, bizarrely, an MPEG video card used for downlink. Nowadays a small transceiver is used, which both receives and sends data. This is attached to the side of your house or office and pointed in the direction of the satellite during installation (for more information about services in the UK, see **www.btopenworld.com/satellite**).

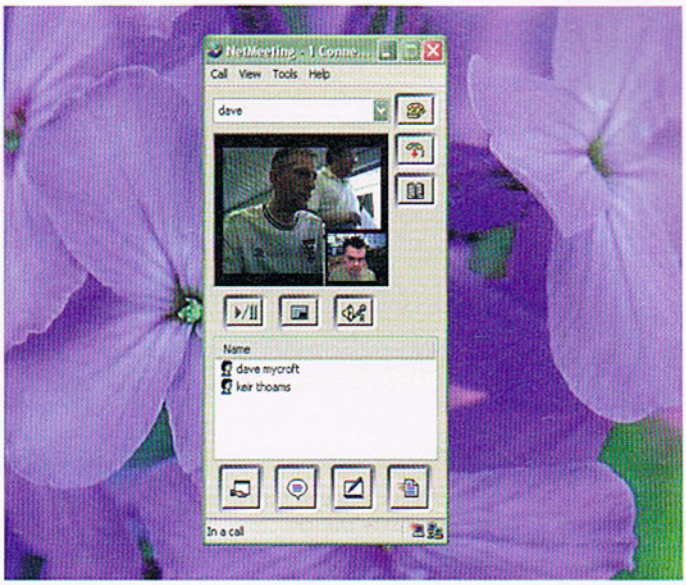
There's even a fourth way to send and receive broadband, which sounds strange but apparently works – via power lines. In the UK this is still in testing stage and, at the time of writing, details are scant. It appears a modem-like device is plugged into one of your household electrical sockets, from which Internet data is received. For more details on this service, which is being offered in many countries, visit **www.plca.net**.

But what if you've already got your shiny-new high-speed connection? You'll want to know what you can do with it, and this feature is for you. We outline software you can use to get the most from the Net and also detail important security measures you should take to ensure you're safe whilst online.

Keir Thomas



Chances are that your favourite instant messenger program supports video and voice communications, so no download is necessary!



NetMeeting is built into most versions of Windows and offers a quick way to video and audio conference with another person

Communication

Broadband offers speeds so fast that digitally communicating with another by voice or even video becomes a reality. Aside from the obvious benefits of ever more personal communication, this cuts down on the cost of phone calls, particularly to overseas locations. But the best news is that all the popular instant messaging programs usually incorporate video and/or audio communication facilities.

It's worth bearing in mind that a very good video and audio conferencing program is built into most versions of Windows from 98 upwards. NetMeeting is being downplayed by Microsoft in Windows XP, but it's still present – simply browse to \Program Files\ NetMeeting, and run 'conf.exe'. Users of older Windows operating systems should find a link to NetMeeting in their Start menu.

Although NetMeeting is primarily a business product, it works great for home users although it's primarily designed to use the Microsoft Directory, a huge listing of online users. If you prefer more privacy you can also use the program to talk directly to another PC by simply typing in their IP address (to find this in Windows 9x/Me, click Start/ Run and type 'winipcfg'; in Windows XP, click Start/ Run, type 'command', and then type 'ipconfig').

NetMeeting has some cool features, such as the ability to setup a virtual whiteboard on which you and your co-respondent can draw pictures together, but a dedicated video conferencing package like PalTalk (**www.paltalk.com**) offers much more. Alongside video, audio and text chat (or a combination of all three), you can chat to several other people at the same time. You can even meet new people online although, as you might expect, this is one area where you should be careful, considering the high quantity of weirdos out there online!

Yahoo! Messenger also involves a Webcam component which lets you communicate via video although, as with all these instant messaging programs, you first need to sign-up online for a username. The same is true of MSN Messenger, which requires a Hotmail passport, but which also allows video and voice communication along with text.

Making PC to PC video calls is all well and good, but if you want to phone an actual landline connected to an actual telephone, you'll need other software. Such programs are usually free but in order to get a phone number you'll have a pay a subscription fee (or a one-off charge). Calls are

Videoconferencing – does it work?

As discussed in the main feature, a broadband connection brings the possibility of videoconferencing – communicating with another person or group of people via a webcam so that you can see as well as talk to them.

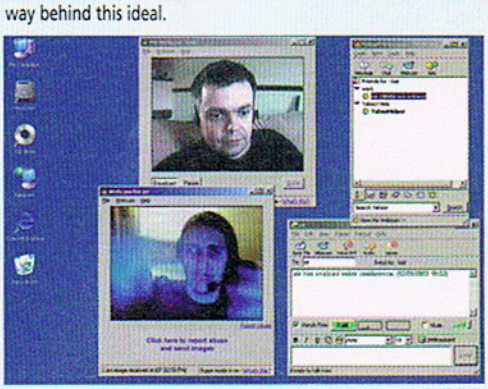
This sounds very promising for those with relatives abroad but the truth can be rather lacklustre. To demonstrate this, we set up a test connection between a 512Kbps ADSL connection and a similar speed cable modem connection. We used Yahoo Messenger's webcam and audio communication facilities.

For starters, the video is choppy – rather than having a fluid 25 frames per second, as with TV, it's more a case of five frames per second (at the maximum 320x240 resolution, although shrinking the picture size didn't really improve the frame rate in our test). This means that lips aren't synched with the words coming out of them, and if somebody moves quickly then a blur is left in their place.

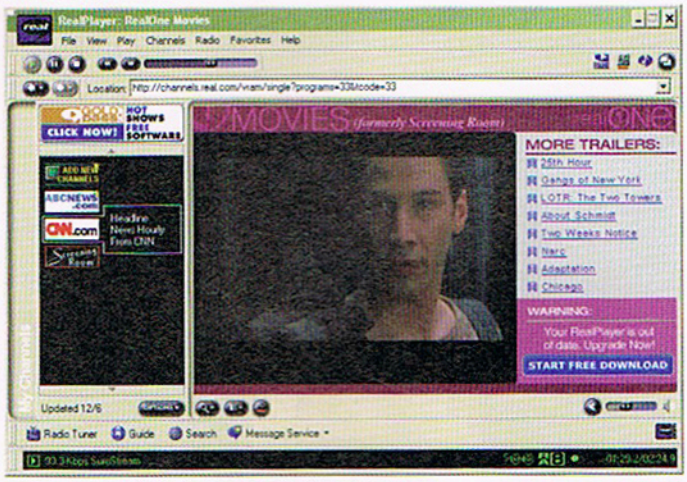
The picture quality was quite good, however, and we took advantage of Messenger's Super Webcam feature which leads to more detail and less 'jpegification', whereby the picture looks muddy and indistinct.

The audio was only half duplex, meaning that only one person could speak at once – if you spoke, you cut the other person off. Coupled with the slight delay of Internet communications, this meant chatting to the other person took some getting used to. But it wasn't impossible, and other videoconferencing programs (like Microsoft NetMeeting, built into Windows) offer telephone-like full duplex voice communications, which should eradicate this problem.

Video communication isn't impossible, or even difficult. It just requires practice and you definitely shouldn't expect instant communications as in the movies – current technology is still a little way behind this ideal.



You can see the person you're talking to with videoconferencing, but the technology is by no means perfect



Click around within RealPlayer and you'll find lots of online content available for free, such as movie trailers

also usually charged per minute. Ideally you should find a service for your country, although PC-to-phone services are usually used to make overseas phone calls – it's cheaper to use a standard landline phone to make calls within your own country.

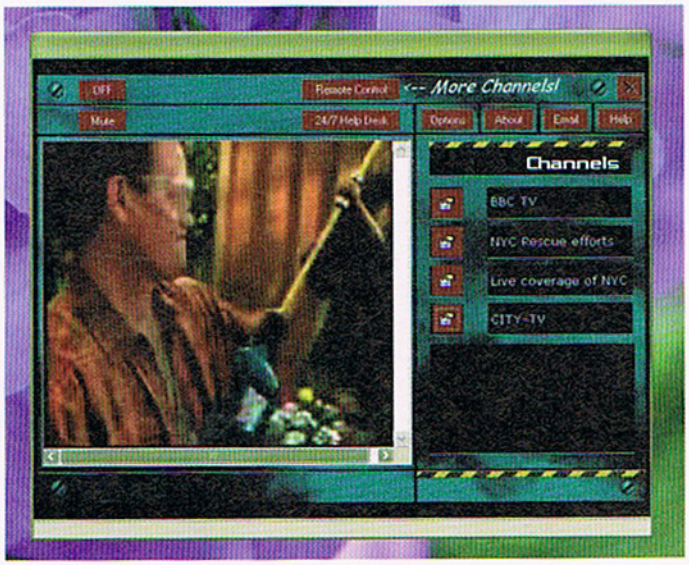
For UK users, pc2call (**www.pc2call.com**) is worth taking a look at, although, as mentioned, most US-based services will accept any user regardless of location, provided they have a fast enough Internet connection and a credit card by which to pay for their calls. go2call is a similar service which those interested should investigate but at the end of the day it's worth shopping around to get the best price per minute value. A site like **www.geocities.com/Athens/Agora/4229/free_international_telephone.html** helps you compare providers side by side.

The programs usually work in two ways – via a website applet, or via a downloadable program which you keep on your desktop. In both instances you're presented with a numeric keypad into which you should enter the phone number of the landline you want to call (including international prefixes).

If you have a fast connection, you can call landline phone numbers to speak to non-Net equipped individuals, but you have to pay per minute

Multimedia

If you believe the hype, broadband was introduced for only one reason – to bring multimedia to the masses. It has been implied that an ADSL connection is reason enough to throw your TV and hi-fi in the bin. Regardless of what the ad-men say, it's true that a faster connection means you can watch high-quality video and listen to CD-quality audio but, once again, it's probably the case that you'll have some of the software you need already installed. You just have to make much better use of it. Take RealPlayer as one example (or RealOne as it's called in the latest incarnation). Whilst on dial-up you ignored those irritating 'click me!' adverts offering movie previews, TV shows, and radio stations, now you can click on them with impunity – no longer will you have to deal with a blurry postage stamp-sized window when watching video. Now you can watch full-screen video complete with stereo audio (just about!).



The Television promises to redefine the Internet by making available high quality online TV stations

The same is true of Apple's QuickTime Player, or Windows Media Player – just click around when the program starts and you'll unlock a world of free online multimedia content.

There are some dedicated programs which help you tune into online TV stations, which are rare but growing in number. One example is The Television (**www.evbcn.com**) which grandly proclaims itself "the single biggest breakthrough in the Internet since the creation of the Internet browser". The reality at the moment is far from this – as we write, the service is down for repairs with only one or two channels available. However, the program promises a lot and is well worth checking out when it goes back

Possible Net speeds

Technology	Download speed	Notes
Mobile phone	9,600bps	Connect a mobile phone to your PC and get online... slowly. Turn graphics off and basic Web browsing is possible.
Modem (V.34)	28,800bps - 33,600bps	Modem speed just about capable of browsing the Web without too much waiting around.
Modem (V.90)	56,000bps	Rethink of old technology to squeeze out more speed, involving new PCM technology.
ISDN (single line)	64,000bps	Turn your phone line into a digital connection for a speedier Net. Needs special hardware and can be expensive.
ISDN (double line)	128,000bps	Double-speed ISDN, simply by using two phone lines.
ADSL	(256,000bps – 2Mbps)	UK's most popular way of getting broadband – turns phone line into digital Net connection. Maximum speed depends on how much you pay and your distance from telephone exchange.
Cable	(150,000bps – 1Mbps)	If you have cable TV in your area, consider getting broadband via a cable modem. Often cheaper than ADSL.
T1	544Mbps	If you have the cash (and it's VERY expensive), plug yourself directly into the Net with a T1 fibre-optic connection.
OC192	9.6Gbps	Thinking about running your own ISP? OC192 is capable of transmitting 9,600,000,000 bits per second – more than enough to download the odd .mp3.

How broadband works

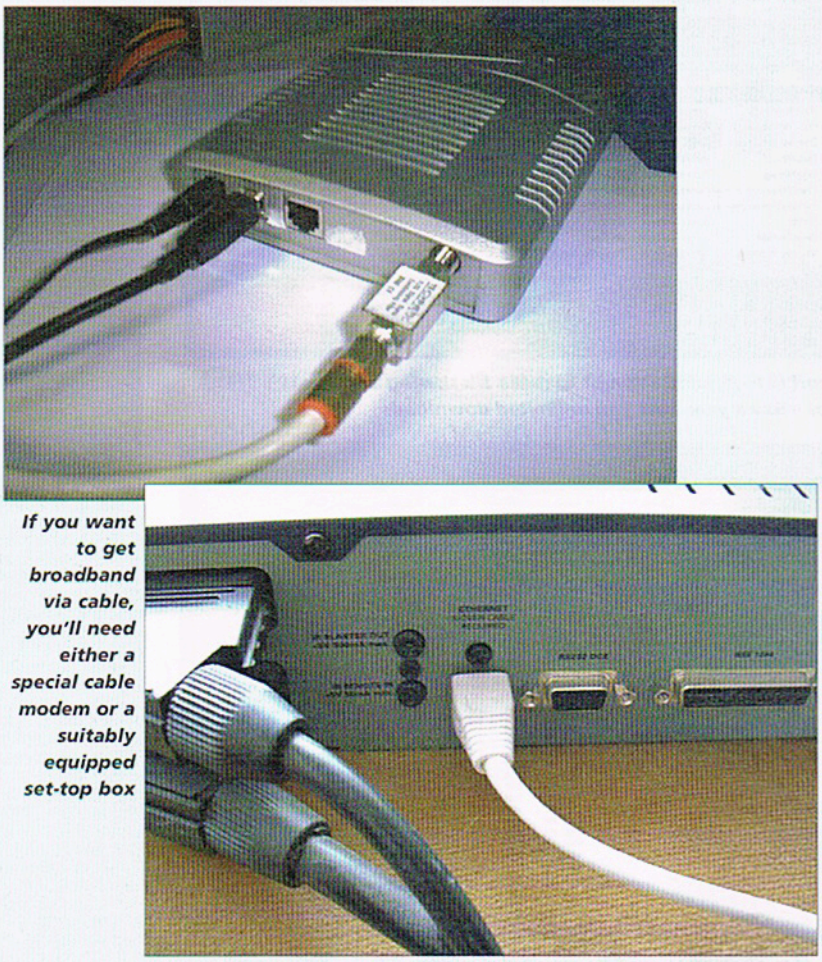
It might come as a surprise to many but, despite the technological strides claimed by broadband service providers, the technical details behind high-speed Net connections are very similar to those of a dial-up modem.

ADSL takes advantage of higher quality phone lines. Better manufacturing means the copper wires that handle voice calls (the wires that come from the poles to your house, and underground to the exchange) are, in fact, capable of carrying higher frequency ranges in addition to voice calls. This means that the broadband Internet signal can occupy these higher frequencies which are largely inaudible on standard voice calls, although a 'microfilter' is needed to clear-up any crossover interference.

To use ADSL, the local phone exchange must be converted to the technology. As well as allowing you to go online with your ADSL modem, the BT engineers also have to connect the exchange to a large 'backroom' collection of computers which actually provide the Internet connection.

Even if your exchange is converted, getting ADSL isn't always possible – it only works reliably over certain distances (measured between your home and your local phone exchange). With rate adaptive ADSL, the standard used in the UK, this can't exceed 5.5Km.

Cable modems work in a slightly different way. These take advantage of a cable company's ability to transmit Internet data across the same cables used to provide TV and phone services. The modems still modulate and demodulate data for part of the distance but vastly different technology is used beyond this, and the Internet signal is 'piggy backed' onto the TV signal. Your Internet data is also sent to each local cable modem, like in Ethernet networks – it's just that your modem has the permission to accept the data.



If you want to get broadband via cable, you'll need either a special cable modem or a suitably equipped set-top box

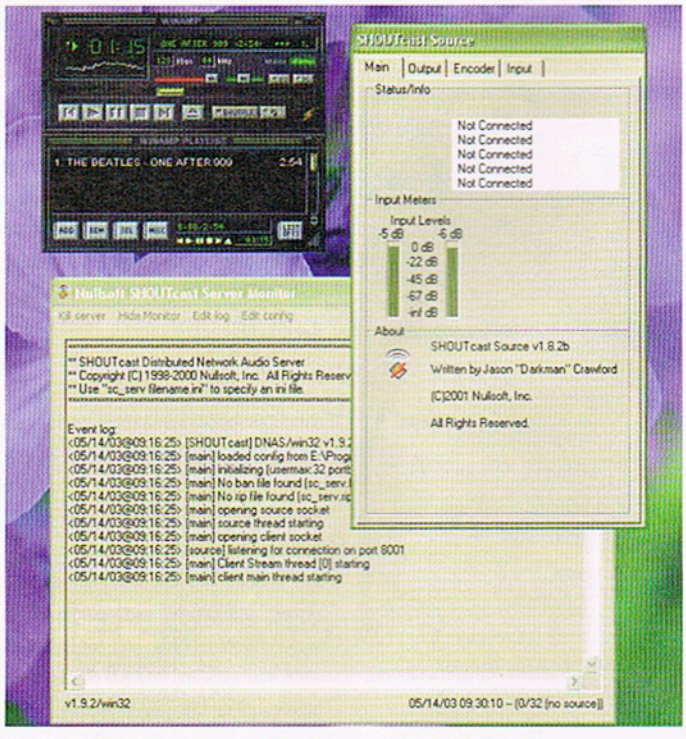
online later this year. It appears to organise online TV channels and video content, making finding what you need an easy process.

The best way to find high-quality video content, however, is to visit websites and see what they have to offer. Most news sites, like BBC News (**http://news.bbc.co.uk**) or Sky News (**www.sky.com/skynews/home**) offer video news reports, for example, making it possible to construct your very own news bulletin.

Whilst it's not yet fair to say that a broadband-equipped PC can replace your TV set – few full TV shows are available to view online – many sites offer clips of shows, or trailers. Explore the site of US-based ABC TV (**www.abc.com**), for example, and you'll find highlights of most shows available to watch online. The same is true of the UK site dedicated to Channel 4 (**www.channel4.com**). To track down more Web-based TV content, visit **http://witv.com/portal.htm**, which lists what's available, on a country by country basis.

Whilst watching TV online is still in its infancy, listening to the radio online is a completely different matter. Not only can you listen to many established stations by visiting their homepages, but you can also listen to new digital-only stations. There's

> It's the single biggest breakthrough in the Internet since the creation of the browser



Turn yourself in a virtual DJ by broadcasting your .mp3 collection to the world with the SHOUTcast server

Install multiple operating systems on your Mac

Installing multiple versions of OS X allows you to test software and also run earlier editions. What's more, setting it up is easy

Difficulty: Beginner **Time needed:** 45 minutes

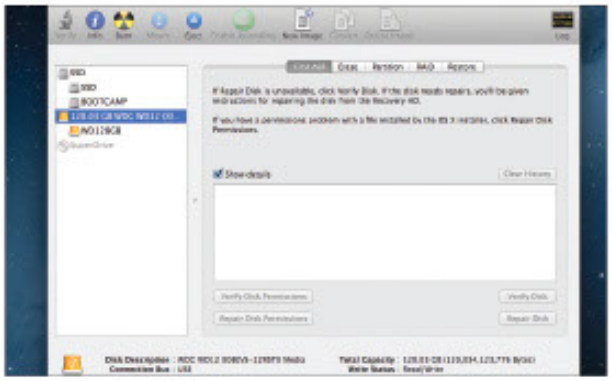
Macs are able to boot from just about anything – from the disk inside the computer to removable storage attached by USB, FireWire or Thunderbolt. This provides a lot of freedom for those who want to install multiple versions of OS X, perhaps for testing purposes or simply to boot into so that others can use your Mac without fear of damaging the primary setup.

Installing OS X on an external drive is straightforward, but the disk must be prepared in the correct way. Installing a second version of OS X on a Mac's internal disk requires repartitioning, which again is straightforward although carries with it the very slight risk of data loss, so be sure to back up your data first.

In the steps below, we first look at installing OS X Mountain Lion on an external drive, then at installing a second instance on your Mac's hard disk. We then look at how to install the older OS X Lion alongside OS X Mountain Lion.

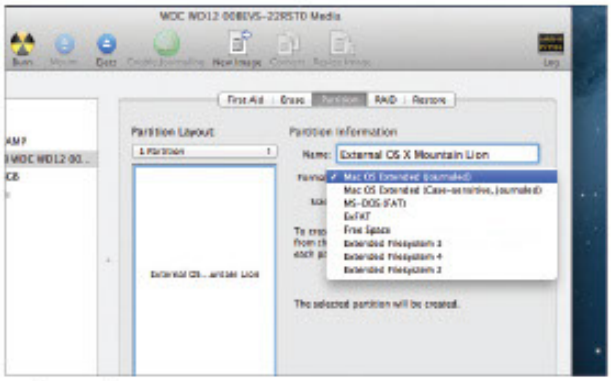
"Macs are able to boot from anything"

Disk Utility | **Install multiple operating systems**



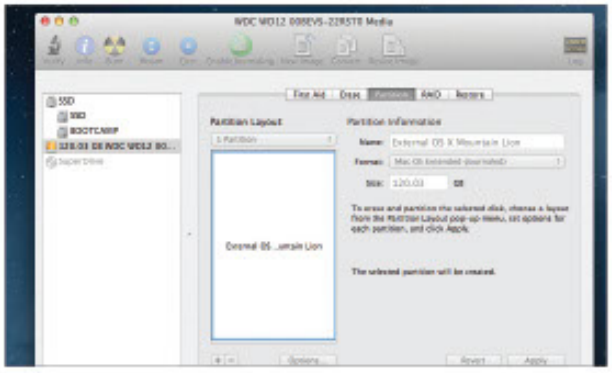
1: Attach the disk

Attach the storage and then open Disk Utility, which you'll find in the Utilities folder of the Applications list. Select the disk's entry on the left – it'll be coloured orange and identified by the USB, FireWire or Thunderbolt symbol.



2: Set up the partition

Click the Partition tab and, in the Partition Layout drop-down, select 1 Partition. Under the Format drop-down list, select Mac OS X Extended (Journaled). Type a name, then click Options and ensure GUID Partition Table is selected.

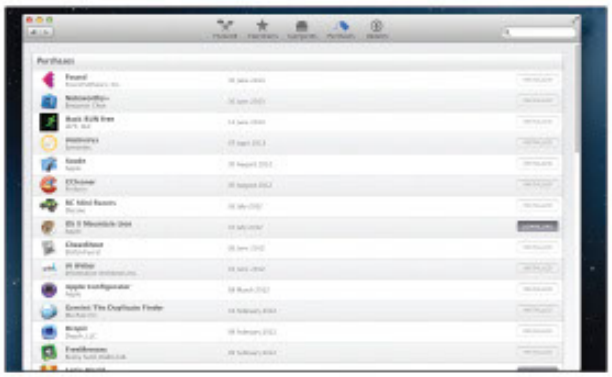


3: Repartition the disk

Click Apply and then the Partition button in the dialog box that appears. Repartitioning will then take place and you should find it completes very quickly. Once it's finished, you can close Disk Utility.

4: Find the installer

To install OS X Mountain Lion, you'll need the installer package. If you already have this it'll be listed in your Applications list as 'Install OS X Mountain Lion'. If not you'll need to download it again, as described next.



5: Download the installer

Open the App Store and click the Purchases tab. Scroll down until you find the entry for OS X Mountain Lion and click the Download button. If you intend to install the older OS X Lion later, download it too.

6: Start the installer

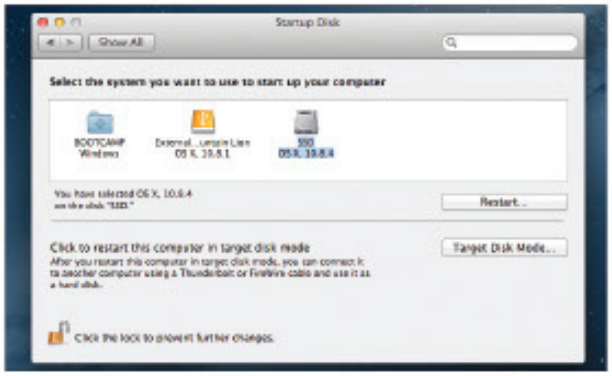
Once the download has finished (at over 4GB it may take some time), return to the Applications list and then double-click Install OS X Mountain Lion. Work through the first few installation steps, then click Show All Disks.

7: Select the disk

Select your newly prepared external hard disk. Save any open files and click Install, then type your login password when prompted. After copying across some files, your Mac will prompt you to reboot so installation can take place.

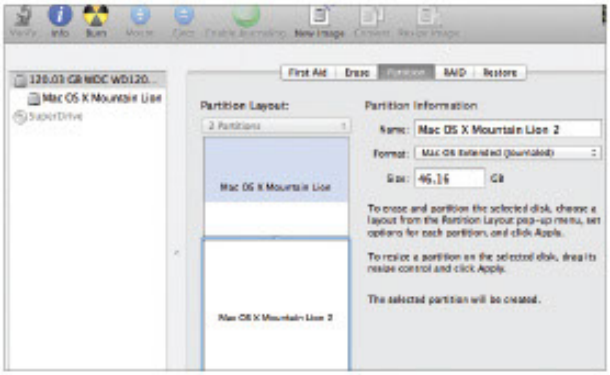
8: Boot options

Don't disturb your Mac until installation has finished! When it has finished, it will boot into your new installation every time. To boot into your original OS X installation, hold down Alt while booting and select the internal hard disk.



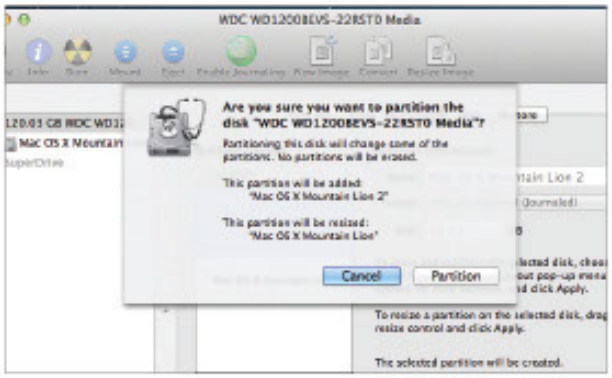
9: Permanent boot options

To make a permanent switch back to the operating system on your Mac's internal disk, open System Preferences, then click the Startup Disk option. In the list that appears, select your internal hard disk, then click Restart.



10: Split the partition

To create a new install of OS X alongside the one already on your Mac's internal hard disk, open Disk Utility and select the Partition tab. Click the small '+' button at the bottom left. This will split the existing partition.



11: Repartition

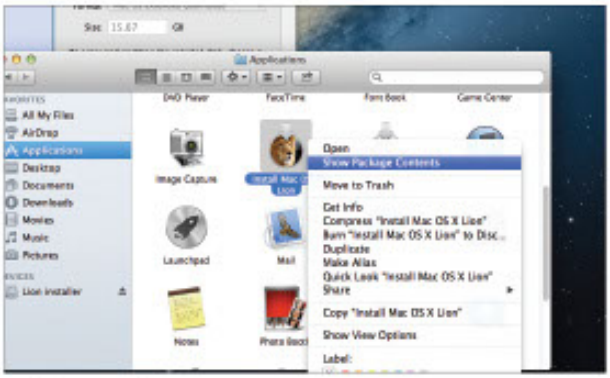
Drag the small handle between the two partitions to adjust their relative sizes. You can see the size of each by clicking them and looking at the Size field. Once you're happy, click the Apply button to start the repartitioning process.

12: Install OS X

Follow the earlier steps about installing OS X onto an external disk, but this time choose the new partition when the Installer runs. You can again choose between installations of OS X by holding down Alt when your Mac boots.

13: Install Lion

To install the older OS X Lion (10.7) you'll need to download its Installer (see step 5) and transfer its files to an 8GB or larger bootable USB stick or SD card. Once the Installer's downloaded, open Disk Utility.



14: Partition the storage

Select the USB stick or SD card from the left list, then follow steps 2 and 3 to partition and format it. Give it the name 'Lion Installer'. Then right-click the Lion installation package in Applications and select Show Package Contents.

Virtualised Mac

Running OS X in software

Using virtualisation

Using a virtualisation tool like VMware Fusion (www.vmware.com/fusion), you can install OS X in a 'software Mac', without external drives or repartitioning. Put simply, OS X will run in a window on the desktop

Booting to recovery

When installing OS X Mountain Lion or Lion in VMware Fusion, you'll boot to recovery mode. The partition is created automatically by Fusion, so all you need to do is click Reinstall to start the installation

Memory demands

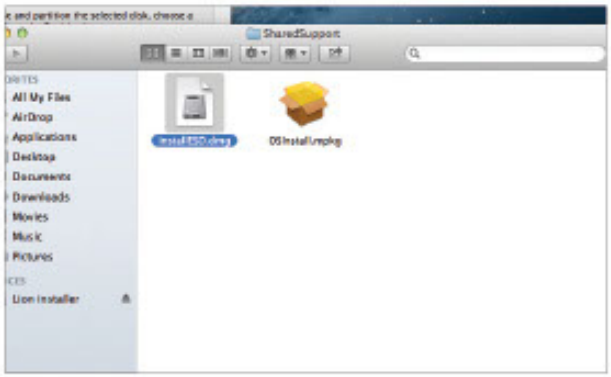
You'll need at least 4GB of RAM because the virtual machine demands 2GB. For best results, your Mac should have at least 8GB of RAM and you should give half to the virtual OS X installation

More than two

Why stop at only two operating systems? And you're not limited to just OS X either – with a little forward planning you could add Windows, Linux (see page 188) and other instances of OS X – although you'll need to use Boot Camp to add Windows first of all and leave space for the others when choosing a partition size.

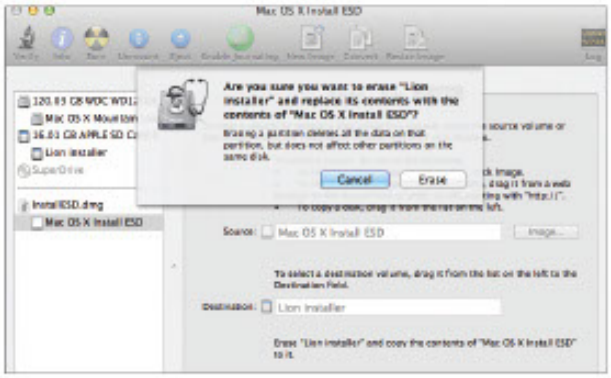
Installation source

During setup, when VMware Fusion asks for an installer disk, select the OS X installation package within Applications. Fusion will detect where the required installation files are, then boot into recovery mode



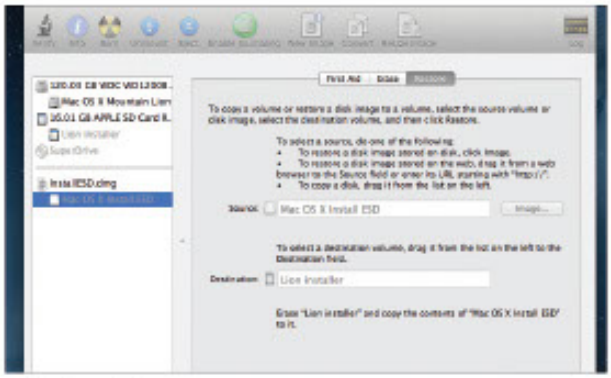
15: Open the image

Open the Contents folder, then SharedSupport, and drag the InstallESD.dmg file to the left-hand side of Disk Utility beneath the list of drives. Click it, then select Open on the toolbar.



16: Restore the image

Once it's finished, select Mac OS X Install ESD in the list on the left, then click the Restore tab. Drag and drop the entry that reads Lion Installer from the left to the Destination field, and click the Restore button.



17: Wait while writing

Click Erase when prompted, then wait while the stick/card is written to. Once it's finished, don't forget to create a new partition on the internal hard disk (steps 10 and 11), or attach an external disk for OS X Lion to be installed to.

18: Select Lion

Reboot your Mac and then hold down Alt before it boots. Select the orange Mac OS X option, then select Reinstall Mac OS X Lion from the recovery menu. Be sure to select your new partition or external hard disk when installing.

Light Bulb Moments

Which energy-saving bulb should you choose? Keir Thomas sheds a little light on the subject.

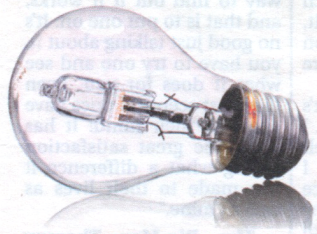
IT'S just four years since it finally became illegal for shops to sell the good old light bulb that had been around for 100 years. In reality, though, most of us made the jump to energy-saving "CFL" light bulbs over a decade ago.

Nothing stays still for long when it comes to technology, however, and you'll now find two additional types of energy-saving household light bulb on the shelves: LED and halogen.

You might be tempted to think these are automatically superior compared to the older CFL technology – but you'd be wrong.

Choose the wrong type of bulb and you could pay over the odds, or even end-up with sky-high bills – just like in the old days!

Halogen



Halogen bulbs cost around the same as CFL energy efficient bulbs but look an awful lot like the old-fashioned (and now banned) incandescent bulbs.

They're the same distinctive shape and they also get too hot to touch, unlike both CFL and LED light bulbs.

Now for the bad news: compared to other energy-efficient light bulb technologies, halogen light bulbs aren't actually very energy efficient. They also pop as quickly as old-fashioned light bulbs. In other words, they're actually quite expensive in the long term.

Switch your household to halogen bulbs and some estimates say you could be paying £10-£20 more on each bill.

The only real benefit of halogen light bulbs is that they can be used with a dimmer switch to vary their brightness, unlike other energy-efficient bulbs.

Some types of LED light bulbs can be dimmed but it depends on the type of dimmer switch you have and, well, it gets very complicated. In contrast, a halogen bulb will just work.

LED

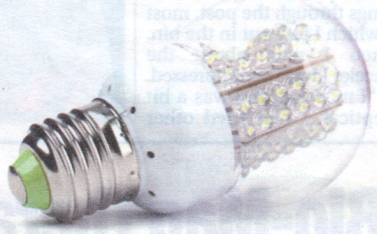
The higher asking-price of LED light bulbs – around £5 compared to perhaps £2 for the older-style CFL energy-efficient bulb – might make you think you're buying the luxury version of household lighting.

It's certainly true that a good LED bulb uses half the electricity of even a CFL energy-saving bulb.

However, CFL light bulbs don't cost a lot of money to use, and cutting the electricity used for lighting makes little appreciable difference to your bills.

LED bulbs last for years, and are pretty tough to boot – drop one and it probably won't smash, unlike pretty much every other kind of bulb.

In other words, the real reason to switch to LED light bulbs is to be even better for the environment. While this is very admirable, that high up-front cost can be hard to swallow.



Types of energy-efficient bulb

LED

LED (light-emitting diode) light bulbs look like old-fashioned bulbs but usually have a plastic cowling covering the bottom half of the bulb. They're usually bright and have a very white light compared to other energy efficient bulbs, unless you specifically choose the warm white versions.

CFL

Cheap and sold everywhere, CFL (compact fluorescent lamp) bulbs are identifiable via their twisty thin tubes, although some have straight tubes arranged into inverted U shapes. Increasingly, modern CFL bulbs hide the tubes within a traditional-looking outer light bulb-shaped glass case.

Halogen

Halogen bulbs look a lot like the old-fashioned incandescent light bulbs that are now banned, but look closely inside and you'll see a glass mantle that contains the filament. Unlike CFL or LED light bulbs, they get too hot to touch!

Technophobia

Is it a mistake to dismiss spelling and grammar checking tools out of hand? Keir Thomas looks at what's on offer

PROOFING TOOLS FREIND OR FOE?

Many creative writing teachers tell you to turn off proofing tools in your word-processing program – which includes spelling and grammar checkers. For some time I've wondered whether this advice is too hasty.

As you might expect, as an anti-Luddite I believe we should accept help from computers whenever possible, and be grateful we live in a time where such help is available. Therefore, this month I attempt to show how proofing tools can help any writer – provided the writer remains in control and watches out for caveats.

Bending the rules

First, a question: are proofing tools useful nowadays? Spell checking certainly is; even if your spelling is perfect you will still make typos that it can catch. But when it comes to grammar, a big difference compared to even a few decades ago is that rules are broken or bent out of shape on a daily basis.

For example, despite being arguably the pillar of English usage, the BBC refers to organisations such as sports teams as plural rather than the technically correct singular. Similarly, any boldly going *Star Trek* fan will tell you the split infinitive verb rule isn't as tight as it once was, while sentence clauses or even discrete sentences are increasingly separated by inelegant dashes or commas. And sentences are allowed to start with conjunctions, while prepositions can be used to end them with!

There are many more examples, so making your writing 'grammatically correct' can be as damning as getting it wrong. An inept editor might think your work contains elementary errors.

Perhaps the bottom line is that any computerised proofing tool is only as useful as your own knowledge of the requirements and rules – both formal and informal. Proofing tools are for checking your writing and should not dictate its content or style.

Spill chucking

Let's dig down into spell checking. Because most computer software originates in the USA, a common issue we Brits face is that the word processor's spell-checking dictionary defaults to the American English setting.

An amazing number of writers I know grumblingly work around this rather than fixing it. While most know to avoid errors such as *color*/*colour*, the American English dropping of double letters in many words such as *labeled*/*labelled* is not only less well known but also harder to spot on screen.

However, switching the default language for new documents is easy. In Microsoft Word, click the File ribbon, and then the Options menu entry at the left. In the dialogue box that appears, click the Language entry in the list at the left. If there's already an 'English (United Kingdom)' entry in the list, select it and then click Set As Default.

If there's no entry for UK English in the list, click the Add Additional Editing Languages dropdown list, find 'English (United Kingdom)' within it, then click the Add button alongside. Then follow the earlier steps to ensure it's set as the default.

To switch the language setting of an existing document, highlight all of it (Ctrl+A) and then click the 'English (United States)' entry on the status bar at the bottom. Then select 'English (United Kingdom)' from the dialogue box that appears.

In a questionable bid for cosmopolitanism a minority of word-processor dictionaries mix US and UK English, permitting the likes of *color* as well as *colour*. They're aiming to represent the woefully lax 'Internet English'. My advice if this malaise affects your software: switch to something better. It has its faults but Microsoft Word still can't be beat for most writers.

Ways of correction

Word-processor proofing tools typically work in three different ways. The first is called auto-correct, in which errors are instantly swapped out as soon as you type them, for what the word processor believes is correct.

The second method is where errors are underlined on-screen as you type, but not automatically corrected. Spelling errors or typos are underlined in red; grammar errors are underlined in either blue or green (although might also be underlined in red). Hovering the mouse cursor over the underlined word or phrase, or right-clicking it, will summon a pop-up window or menu showing either the suggested correction or an explanation of what the error is supposed to be.

The third method is the traditional manual sweep-through of the document in which clicking the option

Continued overleaf ▶

Continued from previous page

makes a dialogue box appear, and anything the word processor believes is incorrect is excerpted, with a suggested correction shown beneath. You can select whether to accept or reject the suggestion.

Because the computer can be wrong when identifying errors, especially when it comes to grammar, turning off auto-correction is a good idea. You'll find the setting in Microsoft Word by clicking the File ribbon, then the Options menu entry, then the Proofing entry. Click the AutoCorrect Options button. Subsequently remove the ticks from all the boxes within the AutoCorrect tab and the other tabs; at very least remove the tick alongside Automatically Use Suggestion From The Spelling Checker.

To turn off underlining of errors, which can be distracting when you're writing, select the File ribbon, then the Options menu entry, and select Proofing from the menu. Then remove the tick alongside the Check Spelling As You Type heading, and the Mark Grammar Errors As You Type heading.

To undertake a manual pass-through of the document, click the Review ribbon and then the Spelling & Grammar button.

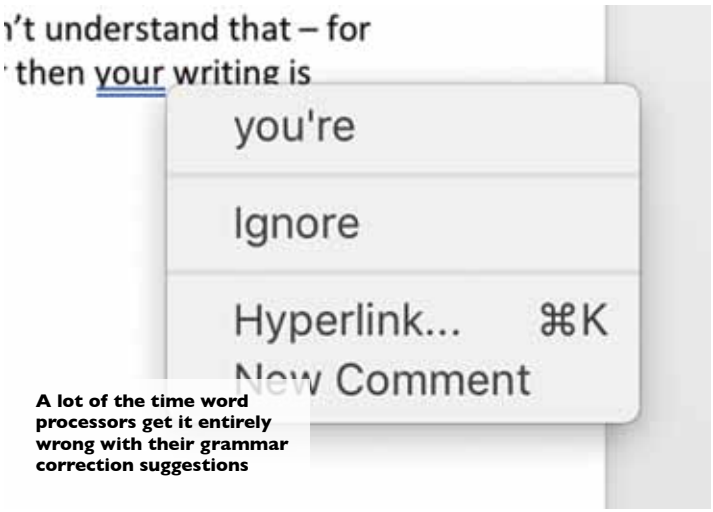
Tools like ProWritingAid aim to catch just about every fault it's possible to make when writing

Where's your grammar?

While spell checkers are *usually* correct – especially if you keep updating your personal dictionary with customised spellings – grammar checkers are wrong much of the time. This is because true grammar checking requires actual understanding, and computing technology just hasn't reached that stage yet.

Grammar checkers are also obsessed with the *passive* and *active* voice, which mirrors the preferred style of the US educational establishment. Many people in the UK haven't even heard of passive and active – I'm pretty sure they weren't even mentioned at my school – but if you want to know more just hit Google, where you'll find thousands of explanations.

In the latest 2016 release, Microsoft Word's grammar checker has been virtually eradicated. Apparently, the goal is to add a new tool soon, but gone is the Styles option of earlier releases of Word, in which you could choose how strict you wanted the grammar checker to be (with the Formal setting being like having a rather dense manager sitting on your shoulder, incorrectly criticising nearly every sentence you write!).



A lot of the time word processors get it entirely wrong with their grammar correction suggestions

Instead, what's left of the grammar checker now only searches for elementary errors, such as wrong apostrophe usage.

However, a new generation of writing tool has taken the concept of grammar checking and run a mile with it. In addition to the likes of basic verb and noun agreements these tools check for over-writing, clichés, redundant phrasing and much more.

While they're still inclined to make mistakes in what they flag as incorrect, LanguageTool (www.languagetool.org) and After the Deadline (www.polishmywriting.com) are good free-of-charge examples. You simply paste your copy into the web page to check it.

However, I'm grateful to the makers of ProWritingAid (prowritingaid.com), who invited me to take a look at the premium version of their writing tool. This costs $40 per year and includes a plug-in for Microsoft Word so there's no need to check your work via their website.

I used its online checker to look over not only some of my own work but also some snippets from news sites. Its suggestions were genuinely interesting, if not acutely useful – it told me to replace 'during the course of' with the simpler and more readable 'during', for example, and spotted some unclosed quotation marks in written dialogue.

By identifying vague word usage, it allowed me to considerably tighten up some journalism.

> *It's like having a rather dense manager sitting on your shoulder, criticising every sentence*

While I can't argue that proofing tools such as ProWritingAid are a necessity, they certainly provide an invaluable perspective on your work. For example, even if you disagree when a long sentence is highlighted as being difficult to read, it'll still make you consider that sentence afresh in a whole new context – and how many of us become word-blind to our own texts across hundreds of drafts?

In my opinion, rewriting to avoid even a questionable error flagged by a proofing tool can be a healthy thing – which is why simply ignoring or deactivating proofing tools can be a hasty move.

• *Keir Thomas has been writing about computers for more than two decades. He also offers personal technical support and upgrade services for Apple products in the Manchester, Stockport and north Cheshire/ Derbyshire areas. See www.mancmacsupport.com*

GETTING GOOD PUBLICITY

Keir Thomas talks to award-winning literary publicist Louise Rhind-Tutt to discover the secrets of her trade

Grey Trilby Photography

A publisher friend once said that if she were forming a small press from scratch, she'd hire one editor, one cover designer and two publicists. The first two roles are known by most people. The latter might come as a surprise.

But not to Louise Rhind-Tutt of LRTPublicity (www.lrtpublicity.co.uk) who is an award-winning freelance literary publicist. Her clients include Random House, New Holland Publishers, McGraw-Hill and National Geographic Books, while author clients have included veteran novelists David Lodge and Susan Hill as well as the estate of George Orwell and celebrity authors Cesar 'Dog Whisperer' Millan and Buzz Aldrin.

We bent her ear to find out just what literary publicity involves, and what the growing number of self-published authors can learn from her.

What it involves

Many authors are shocked to learn that the hard work has only just begun once their book hits the shelves.

Over 184,000 books were published last year in the UK alone, says Louise, so the belief that a work will stand out on its merits alone is naive.

'These days authors very much need to be active in promoting their book. They can't just sit back once their book is released.'

However, authors need to understand what publicity is.

'Publicity is different from marketing or advertising. Those things are *paid-for* media, whereas publicity or PR is *earned* media. Publicity involves convincing a reporter or editor to run a positive story about your book, which then runs in the editorial section.'

If you see or hear a professional author being interviewed on television or the radio, or if their book is reviewed anywhere, then it's very likely that a publicist will be behind it. However, Louise points out that publicity can also take many other forms, including articles written by authors, or profile interviews, or author appearances at festivals or events – from intimate bookshop or library events to large public lectures or debates.

'You have to be creative, but also highly focused,' she says.

Unsurprisingly, the internet is a key medium nowadays.

'My work often involves increasing the visibility of an author's presence online – from reviews on blogs to virtual author tours and social media. I keep an eye on the news agenda and what people are talking about on Twitter, as this can often lead to author articles or opinion pieces in the media.'

How it's done

The fact that publishers often staff whole departments with publicists provides a clue that publicising a book takes skill and, more importantly, time.

'The first step is to know what media you could possibly send your book to. There's no real shortcut to this – you have to completely immerse yourself in it. Get to your local newsagents or the library. Look at the publications that surround your subject matter. Research which publications or broadcast media, or festivals, you think would be relevant.'

There's a reason for the hard work.

'Eighty per cent of journalists say lack of understanding of their publication is their biggest frustration when dealing with press relations people. There really is no shortcut to understanding the media you want to approach.'

Although researching online publicity doesn't require you leave the house, authors still need to be wary.

'Bloggers get very fed up with being pitched ideas that just aren't relevant to their site, in the same way that print journalists do. So do your research and find out who is likely to be interested in your work.'

Although good publicity comes at a price, Louise says people shouldn't view the experience negatively.

'It's hard work, yes, but

I also like to think of the research as one of the perks of my job. A Sunday afternoon spent reading through a pile of newspaper supplements or magazines doesn't have to feel like hard work!'

As for tricks of the trade, Louise mentions Google as an obvious starting place but there are specific software tools, such as Cision UK (www.cision.com/uk). This is a paid-for service with a handful of useful free extras, such as a blog that frequently lists the top 10 UK bloggers covering different areas – the top UK film blogs, for example, or young adult blogs. She also suggests people look at the Media.info website (http://media.info/uk), which contains a searchable database of media contacts, and FeaturesExec Media Bulletin (www.featuresexec.com/bulletin), whose daily email she particularly recommends.

> *"Author publishes book" is simply not a story in itself*

Common sense goes a long way.

'Only pitch ideas that are relevant, and do it politely. Always ask if it's a good time to talk before you start chatting away. Don't call just to see if the person concerned received your email – journalists tend to get very frustrated by the follow-up call. And keep attachments small: you can always send high-res versions of things like images if they are requested.'

Working with authors

Authors need to bear in mind that they're as much a part of the publicity process as the publisher or publicist.

'The key thing to remember is communication,' says Louise. 'The author knows their book and subject matter better than anyone, and a good publicist will know the right places to approach for coverage. In working together, they can come up with interesting angles and ideas for features, etc that may help in terms of approaching the media.'

The author needs to think just as creatively as when they were writing the book and Louise points out that 'Author publishes book' is simply not a story in itself.

'So you need to look at what can be the story. Perhaps the author has an interesting personal story that could provide a hook.

'I always talk to authors in detail about their work and about themselves and their expectations for publicity before we start work on any new project, either in person or via phone or Skype or email if that's not feasible. It's important to get a feel for the story behind the book.'

The advice is again simple.

'Think like a journalist. What is the story? How does the story fit in with that particular publication and its readership? There may be an emotional personal angle, which would be of interest to the media, but only if an author is prepared and happy to speak publicly about it.'

All possible approaches are discussed.

'An author may absolutely love speaking on live radio or it may fill them with dread, or they might be happy to be part of a panel at a literary event but hate the thought of doing a solo talk.

'It doesn't help anybody to have an author in a situation where they feel uncomfortable. Working closely with the author, gauging what they are happy to do in terms of promotion and where their strengths lie is, for me, an integral part of any campaign.'

Advice for self-publishers

Louise has good and bad news for authors who choose to take the DIY route and publish themselves.

'I don't think there is the same snobbery about it as there maybe was a few years ago. The success of EL James and her *Fifty Shades of Grey* trilogy has done much to overturn the stereotype of a self-published author.

'Self-published books have their own set of issues in terms of approaching the media, though – many publications still do not cover self-published works. It's a case of finding other ways to get that word-of-mouth coverage.'

As with EL James, Louise advises self-published authors to use what they already have.

'Several self-published authors have a ready-made fan base for their work, but making content available is not necessarily the same as making it readable, and publishing and promoting a book is a different skill to writing.'

The ice is slowly melting within higher echelons of the media, however.

'Things are starting to change, which is a promising sign,' says Louise. 'The *Guardian* newspaper, for instance, has championed self-publishing often in recent months and earlier this year launched the Guardian Legend Times Self-Published Book of the Month prize to celebrate and showcase the best self-published novels out there.

'New companies such as Reedsy (reedsy.com) allow authors to find and collaborate with expert editors and designers to take their book to another level, and they will soon be integrating publicity into the platform as they look to help authors get the best out of working with publicists.'

Does Louise see a future where the focus moves away from big publishing houses?

'I have taken on a few self-published clients over the last couple of years – as well as from extremely small independent publishers – and whilst the majority of my work comes via traditional publishers it's certainly not a strand of publishing I would choose to ignore.

'It is an enormously busy sector and quality may not be the first word that springs to mind for many people, but there is no doubt that self-publishing is an appealing option for many extremely talented authors.

'One of the crime authors I worked with went on to pick up the attention of a large traditional publisher after the word of mouth that her self-published book received across the crime blogs and social media communities.

'Self-publishing is starting to be seen as part of publishing in general, it seems, which is very encouraging.'

LOUISE'S TOP 5 TIPS

1. When approaching journalists, your main headline should be devoid of jargon or adjectives – it should be short, snappy and let's not forget, tweetable.
2. Think like a journalist. How will your story fit into their publication, blog or website?
3. If readers engage with you as a brand, they will do your PR for you.
4. As a rough guide, around 80 per cent of your social media posts should be about sharing useful information or what you find interesting or entertaining, and 20 per cent can be about your own book.
5. Network! Both in the real world and online.

WHAT I WISH I'D KNOWN ABOUT...

NEW SERIES

Getting my first novel published

Keir Thomas introduces a new series allowing you to benefit from the mistakes and wisdom of highly successful authors

Welcome to a new series where successful authors pull back the curtain and reveal secrets of their trade – including what mistakes they made to get to where they are. This month we're looking at getting a first novel published.

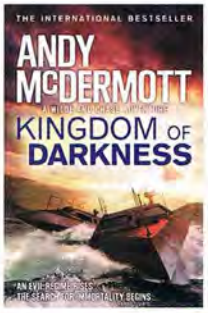
The writers gathered around our virtual table are diverse. In addition to being a novelist Rosie Garland is a poet, punk goth singer and cabaret chanteuse. Her second novel, *Vixen* (The Borough Press), has just been published in paperback and her first novel – *The Palace of Curiosities* (HarperCollins) – won the *Mslexia* Women's Novel Competition in 2012.

Anthony Riches recently published *The Emperor's Knives* (Hodder & Stoughton), the seventh in his highly acclaimed Empire sequence of historical fiction set in Roman times. Anthony researches and travels extensively for his work, blogging about his experiences at his site. Recently he completed a charity walk in Roman Centurion uniform that ended at the Coliseum in Rome.

Andy McDermott is author of the recently published *Kingdom of Darkness* (Headline), which is the tenth novel in his successful Nina Wilde / Eddie Chase series of adventure thrillers. Andy's first work, *The Hunt For Atlantis*, was the first of several of his novels to spend time on the *New York Times* bestseller list.

The craft

Let's start at the beginning: completing a novel, finding an agent and somehow getting it on bookshop shelves. All three authors tell the same story of hard work and rejection. Anthony points out that his writing career started twenty years before



> "Maybe nobody wants your first novel. Or your second, or third, fourth, fifth... But if they want your ninth, then it'll all have been worth it."

his first publishing success, while Rosie waited twelve years until the fourth novel she wrote was picked up. Andy snagged a publishing deal with the ninth novel he'd penned.

'I wish I'd known more about what some people call the craft of writing fiction,' says Anthony. 'There is a set of rules that needs to be followed if your story is going to find an agent and a publisher.'

This can be as simple as 'show don't tell', he says, explaining that as an historical fiction writer he made the mistake early on of simply retelling his research in the narrative, rather than using characters to do so, or via other narrative tricks. Don't tell the reader *there are six centuries in a standard legion cohort*. Do tell them that *the last of the cohort's six centuries is marching onto the parade ground.*'

Andy mentions how the outline for his first unpublished novel was 'a single page of A4 with a vague timeline of events' that took a year and a half to write and was 'terrible'. His second attempt at a novel was planned meticulously and was completed in a month and a half.

'Lesson learned,' he says. 'That's how I've worked ever since. It still took several more stories – in different genres, everything from comedy to sci-fi – before I found my feet.'

Following on

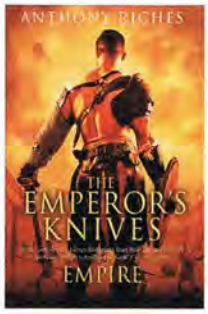
Once Rosie's first novel was published as part of her two-book deal with HarperCollins she anticipated simply picking up and polishing one of her earlier novels. Her editor had other ideas, suggesting she 'create something fresh'.

'At first I resisted,' says Rosie. 'But she was absolutely right. Each of my previous books taught me how to write better novels, how to improve my craft. I took that learning and created *Vixen*.'

Rosie suggests her experience proves the core message of Malcolm Gladwell's book *Outliers*, saying: 'The key to success in any field is, to a large extent, a matter of practicing a specific task for a total of around 10,000 hours.'

Similarly, Anthony 'spent so long getting the right style of writing and being comfy with my voice' that his next two published books came easily. If he had an issue, it was one of motivation: 'It's easy to suffer a hangover after that first book has burst from you but isn't published yet, especially if you're still working [a day job]. The answer is just to write, every day, even if only a few hundred words.'

Andy mentions the potential importance of a big-name publisher when it comes to a first book launch: 'I was fortunate to make my first sale



"It's easy to suffer a hangover after that first book has burst from you but isn't published yet, especially if you're still working."

to Headline, who as a major commercial publisher handled the majority of the promotion work like getting review copies to the right people and arranging interviews.'

Editing

Getting a book noticed by an agent is the first hurdle, of course, but perhaps because of their long apprenticeships our three authors reported few issues with the editing stage once a publisher was found.

'*The Hunt For Atlantis*, my first published novel, actually changed very little between being bought and finally published,' says Andy. 'I'd thought of the title as only a placeholder and assumed someone would come up with a better alternative but as it turned out everyone loved it. Most of the editorial changes were trims to keep the pace frantic throughout.'

Rosie offers cautionary advice: 'Welcome editorial input but don't agree to everything they say. After all, it's your novel. To sift out the right from the wrong I ask myself: is this editorial suggestion designed to create a better novel? Or is it the editor steering me towards the novel they want to write?'

Business

Anthony's first published novel followed a curious rule of sixes: it was picked up by the sixth agent he approached, and then picked up by the sixth publisher that the agent approached.

'The one thing that could have been better would have been for more than one publisher to have wanted the book,' he says, referring to auctions that are sometimes held for rival publishers to purchase the rights. However, he also sounds a note of caution: 'Some of the money that gets thrown round in auctions is amazing. The downside is that publishers then sometimes have institutional "buyer's remorse" and spend nothing on promo.'

Some within the industry, he says, have a withering description for this occurrence: 'Large advance, short career'.

Rosie languished on the lists of two separate agents before ending up with her third, a former staff editor at Simon & Schuster, and with whom she achieved her success: 'She was wonderful and believed in me,' says Rosie, although in the fast-moving world of publishing that agent has since moved on to head Faber's global fiction list. She's thrilled with her latest agent but all of this is stark contrast to previous agents, one of whom simply stopped returning her emails: 'I've learned the hard way that if your agent isn't the right fit, then look elsewhere. I took matters into my own hands and entered the novel competition that launched me into print. If in doubt, do it yourself.'

Rosie and Andy are now full-time writers but despite his success Anthony cautions against giving up the day job, suggesting authors only do so if an advance is enough to pay a salary for some time: 'Getting back into that highly specialised niche you made good money from might be well-nigh impossible once you've been out of the business for a year or two.'

He points out that he uses travelling that his day job demands as a perfect excuse to write.

Promotion

'I wish I'd known it was really my job to do promo!' says Anthony, who adds that book readings and signings are 'lovely' even though most authors fail to attract more than a handful of people.

'Fans are marvellous, even when most of us only ever get a handful to a signing, but a bit of a waste of effort for just that reason. If your fans want a signed book and live hundreds of miles away, tell them to go to a specialist like Goldsboro Books for their signed first edition.'

Online isn't any easier, he says: 'It's really hard work, and easy to get sucked into doing more Facebooking and tweeting than writing – which would be a bad thing!'

Rosie emphasises the need to make readings 'sparkle', saying, 'The last thing I want to do is mumble through, strangling the life out of my words.'

Her experience performing as a rock star, poet and burlesque performer undoubtedly helps, but she says a creative approach to promotion can make all the difference and, as with Anthony, she advises against leaving it all to the publisher or agent: 'When *The Palace of Curiosities* came out, set in a Victorian circus, I discovered a wonderful sideshow troupe of the same name (**www.palaceofcuriosities.com**). We combined my readings with the sideshow and created an unusual and successful tour of book festivals in 2012.'

Signed to major publisher Headline, Andy is happy with the work they do promoting the book but says things don't always run smoothly. With his first book he was booked for a chat on Talk Sport radio, 'which even going in I thought was an odd choice. Not only had the interviewers obviously not read the book, they hadn't even glanced at my bio. It made for a bit of an awkward broadcasting debut.'

©Jonathan Bean

"Welcome editorial input but don't agree to everything they say. After all, it's your novel."

Don't give up

Asked for their last pieces of advice, our three authors are unanimous: Don't give up.

'One rejection doesn't necessarily mean that your story is rubbish,' says Anthony. 'It could just mean that the reader was having a bad day, so keep trying. Writing may be difficult at times, but being a writer is great! So get on with it!'

'Never give up, ever,' says Andy. 'Maybe nobody wants your first novel. Or your second, or third, fourth, fifth... But if they want your ninth, then it'll all have been worth it.'

'Write because you love it,' says Rosie, 'Keep going, even when it feels hopeless. Especially when it feels hopeless.'

CHAPTER 15

Working with Text Files

Windows views text files as just another file type, but to Ubuntu, they can be essential components that make the system work. Configuration files are stored as plain text, and program documentation is also stored as text. This is clearly different from Windows, where it's very likely any information you're supposed to read will be contained in a Windows Help file, a rich text format (RTF) file, or even a Microsoft Word document.

Because of the reliance on text files, the shell includes several commands that let you display, edit, and otherwise manipulate text files in various ways. Learning to use the shell, and therefore learning how to administer your Ubuntu system, involves having a good understanding of these text tools. You'll use text tools for editing configuration files and viewing log files, as just two examples.

Viewing Text Files

You can easily view files using command-line tools, including `cat`, `less`, `head`, and `tail`. The simplest command for dealing with text files is `cat`.

Using the cat Command

When followed with a filename, the `cat` command will display the text file on screen:

```
cat mytextfile
```

`cat` is short for concatenate, and it isn't designed just to display text files. That it can do so is simply a side effect of its real purpose in life, which is to join two or more files together. However, when used with a single file, it simply displays its contents on screen.

If you try to use `cat`, you'll realize that it's good for only short text files; large files scroll off the screen.

Using the less Command

Because `cat` works well only with short files, and to give you more control when viewing text files, the `less` and `more` commands were created. The `more` command came first but was considered too primitive, so someone came up with `less`, which is preferred by many Linux users. However, both are usually available on the average Linux installation.

■ **Note** The `less` and `more` commands are sometimes known as *pagers* because of their ability to let you scroll through pages of text. You might still hear them referred to as such in the wider Linux community, although the term has fallen out of use.

Let's look at using `less` to read the Eye of Gnome `README` file, which contains information about the current release of the default Ubuntu image viewer. The file is located at `/usr/share/doc/eog/README`, so to use `less` to read it, type the following:

```
less /usr/share/doc/eog/README
```

You can scroll up and down within the `less` display by using the cursor keys. If you want to scroll by bigger amounts of text, you can use the Page Up and Page Down keys. Alternatively, you can use the spacebar and B key, both of which are commonly used by old-hand Linux users for the same function. In addition, the Home and End keys will take you to the start and end of the document, respectively.

A useful command option to use with `less` is `-M`, which adds a short status bar to the bottom left. Alongside the filename, you'll see how many lines the document has and which line you're currently up to. In addition, you'll see, as a percentage, the amount of document you've already read through, so you'll know how much is left.

`less` lets you search forward through the file by typing a slash (`/`) and then entering your search term. Any words that are matched will be highlighted on screen. To repeat the search, type `n`. To search backward in a file from your current point, type a question mark (`?`). To quit `less`, simply type `q`.

Although it's supposedly a simple program, `less` is packed with features. You can see what options are available by reading its man page or by typing `less --help`.

Using the head and tail Commands

A couple of other handy commands that you can use to view text files are `head` and `tail`. As their names suggest, these let you quickly view the beginning (head) of a file or the end (tail) of it.

2. You can now close the Terminal window, and the screensaver will continue to play in the background after a momentary delay. Ignore the warning that appears about terminating an application.

3. If you get tired of the screensaver, open a Terminal window, and type the following:

```
killall ScreenSaverEngine
```

Note that this tip isn't ideal for regular use on portable Macs because it places a small additional drain on the battery. However, desktop Macs or portable Macs connected to power sources shouldn't see any downside.

Tip 120

Add Folders of Wallpaper Images

Here's a tip if you're a fan of downloading lots of wallpaper from online sources.

Copy your downloaded wallpaper images to their permanent location on your computer (that is, within your Pictures folder, for example), and then open System Preferences (Apple menu→System Preferences) and the Desktop & Screen Saver panel. Select the Desktop tab; then just click and drag the folder onto the left pane of the window, under the iPhoto heading. This will instantly add the files to the list of available wallpapers, and this can be repeated with any other folder containing images.

To remove the folder later, again open the Desktop & Screen Saver pane within System Preferences, select the folder in the list, and click the minus symbol button at the bottom of the list.

Incidentally, if you're choosing a new wallpaper in the Desktop & Screen Saver pane of System Preferences, you can make the thumbnail previews bigger by placing the mouse cursor over the thumbnail previews of the wallpapers and using the pinch-and-expand gesture—placing a finger and thumb on the trackpad and moving them slowly apart (if your Mac uses a multitouch trackpad, of course!).

Tip 121

Put Notebooks in Deep Sleep

Mac notebooks use magnetic case closing mechanisms to keep the lid shut, rather than physical clasps. This makes opening them much more convenient, but it also means they can open themselves sometimes, while in a travel bag, for example. Once open, they can switch themselves on and thus waste battery life. They might even create a hazard during a flight if the wireless hardware activates.

If this is a problem for you, you can set your MacBook to hibernate to disk when the lid is closed, rather than simply go into sleep mode. This turns the computer off completely, rather than keeping the memory alive with a trickle of battery power.

Note that this is arguably not a good choice for Macs with a solid-state hard disk (SSD), such as MacBook Air computers. It will mean that every time the computer powers down, a multigigabyte hibernation file is saved to the hard disk, usually slightly larger than the size of your computer's RAM (that is, 4GB or 8GB). In theory, this can wear out SSD more quickly.

Setting Up

This tip changes a firmware setting for the entire computer, so it will affect all users.

Open a Terminal window, and type the following:

```
sudo pmset -a hibernatemode 25
```

You'll need to enter your login password when prompted. The changes should take effect right away.

Putting to Sleep and Waking

Give your changes a try by closing the lid and waiting a minute or two for it to hibernate. Then wake your computer (remember, you'll now need to press the power button each time). Waking a hibernated computer takes a few seconds longer as the RAM contents are read in from disk, but it's still fast enough for everyday use.

Putting Desktop Macs to Sleep

For what it's worth, it isn't just portable Macs that hibernate—desktop Macs support it too. Once you've changed the setting as described earlier, click Apple menu→Sleep to hibernate. After a minute or so, the computer will completely power down. To wake the computer from hibernation, depress the power button as usual.

For desktop Macs that take a long time to boot from cold, hibernating can save a few seconds each time you boot.

Restoring the Original Setting

To return to the standard sleep mode later, open a Terminal window, and type the following:

```
sudo pmset -a hibernatemode 3
```

Tip 122

Fix a Slow Boot

If you find there's a huge delay after the desktop first appears until the computer becomes usable, try cleaning up your desktop by removing as many files, folders, and aliases as you can without impeding your workflow. Either create folders and file things away in them or put things where they're supposed to go in your Documents, Movies, and so on, folders. Try to have as few icons on your desktop as possible, and definitely try to avoid any that might be automatically turned into thumbnail previews, such as movies and pictures, because this adds to OS X's workload when it's already busy loading the system at boot time.

You can try turning off icon thumbnailing by right-clicking a blank spot on the desktop and selecting Show View Options. In the dialog that appears, remove the check from Show Icon Preview. Close the dialog box. The changes take effect immediately.

Also consider pruning the number of programs that start when you boot—see Tip 134, *Control Start-up Apps*, on page 153.

CHAPTER FIVE

Hands-on at the command-line

This chapter looks at what some consider the most fascinating and useful aspect of Linux: the command-line. The chapter explains:

- How to understand what the command prompt is telling you;
- How commands work (i.e. arguments and options);
- An overview of useful day-to-day commands;
- Tips and tricks to let you work efficiently;
- Using root powers at the command-line;
- Dealing with crashed or stalled programs;
- Understanding and manipulating file permissions;
- Advanced tricks (redirection, piping and brace expansion).

All about the shell

When we talk about the "command-line", we're talking about issuing typed commands directly to Linux. Most commands relate to manipulating files, while some administer the system. The command-line offers power and flexibility, at the expense of a slightly steep learning curve and—arguably—a lack of intuitiveness.

bashed about

The command-line utilized in Ubuntu is known as `bash`—the *B*ourne *A*gain *SH*ell. This is an evolved version of the Bourne `sh` program, one

of the oldest command-line programs for Unix. Most people agree that bash offers the best all-round mix of functionality and ease-of-use.

Command-line programs are sometimes known as *shells*, and the term comes from the fact that—like mollusks and crustaceans—the shell "wraps around" the delicate interior of the operating system, protecting it from accidental damage!

> **NOTE** A graphical user interface is sometimes referred to as a shell because, by the above definition, it has the same function as a command-line prompt.

Other shell programs are sometimes used under Linux instead of bash. Perhaps the most popular are Korn Shell (ksh) and C Shell (csh). Both are geared towards programming and it's unlikely you'll ever come into contact with them. bash is the default in most popular Linux distros.

To DOS or not to DOS

You might be wondering if the Linux command-line is similar to Microsoft DOS. They're distant cousins rather than siblings. DOS was a clone of CP/M, that itself borrowed much from the Unix command-line. Some DOS knowledge will give you a head start, but you will have to unlearn as much as you learn!

Understanding the prompt

Let's get stuck-in straight away.

Starting a command-line session

There are two ways to start a command-line session: by running a desktop terminal program (sometimes known as a *terminal emulator*), or by switching to a *virtual console* (also known as a *virtual terminal*). In both cases you're accessing exactly the same command-line.

To switch to a virtual console, hit Ctrl+Alt+F2. The GUI will disappear and be replaced by a login prompt. Don't worry—your desktop is still there, and you can switch back to it by hitting Ctrl+Alt+F7. It's just that the virtual console needs to take over the screen.

> **NOTE** There are *six* virtual consoles, and they're accessed by hitting Ctrl+Alt and F1, F2, F3, F4, F5 or F6. The console on F1 is used for debug and log output, so is best avoided.

Login by typing your username, and then the password. You won't be prevented from logging in because you're already logged in at the desktop—under Linux a user can login as many times as she wants.

As you might be realizing, a virtual console session is a little clunky. A more convenient way to access the command-line is to use a terminal program. This provides a command-line right there on the desktop.

Logout of the virtual console by typing `exit`, and switch back to your desktop (hit Ctrl+Alt+F7). Then open a terminal window by clicking Applications ⇨ Accessories ⇨ Terminal.

This time there's no need to login, because the terminal window runs as part of your desktop environment, and that's already logged-in.

> **NOTE** So why use a virtual console? Well, they're very useful when things go wrong. If the GUI crashes, you can switch to a virtual console to try and fix things. Even if there's no GUI subsystem, the virtual console will still be there. It's a permanent fixture of Linux.

Knowing who you are

When the terminal program appears, you'll see something like this:

- `keir@keir-desktop:~$`

This is the actual command-line prompt, often shorted to "prompt".

The first part of the prompt shows your username. In this example, taken from my test PC, the user is `keir`. After the @ sign is the name of the computer, commonly referred to as the *hostname*. This was set during installation of Ubuntu, on the same configuration screen where you chose your username.

The hostname is how the computer is known on the network. It isn't very important if your computer only connects to the Internet via a router or modem, but it's vital if Ubuntu is used in a server environment, or if you intend to remotely access it across the Internet.

As you can see, the computer in my test PC setup is called `keir-desktop` and so, reading the full prompt, we can see that the user named `keir` is logged in at (@) the computer named `keir-desktop`. In other words, the first part of the prompt is all about *who you are* and *where* you're logged in.

Knowing where you're browsing

After this is a colon. This separates the physical location part of the prompt from the rest, that tells us the location in the filesystem—which folder we're currently browsing. We see a ~ symbol (known as a *tilde*). This is shorthand that always indicates the user's `/home` folder. When you see a tilde, imagine the path to your home folder instead.