How safe is your identity?

Think your personal details are secure? Our research shows you may be revealing more than you expect online

Most Facebook users surveyed by Which? in May 2012 say they're worried about strangers accessing details they've posted. And 59% told us they can't keep up with the number of changes Facebook has made to its data security settings – an 11% rise since the last survey we ran in September 2011.

In our latest investigation into identity theft, we found details that can be used to commit ID fraud and other crimes accessible on Facebook and elsewhere on the internet. We hired online security experts to find out as much as they could about 10 volunteers, including a family of four and Which? editor Martyn Hocking. Our volunteers (see opposite) were all disturbed by how much personal data was available, especially as they all considered themselves to be internet savvy.

ID FRAUD GROWING

ID fraud is on the rise. Almost 36,000 cases were recorded in the first three months of 2012 – a 40% rise over the same period last year. In addition, facility takeover fraud – where someone unlawfully obtains and uses details to access a victim's account and operate it for financial gain – has almost doubled, with 10,501 cases reported in the first quarter of this year.

Richard Hurley, communications manager of fraud prevention service Cifas, says the rise is linked to online activity. 'The internet is a constantly evolving platform for consumers and, therefore, fraudsters. As a result, vast amounts of data can be stolen by stealth. In 2011, 74% of all identity frauds and 62% of all account takeovers had the hallmarks of having been both enabled and carried out online.'

ID fraud affects all of us, even if indirectly. Victims may get their money back if it's deemed they took reasonable care against fraud (see 'Stay safe offline, too', p71), but other costs, such as higher insurance premiums, are often borne by retailers and banks. And ultimately, these costs are passed on to consumers.

DETAILS PEOPLE DIVULGE

Since the advent of Facebook and other social networking sites, people are more willing than ever to make personal information public online. In a recent survey of 2,000 UK adults, 18% said they'd publish their town of birth online, while only 3% would give this information to a stranger over the phone; and 24% would state where they'd studied, while only 1% would do this over the phone.

Privacy settings that hide personal details can be applied to sites such as Facebook. But with more than half of those we surveyed saying they can't keep up with changes to these settings, it's easy to see how users might be unaware of what they are making public.

We contacted Facebook with our survey results, and it told us it has built-in tools which give users the ability to clearly see what they share, and with who, at the time they post.

WHAT FRAUDSTERS LOOK FOR

The act of searching for personal data on the internet with criminal intent is known as 'phoraging'. A determined ID fraudster may phorage around websites such as 192.com (see 'What is 192.com?', p70), Facebook and business networking site LinkedIn for >

PHOTOGRAPHY BY: CORBIS

Which? investigation

Using only their names, rough ages and an idea of where they live, our online security experts set about investigating three Which? employees and our member family. All information found was freely available on the internet at the time of the research.

Before we revealed the results to our volunteers, we asked them how careful they thought they were with their personal information online. Our experts gave each volunteer a security rating and advised them how they could be safer online.

Family details online

Which? readers Peter and Sarah told us: 'I think we are careful about our online usage. Our children both know never to share passwords, etc. They use Facebook and we've made sure that only friends can see their posts and pictures.'

Security Rating

Our experts found details of the family members through their extended family's Facebook pages. This led to further insight into their lives, including education details and photos of their home's interior. House pictures could be useful to a prospective burglar, as well as giving an indication of the owner's wealth.

Information found

Peter

Age, home address, occupation, mobile number, street photos, email address, area of work.

Sarah

Home address, names of mother, brother, sister and niece, recent whereabouts, occupation, maiden name, extensive family photos on Facebook, children's names.

Emily

School subjects, middle name, music tastes, area of residence, some publicly available photos on her Facebook profile.

Fraser

Date of birth, some publicly available photos on Facebook.

Our experts' verdict

The family were advised to make sure that friends and the wider family don't disclose information about them – although Peter doesn't use social networking himself, a worrying amount of information has been published online about him by his mother.

Although the children have secured their social networking profiles well, Sarah needs to restrict access to her account under the privacy settings. She should unpublish her mobile phone number as it could be a target for phishing attacks.

Photos of home interior found

Which? editor Martyn Hocking told us: 'I suspect there is a lot of information about me online. My job puts me in the media regularly and I am fairly active with social media. Most of my Facebook info is locked up but you can find out about me in press releases, on LinkedIn and so on.'

Security Rating

Not all of Martyn's Facebook information was secure.

Information found

Job title, phone number, home addresses, photos of his home's interior, purchase price of home, wife's name, career information.

Our experts' verdict

Martyn should remove photos that show the inside of his house – these could be an invitation for burglars to snoop around. He also needs to tweak his Facebook privacy settings to restrict who has access to his profile. An innocent status update saying that he was doing DIY in his weekend home could be an invitation for a burglar to visit his other house, knowing that Martyn wouldn't be there. It's good online practice to only disclose this afterwards.

Targeted phishing attack possible

Which? researcher Hazel told us: 'I'm fairly savvy, and try to make sure I don't divulge too much. But I'm slow to update privacy settings – I can't keep up with all of Facebook's changes! I've got a few accounts online that I never use, but haven't gone back to check what info is shown about me there.'

Security Rating

Our security experts found that Hazel has shared a lot of information about herself – enough for a hacker to execute a very targeted phishing attack. They advised her to improve her online security.

Information found

Job title, previous address, place of birth, personality traits, photos of old home, substantial amount of personal photos across various social networks.

Our experts' verdict

Hazel should reduce the amount of information she posts online, and change the privacy settings on her social media accounts to restrict strangers from viewing her photos. She could also delete the social networking accounts she never uses.

Phone number and address found

Which? executive assistant Ros Mari told us: 'I probably have a public profile due to my online business. It's been running for 12 years so I expect there's information about it in directories and other sites. But there shouldn't be much personal information about me online.'

Security Rating

Ros Mari's security settings on the various social network sites she uses are good and she shares only general details about herself there.

Information found

Job title, interests, nationality, photos, address, phone number.

Our experts' verdict

Ros Mari should be careful when posting information about her interests, as these could be used by a hacker to guess passwords or form a targeted phishing attack. She should also consider removing her phone number.

GO ONLINE For more information on how to protect yourself from ID fraud, including our useful video advice guide, go to **www.which.co.uk/idprotect**

nuggets of information to build up a profile of a victim or guess passwords.

For example, they may find a birth town, a date of birth or even a birthday greeting posted on a Facebook profile, while 192.com provides full address details – both present and past.

In the world of ID fraud, getting some personal information is a ticket to getting more. Having already found contact details on the internet, a fraudster may email a potential victim posing as a genuine organisation, such as a bank, in an attempt to secure more information.

When this is done in a targeted way it's called 'spear phishing'. Emails of this nature may display the recipient's full name, or have some references to their personal life, to appear genuine. These targeted emails are on the rise, and are far more successful for fraudsters. Research shows that a targeted email is more than 20 times more likely to be opened than a general phishing email, and 10 times more likely to be clicked and acted on.

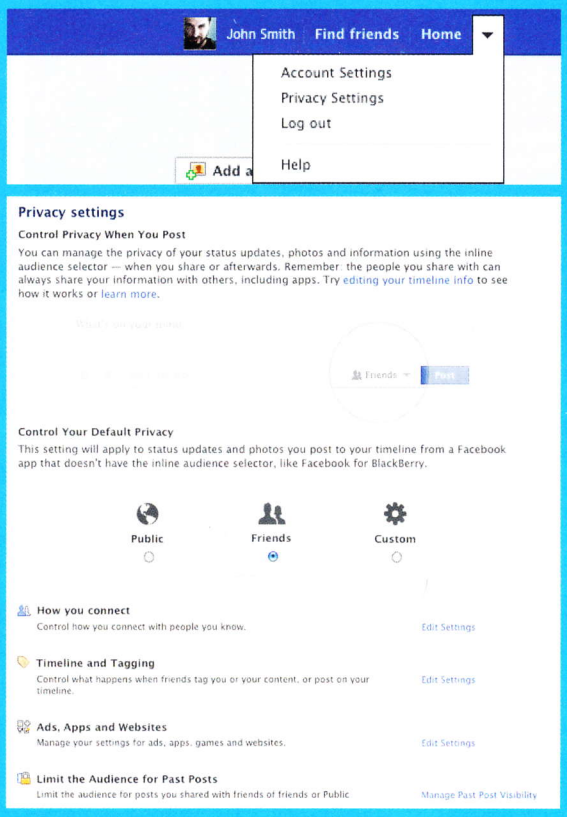
If a fraudster finds or guesses enough information to pretend they are you when dealing with an organisation that you deal with, they can access accounts, change addresses, transfer money, order statements, run up credit cards, order new cards and even open new accounts.

WHAT IS 192.COM?

192.com is an online directory of UK residential and business records. Built from electoral rolls, Companies House data, phone directories and the Births, Marriages and Deaths Index, the records are intended to be useful for anyone wishing to contact friends and family, and to check and verify small businesses and individuals.

You can find top-level address information and phone numbers free, or pay for access to more detailed records. These aren't complete, but you may be able to find age, full address, length of residency, property information and birth, marriage and death records. Birth records usually contain a mother's maiden name – particularly useful for an ID fraudster. You can complete a form available on 192.com's website to request that your listing is removed.

Also consider removing your details from the edited version of the electoral roll. Do this by filling out the relevant section of the electoral roll form sent out by your local authority each year.



Facebook Timeline

Facebook Timeline is a new feature being rolled out on Facebook, which visually displays all of your activity going back to when you signed up. Photos, friends added, status updates and anything you've posted are all on a single page, indexed by year and month.

It makes it easier for other users to see what you've been up to, but also potentially to find personal details that you'd rather not reveal.

To restrict access to your Timeline to friends only, click on the arrow in the top-right screen next to 'Home', choose 'Privacy settings' from the drop-down menu, scroll down to 'Limit the audience for past posts' and click on 'Manage past post visibility'.

To modify, remove, or change the privacy settings of any basic information you have added to your Profile summary, from your profile page click on 'About' ('Info' if you're not using Timeline), click on 'Edit' in the relevant box, and either modify your information, or click on the little drop down menu on the right of each piece of information to change your privacy settings.

Checklist

How to protect your identity online

- Only accept social network friend requests from people you know. Someone posing as an interesting person asking to become friends may actually be an ID thief.
- Limit what you post. Do you really need to share your email address? Most social network websites have a messaging service built in. Avoid posting your birth date, phone number and other sensitive personal information.
- Use passwords that are hard to guess. In a survey of 2,000 UK adults, 57% said they use data easily available on social network sites, such as a pet's name or a favourite sports team.

  Instead, use long passwords that contain a mixture of upper and lower-case letters, numbers and symbols. Avoid using a simple word that appears in the dictionary, as password hacking software may be able to guess it.
- Check your social network privacy settings (see 'Facebook Timeline, above).
- Try Secure.me. This Facebook app scans your page and alerts you if it finds information that it deems is risky.
- Change passwords regularly, and use different passwords for different accounts.
- View emails and calls that you weren't expecting with suspicion, regardless of the apparent name of the organisation contacting you. Don't respond to any unsolicited emails/calls asking for bank details.
- Keep your internet browser and computer security software up to date. Good software will alert you of any attacks on your security. See reviews of 21 packages at **www.which.co.uk/security**
- When shopping online, check that the web address changes from 'http:' to the more secure 'https:' at the checkout.

Stay safe offline, too

Not all ID fraud is hi-tech, of course. We all handle receipts and bank statements as part of our everyday lives. Crumpling them up and throwing them away isn't a safe way to dispose of them, as they may be found by a fraudster. A good shredder will destroy your personal details on these documents effectively (see below).

ACT QUICKLY

Unexpectedly being refused credit, seeing suspicious activity on your bank or credit card statement and not receiving mail in the post are possible signs that you may have been an ID fraud victim.

If you are, act quickly. You may be contacted by your card company or bank – otherwise contact them and call the police to get a crime number. Make a note of phone calls (the time, date and who you spoke to) and keep any correspondence.

Under the Consumer Credit Act and Lending Code, you're not liable for debts of more than £50 run up by a fraudster, or any amount at all after the card is reported missing, provided that you've not been grossly negligent or fraudulent – for example by writing down your Pin number and keeping it in your wallet. Although the most you'll pay is £50, this amount is often waived by the bank or card provider.

If something has put you at risk of ID fraud, such as sensitve documents being stolen, contact Cifas as well on 0330 100 0180 or at www.cifas.org.uk. It will flag your name with the businesses registered with it to allow for extra security checks before any transaction can take place.

Checklist

How to protect your identity offline

- **Keep your important documents,** cheque books and cards safe and well hidden.
- **Shred important documents and receipts** that you no longer need.
- **When you move house,** immediately tell all organisations you deal with. Use Royal Mail's redirection service for a year after you move to make sure any mail is sent on to your new address.
- **Be extra vigilant** if you live in a block of flats or your mail is delivered to a communal area, as it's is easier to steal.
- **Alert Royal Mail** if you suspect your mail is being stolen.
- **Sign up with a credit reference agency** to receive a regular copy of your personal credit file. Go to **www.which.co.uk/report** for more details.

CASE STUDY

Credit checks

Karen Crook | 50 | IT manager | Linlithgow, West Lothian

Being a victim of ID fraud is especially baffling if you're very careful with your personal information. Karen Crook shreds documents, doesn't use social networking websites and only rarely shops online.

But earlier this year, a Littlewoods credit account was opened in her name and £630 spent on it buying rugs, bedding and furniture, with the goods to be delivered to a different address.

Karen checked with Littlewoods' fraud department and discovered that the account was opened even though the date of birth and number of years she'd been living at her address were incorrect.

Karen told us: 'I'm amazed how easy it's been for someone to get credit in my name, and I cannot see the point of the credit check if the searcher simply ignores the fact that some of the data was incorrect. It's caused me a lot of worry and hassle.'

We spoke to Equifax, the credit reference agency that carried out the credit check. It told us that there was no date of birth or previous address information on Karen's record, and that they informed Shop Direct (Littlewoods' parent company) that some data was missing. Based just on the information from Equifax, Shop Direct could not positively confirm date of birth and previous address, but it opened the account anyway. Shop Direct told us it carries out other fraud checks before account opening. But it appears that in this case, the checks failed to spot the fraudster.

LISTEN TO A PODCAST

On 29 May Oliver Crofton of Vigilante Bespoke, who investigated our volunteers, will speak with Deputy Technology Editor Andy Vandervell about how you can protect your digital data better and reveal just what data he was able to dig up on him. Also featured is technophile Stephen Fry, who'll be telling us about the gadgets he uses everyday. **www.which.co.uk/stephenfry**

Best Buy shredders

Not all shredders are the same. Go for a diamond-cut or cross-cut model for the best security. These machines shred documents into small pieces that are very difficult to put together again.

Strip and ribbon-cut shredders cut documents into long strips – these strips could potentially be pieced together by a determined thief.

Our best model on test is the Fellowes DS1. Alternatively, the cross-cut Swordfish 1000XC (£80) and diamond cut Swordfish 700DC (£49) are both Best Buys and available online.

Fellowes DS1 £90

Which? test score 90%

PROS This cross-cut shredder gobbles up paper, card, laminated documents, credit cards, paperclips and staples, all without hiccups. It takes 14 sheets of A4 in one go and has a large bin for the waste. There's also a touch-sensitive safety strip around the mouth, which stops the cutters if a hand strays too near.

CONS The touch-sensitive safety feature is a little oversensitive.

Cheapest high street store Comet, Robert Dyas