Digital Criminal Report

www.legalandgeneral.com

Legal & General

Executive Summary

Users of social networking sites are giving away vital information about themselves and their whereabouts which is being used by professional burglars to establish a list of potential targets, according to *The Digital Criminal Report*.

A survey of more than 2,000 social media users found that nearly four in ten, 38 per cent of users of sites such as Facebook and Twitter have posted status updates detailing their holiday plans and a third, 33 per cent of people have posted status updates saying that they are away for the weekend. Coupled with the finding that an alarmingly high proportion of users are prepared to be 'friends' online with people they don't really know, this presents a serious security risk for people's home and possessions.

Nearly a quarter, 23 per cent of social media users have discussed holiday plans "wall-to-wall" – outside the privacy of their own page – and 17 per cent of users reported seeing people's residential addresses posted on pages that can be seen by strangers.

As part of the report, an experiment was conducted to see how many UK social media users would accept a 'friend' invitation from a complete stranger. Of 100 'friend' or 'follow' requests issued to strangers selected at random, 13 were accepted on Facebook and 92 on Twitter, without any checks.

The survey confirmed that a large proportion of users use social media sites to connect with people who are essentially strangers: 79 per cent think they are a great way to track down people they "met on holiday", three quarters (75 per cent) feel that they are a good way to meet "friends of friends", and nearly half of people, 47 per cent like to use sites to meet new people based only on the person having a nice picture.

Other findings include:

- Nearly half, 48 per cent of respondents have no worries about the security or privacy of social networking sites.
- Of all social networking sites, Facebook creates the most concern with 46 per cent of respondents feeling that there are some security and privacy risks.
- The younger you are, the more likely you are to give information away concerning your whereabouts, with nearly two-thirds, 64 per cent of 16-24 year olds sharing their holiday plans – which could be a cause for concern for parents.
- 34 per cent of respondents have seen somebody else's mobile number posted on their social networking profile.
- 70 per cent of users think that social media sites are a great place to share photos of their cool new purchases and presents.
- Nearly one in ten, nine per cent of respondents have included their own mobile number and five per cent have included their address in the personal information section of social networking sites visible to friends.
- Some people are sharing mobile numbers and addresses directly with strangers: six per cent have written their phone number and three per cent have written their address "wall-to-wall" or on pages open to those who are not accepted contacts.
- Men are more blasé about personal information – 13 per cent have included their mobile number on their profile compared with just seven per cent of women and nine per cent of men have included their address compared with just four per cent of women.

This report alerts people to the fact that burglars are using social media sites and the ways in which they may be targeting their home and the tips we can all take to reduce the risk of being a target. We hope that this report will help people to enjoy using social media sites without putting their possessions and their homes in danger.

Introduction

Over recent years, as the internet has become an everyday tool for the vast majority of people[1], criminals have sought to capitalise on its use and cyber crime has firmly embedded itself in the consciousness of the mainstream media. As a result, the majority of us are aware of the existence of "phishing" e-mails[2] and suitably perturbed by the idea of somebody using the internet to commit identity theft[3] but there are other dangers posed by the development of the internet and social networking sites.

These days, people are often browsing the internet instead of trudging down the high street to buy clothes and groceries.[4] But it is not just the honest citizen who is surfing the web for a new television or an iPod. And the internet is not solely the preserve of the cyber thief. The good old-fashioned burglar is stepping into the 21st century and using Web 2.0, to help step through our front doors.

The Digital Criminal Report from Legal & General's general insurance business investigates how the internet and social media phenomenon is aiding and abetting criminals to commit burglaries more easily, and with a reduced risk of getting caught.

Getting to know all about you

Social networking sites are great fun, and people – rightly – want to use them to share things with their friends.[5] But social networking often takes private conversations into a more public forum and allows hundreds of people to effectively listen in.[6] People are passing on information to other users unwittingly and without due consideration of the risks involved.

A survey of more than 2,000 social media users conducted by Legal & General's general insurance business as part of this report found that nearly half have no worries about the security or privacy of social networking sites. Their habits are endangering the security of people's homes.

To produce this report, Legal & General worked with reformed burglar Michael Fraser, of BBC's *Beat the Burglar* programme, to investigate the very real threats to the security of our homes from social networking and the internet. Michael demonstrated a number of ways that criminals are using the web today to help them commit burglaries and how our lax attitudes in the way we use social media are exposing many of us to an increased risk of being a target.

The Sofa Stake-out

Michael was able to demonstrate how a burglar can use the content we share on sites such as Facebook, MySpace, Bebo and Twitter, to build a profile of a person to determine whether they are a suitable target and then "case the joint" using tools such as Google Earth and Street View.

1. http://www.nielsen-online.com/reports.jsp?section=pub_reports_intl&report=usage&period=monthly&panel_type=1&country=United%20Kingdom
2. http://www.birminghampost.net/birmingham-business/tm_objectid=17779433&method=full&siteid=50002&headline=consumers--confident--about-buying-on-the-web-name_page.html
3. http://www.computerweekly.com/Articles/2009/04/20/235682/most-britons-fear-recession-will-increase-id-crime.htm
4. http://www.dft.gov.uk/adobepdf/162469/221412/221513/438774/homeinternetreport.pdf
5. More than 1 billion photos uploaded to Facebook each month, more than 10 million videos uploaded each month, more than 1 billion pieces of content (web links, news stories, blog posts, notes, photos, etc.) shared each week and more than 2.5 million events created each month. (Global statistics) Facebook statistics: http://www.facebook.com/press/info.php?statistics
6. The survey by Legal & General of 2,000 social media users found that 37 per cent of facebook users, for example, have over a hundred friends

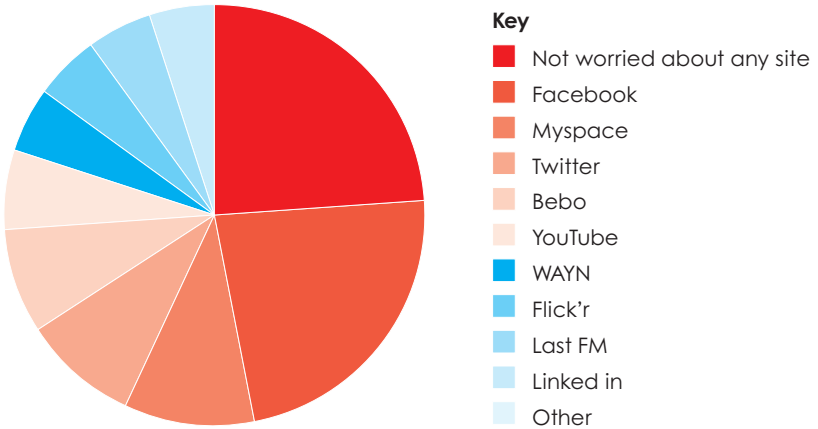
Part 1 – Online chatter seen as *safe as houses*

The rise of social networking sites has been explosive and they have revolutionised the way many people interact with their friends and family. A recent study by ComScore, a specialist digital market research company, found that nine out of ten 25-34 year old UK internet users visited a social networking site in May 2009.[7] The same research found that 29.4 million people accessed at least one social networking site in the UK in May, averaging 4.6 hours per visitor during the month – Facebook.com ranking as the most visited social networking site.

Yet in many respects our understanding of the security risks associated with these sites has lagged behind and this understanding desperately needs to catch up. As part of *The Digital Criminal Report*, Legal & General's general insurance business asked 2,000 British users of social media sites about their use of, and attitude towards, sites such as Facebook, Twitter, Myspace and Bebo.

Worryingly, British social media users are blasé about the security risks associated with social media sites – nearly half of respondents (48 per cent) have no worries about the security or privacy of social networking sites at all. Facebook is seen as the riskiest site for those who do foresee danger with 46 per cent of social media users feeling that there are some security and privacy risks.

Figure 1 Concerns about the security and privacy of various media sites



7. http://www.comscore.com/Press_Events/Press_Releases/2009/7/Nine_Out_of_Ten_25-34_Year_Old_U.K._Internet_Users_Visited_a_Social_Networking_Site_in_May_2009

Shouting about it

The research identified that many of us give away vital information and personal details to those who are "friends" or "followers". But the lines are evidently blurred between those who are bona fide pals and who are primarily "virtual friends" and some of these might not be your friends at all.

People are willing to make friends with people who they barely know. For example:

- 92 per cent of respondents feel that social media sites are a very good way to get back in touch with people that they have not seen for years
- Three-quarters feel that social networking sites are a good way to meet friends of friends
- Nearly eight in ten (79 per cent) consider social networking sites a good way to connect with people they met on holiday.

In some of these cases, the people that they are allowing to view all of their online posts are not particularly well known to them, and unfortunately may not have honest intentions.

In support of this report, an experiment was conducted to see how many UK social media users would accept a 'friend' invitation from a complete stranger. Of 100 'friend' or 'follow' requests issued to random strangers, 13 were accepted on Facebook and 92 on Twitter without any checks. This reaction could result in a complete stranger potentially being able to learn about a person's interests, location and movements in and out of their home.

Many people become involved in conversations online that unwittingly make them vulnerable by giving away details on their interests and hobbies.

A sucker for a pretty face

Most alarmingly nearly half of social media users (47 per cent) are willing to accept friend and follower requests based only on the person having a nice picture. Perhaps unsurprisingly more men (59 per cent) than women (42 per cent) were prone to falling for a pretty face.

Some of the people who are most susceptible of falling into the confidence of someone who is not to be trusted are those who are perhaps lonely and looking for love.

Michael Fraser says: "Women can target single men very easily: most single blokes will be happy to make friends with a good-looking woman who approaches them online, and then offer seemingly harmless information about their interests, whereabouts they live, whether they are into travelling, whether they are going on holiday any time soon… Once the conversation switches to Instant Messaging, it becomes even easier to extract information. Single men will jump at the chance to develop what they think is a genuine relationship."

PERSONALITY PROFILE OF TARGETS FOR THE PROFESSIONAL DIGITAL CRIMINAL:

The Animal Lover – less security-conscious, maybe a sign of a lonely person who will make friends with you online

The Chatterbox – people who just love to share information with anyone, build up a big bunch of friends online

The Loner – usually single people, who want to increase their friend total on social networking sites to make it appear that they are more popular

The Holiday Snapper – people who use social networking sites to talk about their holiday plans, share photos with friends and the world. These people also clearly have money…and possessions worth stealing

The New Joiner – newcomers to social sites are good targets. They start off with no friends, so a friend request and a message welcoming them and asking them about their interests will likely be accepted happily…

Groups and Fan pages on Facebook can be another good place to target – people reveal information on these pages about their interests and holiday plans, and you don't have to be accepted as a friend to see what they are saying. These are public conversations.

New joiners are also at risk. New members of sites like Facebook or Twitter tend to be slightly more naïve about its use and are initially overly keen to boost the number of friends/followers that they have, without considering the consequences.

Part 2 – Building a picture – Facebook, Twitter, Myspace etc

Why get to know you?

Social networking sites are most appealing for burglars as a way for them to get to know their target, without making an obvious connected link to the crime. Building up a personality profile and gathering knowledge not only gives the professional burglar the information he or she needs to target potential victims effectively – it also helps them to get away with the crime.

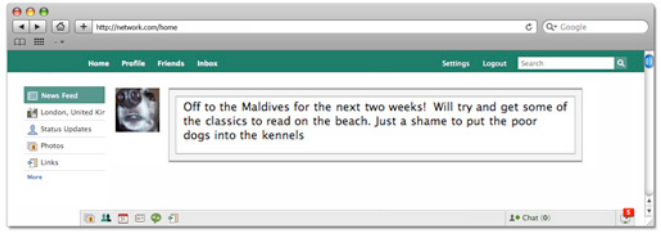
***Beat the Burglar*'s Michael Fraser says:**

"If a nosy neighbour should see a burglar removing a plasma screen from next door's house, and challenges the burglar, 99% of the time the burglar will get away with it if they answer with a nonchalant but slightly informed response so it sounds as though he is familiar with the victim. For example, 'Oh, Paul and Sue are having a rough time. He's moving in with me for a few days so I'm collecting his stuff for him'. There is a significant excitement factor for the digital criminal – can I find out that one extra bit of information about this person, this target, that will make the difference to carrying this off if challenged? He or she will be excited if they succeed in getting this."

The internet and social media now enable a burglar to start to assess the potential profitability of a victim by simply monitoring their social networking activity online, rather than walking the streets or driving around a potential location.

The Queen's English for a King's Ransom

A professional burglar will be looking for specific targets – normally wealthy, working individuals or couples – who will have the most profitable contents to steal. One way in which he will be able to establish his target's value is their use of language. He's unlikely to target somebody using reductive text speak.



Snoop Doggy Dog

The digital criminal is also very interested in knowing your attitude towards cats and dogs. While many may think that their dog is a deterrent, burglars traditionally used to look for 'Beware of the Dog' signs and doors or flaps for a pet to get in and out of a home.

Cats mean cat flaps – which make doors easier to break through as typically people do not reinforce the door around the section that has been replaced by the flap. Dogs mean lots of walking, going in and out through the front door, which means it is rarely fully locked, or will have less security, because of the inconvenience. With either, it means that burglar alarms are likely to be switched off so that they do not go off in response to the animal's movements.

Now a burglar can establish that someone is a pet owner by simply monitoring his prospective victim's Facebook/Twitter posts or by reviewing their listed interests and the groups they have joined. The group entitled "Dogs" has over 716,000 fans and is regularly updated with posts from people celebrating their dogs on the "reviews" page.

A picture tells a thousand words

People love to share photos online, but this can be potentially valuable information for a professional burglar as well. Our survey discovered that 70 per cent of users think that social media sites are a great place to share photos of their cool new purchases and presents.

People also frequently post photos of their pets – revealing that they are a pet owner which means a double whammy for them as a potential target for a burglar as previously discussed.

People also post photos of house-warming parties or summer BBQs, which show the interiors of homes, putting on display their home contents to the Digital Criminal as well as providing visual knowledge of entrance/exit points.

Michael Fraser says: "There is a certain 'keeping up with the Joneses' factor about people displaying their new purchases online. They are excited and want to show their friends. But when it comes to expensive items that are sought after on the black market, such as high definition televisions for example, it is advisable not to tell the world that these are now in your home."

Inviting them round

In reality, if the digital criminal identifies you as a prime target to burgle, he or she has the means and the know how to find out your address. But some of us don't even put them to the trouble of having to find this out.

A number of social networking sites include a section where you can display your address and mobile number amongst the "profile information". Sensibly, most people decide against including this information, but research carried out for *The Digital Criminal Report* found that 34 per cent of UK social media users have seen somebody else's mobile number posted and 17 per cent have seen somebody else's address.

Nine per cent have included their mobile number and five per cent have included their address in the personal information section of social networking sites visible to friends. And though a small percentage it is worrying that six per cent have written their phone number and three per cent have written their address "wall-to-wall" or on pages open to those who are not accepted contacts.

Men are more blasé about personal information – 13 per cent have included their mobile number compared with just seven per cent of women and nine per cent of men have included their address compared with just four per cent of women.

Once a burglar has established that you are a viable target and that he has enough information about you to blag his way out of a confrontation, if you post your address, it's simply a matter of getting a map up online or checking out Google Street View to check the type of area and the actual location of a property. Of course, they'll also establish when you are out of the house…

Part 3 – Establishing the owner's whereabouts

Given that "updates" and "tweets" are relatively public conversations, the danger in sharing updates about prolonged absences from the house with digital criminals is clear. Yet many of us are happy and eager to update our online friends about holiday plans, letting prospective burglars know how long we are likely to be away and the property empty.

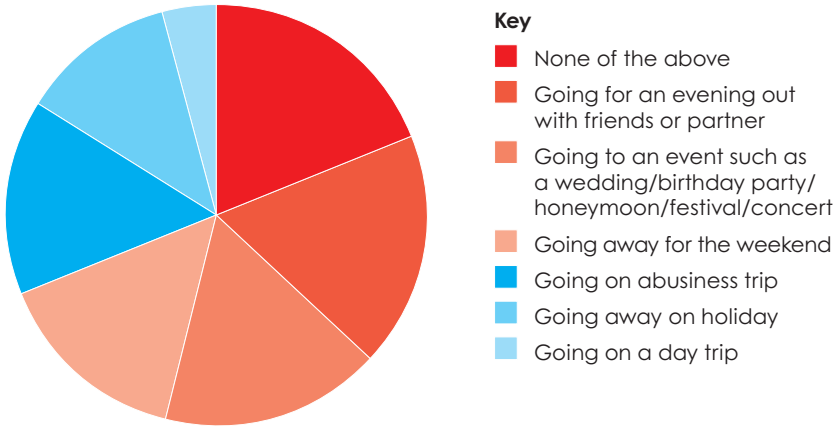
Well over a third (38 per cent) of social media users have posted updates detailing their holiday plans. Even more alarmingly, many social media users are prepared to share this information "wall-to-wall" or on fan/event pages which can be seen by a wider audience than just those users who have been approved as "friends". 28 per cent of people have written their holiday plans "wall-to-wall" or in replying to event invitations.

It is not just holidays we ought to be cautious about, a burglar will be interested to know that you will definitely be away from home, even if it is just for a weekend or a few hours. Four in ten (40 per cent) of social media users have posted updates on social networking sites about their plans to attend certain events such as a wedding, a party, a concert or a festival and a third (33 per cent) have updated to say that they are away for the weekend.

People posting updates about their wedding are particularly at risk – they are announcing that they will be away from the house for a number of weeks and that it is probably full of brand new, expensive goods. Whether you are honeymooning in Phuket, camping in Bognor or rocking out in Glastonbury, Michael advises people to be more reserved about advertising that they are leaving their homes vacant for a significant period of time.

Michael Fraser says: "A quick scan of your own Facebook 'news feed' over the last few weeks will reveal at least one or two people informing you that they are off on holiday – but who else are they informing? Some people even join groups and fan pages about their travelling exploits and comment on these pages about the trips they have coming up to total strangers."

Figure 2 Changes to status updates and posts when going away



Part 4 – The Sofa Stake-out: Casing the joint

If a burglar has identified you as a worthwhile target and knows that you will be away, he could be reviewing your house within minutes on internet satellite mapping tools. Google Earth and Google Street View are a core part of the digital criminal's arsenal according to Michael Fraser:

"You can tell an awful lot about a person from the visual identity of the house they live in – which is one of the reasons why Google Earth and Street View are so potentially dangerous."

It's not just that you can scope out entrance and exit points. You can also tell who lives in a particular house by the colour it is painted. You can see if they have kids if there are toys or a paddling pool in the garden – you then know that the house will probably be empty at school run time. You can see whether there are patio chairs – and how many, whether there are cat flaps, what kind of car is parked outside, whether the lawn is mowed or not, whether the windows are clean, whether the burglar alarm is dirty etc.

Michael continues: "Using Street View, I can see if a door has two locks, or just one – I can probably tell if the lock is a dead bolt or not, and so assess how easy the door will be able to break. I can see if there are bars on the windows and if there are bushes or trees covering entrance points to facilitate a well-hidden break-in."

"I can also see if there is a wheelie bin. A burglar will use a wheelie bin as a ladder to get into your house."

According to Michael, burglars are often working in teams, one identifying a target online and one actually carrying out robberies. They may hardly ever meet and will probably only communicate over untraceable, pay-as-you-go mobile phones, so making a connection for the Police will be virtually impossible. The burglar who actually commits the robbery may not have done any of the online "casing", making the link very difficult to establish in terms of catching all of those responsible.

Google Earth and Street View are tremendously impressive and useful tools but people should be aware that the internet evolution has changed how some criminals operate. Securing and protecting your home is imperative.

Part 5 – Considerations for the insurance industry

Clearly people's habits on social media sites can potentially make them more vulnerable to being burgled. This is an emerging and very real risk and one that the insurance industry will have to monitor extremely carefully.

The huge growth in social networking is now starting to raise the issue of the risks it can pose for insurers by facilitating burglaries. The fact that young people are most likely to post compromising information (16-24 year olds ranked the highest in every case worst offenders for posting details about their whereabouts) indicates that these could be the households most at risk.

However, the insurance industry is aware that with increasing acceptance of social media the standard risk indicators may need to be reviewed. Any new risks and patterns in crime and claims are continually monitored to ensure the implications do not impact viable business models and also importantly that there continues to be fair pricing of premiums for consumers. This social networking trend is clearly one that is making home insurers sit up and take note.

Research methodology

The research was conducted by Opinion Matters, an independent pan-European market research agency, between 24 July and 3 August, 2009. A total of 2,092 regular social networking users (defined as using a social networking application at least once a week) were polled across the UK.

Experiment methodology

100 friend requests were sent to strangers selected at random on both Facebook and Twitter during August 2009, with the number of acceptances recorded.

ADVICE FOR SAFE SOCIAL NETWORKING:

Don't give out information that might reveal more about you than you want people to know

Remember that what feels like a private conversation can often be watched online by friends of friends, or complete strangers

Think about using a fun fake name instead of your real name

Think about the profile photo you use – it might not be a good idea to make yourself appear like someone who is likely to own lots of expensive gear!

Think about the way you write online – it may seem strange, but professional burglars will be put off by people who abbreviate their posts or use 'text language' (e.g. ur instead of your), as, rightly or wrongly, they appear less wealthy

Don't post details of when you are going on holiday, or when you are going to be leaving the house unattended.

Legal & General Assurance Society Limited.
Registered in England No. 166055.
Registered Office: One Coleman Street,
London EC2R 5AA.

www.legalandgeneral.com

August 2009.