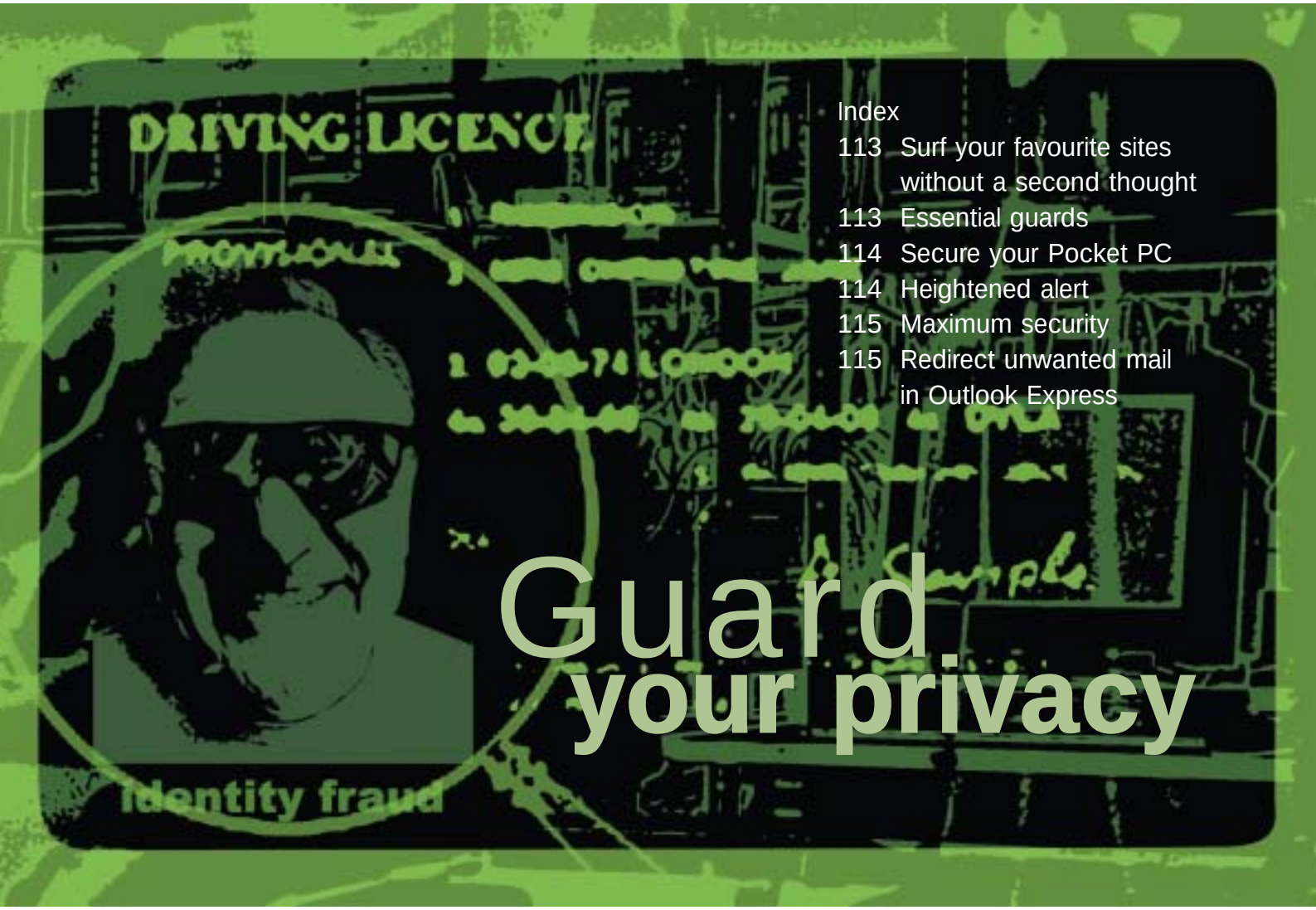
workshop



Index

113 Surf your favourite sites without a second thought
113 Essential guards
114 Secure your Pocket PC
114 Heightened alert
115 Maximum security
115 Redirect unwanted mail in Outlook Express

Guard your privacy

Nowadays everything we do and every transaction we undertake seems to be tracked and recorded. Our details are sold and otherwise exploited and, in return, we get more spam than ever. Daniel Tynan explains the steps required to take back your privacy

As this issue's Broadband Advisor feature illustrates (see page 128), our increasing reliance on the internet for communication is attracting some unwelcome attention. It's possible for our each and every keystroke to be noted and reported back to whomever it will prove useful – whether it's your boss, a jealous colleague or a hacker who gets lucky.

Usually, such monitoring activity merely serves to make us nervous and a bit more cautious about the content of our emails and how secure our server is. But if someone does manage to get their hands on information about you, whether via a website or electronic communication, they can exploit it in all sorts of ways.

The most obvious is making illicit use of your credit card details, but your name and address can be abused too. There's an increasing trend towards data collection and sharing which is valuable for marketing purposes, for example. But, taken to the extreme, with a few key pieces of information it's actually possible for someone to completely take over your life.

In February of this year, for example, a holidaymaker from Bristol was arrested by the FBI while in South Africa and accused of conning US citizens out of several million dollars. It wasn't until several days after making international news headlines that it finally emerged that 72-year-old Derek Bond was the victim of identity theft.

Just a few weeks earlier, BBC reporter Paul Kenyon stole home secretary David

ILLUSTRATION: SARAH AULD

Blunkett's identity to show how easy it was to do so. A name and address were enough to set the ball rolling and enable Kenyon to lay claim to Blunkett's birth certificate and to then procure a provisional driving licence.

Neither example was effected using a PC but identity fraud is already the fastest growing crime and insecure electronic communications only make it easier still. These days, what you do online can affect you offline and vice versa.

If you want your personal life to remain just that, the best defence is to closely guard your PC and its contents and to make sensible use of communications. Here's how to ensure that your privacy remains secure.

Essential guards

These tips give you an excellent start in regaining your privacy with little sacrifice or effort.

• Opt out early and often If a website offers you the opportunity to receive 'special offers' from 'valuable sponsors', politely decline. Most sites are unlikely to abuse contact information but they may share data with third parties or be bought out by a company with less regard for your privacy.

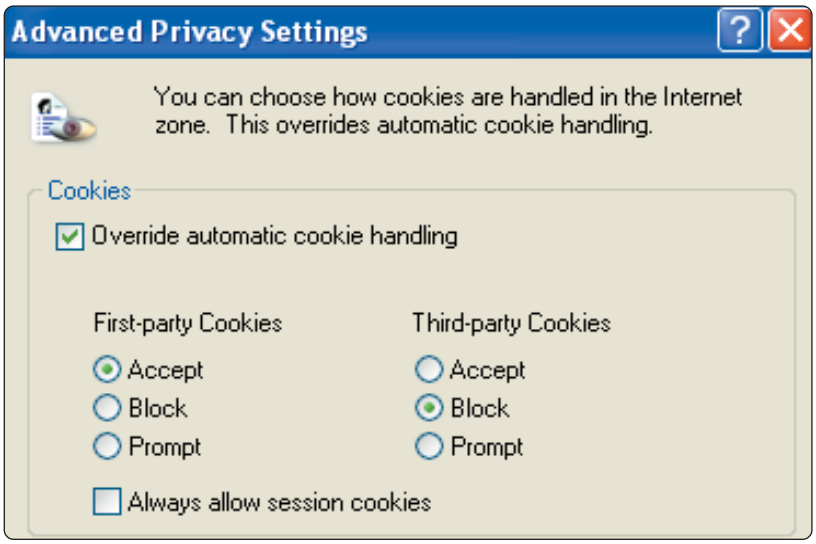
• Don't get personal at work If you use your employer's PC or internet access to send a personal note, there's not a lot to stop them reading it, though there ought to be a clear communications policy outlining email use and what use may be made of monitored information. For personal messages use a private web mail account.

• Surf smarter Your boss may watch where you go on the web so save online games and chatrooms for your own time. Don't do anything on your work PC that you wouldn't do if you knew someone was staring over your shoulder, is the advice of the Privacy Foundation (www.privacyfoundation.org).

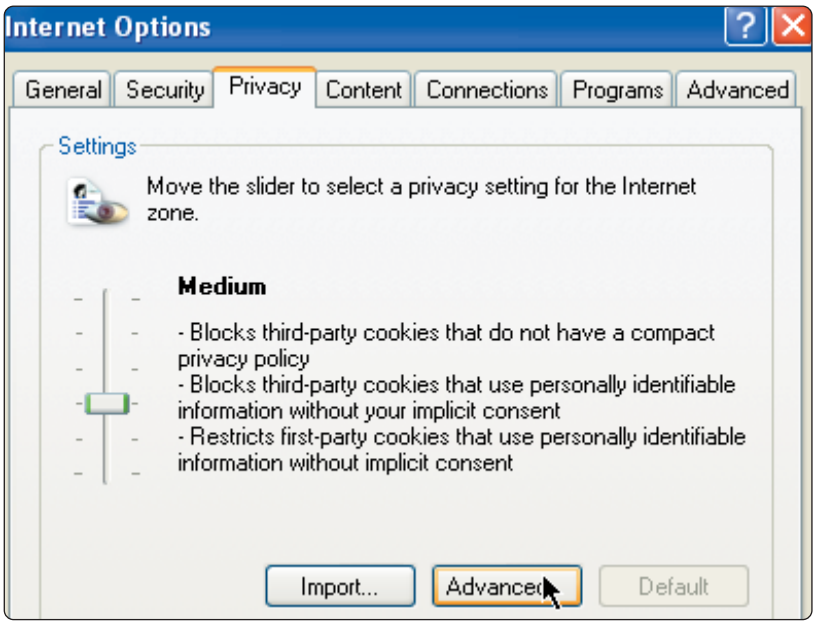
• Use a front Establish a second account with Hotmail or Yahoo Mail and use it when registering at websites so spam goes there instead of clogging up your primary inbox. Similarly, don't publish your private email address on your personal website or in online discussion forums where spambots can harvest it.

Surf your favourite sites without a second thought

One of the simplest methods of covering your online tracks is to block the third-party cookies that monitor your movements, often in the name of assisting your logins to favoured sites. Shareware packages such as Cookie Crusher are one answer, but it's cheaper to start by adjusting your browser settings to be more discerning.



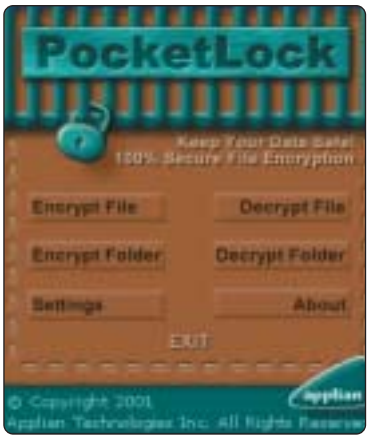
1 Launch Internet Explorer and, from its toolbar, choose Tools, Internet Options, Privacy to bring up a sliding access scale and site-by-site permission settings. Adjust these as you see fit



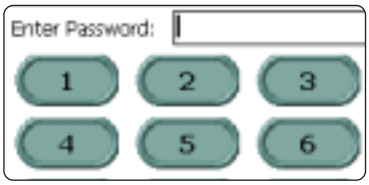
2 Internet Explorer provides a range of security settings. Under the Privacy tab, click Advanced and tick the box to set IE to override automatic cookie handling. Then select the Block radio button under the handling options for third-party cookies. Now, however much you like a particular site, its owners won't be privy to where else your loyalties lie

Secure your Pocket PC

Should you lose your laptop or PDA, someone else is likely to find it. But if you encrypt your files the finder won't be able to get to your data. CenturionSoft's (www.centurionsoft.com) SoftClan E-Cryptor secures files on your laptop with 128bit encryption; LinkeSoft's (linkesoft.com) Secret 2.7 shareware does the same for Palms; while Applian's (www.applian.com) PocketLock program works with Pocket PCs.



1 Data encryption is especially important if you're using a mobile device. Download Applian's PocketLock and choose a numerical password which grants access to the encryption program



2 Select the folder in which encrypted files are to be stored on your Pocket PC device. You should now be able to send and receive files without fear of interception

• Keep it to yourself Most sweepstakes, surveys and product warranty cards are merely cheap ways of gathering your data. Unless you're getting something of real value in exchange, don't bother filling them out.

• Be antisocial Guard your National Insurance number jealously. Few entities beyond the Inland Revenue and your employer really require it and access to it makes it all too easy to cross-reference databases that should never come near each other.

• Check your credit history Order an annual credit report. If you're a victim of identity theft you'll have a better chance of catching it early and you'll minimise the hassles in recovering your financial health, claims the Privacy Rights Clearinghouse (www.privacyrights.org). You can order reports for £2 or £3 from Equifax (www.equifax.co.uk), Experian (www.experian.com) or Trans Union (www.tuc.com). It's free if a lender has recently turned down your credit request.

Heightened alert

The following tips take a little more effort, but they can buy you a lot more privacy. Some require you to install and configure software, while others may take longer to prove their worth. Register your details with marketing controlling bodies and opt out where you can and you'll find the flow of unwanted mails will abate eventually. Finally, don't lose a healthy dose of cynicism – it will stand you in good stead.

• Ease your pane Leaving open the Preview Pane in your email program could allow malicious spam messages to launch JavaScript apps on your PC. To close it in Outlook Express, select View, Layout and then uncheck the Show Preview Pane box. In Netscape Mail, highlight a message in your inbox, open the View menu and uncheck Message.

• Engage in counterespionage Many free applications (especially file-sharing programs) install spyware software that tracks your movements online and sends ads based on your perceived interests. To detect and delete spyware, use a utility such as Lavasoft's Ad-aware (www.lavasoftusa.com/aaw.html).

• Install a firewall Essential gear for broadband users, a firewall such as Zone Labs' ZoneAlarm (www.zonelabs.com) is useful for anyone who logs a lot of internet time. Besides fending off hackers, firewalls can tell you if any program (such as a Trojan horse or spyware) is trying to send data to the net behind your back.

• Be wary of attachments A good antivirus app such as Norton's is essential, but commonsense also helps. For example, never open attached files unless they're from someone you know and you were expecting them. Friends could unwittingly send you a virus, so check with them first before opening dubious attachments.

• Lower your profile Ask to be removed from online directories – unless you want everyone to have access to your name, address and phone number. The site's privacy policy will usually tell you how to do this. For example, look at http://yell.com/legal/privacy/home.html.

• Unsubscribe with caution Some unsolicited email is sent by legitimate groups that honour unsubscribe requests. But spammers use such requests to verify email addresses and send you more spam. How do you tell the difference? If the email tries to drive you to a website, look up the site's domain registration on Whois (www.whois.net).

Does the record list a valid phone number and street address? Most spammers use fake addresses or mailboxes. Is it coming from overseas? Many spammers operate offshore. Is the administrator's email address from a free account? Legitimate businesses typically don't use them. If you're still unsure, delete and don't unsubscribe.

• Get delisted Tell the Direct Marketing Association to take you off its members' lists. You can do this for a nominal fee online or for free by post. This will reduce (though not eliminate) the junk mail, spam and unwanted calls you receive, but you may not see a difference for about six months.

• Disapprove credit offers It is possible to opt out of getting preapproved credit offers by calling the credit reporting agencies such as Experian we've already listed. You'll need to give your address, phone number and National Insurance number. This cuts down on junk mail and makes identity theft harder for crooks who might steal such offers from your mailbox.

Maximum security

You don't have to look very hard on the internet to find reports of the far-reaching effects of both internal and external hacking. A Coca-Cola employee recently demonstrated his concern for 450 of his fellow workers by accessing their salary information.

The onus was then on the victims to check their credit cards and banking details hadn't been abused while Coca-Cola ended up footing the bill for concerned employees wanting copies of their credit reports.

If you've ever been the target of an identity thief – or worry that you one day will be – you're probably willing to trade convenience for confidentiality. The following steps show you how to ramp up your security measures to the max.

• Scramble your messages If you must send sensitive mail (such as salary details or trade secrets), make sure you encrypt the text. Try these tools: PGP (www.pgpi.org), Indicii Salus (www.indiciisalus.com) or Sendmail (www.sendmail.com). Recipients need these tools too so they're able to read your encrypted mail.

• Protect your plastic Call your bank, obtain a credit card with a low limit and use it only for online purchases. If someone fraudulently misuses it you can dispute the charges and close the account with minimum hassle. And consider getting disposable credit cards – numbers linked to your account valid for only a single purchase.

• Don't get fresh Let your data go stale so that it's no use to anyone. Don't update address, telephone or other personal info as it changes. Your data will eventually become obsolete and in the meantime you won't be troubled by unwanted mail or other attempts to contact you.

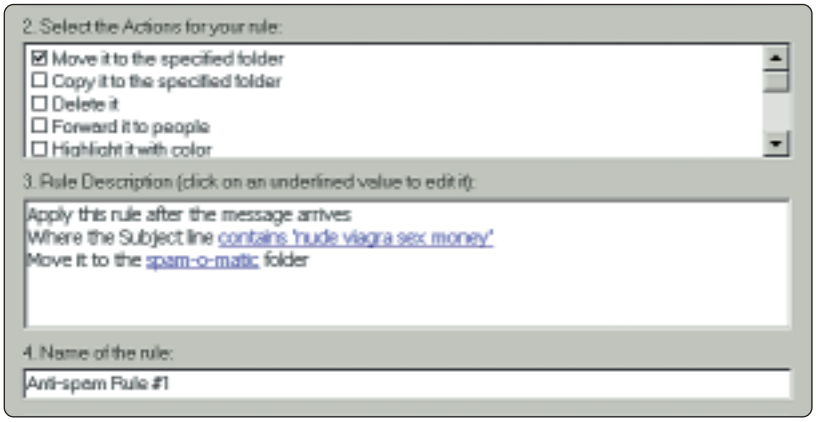
• Be circumspect Tony Soprano never spills the beans when he's on a mobile phone and neither should you. Wireless communications are still not totally secure so never transmit sensitive data wirelessly from your PDA or laptop.

• Use a PO box If you must give a mailing address, rent a post office or private mailbox to help keep your personal address confidential and stop the identity thieves in their tracks. ■

Redirect unwanted mail in Outlook Express

A wash in a flood of spam? Use your email package's mail filters to stem the tide. They won't stop the deluge entirely, but they can slow the flow. The following mail filters work with Outlook Express 6.x. It works by rerouting incoming mail according to user-defined rules and, if you so choose, you can then examine the filtered mail at leisure before permanently trashing it.

1 In Outlook Express select Tools, Message Rules, Mail. If one or more rules have already been set up, click the New button. In the New Mail Rule dialog box, select the conditions under which the filter rule should be applied. You probably want to prevent emails containing offensive words in the subject heading, for instance, so tick the appropriate box to tell Outlook this. Select the action you want the filter to perform. Here, we've asked Outlook Express to Move it to the specified folder



2 In the Rule Description box, select the underlined phrase in 'Subject line contains specific words' and enter keywords that you want block: nude, viagra, sex and money are good starting points. Then hit ok. Specify (and name) the folder where you want spam to be redirected and, when prompted, choose a name for your filter rule