

How to keep secrets safe when online snoops watch every click you make

WE'RE not usually prepared to share personal information about ourselves with people we have just met. You'd think we would be even more careful with people we've never met - but when we're online in the safety of our own homes we don't give it a second thought.

Our innocence in our online dealings - the way so many of us now conduct personal and business activities - leaves us very exposed. We're like sleepwalkers, blissfully ignorant of the danger but with each online click we're coming under the intrusive gaze of a surveillance society.

You know things are getting serious when officialdom voices its concern. The Information Commissioner's Office has reacted strongly against new Home Office plans to create a massive database of our phone calls, e-mails and internet activity. If it sees this as an attack on our civil liberties, why aren't we more concerned - and more careful?

It's all too easy to put our private information into the public arena without realising who might end up seeing it. We post online photos, details of relations, political views, even information about our sexual orientation on to sites such as Facebook, yet it's so easy for anybody to access and share this wealth of personal data. It's common knowledge that employers and prospective employers will check out your Facebook pages.

THE more we use the internet, the greater the risk. If you think you're shielded by Britain's data protection laws (intended to prevent information being used without prior knowledge or control), you're not. The onus is on us to protect the information that we put on to websites.

Even for people who avoid social networking, it's still difficult to ensure the security of personal information. Something as simple as sending an e-mail is also risky. These travel across the internet and can easily be intercepted. They're about as safe as sending a postcard containing personal and confidential information.

Search engines, webmail providers and internet service



KEY RISK: Private details can be made public via the internet



David Ford
Computer security expert

providers capture and store massive amounts of information on us, recorded and taken from our daily internet activity.

Take Google. You only have to look at its privacy policy to see how much information it has access to: personal information, details of searches we make and information about the websites we visit are just some examples of what Google collects "in order to provide (its) full range of services".

Just in case you weren't clear, its "full range of services" includes selling targeted advertisements to you based on this very data.

In fact, eavesdropping on our internet activity is pretty big business. To date, the UK's three largest internet service providers (BT, TalkTalk and Virgin Media) have signed up to Phorm, a company that acquires and analyses your

personal data and uses it to place adverts on behalf of companies. By going through your internet service provider, these companies have access to a much broader pool of information, allowing them to build up a detailed profile of you.

We spend billions each year online. We entrust our debit and credit card details to the computer systems of large and small companies alike. For most of us there's no comeback but for some it can mean the emptying of their bank account.

There are criminal websites where credit card details can be purchased by the thousand for as little as 25p each. The banks and credit card firms want us to carry on using our plastic so the losses are usually made good in the end but who needs the aggravation?

How can you prevent it? Unless you're prepared to give

up shopping online altogether, there's not much you can do.

You could improve your chances by only shopping with reputable companies - although the well-known TK Maxx and Cotton Traders both had thousands of card details stolen from them in the past couple of years. They have both since rectified the problem. If you use a PC and bank with Cahoot you can use its webeard, which issues a unique number for every transaction. Short of that you have to hope that you're not one of the unlucky ones.

So if no one else is going to protect you, what can you do about your privacy generally?

First, make sure the people who carry your data will respect your privacy. You need to read those terms and conditions when you sign up to services, especially the free ones - do you really think people give away something for nothing? Make sure your internet service provider isn't selling your data.

Don't use a free e-mail provider unless you never say anything confidential in your e-mails. A Chinese journalist was jailed for 10 years because Yahoo! had no choice but to provide the country's authorities with details of an e-mail he sent through them.

SECOND, look after your confidential information. If you're typing data into a web form, check the connection is secure - there'll be a padlock on your browser to show you. Use encryption for confidential e-mails.

Third, think twice every time you're about to type your secrets on to the internet - it may seem like a good idea to tell your friends your latest exploits but imagine them on view to strangers or still there years later.

It's easy to conclude that while the beauty of the internet lies in its ease of use and availability of information, this is also one of its biggest drawbacks. It's now time to snap out of online "sleepwalking" and wake up to exercising the same caution that we do in everyday life.

So, if you don't like the idea of the postman reading your mail and you'd rather that a prospective employer didn't have easy access to photos of your weekend exploits, it's down to you to make sure your electronic fingerprint is secure and not going to cause you harm - because no one else will.

Exercise the same caution that you do in everyday life



securecoms
keeping your business your business