readers' writes

Oh dear. We haven't got much right recently. One reader takes issue with a software review in the January 02 issue, while another wants us to get our facts right about wardriving. Someone did find something useful in the February issue, however: another reader's letter

Doorstep undesirables

Can anyone explain to me why the price of the DVD edition of *PC Advisor* is a whole £2.50 more than the CD edition?
Dave Allen, via email

Nel Staveley-Dick replies: we always aim to produce a magazine of the best quality at the lowest possible price for our readers. However, the greater cost for the DVD production is something we cannot avoid. The DVD itself is more expensive to buy and reproduce. It also includes additional programs and video not available on the CD, all of which inevitably push up the price.

Wireless access wars

Two articles recently appeared on PCAdvisor.co.uk regarding the topic of wardriving and wireless networks. These seem to be misguided, however, as to what wardriving is, how it is done and the code of ethics that wardrivers follow.

In the first article I found the quote: "Hackers can intercept unencrypted files by using a computer to dial through lists of telephone numbers searching for data, or by setting up a homemade antenna to detect insecure networks which is known as wardialling."

Wardriving does not involve dialling telephone numbers. Wardriving uses homemade antennas and wireless-equipped computers to detect secure and insecure wireless networks.

From the second article I found the following quote: "Allegedly, so-called 'war drivers' looking to take down corporate networks use similar systems every day."

We do not look to take down corporate networks. Wardrivers only look for the wireless access point's presence and plot it on a map. We do not in any way attempt to gain access to the network behind this access point or try to break into it.

The analogy would be to dial a phone number, hanging up after the first ring. We know there's a phone on the other side, but have no idea about what's behind it – and we don't try to find out what's behind it. Our only purpose is to alert users of wireless networks about the risk of not securing them.

Here's another quote: "People look for unprotected high-speed bandwidth and then use it to download loads of files." While a number of people will use insecure access points for these purposes, they wouldn't be wardrivers.

Wardrivers do not stop when we find an access point and try to perform these activities. We just keep moving which, given the range of these wireless networks (a hundred yards at best), means we're only in range of it for a few seconds. Not even enough to find out what's behind the access point.

Someone that breaks into these networks via a wireless access point is a criminal, plain and simple. We take very specific measures, such as disabling vital network protocols on our computers, to make sure that we do not connect in any way to the networks behind the wireless access points we find.

A good proportion of wardrivers hold security certifications that would be instantly revoked if we performed any such illegal activities. We would also be banned for life from obtaining any certification (and probably a job) in security or IT. So we have to be very careful about what we do.
Michael Puchol, security consultant, Sonar Security

Andrew Charlesworth replies: we're very grateful for your clarification of the issues surrounding wardriving and for a firsthand account of your activities. There's an update on these issues in this month's Behind the news on page 26.

Getting directions

I was disappointed with the review of the GPS 3400 Navman on page 52 of your January 03 issue. I found that the remarkably sensitive GPS (global positioning system) receiver works well whether outside, inside a moving car or in a boat cabin, with no need for a separate external antenna and power supply. (Its own 'iffy' car power supply can easily be adapted to fit any vehicle.)

Navman is very versatile and the positional precision and name detail of even the most insignificant streets in country towns, shown by the supplied road cartography, is impressive. In addition to the supplied road cartography I have mine running with a vast tract of detailed Ordnance Survey maps and two separate sea navigation systems with abundant marine charts. I can use it to guide me on roadmaps to Dartmoor, switch to maps for walking or cycling then, next week, use it on my boat.

I was a total cynic about PDAs (personal digital assistants) until I installed Navman on to my iPaq device. It now gives me a great deal of enjoyment,

← Unlike our reviewer who wasn't impressed with the Navman GPS 3400, Colin Jones sees it as a useful and enjoyable device

whether I'm using it for navigation, business or boat assistance.
Colin Jones, via email

Calmed by a cup of coffee

What a super service you have rendered me, and I guess many other people, by publishing George Monaghan's letter as the Star letter in February 02's Readers' writes.

I was on my way out to buy an upgrade from Windows 98 SE to XP, plus the necessary extra RAM to run it, when I paused to read Readers' writes over a cup of coffee. How pleased I am to have saved a useful sum of money, plus the raised blood pressure I would suffered had I, too, had my PC seize up on me because of Bill Gates' snooping software.

Please tell us when Microsoft has cleansed XP of that nasty feature so that we will know when we can safely upgrade. Meanwhile, it's 98 SE for me, warts and all.
Bob Ford, Suffolk

Broadband of contention

So here I am, all ready for broadband. My phoneline is capable and the price, if not that cheap, is worth it for the potential of 24-hour high-speed access so those 'site under construction' Flash animations will only take 10 minutes to load. Great. Until, that is, one looks at the ridiculous small print of many ISPs' conditions. None will guarantee not to accidentally pass on viruses or Trojans and so on (fair enough) but most insist that you, the customer, are responsible for any you transmit. If the ISP inadvertently lets a virus through then it's the customer's fault!

Rife is the condition that the service can be down or withdrawn for any reason without a refund, so forget the expense of computer equipment or technical staff. An ISP only needs to employ someone skilled in taking your money. Most service providers have also inserted a clause exempting themselves from having to provide a service 'fit for the purpose', which I thought was illegal. Add to that their 'right of access' and don't be surprised if signing up obliges you to provide ISP staff with free B&B if you happen to live somewhere pretty.

My main point is, with hundreds of pounds at stake, how many current broadband service contracts are actually worth the pixels they're displayed with?
Will Walker, Norwich

Banking on online security

Recently while on the internet I received a pop-up message stating that my bank details could be seen and accessed while online. If I wanted to obtain better security I should click the ok button immediately. I may be a bit of a pessimist but something didn't sound right, so I disconnected.

Later, using the Restore CD provided with my laptop, I wiped the hard drive in the hope I would erase all data and have a 'clean slate' so to speak. Am I correct or are my bank details still visible? And was this a genuine Windows warning or just some hacker trying to access my husband's hard-earned cash?
Jak Harrison, via email

Ursula Seymour replies: it's always a good idea to be wary of such claims as internet and email scams proliferate. But you'll probably find that this pop-up was an advert for some kind of software that promises to keep your bank details hidden from potential hackers, rather than the result of anyone actually trying to access your personal information.

If you do use your computer to surf the web, particularly via an always-on broadband connection, it is well worth investing in some reputable firewall software that will keep all your details locked away from prying eyes. Norton and McAfee both offer such software, and Norton Personal Firewall 2003 (see review February 03) offers a special feature that allows you to ensure any personal details you want to keep safe are never sent out without your permission. ■

Star letter

I read with dread about the new Teleadapt SIMbackup product mentioned in February 02's Top gear (page 35). This easy-to-use device is designed to copy SIM card information to provide users with a backup.

This means that thieves who target mobile phones will now be able to copy a SIM card, rewrite theirs and use someone else's account. The best bit is that phone companies don't check the IMEI number of phones, just the SIM card number. I admit the SIMbackup device may only read the phonebook, but it's just a stone's throw from copying SIM cards completely. The technology already exists.
Matthew Webber, email

Ursula Seymour replies: the SIMbackup requires you to enter the security code for your SIM card, so really it is no different from when a thief steals your phone with the card intact. This technology doesn't actually change the situation, it simply makes it easier for you to back up the numbers held on your phone.

Our star letter writer wins a Canon SmartBase MPC400, worth £249 inc VAT. This four-colour, multifunction device combines a printer, copier and scanner in one compact flatbed unit. See www.canon.co.uk/multifunction for more information.

If you want to air your views in these pages, please write to* PC Advisor, *FREEPOST 20 LON87018, London W1E 4AN, fax us on 020 7580 1935, or email us at pcadvisor_letters@idg.com. Please mark emails 'Readers' writes' in the subject heading.