

Is Wifi Safe?



Edexcel Extended Project Qualification

James Frost

What is Wi-Fi?

Wi-fi is a means by which electronic devices and computers exchange data wirelessly using radio waves through a computer network WLAN (Wireless Local Area Network). There are many devices that can connect to wireless networks, ranging from smart phones to laptops. Any device that can connect to a wireless access point can then access any network resource while still connected to the hotspot; the most obvious resource being the internet. Wireless hotspots can have a range varying from a few feet to a few miles, BT open zone being an example of the latter.

Wi-fi works by using a devices wireless adapter to translate data into a radio signal and transmit it using an antenna. A wireless router then receives the signal and decodes it. The router then sends the information to the Internet using a physical, wired Ethernet connection. The process also works in reverse, with the router receiving information from the Internet, translating it into a radio signal and sending it to the computer's wireless adapter.

Wireless networks provide convenience, mobility, and are cheaper to realize than wired networks in many cases. However the convenience, productivity gains, and cost savings of wireless networks are accompanied with a new set of vulnerabilities. Citation [What is Wifi?]
[Wifi]

I have split my project into two sections; the first is the data security implications of using wireless networks, and the second is the health implications of widespread wi-fi use.

Data Security Implications of Using Wi-Fi

The main security drawback of using wireless internet is how easy it can be to connect to it compared to a wired connection. For example, with a wired connection you have to be physically wired into the network, whereas with wireless internet you just have to be within range of the access point; you don't even have to be in the same building. In my home I picked up six wireless networks from our neighbors, in addition to our own. This is a major risk to the security of any wireless access point; the fact that anybody in range can easily access the network. This is the reason why many access points use passwords and encryption keys.

Encryption

The most common wireless encryption used in a WLAN (Wireless Local Area Network) is Wired Equivalent Privacy (WEP), first introduced in 1999. WEP is a security algorithm for wireless networks designed to give them the same level of security as wired

James Frost

networks. However, WEP has been shown to have several flaws.

WEP works by using secret keys to encrypt data. Both the device and the receiver must know the secret keys. Part of the encryption key is taken up by a variable called the Initialization Vector (IV). When a packet is sent it is encrypted using the secret key and the IV. This makes the packet look like random data, and therefore makes the packet unreadable to an outsider who does not know the security key. When the packet is received it is unencrypted, making the packet readable again.

This method of encryption is unsafe for several reasons; firstly, the IV values can be reused. Reusing keys is a major cryptographic weakness in any systems security, making it easier for third parties to be able to decrypt the packets being sent.

In fact, reusing IV keys is inevitable. IV keys are 24 bit (24 characters) long. This gives about 16.7 million IV key possibilities. This sounds like a lot, but on a single busy network this number can be achieved in a few hours. This means that reuse is unavoidable, making it easier for third parties to be able to decrypt the packets.

Weak IV keys are also susceptible to attack. Some keys, based on combinations (e.g. aabbcc etc) don't provide sufficiently random data, meaning packets can be decrypted. These are only a few of the weaknesses with WEP. It can take only 10 minutes for a hacker to crack a lowercase password that is only 6 characters long ^{Citation [Darell]}. This was demonstrated in 2005 by FBI Computer Scientist James C. Smith, whose team of FBI agents broke a 128 bit (128 characters) WEP key in about three minutes ^{Citation [Cheung, 2005]}.

Wi-fi Protected Access (WPA) and Wi-fi Protected Access 2 (WPA2) became available in 2003 to solve the issues with WEP. Both WPA and WPA2 are more secure than WEP, yet both these security protocols have flaws; WPA and WPA2 are vulnerable to brute force attacks if users rely on a weak password. A brute force attack is guessing all the possible values of a password until the correct one is found ^{Citation [Brute Force Attack, 2009]}. A third party may use this method with a list of common passwords to gain access to the wireless network. There are even websites that offer wireless network brute forcing services, using their extensive word list of common and obscure passwords and their powerful processor. Some of these sites claim it takes on average 20 minutes for them to gain access to a network via brute force. However, if a truly random password of thirteen characters or more is used, the wireless network should be secure from most brute force attacks. ^{Citation [Moskowitz, 2003]}

However, these encryption methods only work if an encryption key is set; by default, most Wi-fi routers do not have an encryption key set. For users who are not so tech savvy, they may not set an encryption key. This means that anyone can access their wireless network, meaning potentially hundreds of unsecured Wi-fi access points in the UK.

Even if your network is secured with a strong password, hackers could still gain access to your wireless network by breaking the encryption. This is most commonly done by using James Frost

a packet sniffing program (usually on Linux, as Windows cannot sniff packets). Firstly, hackers collect information about its configuration and associated clients, such as BSSID (Basic Service Set Identification; the MAC address of a wireless access point), channel and Access Point name *Citation [Reconnaissance of wireless networks]*.

To crack WEP encryption, about 5 million encrypted packets must be captured. This is because out of the possible 16 million IV keys, 9000 of them are considered vulnerable. By capturing 5 million packets, there will be roughly 3000 weak IV keys. These weak IV keys are then supplied to an algorithm which determines the WEP key. Fortunately, capturing enough packets and successfully cracking WEP encryption can take weeks, or even months. However, this process can be sped up by injecting packets into the network *Citation [Cracking of Wireless Networks]*.

WPA can be cracked when the pre shared key is shorter than 21 characters. Firstly, an authentication 'handshake' packet must be captured. This can be through a legitimate authentication or through a forced authentication by sending de-authentication packets to clients. The MAC address of the client that asked for authentication and the access point that gave authentication must then be hashed, and the crack is complete *Citation [Cracking of Wireless Networks]*. WPA2 can be attacked by using the WPA-PSK attack, but this is largely ineffective and inconsistent.

To further protect yourself from the risk of having your network cracked, you could use WPA or WPA2 with a RADIUS (Remote Authentication Dial in User Service) server. RADIUS is a protocol that provides AAA (Authentication, Authorization, and Accounting) management for computers to connect, and use a network service. RADIUS uses an external server to verify the user in a three stage verification process; the configuration of the device trying to connect to the WLAN, the wireless access point and the RADIUS server. Combine these in the right configuration, and users are either let on or denied access to the WLAN depending on credential validity. Encryption keys are set up for every session (if not every packet, depending on how the network is configured) to further secure the session *Citation [RADIUS]*.

Using this method is more secure, however if the RADIUS server is compromised, then so are all the connections to the server (e.g. everyone using the WLAN). RADIUS is also considerably more complicated to set up than standard encryption methods, and may require third party services, for example paying for RADIUS server access. This means that the majority of access points do not use RADIUS, and those that do are mainly businesses.

Other Security Measures

Because of the vulnerability of the encryption methods to being hacked, the use of 'two factor authentication' security methods are becoming more popular. A two factor authentication requires the presentation of two or more of the three authentication factors; knowledge factor, possession factor, inherence factor. The knowledge factor is usually a password or pin, the possession factor is usually a security card, and the inherence factor

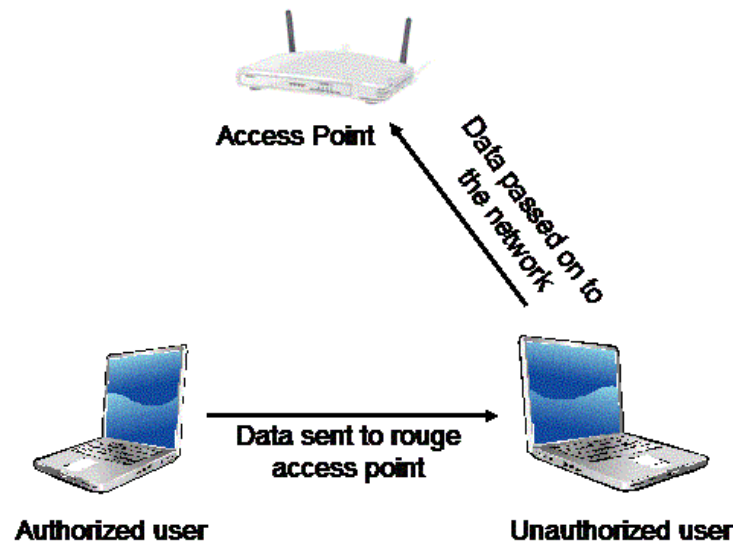
is usually a biometric characteristic, such as a finger print.

For most users, an encryption key and security card are sufficient to keeping the network safe from even the most determined hackers. However, setting up a two step authentication process can be costly, as it requires dedicated software and hardware that isn't commercially available. Because of this, two factor authentication is most commonly used by businesses, where the potential loss they could make from having their network compromised outweighs the cost of implementing the system. Even then, only the most security conscious companies implement a biometric system, as this is very costly

Threats to Data Security

So if the third party has gained access to your wireless network, what can they do? Firstly, they have access to the internet through your access point; this means anything they do on the internet through your wi-fi will be traced back to you. A few examples of this would be pirating files, theft of intellectual property rights, and hacking. As this can be traced back to your wi-fi network, this can have serious legal implications for you, as you have very little proof that it wasn't you that committed these offences.

Secondly, the third party could steal your personal information, passwords, even identity through wi-fi. There are several ways the third party could do this, the most common being a man in the middle attack.



A basic man in the middle attack Citation [Roche, 2007]

This form of attack is illustrated in the diagram above; the third party, the 'unauthorized user' in this case, puts themselves between the authorized user and the wi-fi access point, telling the authorized user that it is the access point, and the access point that it is the authorized user. This means that all packets exchanged between the authorized user and the access point go through the third party. The third party relays messages between

them, making them think they are communicating over a private connection, when the entire conversation is controlled and monitored by the third party; the third party can even inject new packets.

Once the third party has access to the information being exchanged, the hackers can use a program, such as Cain and Abel (a password recovery tool), to capture any private information being exchanged such as log in details, personal details, credit card details, etc.

However, a man in the middle attack could also be used to greater effect when larger numbers of people are connecting to a single wireless network, as this allows them to steal more information, etc. Hackers can do this by setting up a fake open wireless network in a public place that uses an already existing wireless network. An example of this would be going into a airport and creating a fake wi-fi network called 'Best Free Airport Public Wi-fi,' that connects to the internet using an already existing wi-fi, for example a café. The unsuspecting users then connect to the hacker's fake wi-fi and browse the web, not knowing that the hackers have access to and are storing all the private information being sent to and from the user's computer.

Alternatively, the third party can name their wi-fi network after a common wireless network that many people have connected to, for example BT-Open Zone. This means that many devices will connect by default to the hacker's wi-fi.

There are several methods that can be used to further protect your data when using unsecured networks; the most obvious being to encrypt any packets exchanged between your device and the router. This is usually done using the HTTPS protocol (Hypertext Transfer Protocol Secure). This simply 'layers' the HTTP protocol over the already existing SSL/TLS protocol, thus adding the security of the SSL/TLS protocol ^{Citation [HTTP Cookie]}. You can also use a VPN (Virtual Private Network). A VPN provides security so that traffic sent through the VPN connection stays isolated from other computers on the intermediate network, meaning that anyone trying to access your data cannot. However, many people neglect these methods of ensuring a secure browsing session on public or unsecured wi-fi ^{Citation [Microsoft, 2001]}.

Once the third party has access to this information, there are several things it can do with them; it could use the personal details to steal the person's identity, it could commit fraud with credit card or bank details, it could use the hacked accounts to spam, or simply sell the details on to a third party.

Thirdly, once the third party has access to your wi-fi they could use this access to put a malicious program onto your computer. There are many malicious programs they could use; for example, key loggers that log every keystroke (including passwords,) and send them back to the third party, a Remote Administration Tool (RAT) that gives the third party complete admin control over your computer, or as is most common, connect your computer to a botnet which the third party controls. This means that your computer could be used to send spam, take part in DDoS (Distributed Denial of Service) on websites or

take part in mass fraud.

Research

So how real is the security threat posed by using wireless networks? According to ispreview.co.uk, 'the number of unsecured wi-fi networks has declined from 25% in 2006 to 6% in 2011', but '77% of people with a secured wi-fi link would disclose the pass code to a friend,' and just 11% of firms provided guidance for staff on how to keep their data secure ^{Citation [Jackson, 2011]}.

CPP, a life assistance company, conducted a study across six UK cities and found that almost 40,000 private home wi-fi networks lacked adequate protection, and nearly a quarter of these networks had no password whatsoever. It also found that roughly half of home wi-fi networks could be hacked in less than 5 seconds ^{Citation (UK Report Exposes Poor WiFi ISP Security and Potential for Illegal P2P Abuse, 2010)}. UK internet service provider Talk Talk estimated that seven million homes and businesses are currently vulnerable to wi-fi attacks ^{Citation (UPDATE ISP TalkTalk Reveals 7 Million UK Homes Vulnerable to Wi-Fi Hijacking, 2009)}. These statistics, however, do not take into account the open networks in cafes, airports, etc. BT Open Zone has over four million wi-fi hotspots in the UK and Ireland ^{Citation (BT Openzone)}, and a study by the Office for National Statistics showed that 4.9 million people connected through open wi-fi hotspots such as hotels, cafes and airports over the last year in the UK.

I could not find coherent data about the wi-fi connections in and around London, so I did my own research. I did this using my Android smart phone and the WiGLE war-driving application. This app uses the wi-fi feature on my phone to scan for wi-fi's, and records data about the discovered connections, and then uses GPS to position the wi-fi. After a walking a distance of 9.48 miles through London with this application scanning, I had encountered 2776 wi-fi connections. Of these connections that I found, 1833 (66%) wi-fi hotspots used WPA2 security, 499 (18%) wi-fi hotspots used WPA security, 211 (8%) wi-fi hotspots used WEP security, and 233 (8%) wi-fi hotspots were unsecured. However, 138 of the unsecured wireless networks I found were 'Open Zones' (e.g. BT Open Zone) or were mobile phone towers (e.g. Vodafone UK); only 95 were private users. Please see below for a screenshot of my database.





Encryption Method	Percentage
WPA2	66%
WPA	18%
WEP	8%
No encryption	8% (of this 8%, only 41% were private users)

00:24:17:a PlusnetWireless	[WPA-PSK-TKIP+CCMP][WPA2-PSK-TKIP+CCMP]	#####	6	-90	51.53819	-0.15197	80	10	WIFI
00:16:e3:f BTVOYAGER2110-4F	[WEP]	#####	3	-83	51.53819	-0.15197	80	10	WIFI
00:1d:68:8 BTHomeHub-622F	[WEP]	#####	7	-83	51.53819	-0.15197	80	10	WIFI
02:24:17:c BTOpenzone-H		#####	1	-85	51.53819	-0.15197	80	10	WIFI
02:24:17:c BT FON		#####	1	-89	51.53819	-0.15197	80	10	WIFI
c0:3f:0e:0 flat2_27regentspark	[WPA-PSK-TKIP]	#####	6	-84	51.53818	-0.15196	82	10	WIFI
90:01:3b:2 SKY59299	[WPA-PSK-TKIP+CCMP][WPA2-PSK-TKIP+CCMP][WPS]	#####	1	-88	51.53818	-0.15196	82	10	WIFI
00:21:e9:b W-Net	[WPA2-PSK-CCMP]	#####	6	-77	51.53818	-0.15194	82	15	WIFI
c4:3d:c7:3 virginmedia7001796	[WPA-PSK-TKIP+CCMP][WPA2-PSK-TKIP+CCMP]	#####	11	-80	51.53818	-0.15194	82	15	WIFI
5c:d9:98:0 SKY24639	[WPA-PSK-TKIP+CCMP][WPA2-PSK-TKIP+CCMP]	#####	1	-81	51.53818	-0.15194	82	15	WIFI
00:fe:f4:6l BTHub3-NKNW	[WPA-PSK-TKIP+CCMP][WPA2-PSK-TKIP+CCMP]	#####	6	-81	51.53818	-0.15194	82	15	WIFI
00:fe:f4:5l BTHub3-ZS4C	[WPA-PSK-TKIP+CCMP][WPA2-PSK-TKIP+CCMP]	#####	11	-81	51.53818	-0.15194	82	15	WIFI
c4:3d:c7:3 virginmedia4986923	[WPA-PSK-TKIP+CCMP][WPA2-PSK-TKIP+CCMP][WPS]	#####	7	-84	51.53818	-0.15194	82	15	WIFI
4c:17:eb:8 SKY8E5AD	[WPA-PSK-TKIP+CCMP][WPA2-PSK-TKIP+CCMP][WPS]	#####	6	-84	51.53818	-0.15194	82	15	WIFI
e0:46:9a:1 EchoSourcing	[WPA2-PSK-CCMP]	#####	13	-89	51.53818	-0.15194	82	15	WIFI
00:1f:9f:4f O2wireless880403	[WEP]	#####	1	-86	51.53818	-0.15194	82	15	WIFI
02:fe:f4:6l BTWiFi		#####	6	-81	51.53818	-0.15194	82	15	WIFI
12:fe:f4:6l BTWiFi-with-FON		#####	6	-81	51.53818	-0.15194	82	15	WIFI
23415_10_vodafone UK	UMTS:gb	#####	0	-51	51.53818	-0.15194	82	15	GSM
00:01:3b:a BTHub3-WKN5	[WPA-PSK-TKIP+CCMP][WPA2-PSK-TKIP+CCMP]	#####	11	-78	51.53818	-0.15194	82	15	WIFI
00:24:2b:3 BTHomeHub2-ZW8Q	[WPA-PSK-TKIP+CCMP][WPA2-PSK-TKIP+CCMP]	#####	1	-83	51.53818	-0.15194	82	15	WIFI
4c:17:eb:6 SKY68064	[WPA-PSK-TKIP+CCMP][WPA2-PSK-TKIP+CCMP][WPS]	#####	11	-85	51.53818	-0.15194	82	15	WIFI
00:26:bb:7 Marvin	[WPA2-PSK-CCMP]	#####	4	-88	51.53818	-0.15194	82	15	WIFI
06:26:bb:7 Arthur	[WPA2-PSK-CCMP]	#####	4	-88	51.53818	-0.15194	82	15	WIFI
a0:21:b7:f virginmedia3500914	[WPA-PSK-TKIP+CCMP][WPA2-PSK-TKIP+CCMP][WPS]	#####	11	-85	51.53818	-0.15194	82	15	WIFI
a0:21:b7:4 virginmedia0009430	[WPA-PSK-TKIP+CCMP][WPA2-PSK-TKIP+CCMP][WPS]	#####	6	-92	51.53818	-0.15194	82	15	WIFI
12:01:3b:a BT FON		#####	11	-77	51.53818	-0.15194	82	15	WIFI
02:01:3b:a BTOpenzone-H		#####	11	-78	51.53818	-0.15194	82	15	WIFI
02:24:2b:3 BT FON		#####	1	-81	51.53818	-0.15194	82	15	WIFI
02:24:2b:3 BTOpenzone-H		#####	1	-84	51.53818	-0.15194	82	15	WIFI
00:1f:1f:d Edimax AP		#####	11	-85	51.53818	-0.15194	82	15	WIFI
23415_255_vodafone UK	UMTS:gb	#####	0	-51	51.53818	-0.15194	82	15	GSM
00:18:4d:b Flat.Orange	[WPA-PSK-TKIP]	#####	1	-83	51.53818	-0.15194	82	15	WIFI
a2:21:b7:b SKY25376_EXT	[WPA-PSK-TKIP][WPS]	#####	8	-84	51.53818	-0.15194	82	15	WIFI
00:1f:33:1 SKY25376	[WPA-PSK-TKIP]	#####	8	-85	51.53818	-0.15194	82	15	WIFI
2c:b0:5d:f virginmedia7201393	[WPA-PSK-TKIP+CCMP][WPA2-PSK-TKIP+CCMP][WPS]	#####	1	-85	51.53818	-0.15194	82	15	WIFI
00:ac:54:f: BTHub3-ZQRX	[WPA-PSK-TKIP+CCMP][WPA2-PSK-TKIP+CCMP]	#####	11	-89	51.53818	-0.15194	82	15	WIFI
02:ac:54:f: BTOpenzone-H		#####	11	-88	51.53818	-0.15194	82	15	WIFI


The above is a screenshot of the database of information I collected on my walk. In the first, second and third column it shows the MAC address, access point name and encryption type respectively.

From my research I can conclude that the large majority of people (66%) use the currently available highest level of encryption (WPA2), and that only the small minority (less than 8%) had an unsecured network. This contradicts the figures I found online (which were a few years old), and suggests that over the last few years people have become more aware about securing there wireless networks and computers. However, my research may not be a representative sample of the whole country, and it also does not show whether the wireless networks are venerable to dictionary attacks (one of the most basic kinds of attack a hacker could use).

It does not matter how well secured your wireless network is if someone has the ability to hack it. In an attempt to find out how widespread the wi-fi hacking problem is, I went online; a simple Google offered me many in depth guides and videos. A deeper search found a dedicated hacking forum with a whole subsection for wi-fi hacking.

	Cryptography, Encryption, and Decryption For discussion on keys, ciphers, and algorithms often used to keep information secret. Encryption is the art of concealing data and code.	24,167	184,966
	Botnets, IRC Bots, and Zombies Sounds like a horror movie and for some it is. What is a botnet? Topics for botnets belong in this area.	31,667	305,449
	Wifi WPA WEP Wireless Hacking For hacking wireless networks, wep/wpa encryption, sniffers, backtrack, setup, connection problems, aircrack and other wifi related discussions please join this forum.	8,570	71,015
	Phreaking Cells Mobiles and PDA's Phreaking has been around for decades. Learn to hack cellular phones, unlock cells, call tracing, and do reverse phone lookups. All mobile hacking discussion belongs here. iPhone and iPod Touch Mobile Applications	12,974	100,852
	AIM MSN IRC ICQ and IM Hacks If you are into exploiting instant messaging systems then we have a perfect forum for you. Post here for AIM hacks and other IM exploits.	6,155	60,197

In this subsection there were various guides on wi-fi hacking, people asking questions on the subject, even people posting programs for others to download that claimed to hack others wi-fi for you!



A comprehensive guide about wi-fi hacking

Written by Magnur

► **Introduction**

Hello and welcome to my tutorial about wireless networking. Today I'll be teaching you how easy it is to obtain access to a wireless protected network. There are lots of questions coming from the beginners on how to crack WEP/WPA/WPA2 keys and accessing their neighbor's connection. The purpose of this tutorial is to answer them. Judging from the "tutorials" on youtube which are either obsolete, or simply misguiding the listeners, this tutorial will be different. I will be covering all of the aspects and ways of hacking a network and gaining access to the router. This tutorial will be divided in 2 parts, such as WEP and WPA/WPA2 hacking. Please read below on what you need to succeed.

► **Stuff Needed**

- Backtrack 5 - I would suggest GNOME, 32Bit, ISO & Direct
- Compatible Wireless Card
- WPA Word List - Search via torrents to find one

► **List of content**

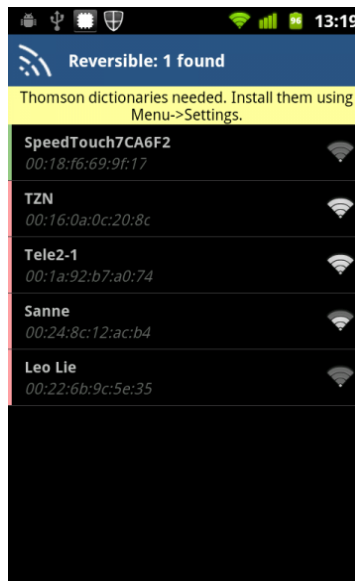
- Making a bootable USB
- WEP encrypted networks
- WPA/WPA2 encrypted networks
- Commands Used

From this I can gather that wi-fi hacking and wi-fi hacking tools are common place and widely shared and accepted on the internet, and anyone can easily access them. This means that anyone with a basic understanding of computers could potentially gain access to a private wireless network. However, due to the nature of wi-fi, the hacker would have to be in physical range of your wi-fi to be able to hack it. This is good, as in most cases it would be unpractical for hacker to bring all their electronically equipment to within range of your network, even with a car. For example, they would need a laptop computer with a wireless card, an antenna mounted on the car, a power inverter, a connected GPS receiver, and a way to connect to the internet wirelessly. This deters most from pursuing this method (called 'War Driving'), as it would be very impractical.

Future of Security Threats

However, with the rapid rise of smart phones, wi-fi hacking may become more widespread. Most smart phones have GPS, wireless, and 3G internet capabilities. Using

my Android smart phone, a quick Google bought up several applications. One application called 'Penetrate,' allowed me to perform dictionary attacks on any wi-fi networks in range. If when setting up a wi-fi access point, a user states that they want to encrypt data, by default an encryption key is chosen for the user. Some users do not change this key. Different makes of router use different default encryption keys. This app reads the type of routers in range of your phone, and then gives you the default encryption keys for that type of router. This is called a dictionary attack, as you are simply trying passwords from a list (or 'dictionary').



Another application called 'Droid Sheep' allowed me to perform basic man in the middle attacks, allowing me access to whatever any users were currently doing on the network. This app was so sophisticated that you even save the cookies (a small piece of data sent from a website and stored in a user's web browser while a user is browsing a website) and use them later on your own computer to access that user's account at a later date!



Perhaps the most dangerous application for Android smart phones is an application called 'Anti' (Android Network Toolkit Capabilities). What makes this application so dangerous is the way that it operates; most smart phones lack the necessary processing power required to hack wi-fi encryption, meaning most applications are limited to basic man in the middle attacks. However, Anti operates in a different manner; the user purchases 'Exploit Credits;' the user then spends these credits on hacking wi-fi connections using the companies much bigger, much more powerful automated server, using the phone as a relay point between the two. This means that someone can have the power of a very large dedicated wi-fi hacking server on their smart phone, making most computer networks very vulnerable.



However, this application is not just used for hacking wi-fi connections; once the wi-fi has been hacked, the application then allows you to do several things on the subject computers, such as open the computers command line interface, eject the CD tray, execute calculator, reboot the computers, shutdown the computers, get the process list, even grab screenshots! The user can also spend their credits on man in the middle attacks, denial of service attacks on the network, replace all images that a target browses on the internet with a picture of your choice, steal passwords and images, all the while formulating a report with all this information and sending it to you via email for later review ^{Citation [ZImperium LTD]}.

Laws

If you have been a victim of this form of hacking, is the law on your side? In the UK the computer misuse act was introduced in 1990, and amended in 2006. The act introduced three criminal offences; unauthorised access to computer material, unauthorised acts with intent to impair operation of the computer, and making, supply or obtaining articles for use in computer misuse offences. If you break these laws you are punishable by a maximum fine of £5000 and up to five years in prison.

However, prosecutions in the UK under the computer misuse act appear to be dropping; Crispin Blunt, prisons minister at the Ministry of Justice released the following information in response to a question by a member of parliament regarding the act.

Year	2006	2007	2008	2009	2010
Defendants for offences under the Computer Misuse Act	25	19	17	19	10

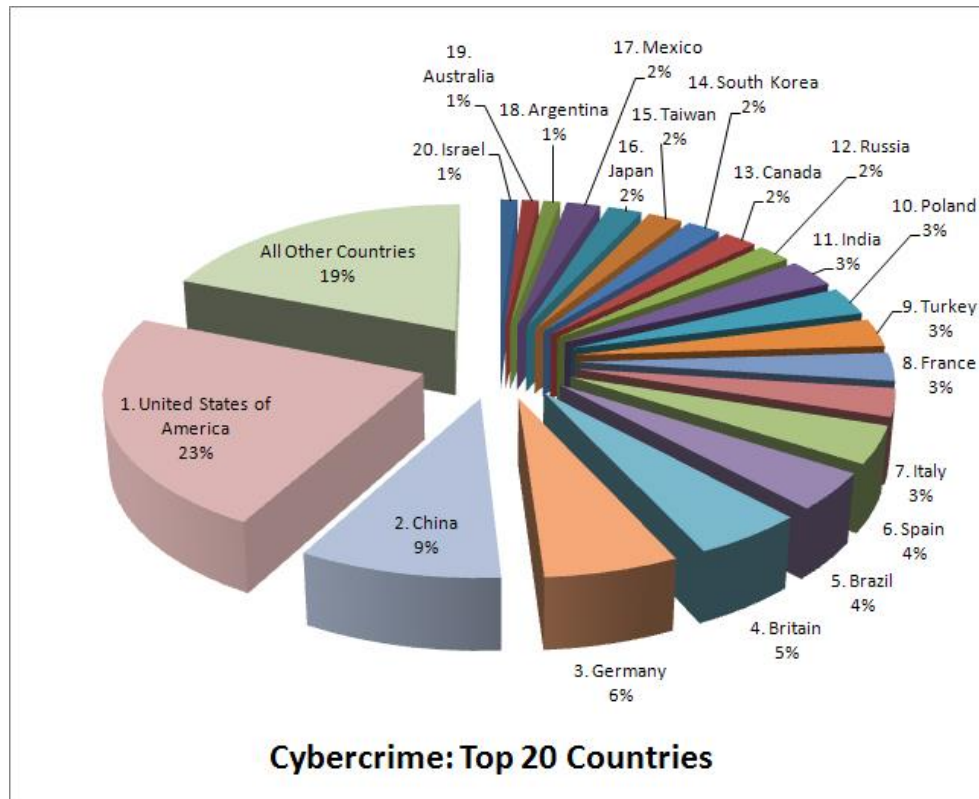
Citation [Parliament]

These figures show that since 2006 the number of defendants under the computer misuse act has been falling, when cybercrime offences are rising yearly:

Year	2006	2007	2008
Total Cyber Crime Offences Committed	3,237,500	3,278,700	3,415,900
Percentage Change From Previous Year	N/A	+1%	+4.2%

These figures suggest that the majority of cyber criminals are getting away with these offences, and that the government is struggling to catch these criminals. From this I can conclude that in the UK if you are victim of cyber crime, there is almost no chance that the person who committed the crime will be brought to justice. Equally, if you commit a cyber crime offence you will also most probably get away with it.

As uncontrollable as the UK cybercrime phenomenon may seem, in some developing countries it is much worse. In Sri Lanka, the Computer Crime act was introduced in 2007. Since then there have been 194 investigations, but no convictions. Please see below for a pie chart of the top twenty nations effected by cyber crime *Citation [194 computer crime investigations ongoing but no indictments yet, 2011]*.



The chart above shows the percentage cybercrime in the top twenty countries. This graph does not take into account population size; for example, USA is more likely to have a higher percentage of cybercrime victims than Germany as it has a considerably larger population. Citation [Cybercrime: Top 20 Countries]

The most serious draw back of computer crime laws is that it is limited in its ability to globally combat cybercrime. To resolve this issue, the 'European Convention on Cybercrime', was adopted by the EU Committee of Ministers of the Council of Europe in November 2001. It is designed to provide a common international method for dealing with cybercrime in Europe.

A case study of international cybercrime law would be the Pirate Bay. The Pirate Bay is a file sharing website set up in 2003, and hosts over 4 million torrents. It is currently the 77th most visited website in the world according to Alexa internet. The Pirate Bay has been accused of pirating \$382 trillion. According to the RIAA, that's 46 times more dollars than actually exists). Yet over the last nine years and many attempts to take the website down (legal and non-legal), it is still providing people with pirate downloads Citation [The Pirate Bay] [RIAA vs The Pirate Bay].

A case study where international cybercrime law has been successful in prosecution would be Napster, a peer to peer file sharing site. On December 7, 1999 the RIAA (Recording Industry Association of America) filed a law suite against Napster. On July 2001, Napster shut down its entire network in order to comply with the injunction. On September 24, 2001, the case was partially settled. Napster agreed to pay music creators and copyright owners a \$26 million settlement for past, unauthorized uses of music.

Because of the size of this fine, Napster was forced to become a paid subscription service
Citation [Napster] .

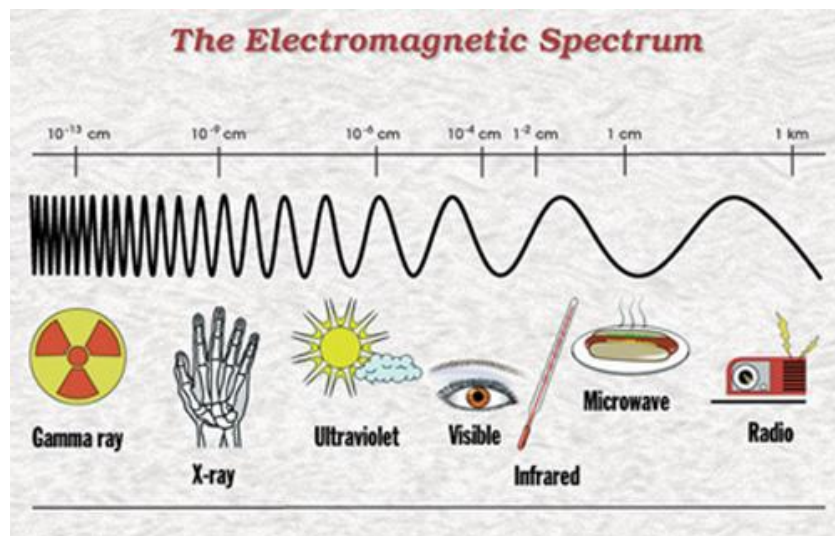
Health Implications of Wireless Networks

A wireless network uses radio waves, like mobile phones and radios do. A computer's wireless adapter translates the data into a radio signal and transmits it using an antenna .A wireless router receives the signal and decodes it. The router sends the information to the Internet using a physical, wired Ethernet connection. This process also works in reverse when the computer is receiving information.

This radio field is one of several different types of electromagnetic radiation (EMF). An electromagnetic field (also EMF or EM field) is a physical field produced by moving electrically charged objects
Citation [Brain & Wilson] .

Radiation poses a health risk as radioactive elements emit high energy particles. If you stand in the way of those particles, they are going to interact with the cells of your body. If the radiation changes DNA molecules enough, the cells can't replicate and begin to die, which causes the immediate effects of radiation sickness; nausea, swelling, hair loss. Cells that are damaged less severely may survive and replicate, but the changes in their DNA can disrupt normal cell processes, like the mechanisms that control how and when cells divide. Cells that can't control their division grow out of control, becoming cancerous, creating tumours.

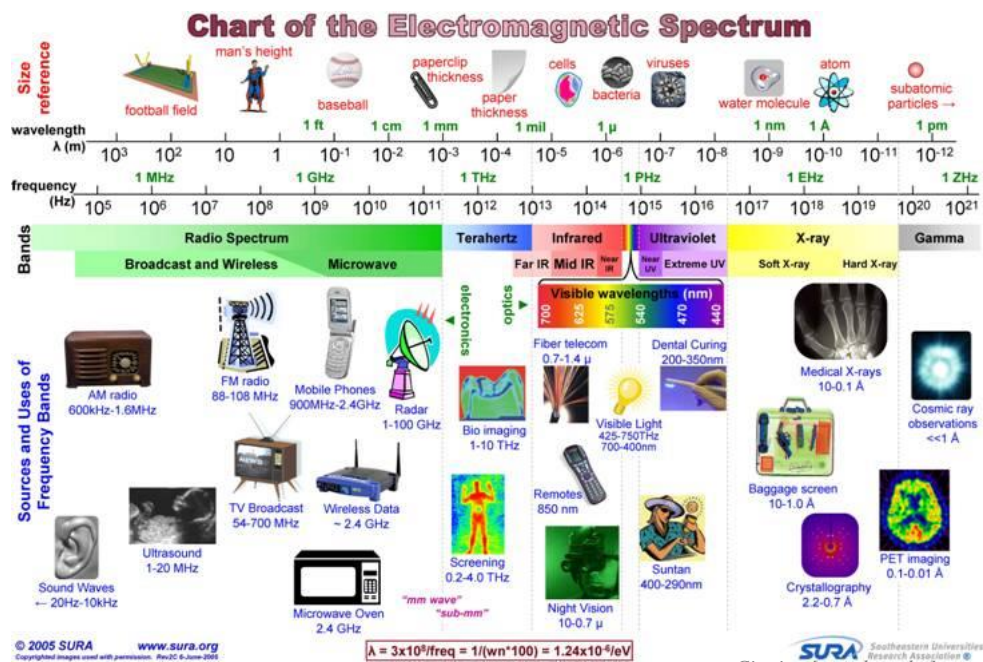
The higher the EMF frequency, the more serious the health effect. This is because the higher the frequency, the more energy the EMF has, meaning it will do more damage posing a more serious health risk. Gamma rays have the most energy (highest frequency) and radio waves have the least energy (lowest frequency)
Citation [Ashford, 2011] .



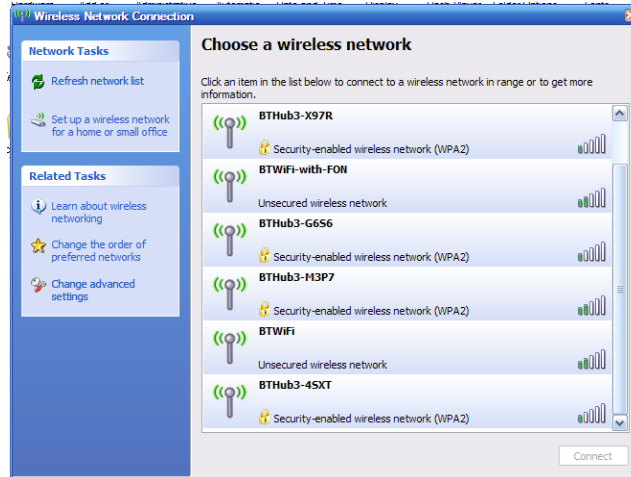
The different types of radiation in the Electromagnetic Spectrum;
Citation [Lorentz, 2005]

However wi-fi radio waves have a key difference to other kinds of radio waves; they transmit at frequencies of 2.4 GHz ($2.4 \times 10^9 \text{ Hz}$) or 5 GHz ($5 \times 10^9 \text{ Hz}$). This frequency is considerably higher than the frequencies used for cell phones (GSM phones use 1.8 or 1.9 GHz and the UMTS 3G phones use 2.1 GHz.). The higher frequency is used for wi-fi as it allows the signal to carry more data, meaning faster speeds *Citation [Brain & Wilson]*.

This level of electromagnetic radiation may not be as high as being exposed to x-rays which is in the range of $3 \times 10^{16} \text{ Hz}$ to $3 \times 10^{19} \text{ Hz}$, but is still a very large and powerful electromagnetic field, and this level of radiation is considered by scientists to be potentially dangerous. To put it in perspective, the typical home or office wireless networks transmit radio signals in the same general frequency range as the frequency that microwave ovens use to cook food *Citation [Safe Space Protection]*.



So how much are we exposed to electromagnetic radiation as a result of wi-fi? Most wi-fi health damage comes when people don't turn off their wireless routers at night; this means that you are being exposed to EMF's at all hours of the day in your own home.



The different wireless networks in range of my house

You are also not only being exposed to your own wi-fi, but also your neighbours if you are in range of their wireless modem. In my own home, excluding our home wi-fi, I am in range of six other wi-fi networks, increasing the amount of electromagnetic radiation I am exposed to.

This does not take into account all the other (potentially more powerful) open wi-fi hotspots that you are exposed to. An example of this large scale open wi-fi would be BT Open Zone, which accounts for 40% of the UK's wi-fi hot spot population. This uses mobile phone masts to cover large areas. As they are covering a larger area, they must use a more powerful EMF. These towers most commonly use Microwaves, which have a frequency of roughly 300 GHz (3×10^{11} Hz); 60 times more powerful than the radio waves used in wi-fi routers. These microwaves can travel for up to 45 miles and can easily penetrate brick and metal ^{Citation [Safe Space Protection]}.

Some of the most powerful cell tower installations are on mountains and hilltops outside of urban areas. These electromagnetic fields have impacted humans, animals and the ecosystem. Studies of people and farm animals living around a powerful electromagnetic field exhibit everything from stress and sleep disorders to birth defects, cancer and Alzheimer's.

Research

In a 9.48 mile walk in London, I encountered 2776 wi-fi connections, which means 2776 electro magnetic radiation emitters. Of these 2776 connections, 150 of them were mobile phone towers, meaning that 150 of these connections I encountered were more harmful microwave emitters.

The image below is a map of the wi-fi networks I encountered on my walk, compiled using the WiGLE war driving application for my Android phone.

So what are the health implications of wi-fi? Scientists are struggling to come up with a comprehensive answer, with the results of scientific studies split 50/50 as to whether wi-fi poses any health risks. Since wi-fi is so new, no studies have yet been done on the long term health effects of wi-fi. However, thousands of studies have been done on the health effects of mobile phones, and so far these studies have found that mobile phone radiation poses no health risk, and may only slightly increase the risk of cancer. However, the long term effects on health of mobile phone use is still unknown, with detectable tumours taking many years (roughly 15 to 20 years depending on the type of cancer) to develop. Because of the potential health implications of mobile phone use, mobile phone companies are now recommending consumers to use the provided headphones and microphone, rather than hold the phone up to their head to minimise potential health implications.

Page 17 of 17

and others. After a review of 2,000+ such studies, the National Institute of Environmental Health Sciences concluded emf's 'should be regarded as possible carcinogens.' We may also generalise the results of studies into microwaves, as they emit similar emf radiation. Some of these studies suggest that long-term exposure may have a carcinogenic effect, suggesting that wi-fi radiation of a similar frequency may also be carcinogenic ^{Citation} *[Microwave Health Effects]*.

Children are especially vulnerable to wi-fi radiation signals as their nervous systems and brains are still developing. Their skulls are thinner and smaller, so the radiation penetrates their brains more deeply. Many schools are now using wi-fi; 70% of secondary schools in the UK have some form of wi-fi installed. This means that we are exposing the next generations to potential health risks that we are unsure of the long term health implications.

What Can Be Done To Negate Potential Health Problems

As of yet, there are no commercially viable, scientifically proven ways that can protect you from emf radiation; however, in some countries such as Sweden, if you are believed to have 'electromagnetic hypersensitivity,' then the government will pay for your house to be painted by radiation proof paint to protect you from outside emf sources ^{Citation} *[Safe Living Technologies]*.

Conclusion

To conclude, in my research I found that the encryption people are using on there wireless networks is more secure than the figures from a few years ago. This may be due to an increased awareness of computer security, propagated through the media. As of yet, there is no reliable method available for cracking WPA and WPA2 encryption making them the most secure method of protecting your network from third parties. However, I found that less than 8% of networks were unsecured and 8% used WEP encryption, meaning that there are still people at risk from third parties easily gaining access to their network, though this number has greatly decreased compared to a few years ago. With increasing numbers of the population using smart phones, I believe this 16% to be at an ever increasing risk of having their network compromised, and in this digital age where an ever increasing part of our lives is online, this can have devastating consequences. The increasing number of people using unsecured, public access points for online banking and other services may also result in an ever increasing number of people falling prey to malicious hackers.

As for the physical aspect of wi-fi safety, time will only tell whether using wireless internet is having any adverse effects on our health. However, judging by similar studies, long term emf exposure can contribute to a number of health issues, and I suspect that with the ever increasing use of wireless networks, we can expect to see adverse effects to people's health.

Glossary

Alexa Internet – A website that provides traffic data, global rankings and other information on thousands of websites

Algorithm - an algorithm is a step-by-step procedure for calculations

Android – a Linux based operating system designed primarily for touchscreen mobile devices

AP Name – Access Point Name

Biometric - the identification of humans by their characteristics or traits

Brute Force Attack - Guessing all the possible values of a password until the correct one is found

BSSID – Basic Service Set Identification; the MAC address of a wireless access point

Ddos – Distributed Denial of Service; when multiple systems flood the bandwidth or resources of a targeted system, usually by using a botnet or coordinated group attack

Encryption - In cryptography, encryption is the process of encoding information so that hackers cannot read it, but that authorized parties can

Ethernet – A group of computer networking technologies for local area networks

HTTP – the data transfer protocol used on the World Wide Web

Linux – a Unix-like computer operating system assembled under the model of free and open source software development and distribution

MAC Address – Media Access Control address; a unique identifier assigned to network interfaces for communications

Packet - In computer networking, a packet is a formatted unit of data carried by a packet mode computer network

SSL/TLS – Secure Sockets Layer/Transport Layer Security; cryptographic protocols that provide communication security over the Internet

SSL/TSL - cryptographic protocols that provide communication security over the Internet

VPN - Virtual Private Network; a technology for using the Internet or another intermediate network to connect computers to isolated remote computer networks that

would otherwise be inaccessible

WiGLE – Wireless Geographic Logging Engine; a website for collecting information about the different wireless hotspots around the world

Windows – a series of graphical interface operating systems

Bibliography

- (n.d.). Retrieved from Parliament:
<http://www.publications.parliament.uk/pa/cm201213/cmhansrd/cm120516/text/120516w0002.htm#1205165002281>
- Brute Force Attack*. (2009, October 30th). Retrieved from Hackosis: <http://www.hackosis.com/brute-force-attack/>
- UPDATE ISP TalkTalk Reveals 7 Million UK Homes Vulnerable to Wi-Fi Hijacking*. (2009, October 21st). Retrieved from ispreview: <http://www.ispreview.co.uk/story/2009/10/21/isp-talktalk-reveals-7-million-uk-homes-vulnerable-to-wi-fi-hijacking.html>
- UK Report Exposes Poor WiFi ISP Security and Potential for Illegal P2P Abuse*. (2010, October 14th). Retrieved from ispreview: <http://www.ispreview.co.uk/story/2010/10/14/uk-report-exposes-poor-wifi-isp-security-and-potential-for-illegal-p2p-abuse.html>
- 194 computer crime investigations ongoing but no indictments yet*. (2011, April 11th). Retrieved from lankanewspapers: <http://www.lankanewspapers.com/news/2011/4/66170.html>
- Ashford, M. (2011, March 16th). *FYI: How Does Nuclear Radiation Do Its Damage?* Retrieved from POPSCI: <http://www.popsci.com/science/article/2011-03/fyi-how-does-nuclear-radiation-do-its-damage>
- Brain, M., & Wilson, T. V. (n.d.). *How Wifi Works*. Retrieved from How Stuff Works: <http://computer.howstuffworks.com/wireless-network1.htm>
- BT Openzone*. (n.d.). Retrieved from Wikipedia: http://en.wikipedia.org/wiki/BT_Openzone
- Cheung, H. (2005, March 31st). *The Feds can own your WLAN too*. Retrieved from SmallNetBuilder: <http://www.smallnetbuilder.com/wireless/wireless-features/24251-thefedscanownyourwlantoo>
- Cracking Of Wireless Networks*. (n.d.). Retrieved from Wikipedia: http://en.wikipedia.org/wiki/Cracking_of_wireless_networks#Penetration_of_a_wireless_network
- Cybercrime: Top 20 Countries*. (n.d.). Retrieved from intellectualltakeout: <http://www.intectualltakeout.org/library/chart-graph/cybercrime-top-20-countries>
- Darell, R. (n.d.). *Hacked: The Average Cost Of Being Hacked [Infographic]*. Retrieved from Bitrebels: <http://www.bitrebels.com/technology/hacked-the-average-cost-of-being-hacked-infographic/>
- ezee-breathe. (n.d.). *Electromagnetic Oscillation*. Retrieved from ezee-breathe: http://www.ezee-breathe.com/electromagnetic_oscillation.htm
- HTTP Cookie*. (n.d.). Retrieved from Wikipedia: http://en.wikipedia.org/wiki/HTTP_cookie
- Jackson, M. (2011, September 13th). *Most British People Happy to Piggyback Online via Unsecured Home WiFi Networks*. Retrieved from ispreview: <http://www.ispreview.co.uk/story/2011/09/13/most-british-people-happy-to-piggyback-online-via-unsecured-home-wifi-networks.html>
- Lorentz, K. (2005, June 7th). *A Famous "FIRST" Launched by NASA to Study Earth's Energy*. Retrieved from http://www.nasa.gov/centers/langley/science/FIRST_prt.htm
- Microwave Health Effects*. (n.d.). Retrieved from Wikipedia: http://en.wikipedia.org/wiki/Microwave#Health_effects
- Mircosoft. (2001, September 4th). *Virtual Private Networking: An Overview*. Retrieved from Technet: <http://technet.microsoft.com/en-us/library/bb742566.aspx>
- Moskowitz, R. (2003, November 4th). *Weakness in Passphrase Choice in WPA Interface*. Retrieved from WNN Wifi Net News: http://wifinetnews.com/archives/2003/11/weakness_in_passphrase_choice_in_wpa_interface.html
- Napster*. (n.d.). Retrieved from Wikipedia: <http://en.wikipedia.org/wiki/Napster>
- RADIUS*. (n.d.). Retrieved from Wikipedia: <http://en.wikipedia.org/wiki/RADIUS>

Reconnaissance of wireless networks. (n.d.). Retrieved from Wikipedia:
[http://en.wikipedia.org/wiki/Cracking_of_wireless_networks#Reconnaissance of wireless networks](http://en.wikipedia.org/wiki/Cracking_of_wireless_networks#Reconnaissance_of_wireless_networks)

RIAA vs The Pirate Bay. (n.d.). Retrieved from <http://img140.imageshack.us/img140/6361/pbriaa.png>

Roche, M. (2007, December 2nd). *Wireless Hacking*. Retrieved from Washington University:
http://www.cse.wustl.edu/~jain/cse571-07/ftp/wireless_hacking/index.html

Safe Living Technologies. (n.d.). *RF Shielding Paint*. Retrieved from Safe Living Technologies:
http://www.safelivingtechnologies.ca/RF/Products_RF_Shielding_Paint_HSF54.htm

Safe Space Protection. (n.d.). *Is Cell Tower Radiation Dangerous?* Retrieved from Safe Space Protection:
<http://safespaceprotection.com/electrostress-from-cell-towers.aspx>

Safe Space Protection. (n.d.). *Wi-Fi Health Dangers & Radiation Health Effects*. Retrieved from Safe Space Protection: <http://safespaceprotection.com/electrostress-from-wireless-routers.aspx>

The Pirate Bay. (n.d.). Retrieved from Wikipedia: http://en.wikipedia.org/wiki/The_pirate_bay

What is Wifi? (n.d.). Retrieved from Webopedia: <http://www.webopedia.com/TERM/W/Wi-Fi.html>

Wifi. (n.d.). Retrieved from Wikipedia: <http://en.wikipedia.org/wiki/Wifi>

ZImperium LTD. (n.d.). *zantiapp*. Retrieved from zantiapp: <http://www.zantiapp.com/anti.html>