UK Wireless Network Hijacking

A CPP white paper

October 2010

Contents

Introduction

3

1.1 Foreword

There is no doubt that we live in an ever increasing mobile and complicated society.

If you had asked the average person in the street five years ago how their identity could be stolen, bin raiding and theft of mail would, certainly, have figured prominently. Today, ask the same question and you're likely to get a multitude of responses including data leaks, institutional theft, bin raiding, phishing, computer viruses, malware, Trojans, botnets and so on.

One area that has had little public discussion is the use of wireless or Wi-Fi networks and how secure these are. As this report highlights, without doubt, Wi-Fi networks pose a risk if they are not properly secured and visible to brute force attack.

The number of people falling victim to identity fraud continues to climb; in the last industry statistics published by CIFAS, the UK's Fraud Prevention Service, nearly 80,000 instances of identity fraud were identified by CIFAS Members in the first nine months of 2010 – an increase of nearly 10% from the same period in 2009. In the same period there was an 18% increase in the number of victims of impersonation; clearly the battle against identity fraud is just beginning and one that requires continued vigilance, perseverance, self-monitoring and management as well as help from industry and private-sector identity protection products and services.

If people take a proactive approach to managing and protecting their identities they are more likely to detect and prevent an attack occurring. And if the worst should happen, at least be able to manage the situation.

Most recently the National Fraud Authority has published a report estimating that every year in the UK identity fraud costs more than £2.7 billion and affects over 1.8 million people and of this figure at least £1.9 billion is the amount gained by the fraudster. These are staggering statistics and should be a catalyst for implementing increased public education and awareness and for consumers to take personal responsibility for their identities.

> "Wi-Fi networks pose a risk if they are not properly secured and visible to brute force attack"

1.2 Industry Facts

- Software security firm, Norton, reported that 65% of web users have been a victim of cyber crime
  (source: Computing 09 September, 2010)
- In the same survey 80% of web users don't believe the cybercriminals will be caught
- Hackers have stolen up to £6 million from online bank accounts in Britain after infecting computers with a virus known as 'zeus'
  (source: Telegraph 29 September, 2010)
- On 24 September, cyber-vigilantes leaked personal information relating to the download of pornographic films on the internet
  (source: guardian 2 October, 2010)
- The police cybercrime unit can only tackle 11% of the 6,000 known organised criminal gangs that regularly use computers for illegal purposes according to the Metropolitan Police Commissioner, Paul Stephenson
  (source: info security 4 October, 2010)
- The US leads the world in numbers of Window PCs that are part of botnets. More than 2.2 million US PCs were found to be part of botnets, networks of hijacked home computers, in the first six months of 2010
  (source Microsoft BBC Technology News 13 October, 2010)

"Software security firm, Norton, reported that 65% of web users have been a victim of cyber crime"

1.3 Research Methodology

ICM interviewed a random sample of 2,022 adults aged 18+ online between 16 - 19 September 2010. Surveys were conducted across the country and the results have been weighted to the profile of all adults. ICM is a member of the British Polling Council and abides by its rules. Further information at www.icmresearch.co.uk

Separately during September 2010, CPP employed the services of an ethical hacker and Senior Vice President of CRYPTOCARD, Jason Hart, who conducted a number of reviews relating to Wireless Networks and Wireless users. The reviews were focused around Wireless WarDriving, Public Wireless Hot Spots and the use of Rogue Wireless Access Points.

- WarDriving: CPP's ethical hacker drove around each of the different cities, looking for wireless networks, using special software on a laptop computer. This was done in both residential and business areas. Following the Wardrive, CPP's ethical hacker monitored the number of visible networks and what security settings were in place.
- Public Wireless Hot spots: The second part of the experiment was to quantify the extent of security problems and raise awareness - not to 'hunt down' targets. The aim was to identify the number of potential users that use public hotpots within a given time frame and understand what potential sensitive information is visible across public hotspots where it could be intercepted by a nearby individual or Hacker also using wireless technology.
- Creating fake wireless hubs: The third aspect of the experiment involved going into public places and creating rival wireless routers to capture people logging on to free Wi-FI. Using specialist software, CPP's ethical hacker recorded the number of people logging-on to the rival wireless hub and what passwords and usernames they were using.

The review was conducted within six cities – Bristol, Cardiff, Edinburgh, London, Manchester and Birmingham.

It is important to note that at no point during this review was any unauthorised access gained to any user of any wireless network.

This report (specifically the survey findings that constitute it) is intended as a reference document to highlight the potential threat that Wireless Networks and devices pose. The survey demonstrates that residential and wireless devices users within Bristol, Cardiff, Edinburgh, London, Manchester and Birmingham today should think about what they may be forfeiting by continuing to utilise wireless network technology without thinking about their online security. The report is designed to highlight and address the potential security vulnerabilities associated with using wireless systems, and to avoid being another 'drive-by victim'.

1.4 Key Findings

Nearly half of home Wi-Fi networks can be hacked in less than five seconds

In an 'ethical hacking' experiment conducted across six UK cities, nearly 40,000 networks were revealed as 'high-risk', opening up the personal data of thousands of individuals. This is because they were immediately visible to wardriving software, which puts them at direct risk from hackers, who, with the right knowledge, can override even the most secure systems. Beyond this, many networks had easily identifiable SSID or "Service Set Identifier", which revealed the name of their business and where it was situated.

City	Total Number of Wireless Networks	Total Number of Public Hotspots	Total Number of Networks with No Security	Total Number Using WEP Encryption	Total Number using WPA Encryption	Total Number Using WPA2 Encryption	Residential Networks
Birmingham	3323	340	916	403	606	998	923
Cardiff	11375	647	1409	813	1073	6494	3412
London	14908	1777	4746	2667	2554	3953	7258
Manchester	2894	650	870	793	0	1231	1663
Birmingham	3753	333	910	587	1142	836	2761
Edinburgh	1956	158	398	260	597	626	1019

> "nearly 40,000 networks were revealed as 'high-risk', opening up the personal data of thousands of individuals"

CPP recruited Jason Hart, Senior Vice President of CRYPTOCard, as our ethical hacker, to conduct a Wardrive experience within the main arterial routes of each city listed above.

During the Wardrive Jason was able to easily identify exposed wireless networks emanating traffic into the street. Once the wireless networks were identified – in total 38,209 – Jason pinpointed the exact frequency, estimated the location of the source, and identified the Wireless ID (SSID) used. The scan also identified whether the WLAN was utilising encryption and any other apparent security characteristics of the network to determine access potential. We found that 20,110 had a good standard of Wi-FI Protected access (WPA or WPA2) providing network administrators with a high-level of assurance that only authorised users can access the network.

However, the fact that nearly 40,000 wireless networks were visible means that they cannot be considered 100% secure. Idappcom, the data traffic analysis and security specialist has reported that the release of ElcomSoft's Wireless Security Auditor (EWSA) software, recently refreshed with the addition of an enhanced WPA2 password recovery facility, is actually a 'brute force' cracking application, meaning that WiFi connections can be longer be considered secure.

Idappcom's chief technology officer has said "The update of EWSA means that, with the professional version installed, hackers can use a computer with up to 32 CPUs and 8 GPUs to crack WiFi encryption using a brute force attack.

"Although the professional version edition costs almost $1,200, it's reportedly possible to download a trail version of the software and crack it using utility files available via filesharing networks ."

According to Idappcom's CTO, the reality is that the software can brute force crack as many as 103,000 Wi-Fi passwords per second, which equates to more than six million passwords a minute – on a HD5390 graphics card-equipped PC.

With regards to company's wireless networks, the arrival of the refreshed version of EWSA means that users can no longer trust that their Wi-Fi connection – unless they use a VPN – is truly secure.

There were, however, over 9,000 that had no security and a further 5,000 that had only Wired Equivalent Privacy (WEP) encryption which is the lowest form of network security and is rapidly being phased-out by businesses and organisations for more secure forms, including WPA and WPA2.

The overall purpose of the Wardrive was to quantify the extent of security problems and raise awareness - not to 'hunt down' targets.

The aim was to identify networks that emanated wireless signals excessively into a public place where it could be intercepted accidentally or otherwise (i.e. by a nearby individual or company also using wireless technology, or by a hacker).

The following processes were not conducted by and were considered inappropriate or outside the scope of this Wardrive:

- Sniffing of network traffic
- Connection to any of the detected networks
- Attempt to crack any encryption keys (WEP, WPA,WPA2)
- Targeting of 'high profile' businesses
- Installation and use of a high gain antenna
- Use of 'cracking' software to decrypt encryption keys

In addition, our ethical hacker did not check any access points for default passwords and made a special effort to make sure he did not connect to any to any of the wireless LANs that were detected. It should also be noted that the survey did not include analysis of the data packets themselves. Instead, the means of positive identification of networks were limited to the following information:

- Wireless Network SSID
- Wireless Network Name
- Encryption type used
- Wireless access point model

In order to conduct the Wireless Wardrive, the following equipment was used:

- Toshiba Laptop with built in Wireless Network Card
- Vistumbler – A wireless network freeware scanning tool http://www.vistumbler.net

The majority of people mistakenly think their networks are secure

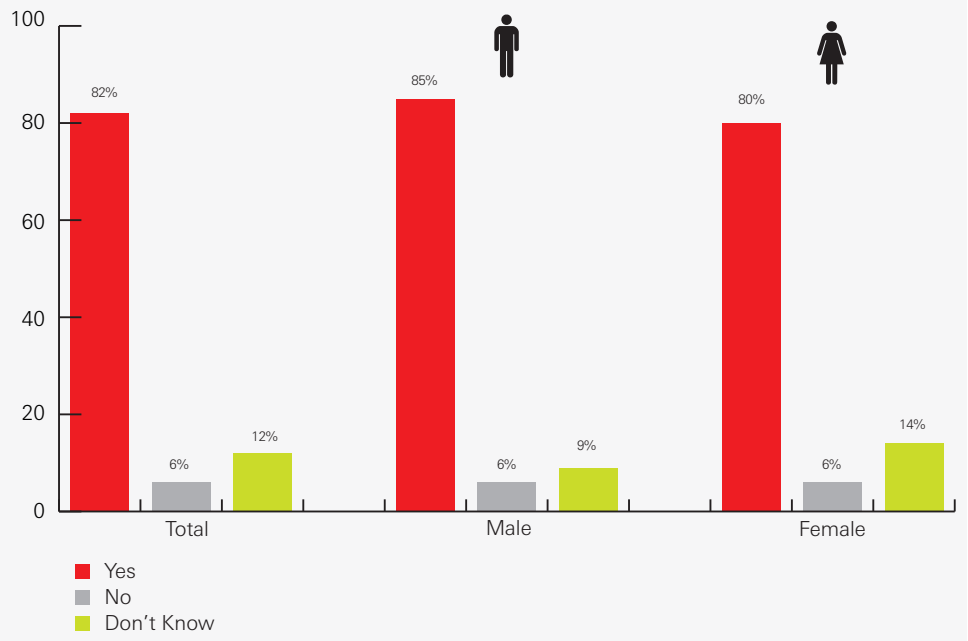
According to the findings, nearly a quarter of private networks in the Wardrive experiment have no password whatsoever attached, making them immediately accessible to criminals. This is despite the majority (82%) of people mistakenly thinking their network is secure.

Even password protected networks are not secure. A typical password can be breached by hackers in a matter of seconds.

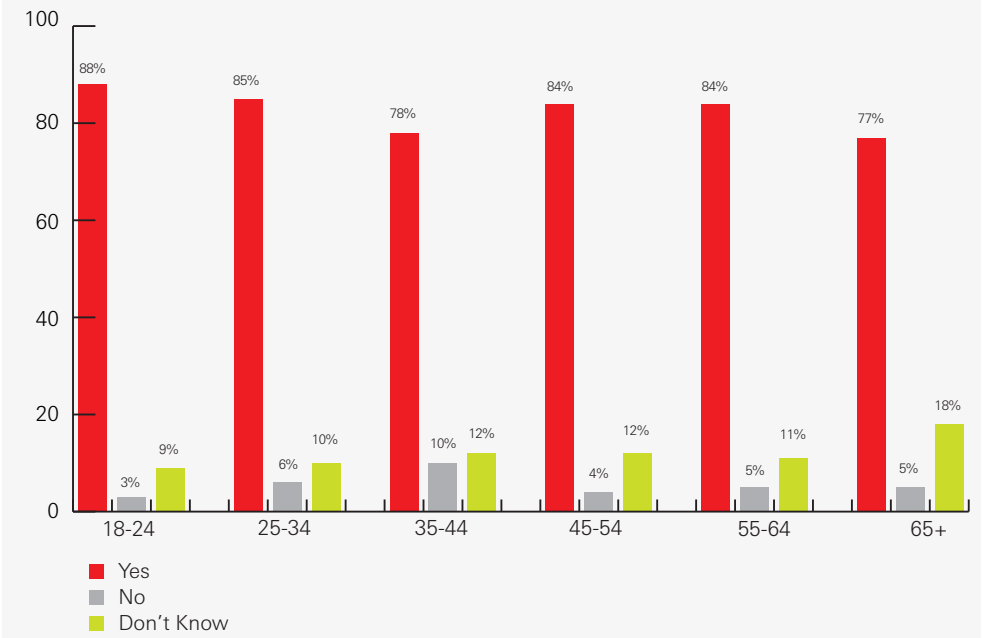
Those aged 18-24 years old are the most (88%) likely to think their wireless network is secure verses 77% of people aged 65+. There are probably numerous reasons for this, but the overriding assumption we can make here is that this demographic are probably the least aware of the technology used and the associated level of risk, protection and threats.

Men tend to be more optimistic than women with 85% thinking their wireless network is secure verse 80% of women.

Q: Do you think the wireless network you use is secure? By Gender



Q: Do you think the wireless network you use is secure? By age...



The majority of people do not think their network has been used without their permission

Hacking into a private network not only allows unscrupulous individuals to 'cloak' criminal activities such as purchasing illegal pornography or selling on stolen goods. It also allows them to view the private transactions made by individuals over the wireless network, accessing passwords and usernames, which can then be used to impersonate the victim and commit identity fraud.

Worryingly, only 4% of people know for certain that their network has been used without their permission, indicating that the vast majority remain ignorant of the risk, or that this may have happened to them.

Those aged 18-24 were the most likely to know for certain that their wireless network has been used by an outside party; perhaps because they are the most familiar with this type of technology and the warning signs. Nearly one in five had no idea whether their wireless had been used without their permission.

Mark, from London:

"On the day before Christmas Eve last year, I arrived home after a night out at the theatre to find that my flat door had been broken down.

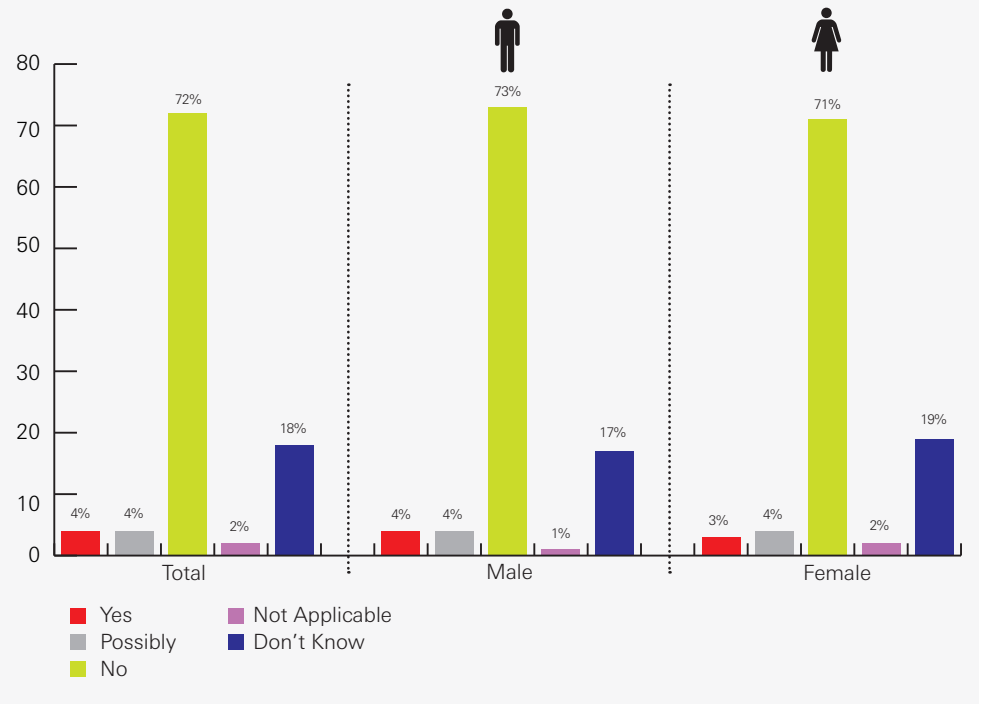
"Initially I thought I'd been burgled, but when I came into my home I discovered a search warrant for stolen goods and instructions to call CID.

"After a very worrying Christmas period, I met with the police and was informed that they'd been acting on evidence that a stolen laptop that had been opened using my wi-fi connection. Putting two and-two together, I realized that I had no password attached to my wi-fi and that it must have been used illegally by criminals.

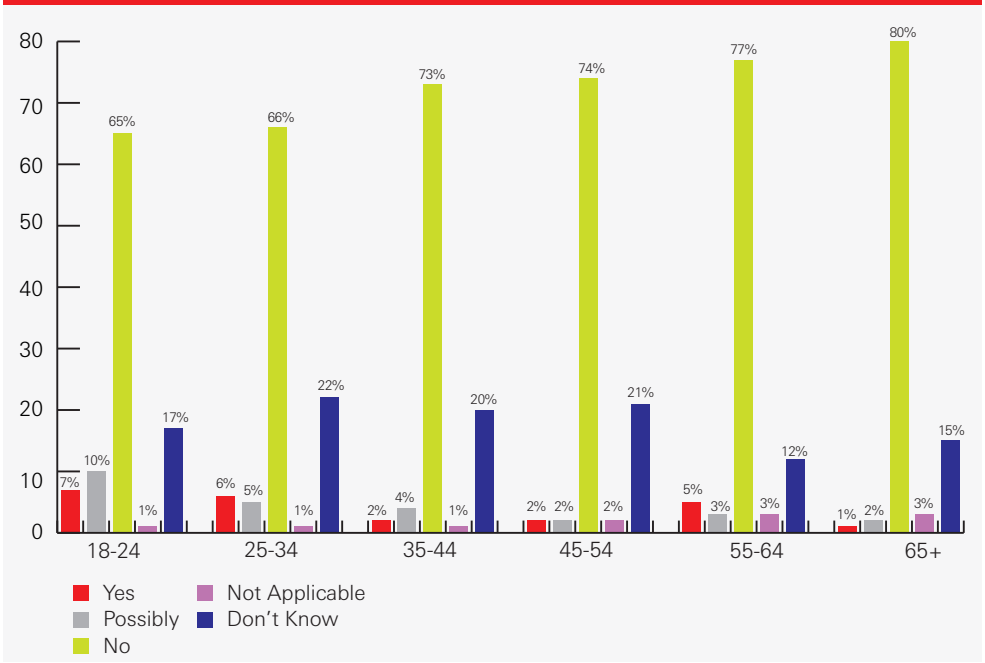
"I was compensated for my door but obviously the episode was very worrying and made me realise just how important it is to secure your wi-fi connection."

> "only 4% of people know for certain that their network has been used without their permission"

Q: Has your wireless network ever been used without your permission...? By gender...



Q: Has your wireless network ever been used without your permission...? By age..



One in six wireless users say they regularly use public networks

This report clearly highlights the dangers of accessing the internet over publicly available networks. While 16% access Wi-Fi networks in open zones e.g. coffee shops, hotels, airport lounges, a further 20% access networks via their mobile phones that automatically connect to wireless networks. However this figure is almost certainly likely to be higher, as many smartphone users either don't realise that their phones use wireless networks, or know that they are programmed with software which automatically connects them to free wireless networks.

Those aged 18-24 were the most likely to connect to a wireless network in an open zone (21%) verses only 9% of those aged 65+.

Only 22% of people said they didn't use a wireless network, but this may not account for their mobile applications that automatically connect to Wi-Fi networks, including smartphones which are designed to connect automatically to openzones where available, often without the user being aware.

In order to review the potential issues around these public hotspots, our ethical hacker, Jason Hart, visited coffee shops and public locations in six cities using basic Wireless equipped (listed below). During the review it was very easy to identify wireless users on the public hotspots and in most case catalogue sensitive data that could have been captured if needed. The data that could have been captured during the review could have been – passwords, usernames and details of the website that the user of the public hotspot was accessing.

The overall purpose of the Hotspot review was to quantify the extent of security problems and raise awareness - not to 'hunt down' targets. The aim was to identify the number of potential users that use public hotpots within a given time frame and understand what potential sensitive information is visible across public hotspots where it could be intercepted by a nearby individual or Hacker also using wireless technology.

We were able to 'harvest', but didn't, usernames and passwords from unsuspecting people at a rate of more than 350 an hour, sitting in town-centre coffee shops and restaurants.

The table below shows the number of people whose wireless networks can could have accessed across the six cities during a one-hour time period, and the level of risk with 100% of opportunities where access sensitive data was possible.

City	Number of people accessed within a 1 hour time frame - Between the hours of 12pm and 1pm week days	Was sensitive data visible (Were permission granted)
Birmingham	18	100%
Cardiff	15	100%
London	45	100%
Manchester	27	100%
Birmingham	34	100%
Edinburgh	14	100%

> "Those aged 18-24 were the most likely to connect to a wireless network in an open zone"

The following processes were not conducted by and were considered inappropriate or outside the scope of this Wireless Hotspot review:

- Cracking of passwords
- Connection to devices
- Use of 'cracking' software

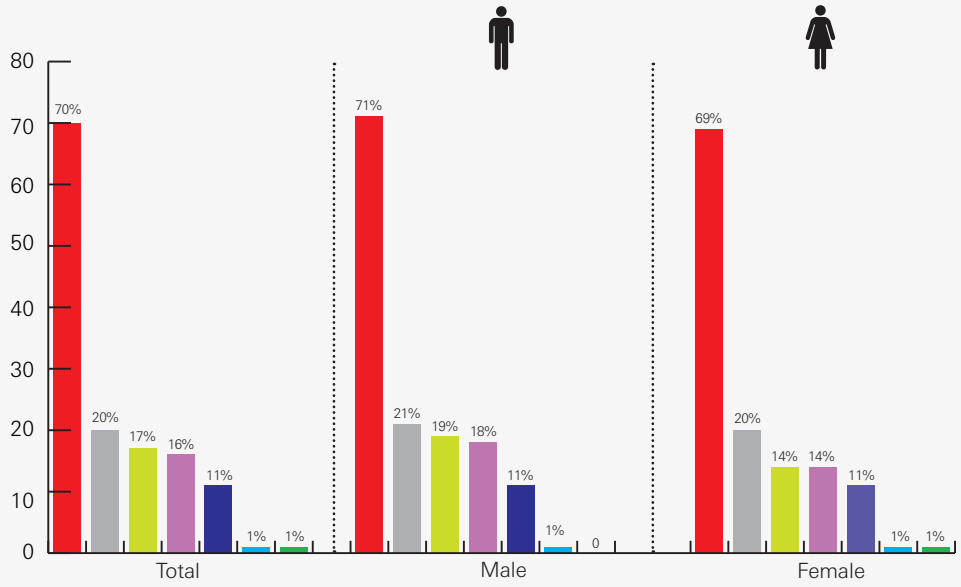
In addition, our ethical hacker did not access or collect any data on the devices or users. It should also be aware during the survey permission was granted from individuals to see if it was possible to retrieve sensitive information during them using Public Hotspots.

In order to conduct the Public Hotspot review, the following equipment used:

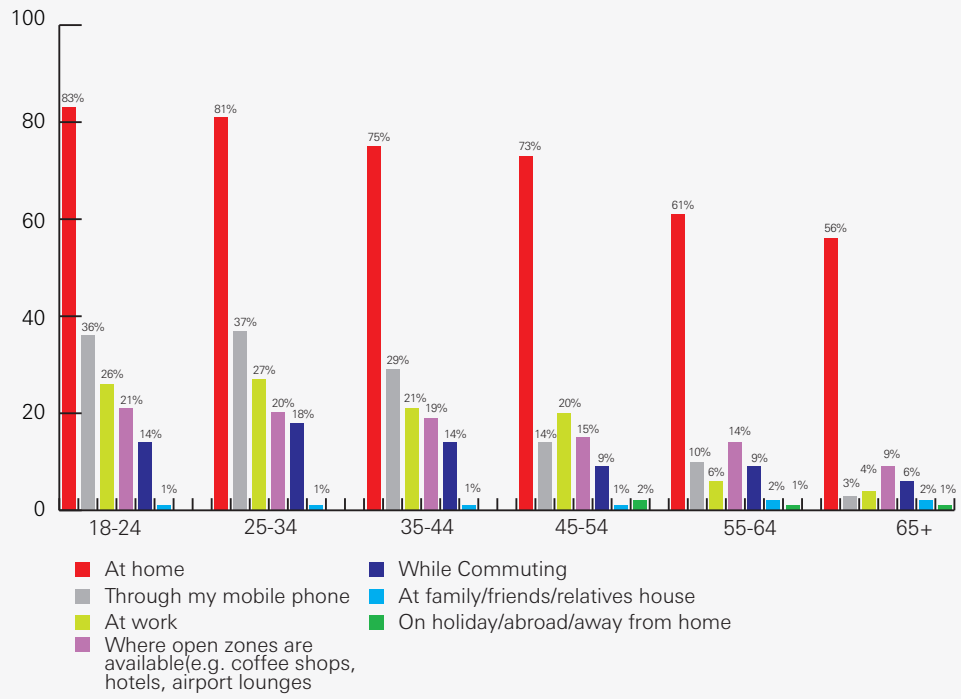
- Toshiba Laptop with built in Wireless Network Card
- A network enumeration tool (used to indentify devices on the public hotspots)
- Cain & Able (this was only used were permission was given by individuals) this was used to capture sensitive data including passwords

“We were able to ‘harvest’, but didn’t, usernames and passwords from unsuspecting people at a rate of more than 350 an hour”

Q: Where do you use wireless networks...? By gender...



Q: Where do you use wireless networks...? By age...



It is easy to attract users to a rogue wireless network

In order to review the potential issues around public hotspots, our ethical hacker, Jason Hart, visited coffee shops and public locations access six cities.

In order to conduct this review Jason used a portable wireless network router connected to 3G broadband connection. The Wireless router was specially named to attract users to connect their wireless device to the Rogue network automatically. This was achieved by using different SSID names.

During the review it was very easy to attract users to the rogue wireless network and in every case it would have been possible to catalogue sensitive data that could have been captured if needed. The data that could have been captured during the experiment could have included passwords, usernames and details of the website that the user of the public hotspot was accessing.

The results below show that in just one hour, more than 200 people unsuspectingly logged onto a fake Wi-Fi network, putting themselves at risk from fraudsters, if they decided to do the same scam, could harvest their personal and financial information. In addition 80 smartphones connected automatically to the rogue network putting the holder of those devices at risk from the capture of their information, without their knowledge. This could include gaining access to personal and work emails, social networking sites or even online shopping or banking sites.

Elsewhere our ICM research told us that 48% of Wi-Fi users, connected to networks several times a day with nearly four out of ten connecting daily. Those aged 18-24 were the most likely to connect several times a day (62%).

> “In just one hour, more than 200 people unsuspectingly logged onto a fake Wi-Fi network, putting themselves at risk from fraudsters”

City	Number of people accessed within a 1 hour time frame with an SSID of a Brand Name	Number of people accessed within a 1 hour time frame with an SSID of free Internet access	Devices automatically connected to rogue device within a 1 hour period
Bristol	16	21	4
Cardiff	12	11	6
London	37	51	27
Manchester	21	32	19
Birmingham	39	43	21
Edinburgh	9	15	7

The overall purpose of the rogue wireless hotspot review was to quantify the extent of security problems and raise awareness - not to 'hunt down' targets and to see if people would just access or trust the access point they were accessing. The aim was to identify the number of potential users that would connect to a rogue wireless hotspot within a given time frame and understand what potential sensitive information is visible publicly across public hotspots where it could be intercepted by a nearby individual or Hacker also using wireless technology. The following processes were not conducted by and were considered inappropriate or outside the scope of this Wireless Hotspot review:

- Cracking of passwords
- Connection to devices
- Use of 'cracking' software

Jason Hart did not access or collect any data on the devices or users. In fact, during the rogue hotspot review he made special effort to make sure that they never collected any information. It should also be aware during the survey permission was granted from individuals to see if it was possible to retrieve sensitive information during them using Public Hotspots.

In order to conduct the Public Hotspot review, the following equipment used:

- Toshiba Laptop with built in Wireless Network Card
- Portable Wireless Access Point
- 3G Broad Band USB device
- Cain & Able (this was only used were permission was given by individuals) this was used to capture sensitive data including passwords

Wireless networks are used for checking e-mails, online shopping and banking

Of those respondents who use wireless networks, 85% use it for checking personal e-mails, 65% for online shopping and 63% for online banking.

Women are more likely to use Wi-Fi networks for online shopping whereas men are marginally more likely to use it for online banking.

Demographically, those aged 18-24 are the most likely to use Wi-Fi networks for online shopping and banking and social networking.

With Wi-Fi networks open to external attack and fraudsters quietly harvesting sensitive personal and financial information, the risk of these common activities is brought into sharp focus. This is especially the case with public WI-FI networks, where many users naturally assume that the public networks they use are legitimate and therefore secure. But as these experiments demonstrate, there is nothing to stop hackers altering the name of a fraudulent network to mimic a legitimate one.

Separately when we asked respondents who use Wi-Fi networks if they had ever logged onto somebody else's unsecured wireless network without their permission, 20% said they had. People aged 18-24 were the most likely (37%) to have done this as opposed to 5% of those aged 65+.

When we asked people why they had logged onto somebody else's Wi-Fi network, over a third (36%) said because it was available, 32% because it was convenient, 28% because it was easy to do, and 14% because they were having access problems with their own wireless network. 5% said they had done so accidentally highlighting the ease to which this is possible.

> "Women are more likely to use Wi-Fi networks for online shopping whereas men are marginally more likely to use it for online banking"

Activity	Total	Male	Female
Checking personal emails	85%	83%	86%
Online shopping	65%	63%	67%
Online banking	63%	63%	62%
Buying or selling goods or sevices (e.g. ebay)	50%	48%	51%
Social networking	48%	43%	53%
Transferring money (e.g. using PayPal	45%	45%	45%
Booking holidays/tickets	40%	40%	41%
Checking work emails	28%	30%	26%
Job applications	18%	17%	18%
Amending work documents	15%	14%	15%
General browsing	2%	2%	2%
Research	1%	1%	1%
News websites	0	0	1%
Searching information	0	0	1%

1.5 Conclusion

Many residential homes and businesses now use wireless LAN (WLAN) connectivity because it is convenient, cheap and easy to install. They allow for mobility around the home and office and deliver great flexibility. Unfortunately, they can also be insecure unless you take appropriate precautions. Unlike wired networks, wireless signals can be intercepted and/or hijacked without the need to physically connect to the network. However the report shows that a large number of people are aware of the issues of security when it comes to deploying a wireless access home, but there still seems to be a lack of awareness in relation to what encryption standard to use when deploying or using a wireless access point and more importantly almost zero awareness when using public and or rogue wireless access points.

The number of rogue hotspots in existence is extremely difficult to estimate - they exist for relatively short periods of time in order to avoid detection, and are very simple to implement and are extremely effective. There is also little need to maintain a rogue hotspot, as they rapidly yield valuable information. The recent findings of this report show that 100% of people accessed a rogue wireless access point if free wireless internet is used as the Service Set Identifier (SSID). Such fake hotspots can even process credit card details and allow internet access. This simple configuration could potentially be the next big thing in identity theft as it has a greater capacity – and yields more accurate results – than current phishing attacks. It is feasible that identities could be stolen using a system like this. Rogue wireless has the potential to be the next big criminal tool; that is providing it is not already.

It is important that people are made aware of the potential risks surrounding public hotspots and that hotspots providers provide a method to reduce the risks of users by means of education and mutual authentication.

The simple fact is that the vast majority of those targeted have no idea their information is visible to other people. But by capturing usernames and passwords from standard e-mail and social networking sites, a Hacker can gain access to sensitive personal and business information. Beyond this, there is nothing to stop them committing credit card fraud, applying for loans or even assuming their victims' identities online.

Wireless network hacking or "wi-jacking" is an invisible crime. Because victims often have no idea that they have been targeted until it is too late, it is extremely hard to quantify. What we can be certain of, is that the number of devices with wireless capabilities are increasing, especially with smartphones, where connectivity is automatic. Alongside this the number of internet-based applications that rely on wireless access has rapidly increased, meaning that the opportunities for wireless network hacking have also risen.

Consumers need to be aware and not bury their heads in the sand because they don't understand the technology or think it unlikely to ever happen to them. If consumers use wireless networks they should ask about security and make it their business to know the level of risk and what needs to be done to protect themselves. With over 80% confident their wi-fi networks are secure, yet with nearly half of home wi-fi networks easily hacked in less than five seconds, this is clearly not the case.

The value of products to protect peoples' identities is brought into sharp focus when you consider the evolving threat of identity fraud enabled by technological developments.

1.6 Steps and ways to protect yourself

Michael Lynch is an identity fraud expert at CPP and offers the following advice to consumers to help protect them from identity fraud. Michael is responsible for the UK Identity Protection portfolio at CPPGroup Plc (CPP).

Michael has been with CPP for 14 years. His experience in financial services extends to customer service, new product and market development and affinity relationships.

During his time at CPP, Michael has helped bring to market one of the UK's market leading services, Identity Protection, which now protects over one million UK consumers from the consequences of this rapidly growing crime. In addition, Michael had used his expertise to create a commercial identity theft product aimed at protecting businesses of all sizes. He has also developed a strong understanding of consumer perception and reaction to identity theft and its consequences. In addition Michael has been responsible for breaking some major identity theft stories in the media, including the availability of fraudulent documents online, car cloning, junk mail and postal theft. Committed to forging industry co-operation to reduce the opportunities for identity theft he is leading the call for consumers to change their behaviour to counter what is becoming an increasingly sophisticated and intrusive crime.

Michael is media trained across print and broadcast and is available for media interviews on the issue of identity fraud.

Steps and Ways to Protect Yourself

1. Use encryption on your wireless access points (WAP) - Make sure you have Wi-Fi Protected Access 2 (WPA2) - the latest security standard introduced by global, non-profit industry association, the Wi-Fi Alliance. You can select products that use this method by looking for "Wi-Fi WPA2" in their specifications. WPA2 can operate in two modes, personal mode and enterprise mode.

   Personal mode – a pre-shared password or pass phrase used for authentication. This is a simple approach that ensures a computer can only get access to the WLAN if the password matches the access point's password.

   Enterprise mode – a more sophisticated method that is better suited to larger organisations needing stronger protection.

2. By implementing a Virtual Private Network (VPN) you can create a secure wireless network. This is achieved by encrypting all of the data that passes over the 'insecure' network so that it cannot be accessed by an eavesdropper.

3. Install a firewall (an electronic barrier that sits on a network server and protects the PCs hidden behind). You can use a firewall in a network to separate an insecure part of the network from the secure area where your most critical data is managed. Businesses that have an existing Internet connection will probably have a firewall already in place, but you should not assume that this would provide protection for your WLAN.

4. All wireless routers should have obscure IDs when they announce themselves to the world. Rather than put in any real information that can make it clear who owns the router or that can reveal your location or business name, use something common like "wireless" or "router 1" that doesn't give away anything critical.

5. Try to position access points, which transfer data between your devices, away from the outside wall of your building to minimise leakage of radio signals. This limits the chances of interception from outside.

6. Don't allow employees to add access points without management authorisation. One insecure access point could compromise your entire network

1.7 For further information please contact:

Nick Jones
Head of Communications
CPP Group Plc
Holgate Park
York YO26 4GA

Tel **01904 544 387**
E-Mail **nick.jones@cpp.co.uk**
Web **www.cppgroupplc.com**

CPP is an award-winning organisation:

- Winner in the European Contact Centre Awards, Large Team of the Year category, 2010
- Finalist in the European Contact Centre Awards, Best Centre for Customer Service, Large Contact Centre of the Year categories, 2010
- Finalist in the National Sales Awards, Contact Centre Sales Team of the Year category, 2010
- Finalist in the National Insurance Fraud Awards, Counter Fraud Initiative of the Year category, 2009
- Finalist in the European Contact Centre Awards, Large Team and Advisor of the Year categories, 2009
- Named in the Sunday Times 2008 PricewaterhouseCoopers Profit Track 100
- Finalists in the National Business Awards, 3i Growth Strategy category, 2008
- Finalist in the National Business Awards, Business of the Year category, 2007, 2009 and Highly Commended in 2008
- Named in the Sunday Times 2006, 2007, 2008 and 2009 HSBC Top Track 250 companies
- Regional winner of the National Training Awards, 2007
- Winner of the BITC Health, Work and Well-Being Award, 2007
- Highly Commended in the UK National Customer Service Awards, 2006
- Winner of the Tamworth Community Involvement Award, 2006. Finalist in 2008
- Highly Commended in The Press Best Link Between Business and Education, 2005 and 2006. Winner in 2007
- Finalist in the National Business Awards, Innovation category, 2005

1.8 About CPPGroup Plc

The CPPGroup Plc (CPP) is an international Life Assistance business offering bespoke management solutions to multi-sector business partners designed to enhance their customer revenue, engagement and loyalty, whilst at the same time reducing costs to deliver improved profitability.

This is underpinned by the delivery of a portfolio of complementary Life Assistance retail products, designed to help our mutual customers cope with the anxieties associated with the challenges and opportunities of everyday life.

Whether our customers have lost their wallets, been a victim of identity fraud or looking for lifestyle perks, CPP can help remove the hassle from their lives leaving them free to enjoy life. Globally, our Life Assistance products and services are designed to simplify the complexities of everyday living whether these affect personal finances, home, travel, personal data or future plans. When it really matters, Life Assistance enables people to live life and worry less.

Established in 1980, CPP has 10 million customers and more than 200 business partners across Europe, North and South America and Asia Pacific and employs 1,900 employees who handle millions of sales and service conversations each year.

In 2009, Group revenue was £292.1 million, an increase of more than 12 per cent over the previous year.

In March 2010, CPP debuted on the London Stock Exchange (LSE).

What We Do:

CPP provides a range of assistance products and services that allow our business partners to forge closer relationships with their customers.

We have a solution for many eventualities, including:

- Insuring our customers' mobile phones against loss, theft and damage
- Protecting the payment cards in our customers' wallets and purses, should these be lost or stolen
- Providing assistance and protection if a customer's keys are lost or stolen
- Providing advice, insurance and assistance to protect customers against the insidious crime of identity fraud
- Assisting customers with their travel needs be it an emergency (for example lost passport), or basic translation service
- Monitoring the credit status of our customers
- Provision of packaged services to business partners' customers

For more information on CPP visit:

www.cppgroupplc.com