

DIGITAL CRIMINAL REPORT 2010.



The rapid growth of social media means many of us are trying to keep up, and in touch, with our friends. In doing so, though, we could unwittingly open ourselves up to unknown threats from increasingly sophisticated digital criminals.

- New 'location-based' services such as Facebook Places pose a significant risk, says Legal & General's latest **Digital Criminal Report**
- 82% people are unaware that their private address information is legally for sale on the internet

A combination of new location-based social networking sites and the availability of private residential addresses for sale on the internet is putting users of social media sites at risk from professional burglars. That is the headline finding of the latest **Digital Criminal Report**, prepared by Legal & General with the help of reformed burglar Michael Fraser.

A location-based service is an information and entertainment service, accessible with mobile devices through the mobile network, that uses the geographical position of the device to locate a person, object or piece of information.

Facebook, which has 500 million users worldwide*, launched its 'Facebook Places' location service in September, which allows people to 'check in' to their current location and share their whereabouts with friends or followers.

The research revealed that 40% of people agree that there is an inherent risk with location-based services because would-be burglars are able to establish their whereabouts. In spite of the awareness of the risks, new location services such as Foursquare and Facebook Places are growing in popularity, with the number of Foursquare users reaching three million in August.**

The potential increase in people using location-based applications could put more people at risk of burglary.

More than half, 54%, of people say they would be worried about using a location-based social networking site such as Foursquare if they suspected burglars had access to their address. And the **Digital Criminal Report** shows that this information is more readily available than many people believe.

IS YOUR ADDRESS AVAILABLE TO BUY ONLINE?

The report shows that anyone can purchase private address information via 192.com – even if the resident is ex-directory, so long as they are on the electoral roll. The vast majority, 82%, of respondents were not aware of this – and 81% said they would be angry or very angry to learn that their address information was available for sale on the internet.

Over half, 53%, of people are ex-directory because of privacy concerns, with 38% believing that being listed in a directory is a security risk. More than three quarters, 78%, of people agree that it should be illegal for websites to share personal information without permission.

Legal & General's **Digital Criminal Report** confirmed that a large proportion of users use social media sites to connect with people who are essentially strangers: 81% agree they're a good way to keep in touch with someone they met on holiday; 73% feel that they are a good way to meet "friends of friends"; and 45% agree they're a good way of contacting people they don't know but whose picture they fancy!

The **Digital Criminal Report**

shows that many people are still unaware of the potential security risks they face when online using social networks:

- 38% say they've seen phone numbers publicly visible on a social networking site (up from 34% last year)
- 17% say they've seen personal addresses publicly visible on a social networking site (no change from last year)
- 10% admit they've included their own phone number as part of their visible profile information (up from 9% last year)

Other findings include:

- The younger you are, the more likely you are to give information away concerning your whereabouts, with nearly six out of ten, 58%, 16-24 year olds sharing their holiday plans – which could be a cause for concern for parents.
- Some people are sharing mobile numbers and addresses directly with strangers: 6% have written their phone number and 3% 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 – 14% have included their mobile number on their profile compared with just 8% of women and 10% of men have included their address compared with just 5% of women.

* Facebook has 500 million users: <http://www.facebook.com/press/info.php?statistics>

** Foursquare passed three million users in August: <http://mashable.com/2010/08/29/foursquare-3-million-users/>

HOW DIGITAL CRIMINALS USE SOCIAL MEDIA

1) If you are broadcasting information about your whereabouts on Twitter or Facebook, then strangers can see when you are not at home, unless you prevent strangers 'following' you.

For celebrities like popstar Lily Allen, who informed us that she was in Paris on 3 October 2010 (below left), acquiring followers can be a crucial strategy for building a fan base. This means that often, letting strangers 'follow' your updates on Twitter is something people actively pursue.



2) New location-based social networking apps such as Foursquare (right), are based on people sharing their current location with friends or followers. Listing your home as a location is not sensible, as anyone using the app in the area can see it, even if they are not your friend.



3) Millions of UK citizens' addresses are publicly available on 192.com, via sources including the electoral roll. You can opt out of this, but we found that 82% of people are not aware they might be listed here. Publicly visible information includes a map of your area, pinpointing your address.



4) Armed with someone's address and whereabouts, a burglar can potentially use Google StreetView to assess routes of entry to a property or whether you have a burglar alarm, before planning whether to attempt to break in.



ESTABLISHED SOCIAL NETWORKS AND THE UNLEARNED LESSONS.

The rise of location-based applications for social networking sites poses a potential threat to people's home security.

It is not just the early users of this new technology that could be giving burglars a tip-off.

Even the 'established' social networking tools such as Twitter, Bebo and Facebook have their risks, unless simple precautions are taken.

By posting wall-to-wall or tweeting detailed information about their whereabouts, users may be allowing strangers to gather information that could be used to target them for burglary. This risk is increased when users allow people they don't really know to become their "friends" or "followers" on these sites, or if they have not set their privacy settings to a sufficiently high level.

In spite of the manifold warnings and media attention, many people still seem to have a casual attitude to sharing their whereabouts on social media sites.

PICTURE PERFECT TARGETS.

An alarmingly high proportion of users are prepared to be "friends" online with people they don't know well, as the figures below confirm. This, coupled with freely sharing personal contact information, presents a serious security risk for people's home and possessions. It is exactly the sort of information that burglars covet.

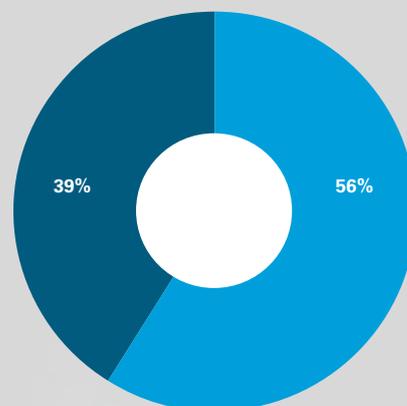
The findings of the **Digital Criminal Report** confirm that a large proportion of users use social media sites to connect with people who are essentially strangers:

- 81% think they are a great way to track down people they "met on holiday" (a marginal increase on last year)
- Nearly three quarters, 73% feel that they are a good way to meet "friends of friends" (roughly the same as last year)
- The old adage that "people change" does not encourage a cautious approach, as 93% of respondents are happy to connect with people that they haven't seen for years.

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.

Nearly half of people, 45%, like to use sites to meet new people based only on the person having a nice picture.

Do you agree social networking is a good way of connecting with people who have a nice picture?



KEY	%
Women	39
Men	56



“IT IS GREAT TO SEE A FALL IN THE NUMBER OF PEOPLE WHO ARE POSTING PHOTOS OF THE LATEST EXPENSIVE PURCHASE THEY HAVE MADE.

HOPEFULLY THIS IS A SIGN THAT PEOPLE ARE BEGINNING TO SEE SOME OF THE RISKS ON SOCIAL NETWORKING SITES. HOWEVER, A VERY HIGH PERCENTAGE ARE STILL WILLING TO GIVE BURGLARS A WINDOW SHOPPING OPPORTUNITY: THEY ARE EXCITED AND WANT TO SHOW THEIR FRIENDS.

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.”

MICHAEL FRASER

ARE HABITS CHANGING?

There is some evidence that people are heeding the warnings about some online behaviour but there is still a way to go. Consumer pressure has resulted in social networking sites being more proactive in concealing data. But there is more that can be done.

This year's **Digital Criminal Report** finds that people love to share photos online, with 64% believing that social media sites are a great place to share photos of their cool new purchases and presents.

This can be potentially valuable information for a professional burglar as well.

Though this figure has fallen by 6% from last year's figure of 70%, it still means that nearly two thirds of users are showing their valuable home contents and possessions to those who follow them online.

Other dangers exist for people who post photos of their pets. Revealing that they are a pet owner might spark extra interest from the savvy digital criminal. While many think that their dog is a deterrent, a burglar seeing

online that their target has a pet will look for doors or flaps for the animal to get in and out of a home. Think of it as a virtual version of the 'Beware of the Dog' signs that burglars often hunt out to give them easier entry into the property.

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



WHAT YOU CAN DO

Personality profile of targets for the professional digital criminal:

- The animal lover – less security-conscious, often 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 – insecure people, usually single, 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 good possessions
- 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...

- Do you really want someone connecting with you on the basis of your picture? Check your security settings to limit who can see your pictures – it will make you less of a target
- If you do accept requests from acquaintances, think about how much of your profile you want to show them. Most can be edited to limit areas of information provided
- If you are attending an event, delete it from your news feed. Details for events are normally open and you could be marking a time in the burglar's diary to strike.

LOCATION-BASED APPLICATIONS.

A significant development over the last year is the uptake of new 'location-based' services such as Facebook Places, Foursquare, Gowalla, BrightKite and Loopt.

Combined with other available social media information, a cyber stalker could easily find out where the user lives, then get real time updates when they are miles away or about to sit down for a meal out, meaning they'll be away for a couple of hours.

The take-up of these services in the UK is heavily driven by the growth of smartphones, such as the iPhone and the HTC Desire, and the user-friendly applications they enable.

The smartphone market has driven a 600% global growth in mobile internet browsing, with the UK coming second behind the US in a list of the top mobile browsers.

Location-based networking services are made possible by the new generation of mobile devices which allow users to post updates detailing their whereabouts – a development that will certainly interest the digitally-savvy burglar.

While location-based services are not yet as well used as the message sharing and micro-blogging that are traditional on Facebook and Twitter, their popularity is growing.

It may seem a small number but 2% of people have been burgled when out and about after posting details of their whereabouts on social media. If growth of location-based services continues, the likelihood is that this figure will rise.

A recent spate of burglaries in America highlights the risk and caused police to issue a warning about location-based services.

Police in the American state of New Hampshire recently smashed a burglary ring which targeted users who posted their location on their status or used Facebook Places, therefore effectively advertising the fact they were not at home.

Within just months of the service being launched, the gang had broken into 50 homes, stealing up to \$200,000 worth of goods.

Michael Fraser says there is no doubt that thieves will take advantage of services that then show exactly where their targets are: "The emerging popularity of location-based services adds a very worrying dimension to the digital criminal problem. It is

so easy for burglars to get hold of people's address details online once they have identified a target.

If a burglar can then simply log-in to a location-based social networking service and see that you are a few hours away from home, it's an open invitation."

DRAMATIC IRONY.

Most people don't appreciate the danger. Only 40% of social media users agree there is an inherent risk in relating their whereabouts with location-based services.

Most social network users are comfortable with sharing their location, so long as prospective burglars are unable to get hold of their address.

Michael says: "The last thing we want to do is to dampen enthusiasm for these new applications as location-based sites can be great fun and also allow people to get loyalty discounts at shops and restaurants.

It is important that people are aware of the risks and behave accordingly. We have seen people 'checking-in' to their own house, which is utter madness. A burglar would then just have to wait until you check in somewhere else to know they have the run of the place."

“WE KNOW FOR A FACT SOME OF THESE PLAYERS WERE IDENTIFYING THEIR VICTIMS FROM THESE SOCIAL NETWORKING SITES.”

NASHUA, NEW HAMPSHIRE, POLICE CAPT. RONALD DICKERSON



i

WHAT YOU CAN DO

- Never log-in at home. Do the benefits of publicising where you live outweigh the potential downside of attracting the attention of a burglar?
- This technology is changing all the time. Allow yourself time to familiarise yourself with it before going public
- Avoid the temptation of logging on whilst on holiday
- Make sure that you are ex-directory and that your address is not easily available online. We have more details on what actions you can take in Part Three.



IF ALL ELSE FAILS, USE EX-DIRECTORY INFORMATION.

The Digital Criminal Report research found more than half, 54%, of respondents would be worried about using a location-based site such as Foursquare. While there are potential risks with Foursquare, without a starting point, the digital criminal has little to go on. However, there are other services available which help to strengthen their arsenal.

If people have done all they can to hide data and yet it is still available, then they need to be aware of their vulnerability. One of the most concerning aspects of digital security is when information people have specifically instructed be kept hidden is readily available to anyone willing to pay for it.

This is too often and too easily the case: there are a whole range of readily available services which catalogue and sell personal information regardless of whether the people it is about want to keep it private or not.

The vast majority, 82%, of people are not aware of this and a similar amount, 78%, believes it should be illegal for websites to share personal information without asking permission.

Four fifths, 81%, said they would be angry or very angry if their addresses were available for sale on the internet, even if they are ex-directory.

More than half, 53% of people are ex-directory because of privacy concerns, with 38% believing that being listed in a directory is a security risk.

Nevertheless, an industry has sprung up simply selling personal data, regardless of the owners' wishes, which is perfectly legal.

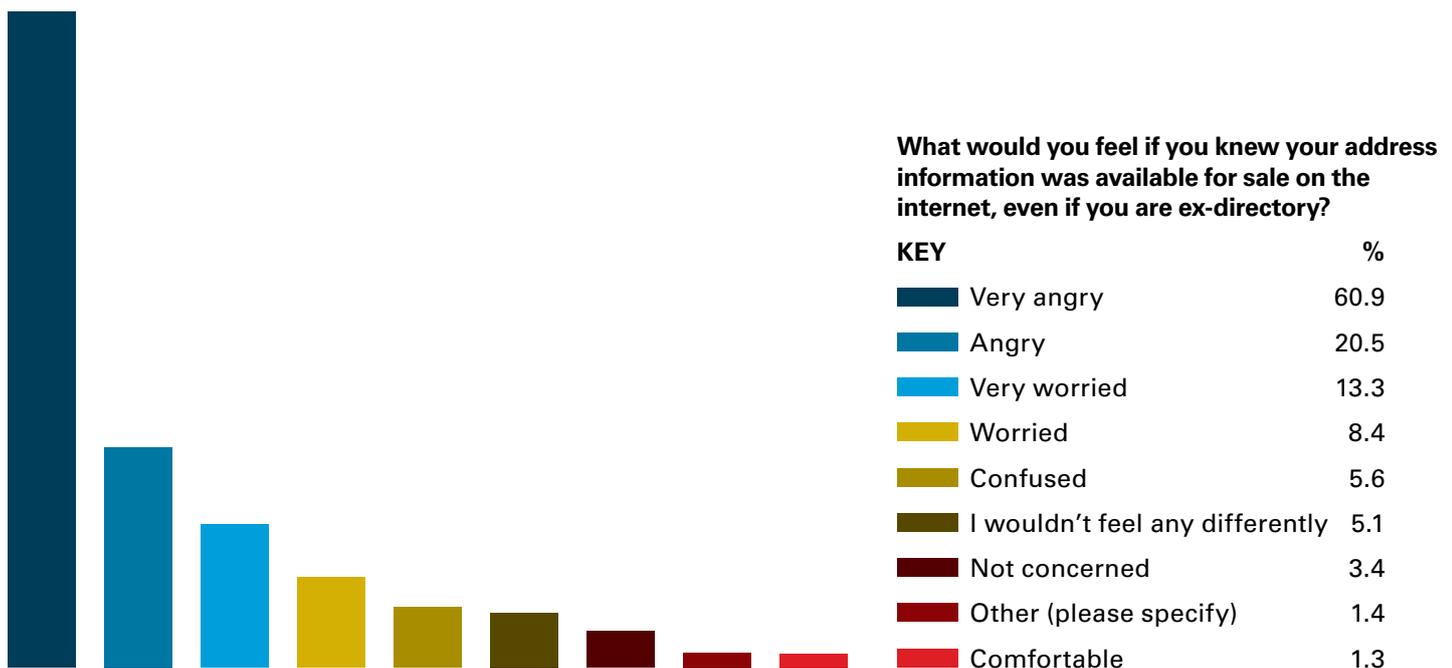
Websites such as 192.com will willingly hand over information such as personal addresses to anyone for a negligible cost and with no security checks on who they are selling to.

STREET VIEW.

Once a burglar has established that you are a viable target and that he has your address and enough information to blag his way out of a confrontation, 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.

Michael says: "Using Street View, a burglar can see if a house has a burglar alarm or not. He 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.

He can also see if there is a wheelie bin. If a bin is left out, the burglar will take it as a sign that the homeowners are away. Plus, the criminal can use the bin as a ladder to get into your house."



“IT’S ALL WELL AND GOOD BUILDING UP A PICTURE OF SOMEONE AND THEIR MOVEMENTS, BUT IF YOU DON’T KNOW WHERE THEY ARE COMING FROM, IT CAN BE HARD TO TRACK THEM.

DIRECTORY SERVICES SUCH AS 192.COM CAN PROVIDE THE FINAL PIECE IN THE JIGSAW BY GIVING BURGLARS A STARTING POINT FROM WHICH THEY CAN PLAN THEIR RAID.

WHAT’S MORE, CERTAIN DIRECTORIES EVEN ESTIMATE HOW MUCH A PARTICULAR PROPERTY MAY BE WORTH. YOU WOULDN’T NEED TO BE VERY BRIGHT TO REALISE THAT IF THE PROPERTY IS EXPENSIVE, THEN ITS CONTENTS ARE LIKELY TO BE REALLY HIGH END GOODS. PRIME BOOTY FOR A BURGLAR.”

MICHAEL FRASER

SEARCHING FOR WHAT INFORMATION IS OUT THERE ABOUT YOU.

People may be surprised about the amount of information that's available about them online.

A good first step is to simply search for your name on a search engine like Google or Bing. See what comes up.

Legal & General recommends searching two sites in particular. These are 192.com and 123People.

192.com – “Find people, businesses and places in the UK with 192.com. Directory enquiries, a people finder, business listings and detailed maps with aerial photos”.

192.com is an online directory that has existed since 1997 and contains almost 700 million records, many of which are free including directory enquiry and local business searches as well as interactive mapping, aerial photography and property reports.

Premium level access to the site will also allow you to search current and historical electoral rolls; birth, deaths and marriages registers; census data from 1861 onwards; and company and director reports.

192.com publishes personal data taken from various public and private data sets:

- Free directory enquires
- Electoral roll
- Directors' database

Details are included on 192.com about these sources, 192.com's privacy policy and how to remove your details from publicly searchable directories.

123People – “123people.com is a free real time people search tool that looks into nearly every corner of the web”.

123People aggregates information related to your name that is freely available on the internet. This might include social networking profiles, for example. It might also include items you hadn't expected would be publicly visible, however, such as your shopping 'wishlist' from Amazon.com.



WHAT YOU CAN DO

- If you wish to be removed from 192.com's copies of the Electoral Roll, you can download the form from <http://www.192.com/misc/privacy-policy/> and mail it to the address given or fax it to 020 7909 2169
- Protect what you can. With 123People it can show others what items you have put on your Amazon shopping list. Write that list down rather than saving with Amazon. There's no point providing burglars with a catalogue of the items that are about to be delivered to your home.

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 is monitoring carefully.

The rise of location-based services adds another layer of complexity and potentially heightens the risk of burglary further, especially when it is so easy for criminals to obtain people's details online.

The fact that young people are most likely to post compromising information indicates that perhaps some youth rating may need to be considered at some point in the future. Those aged 16-24 were by far the worst offenders for posting details about their whereabouts on social networking, ranked the highest in all but one category. Even digitally-savvy people, who might consider themselves aware of the risk and have taken precautions such as increasing their privacy settings on Facebook, should remain vigilant. Their address might still be listed on 192.com, and so tweeting about their location to the wider world could still make them vulnerable.

Legal & General, along with the wider insurance industry, is aware that as social media grows in popularity, this may become a factor that needs to be considered.

Any risks and patterns are continually monitored to ensure that Legal & General continues to provide fair premiums for consumers, and also price policies to reflect the risk to the business.

The **Digital Criminal Report** seeks to increase awareness of these issues and advise people how to stay safe while continuing to enjoy social networking.



Gary Pickering, sales and marketing director at Legal & General's general insurance business, said:

"Since we commissioned our first **Digital Criminal Report** in 2009, social networking services have moved on and more information is now available on people's whereabouts. While we acknowledge the value of these services, people need to be very wary about sharing information that could put them or their homes at risk, particularly if this is with people that they don't really know. We'd certainly advise against listing your home as a location on sites such as Foursquare or Facebook Places to reduce the risk of being a target for burglary.

And always remember that a lot of the time, talking on a social media site is like talking out loud in the street or down the pub: you are never completely sure who might be listening in and picking up valuable information. This includes other people who might be giving away information about your house and whereabouts, like your children or friends, who could send on info to their friends."



WHAT YOU CAN DO

- Check your privacy settings on any social network sites you use. Set them as high as possible without compromising usability
- Be wary of accepting friend requests on Facebook from people you don't know. When tweeting on Twitter, remember that what you say can be seen by anyone unless you have restricted your profile to specific people, so think twice before talking about when you will be out of the house
- Check whether you are listed on 192.com. If you are and would like to be removed, follow the steps on the previous page to have yourself removed
- Don't list your house as a location on Foursquare. It will be visible to anyone using the service in the area
- Monitor how your children, lodgers or other people in your home are using social network services to ensure they are not putting you at risk.



CONTACT US



08000 279 833

Call charges will vary. We may record and monitor calls.



www.legalandgeneral.com



Legal & General Insurance Limited.

Registered in England No 423930

Registered office: One Coleman Street, London EC2R 5AA

We are authorised and regulated by the Financial Services Authority.
We are members of the Association of British Insurers.

December 2010



The research for this report was conducted by Opinion Matters, an independent pan-European market research agency, between 9 and 17 September 2010. 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.