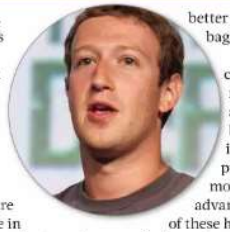
STAY ANONYMOUS ONLINE

DELETE YOUR FACEBOOK ACCOUNT
Turn to p11

With vulture websites scavenging your personal data, it's never been more important to stay private online. Nicole Kobie reveals the 15 best ways to preserve your anonymity

Personal data is so lucrative it's been called the new oil, which presumably makes Facebook boss Mark Zuckerberg (pictured) the JR Ewing of the digital age. Billions of pounds are made (and spent) collecting it as we browse online. Some people say that's the price we have to pay to keep the internet free. Without adverts that can target you using this data, websites wouldn't make money, and would then have to charge you.

That argument, always a shaky one, has been obliterated by the recent Facebook/Cambridge Analytica scandal (see page 11). While some data collection may be acceptable, there's no justification for such a mass abuse of privacy. Are other companies (Google in particular) looking nervously at events, wondering if they'll be the next to come under scrutiny?



Regulators are bound to come down hard on Facebook, forcing it and other similarly arrogant tech giants to change their ways. But *you* don't have to wait until the authorities act. Reclaiming your privacy is a matter of using tools that keep you anonymous online. In this feature we reveal the 15 most effective methods, all of which work better than sticking a paper bag on your head.

We start with urgent changes you can make quickly, such as tweaking your browser's settings so it always launches in private mode, before moving on to more advanced measures. Some of these have side effects that make browsing trickier, as we explain. Staying anonymous requires juggling privacy with convenience.

Not all 15 tips will suit the way you browse the web. Some will be overkill, while others may require too drastic a change in behaviour. It's hard to break habits learned from 20 years spent online. But they are all powerful ways to stop the likes of Mark Zuckerberg making even more billions from your data.

WHAT YOU SHOULD DO

- Browse the web privately so your history isn't saved
- Block adverts that track what you do online
- Stop websites knowing your location
- Beat geographical restrictions using a VPN
- Erase old web accounts you've forgotten about

LEVEL 1: URGENT - WHAT YOU SHOULD DO NOW

1 Swap Google for DuckDuckGo

As well as tracking what you tap into its Search bar, Google collects plenty of other information, including when you typed something and where, then plotting it on a map. That's handy if you want to know whether you searched for 'holiday home in cornwall' from home or work, but otherwise it's simply invasive.

To avoid this kind of stalking you have two options. One is to disable Google's search tracking and location history. Sign into your Google account (https://myaccount.google.com), click the My Activity box at the bottom, then 'Activity controls' on the left. On the following page decide what to turn off, such as the Location History slider, and the 'Web & App Activity' slider (see screenshot below), which will stop Google saving your searches.

The alternative is to wave goodbye to Google, and use DuckDuckGo (https://duckduckgo.com) instead. It doesn't collect any of your personal data, though it does monitor what you search to better understand any misspelt words. It also tracks some searches that go to online retailers because it makes money through affiliated links, taking a cut of any purchases made on them. But none of this can be used to identify you, so it's considerably more private than Google.

To make DuckDuckGo your default search engine in Chrome, click the top-right menu (three vertical dots), click Settings, then under 'Search engine' click 'Manage search engines'. Scroll down the alphabetical list of browsers to DuckDuckGo, then click the three dots to its right and select 'Make default'.

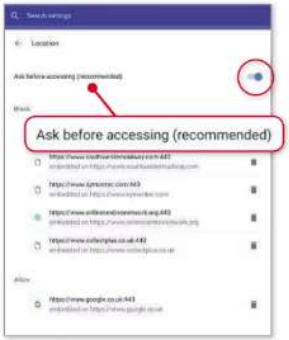
A further option is to also ditch Chrome for up-and-coming rival Vivaldi (named by our sister magazine *Web User* as the internet's best browser). When you use the private mode in its latest version it sends searches by default through DuckDuckGo. That's about as private as you can currently get without veering into the dark web via Tor (see page 58).

2 Turn off location data

Where you are matters to advertisers. From your location data, they can tell where you live, where you work, and plenty of information about your lifestyle. That's why, as well as disabling your location in Google, consider doing so in your browser. The process is similar in Firefox, Edge and Chrome.

In Chrome, for example, click the top-right menu, Settings, then scroll down and click Advanced. Next, in the 'Privacy and security' section, click Content Settings, then 'Ask before accessing' under the Location heading. On the next page click the top-right blue slider to switch off all location tracking. To block all location tracking make sure the top-right blue slider is switched off.

If you feel that's too drastic, ensure the slider is left on, showing 'Ask before accessing (recommended)' (see screenshot above right). This forces websites to ask your permission to track your location, so be prepared to click 'no' rather frequently.



Leave this setting switched on to force sites to request your location

3 Change hidden browser settings

Disabling location tracking is just one of many browser settings you can tweak to reclaim your privacy. But some browsers try to dissuade you from changing them by hiding their privacy options in 'Advanced' sections. They hope you'll think: 'Advanced? I better not touch those then'. This is a cynical ploy, and the truth is browsers don't want you to deactivate settings that may harm their advertising revenue. In an ideal world, privacy options would be upfront in a browser's settings.

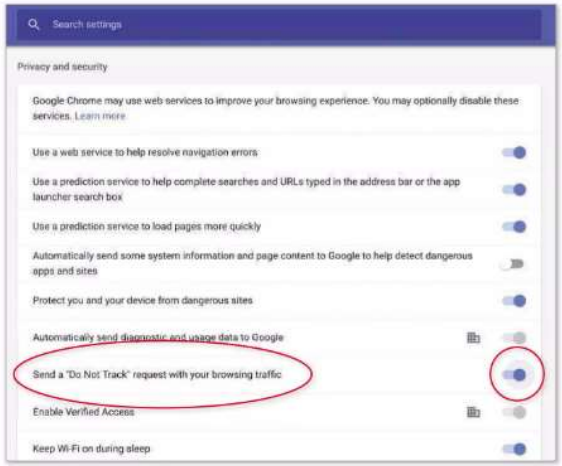
Here, we'll explain how to find these hidden settings and tweak them to your advantage. In Chrome, go to Settings, Advanced, then 'Privacy and security'. here, it's worth clicking the slider that asks websites to comply with a 'Do Not Track' request (see screenshot on page 52). First proposed in 2009, then maintained by two US professors in technology and law – Jonathan Mayer and Arvind Narayanan – this setting aims to reduce tracking across the web. Websites and advertisers can ignore the request, but it's still worth asking. Read more at http://donottrack.us.

In 'Privacy and security' you can also stop sending Google your 'diagnostic and usage data'. The company says this ▶

Disable the 'Web & App Activity' slider to stop Google saving your searches

information helps it to improve its products and services, but that's what they all say. Consider too disabling Autofill if you don't want Chrome to automatically fill in forms with your address details or save passwords for websites. Like many of the privacy options we describe, it comes at the cost of convenience (see box below). Chrome won't remember your details (great!), so you'll have to type them in every time (perhaps not so great). Therefore, before you change a setting, consider how much hassle you're prepared to put up with. And if you think you may change your mind, make a note of how to retrace your steps so you can reverse the setting.

Other major browsers have similar settings in the top-right menu buttons. In Firefox, go to Options, then 'Privacy & Security'. In Edge, click Settings, then View Advanced Settings.



Turn on this slider to ask websites to stop tracking you

4 Force sites to use https

Websites are protected either by HTTP or HTTPS, which are different ways of encrypting the traffic between your browser and a website. That 'S' at the end is key - it stands for 'secure'. If a URL in your browser bar is prefixed by HTTPS, it's using the most secure standard of encryption, making it harder for anyone to eavesdrop on your online activities. Chrome highlights it in green, showing a "secure" lock in the URL bar.

You can't simply enable HTTPS on a website that doesn't support it. That's a job for the site's developers. Some sites already use it by default, but many don't. Others include elements, such as adverts, that don't connect over HTTPS. That's why you should install the HTTPS Everywhere extension (https://www.eff.org/https-everywhere). Built by developers at the privacy campaign group Electronic Frontier Foundation (EFF) and the anonymous browser Tor, it works in Chrome, Firefox, Opera and 'Firefox for Android'. Once installed, it simply forces websites to use HTTPS if they can, meaning you have as much protection as is currently available.

If you want to be sure you're only browsing with this level of encryption, click the extension's icon at the top right of your browser bar, then tick 'Block all unencrypted requests'. This stops you loading websites that don't use HTTPS, which can be frustrating (see box), but will help put pressure on websites that need to tighten their privacy levels.

5 Use incognito mode

Choosing private browsing mode, also known as incognito mode (see screenshot above right), opens a fresh window where you can do whatever you like without your browser saving information on what you searched for or any data you enter into online forms. It's handy if you share your computer with others and want to keep your browsing secret. This isn't as sneaky as it sounds. It can be very useful when you're shopping for a gift for someone because, if they come to use the PC, they won't see any adverts relating to presents you may have looked for, and therefore won't ruin their surprise.

Type this to always launch Chrome in Incognito mode

You can open a one-off private session via the dropdown menu in the top-right corner of Firefox, Chrome and Edge. You can also set Chrome so it always opens in private mode. Right-click the Chrome icon on your desktop, then click Properties. At the end of the 'Target' field, after 'exe."', type a space, then -incognito (as shown in the screenshot below left). Follow the same instructions to do the same in Firefox, then type " -private" at the end.

Browsing incognito doesn't prevent websites from gathering data about your habits, something the latest version of Firefox does restrict (see page 16).

6 Block adverts

There are plenty of reasons to block adverts: they're annoying, they follow you around the web, they can be riddled with malware. There are several tools you can use to do this, and many of them have similar names (Adblock Plus, AdBlock, uBlock and more).

You may be wondering whether you still need them now that Google has built a filter into Chrome that blocks irritating adverts – the kind that play videos automatically or pop up as you scroll down a web page. If a site subjects you to multiple adverts like this, Google will ask it to stop. If the site refuses, Chrome will remove *all* ads on the site. Google's idea is to encourage good advertising standards, so that we're not driven to block *all* ads – and it doesn't lose revenue.

So, should you ditch your ad-blocker, and trust Chrome instead? It's too early to judge. But we doubt Google will go all out to antagonise advertisers that it relies upon.

If you see this screen, Chrome won't remember what you search for

7 Add privacy extensions

Online advertisers are guilty of many privacy infringements, but blocking ads is only the first step. You should also use browser extensions like Ghostery (www.ghostery.com) and Disconnect (https://disconnect.me) to block marketing tools that track what you do online. If you don't mind a site following you, add them to a 'whitelist'.

Privacy Badger (www.eff.org/privacy badger), another tool from the EFF, reveals who is watching you, blocking advertisers only if they stalk you too aggressively. Install it, visit a site with adverts, then click the badger icon to the top-right of your browser bar. You'll see the sites' advertising trackers listed next to sliders, which should all be green.

As you browse and are tracked from site to site, these will change to yellow or red. Privacy Badger deems yellow trackers required for websites to load properly, but will remove unnecessary cookies within them. Red means all trackers have been disabled on a site (see screenshot below).

After 30 minutes browsing, Privacy Badger blocked several trackers on MailOnline (shown in red)

8 Choose a secure messaging app

Over the years we've spotted a trend: the most secure messaging apps have the fewest gimmicks. They're the sensible choice for people who favour privacy over frivolous options like enhancing a selfie photo with a dog face.

We recommend apps that are protected by end-to-end encryption (E2EE). One of the best E2EEs is Signal (http://signal.org), which is fairly easy to use. WhatsApp uses Signal's encryption, but it's designed in a way that dilutes some of the protection. However, it's still more than enough security for most of us. State-sponsored spies may want to look elsewhere.

But wait! Who owns WhatsApp? Yep, Facebook. The same Facebook involved in allegations over data breaches in the last few weeks (see page 11). Happily, legal regulators have prevented the two services sharing users' data, so WhatsApp users can sleep comfortably at night - at least until the next scandal breaks.

PRIVACY vs CONVENIENCE

For many of our tips you'll need to balance privacy with convenience. This isn't a question of tech companies being difficult – some features just need data to work.

For example, if you turn off Google's location tracking, Google Maps won't know where you are. Or browse in private mode and you'll have to log into sites every time, and you won't be able to refer to your browsing history if you forget where you spotted something.

HTTPS Everywhere forces sites to open in their most secure version, but still loads insecure pages, unless you set it to 'Block all unencrypted requests'. That's the most private mode possible, but it means pages that are only HTTP won't be shown, which includes large swathes of the BBC.

Another thing to bear in mind is that some websites now only show content if you disable your advert blocker. You'll have to temporarily turn off your blocker every time you visit the site, or permanently tell the blocker to show ads on that site. Drawbacks to using Tor include waiting for pages to load as the traffic is bounced around. Are these hindrances worth the hassle? It's up to you to decide.

Computer active Reader Offer

2018 VERSION NOW AVAILABLE

NEW READER OFFER!

Norton Security Deluxe – SAVE £70!

For the first time ever we're offering readers discounts of over 60 per cent on Norton's excellent 2018 antivirus software. It protects your Windows PC, Mac, Android and iOS devices with a single subscription

WHAT IT DOES:

- ✓ Blocks viruses, spyware and malware
- ✓ Keeps your identity private
- ✓ Alerts you to dodgy apps
- ✓ Keeps online purchases safe

PLUS: 24-hour support every day

Norton is made by respected US security company Symantec. In our most recent antivirus test (December 2017) it scored 100 per cent for protection – blocking every threat we threw at it

Three devices for one year NOW ONLY £21.99*
Normally £59.99

Buy it from our Software Store at www.snipca.com/25004

Three devices for two years NOW ONLY £39.99
Normally £109.99

Buy it on our Software Store at www.snipca.com/25502

* while stocks last

COMPATIBLE WITH: WINDOWS XP, VISTA, 7, 8 & 10

LEVEL 2: BE AWARE – WHAT YOU SHOULD CONSIDER

9 Delete old online accounts

Don't use Facebook but have an account? Delete it (we explain how on page 11). Every online account you've signed up for has the potential to leak data, intentionally or otherwise. A word game you once played but lost interest in can be bought, and your data sold to a marketing company. The risks add up over several years of browsing. However, deleting old accounts isn't easy, not least because you may have forgotten which ones you signed up for in the first place.

Thankfully, there are plenty of online tools to help you clean up your forgotten online registrations. Deseat.me (www.deseat.me), for example, uses your Gmail or Outlook account to search for anything associated with your email address. From the list provided, click Add to add an account to your 'Delete queue', then click the red 'Delete' button to erase it (see screenshot below). This won't erase your account, but does provide a shortcut to the delete page on the relevant website, which can often be infuriatingly difficult to find. It won't work with *every* account, but it's definitely worth trying.

One word of warning: you'll have to give Deseat.me access to your email (including your messages). After a similar service, Unroll.me, was shamed for selling user data, Deseat.me's developers have been quick to insist that they don't collect or share your private info. Perhaps the final item in your list of accounts to consider deleting is Deseat.me itself.

Deseat.me helps you quickly delete your old online accounts

Choose an unusual address when signing up for a disposable email

Admirably, the service offers itself up for deletion once its job is done.

10 Use disposable email accounts

Email addresses are often the most critical elements of our online identities. They're used for logins to sites and resetting accounts, as well as keeping in touch with family. Consequently, it may be worth setting up two accounts – one for contacting friends and family, and emails that matter, and another for registering for one-off purchases, email subscriptions and the like. This second account will then receive all those annoying newsletters and promotional 'offers' websites bombard you with.

That does mean you're managing two accounts, though Gmail makes it easy to link multiple email addresses to one inbox – click your account icon in the top right, then click Add Account.

But why should you even have to think about emails you don't need? To avoid this hassle, simply use disposable email accounts. You use these just once – to register for a site. If the site sends you a confirmation email with a link to click, use it for this purpose alone, then forget about the account forever.

MailDrop (https://maildrop.cc) is a good choice. It lets you choose your own email address, but make sure you choose a highly unusual name (**mauveyakseatcheese@maildrop.cc** in our screenshot above) to reduce the risk that someone else has already used it. They would stumble upon emails sent to you if they enter the same name.

Be aware that some online services have got wise to people using disposable accounts, and now block emails going to these type of addresses. So if you don't receive a confirmation email, try again with another site, such as Mailinator (www.mailinator.com), GuerrillaMail (www.guerrillamail.com) or Temp-Mail (https://temp-mail.org). There are also browser add-ons to make it all easier, such as TrashMail for Chrome (https://trashmail.com), which will notify you when the disposable account has received the email you're waiting for.

11 Use a VPN

A virtual private network (VPN) is an encrypted tunnel your data slips through, keeping your payment-card details, browsing habits and email correspondence safe from prying eyes. VPNs serve two purposes. First, to keep data safe from anyone 'sniffing' a Wi-Fi connection, preventing hackers from intercepting your data when you browse on a public Wi-Fi network (in a cafe, for example). Second, a VPN lets you access sites blocked by your ISP, such as online TV and film services that are subject to geographical restrictions.

There's one major worry about VPNs. In the wake of US laws whittling away at net neutrality, a wave of fake VPNs popped up designed to hoover up personal data when people thought they were being protected. Meanwhile high-profile service Hola was revealed to be selling user data to a botnet. So you need to be *very* careful about which VPN you choose.

The easiest VPN for beginners is TunnelBear (www.tunnelbear.com), which in March was bought by antivirus software company McAfee. Like all VPNs, it offers unlimited data only in its paid-for version (from £4.23 per month). Also consider using the browser Opera (www.opera.com), which has a VPN built in. ▶

12 Send self-destructing messages

Sending messages that self-destruct may feel a bit James Bond, but they can be useful to us mere mortals as well. They're perfect for sharing passwords or other sensitive information with trusted contacts.

We recommend Privnote (https://privnote.com). Type your message into the yellow box, then tap Show Options, which include deciding when the note will self-destruct ('1 hour from now' in our screenshot right). Next click 'Create note' to create a link to your note. Copy and paste this into an email, then send it to your recipient. They can read the message by pasting the link into a browser's address bar.

You can also send self-destructing Gmail messages using the Chrome extension Snapmail (https://snapmail.co). Install it, then when you send an email tap the green Snapmail button instead of Send. Your recipient will receive a link to the message, which is deleted after 60 seconds.

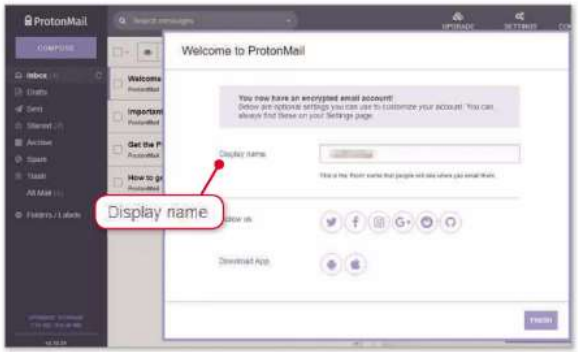
Using Privnote you can set when your email will self-destruct

LEVEL 3: CONSIDER – WHAT TO DO WHEN YOU HAVE TIME

13 Encrypt your emails

Encryption is another privacy option that's not just for MI6. You can use specialised encrypted services such as ProtonMail (https://protonmail.com), which was developed by scientists working at CERN (presumably in their tea breaks from fiddling with the Large Hadron Collider). It's so private that it doesn't even ask for your personal details when you sign up, just your 'Display name' (see screenshot below).

Gmail also encrypts emails, but only in messages sent to other Gmail accounts. We wouldn't recommend trying to encrypt emails in Outlook – it's a real palaver. If you are sending a lot of sensitive information, we suggest you use Gmail or ProtonMail instead.



ProtonMail asks only for your 'Display name' – no personal details

14 Switch to a more private browser

Which browser is best for protecting your privacy? It largely depends on how you configure the settings and what privacy risks you're most concerned about.

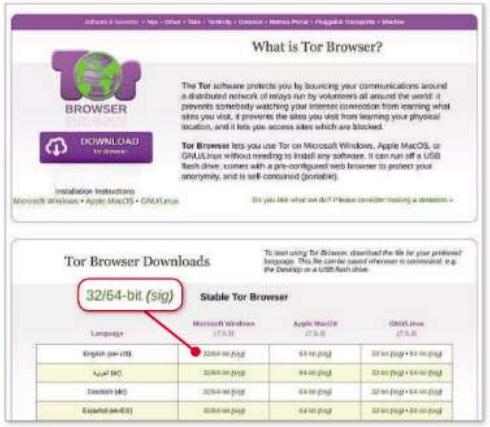
If you don't want Google hoovering up your data, don't use Chrome. Firefox might be a better choice. Its developer Mozilla promises not to share your data with others, and last year created a tab specifically for privacy settings, which is available when you open the browser to make sure you have access. The company has also stopped advertising on Facebook following the Cambridge Analytica scandal. This won't strengthen your privacy directly, but it's a reassuring sign that it takes the problem seriously.

There are other good options, notably Opera (www.opera.com) and Vivaldi (https://vivaldi.com). The latter is made by the founder of Opera, after it was bought by a Chinese consortium (see tip 1 on page 51 for more). Opera has a few key features that help protect your privacy, notably a built-in VPN (see tip 11, page 55) and an advert blocker.

There are two browsers specifically designed with privacy in mind: Epic and Brave. Epic (www.epicbrowser.com) is always in private mode, so all cookies and trackers are deleted when you close it. It won't save details you type into online forms or a record of websites you visit, apart from a short history for the back and forward buttons.

It even blocks ultrasound signals that websites send to your phone to coordinate tracking. Key settings such as Do Not Track are always on, and it uses its own search engine to keep you off Google.

Brave (www.brave.com) also has privacy tools built in, as part of its mission to "fix the web". Co-founded by Mozilla co-creator Brendan Eich, it's easier to use than Epic, though both browsers may feel a little odd after years of using Internet Explorer, Chrome or Firefox. Brave blocks JavaScript, sends you automatically to HTTPS sites (when the option is available), and blocks adverts and trackers. It's currently developing a new feature that makes it easier to use Tor (see following tip) in private browsing sessions.



Click this link to download the Tor Browser

15 Browse the web using Tor

First used by the US Navy, Tor is privacy software that disguises your identity by moving your web traffic across servers, building up layers of encryption like the layers of an onion (TOR is short for 'the onion router'). It gives you a different IP address every time you send or request data, disguising your actual one. Some antivirus programs, suspicious of Tor's privacy techniques, may show a warning when you download it, but it's safe to use. It's now run by a non-profit organisation led by computer scientists in Massachusetts.

To use Tor, you need to download its browser from www.snipca.com/27365. Click the '32/64-bit' link at the top, next to 'English en-US' (see screenshot above). We also suggest you visit www.snipca.com/27364, scroll down and read the section headed 'Want Tor to really work?', which is a handy list of useful information. It explains some of the side effects of using TOR – some browser plug-ins may not work, for example – and warns you about unsafe actions while browsing in Tor, including opening downloaded documents.

As all this indicates, using Tor isn't something you should do lightly. It essentially means entering the dark web, a place of untraceable anonymity, often exploited by criminals. But it's also used by honourable organisations that rely on absolute privacy: the police, medical researchers, whistleblowing journalists, and human-rights groups, for example.

Tor itself is perfectly legal and won't give you a list of dubious websites to visit. It simply provides the means to browse the web without anyone knowing what you're doing. And we mean *anyone*: not Google, Facebook, Mark Zuckerberg, Cambridge Analytica, Donald Trump, Vladimir Putin, Kim Jong-un, Darth Vader or the Daleks. It's your ultimate weapon in the ongoing battle to stay private online. CA

HOW I STAY PRIVATE ONLINE

I write about privacy and security for a living, so you'd expect me to follow a strict privacy regime.

The best advice I can offer is this: do as I say, not as I do. The Facebook/Cambridge Analytica scandal has helped highlight the importance of data privacy, and while the best protection is strong laws that keep Silicon Valley tech giants in line, there are plenty of tools to help. And yet I don't use as many as I should. It's simply too easy to put it all off until tomorrow.

However, I do have Adblock Plus and HTTPS Everywhere installed in Chrome. I've also set my Facebook account so only friends can see it, and regularly go through my Google dashboard (https://myaccount.google.com/dashboard) looking for anything untoward.

I also keep the Facebook app off my smartphone, mostly because it's drains my battery and wastes my time, and use the Private Internet Access VPN (www.privateinternetaccess.com) on my laptop when I'm working in a cafe.

Next on my privacy to-do list, I plan to deactivate Facebook as a half-step towards deleting it, and trying out a browser that's not made by Google (probably Vivaldi).

Also in Facebook, I've removed as much as possible from the list of 'data points' it uses to target adverts. For Google, I've turned off location tracking.

Nicole Kobie

NEXT ISSUE On sale Wednesday 25 April

ON SALE Weds 25 Apr

Can You Beat Dementia Using Your Tech?

Boost your brain and prevent memory loss

Plus
- New Outlook.com tested – better than Gmail?
- Where HAS it gone? Find missing settings

Subscribe to Computeractive at www.getcomputeractive.co.uk