

## 2. Introduction

Computer usage of the Internet amongst consumers is constantly growing. This growth has and is being driven by broadband. The Internet Access 2007 [1] report published by the Office for National Statistics shows that in 2007, 51 percent of households had broadband Internet access. This is a 40 percent increase from 2006. The report also identifies the frequency of Internet use, which is put at 67 percent for adult who access every day or almost every day.

Homes are one of the most popular locations for setting up a small business [2]. Some of the reasons for setting up at home are cost saving and convenience. Hence, the home computer is also used for business purposes. For this reason, home businesses fall into the consumer category.

Consumer Internet usage is very different from Internet usage within a business. The main difference is control and risk management. Small and medium-sized businesses and large enterprises control the Internet usage of their users. These controls are applied to protect the business and their users. For example; I currently work for a medium sized business as a Network Engineer. The business has computer and Internet use policies, which the users have agreed too. User access controls are employed for appropriate permissions. Network and Internet access controls are employed with network segregation, firewalls and Internet proxies. Monitoring and protection are employed with anti-virus, anti-spam and personal firewalls.

Consumers have to fend for themselves on an Internet that is becoming more hostile. I say hostile because of the ever-growing risks. Let just consider one example: An un-patched browser vulnerability that allows a hacker to take control a PC. This could be activated by a malicious Java Script, which materialises itself as a Cross-Site Scripting (XSS) link on a blog website. When the user clicks on link, the software vulnerability is exploited. Let's just consider this example again; do consumers know about XSS or software vulnerabilities? Would they know how to protect themselves against these risks? Now consider all the other threats they are subject too.

The consumer Internet environment is uncontrolled. This is because consumers are not aware of the risks and they do not have sufficient Internet security knowledge or skills. Therefore, for this thesis, I have termed this consumer Internet environment, the uncontrolled environment.

This uncontrolled environment is not a new concept. There are important factors for businesses operating with the consumer market. Consumer PCs are the weak link as they are uncontrolled. Hence, they could provide an avenue for a security breach.

Fraud [3] and breaches [8] [9] are increasing. They are also becoming more sophisticated. Direct to consumer (D2C) business is increasing in the form of e-commerce and e-banking. This is clear from the following reports: APACS (Association for Payment Clearing Services) reported in December 2006 that 48 percent of all Internet users use e-banking [4]. The Internet Access 2007 [1] report reported that Internet purchases by consumers increased by 20 percent in 2007. There is also the trend of home working where a computer is used, which is outside of the control of the business. 76 percent of candidates from the Computers Usage on the Internet survey conducted said that they access their work place computer system solely by entering a password. However, this might be web based email, for example Microsoft Exchange Outlook Web Access (OWA). Also, according to Analyst Gartner [5], home working will increase each year by 4.3 percent. They also state that home workers pose a security threat even with company controlled computers. One of the factors for the increase in home working is the Flexible Working and Work-Life Balance law [6]. This allows parents to make a request to their employer for flexible working if they have a child under 6 or a disabled child under 18. The employers must consider the request seriously and only reject for good business reasons.

This introduction has briefly identified trends and problems faced by consumers and small businesses in this uncontrolled environment. Can the risks be mitigated with new technology with forces users to change their usage habits?

Microsoft Windows Vista and EMV dynamic passcode authentication with card reader devices (specifically the Barclaycard implementation [7]) have been championed by the computing press as security products that will make major impact upon reducing threats. This thesis will investigate what impact each of these

technologies have and how effective they really are when used by consumer users in the uncontrolled environment I have defined. This thesis will also investigate the enforced usability changes employed by these technologies and conclude on their appropriateness.

### 3. Determine the Environment

What is the extent of this uncontrolled environment? We have the common threats and we have threats presented by user actions. The common threats are known and are constantly reported upon so they will be briefly overviewed. The consumer usage threats have been identified through a detailed investigation.

#### 3.1 Common Threats

The year on year growth of malware has slowed but as reported in various threat reports, malicious activity is becoming more sophisticated [8]. The threat landscape has changed from one of mass impact to be more targeted. This has been made possible by the online availability of customised malicious toolkits. Also, phishing emails and websites have become more realistic.

Malware infection can be the source of many problems. Consider the installation of a trojan. This trojan could facilitate the process taking control of PCs, it could steal session cookies and it could install key logging software. Malware controlled PCs form the basis of the robot network (Botnet) which is used for Distributed Denial of Service (DDOS) attacks against networks and for SPAM distribution. SPAM is also a threat, which leads to the installation of malware and spyware. Thus end point protection (Access Control, Anti-Virus and Anti-Spyware) is essential. More importantly, it must be maintained and monitored.

Software vulnerabilities are an increasing major threat area.. [9] The exploitation could be realised from a website which has malicious content when a user clicks on links. Exploited vulnerabilities can allow malware to be installed, thus resulting in the issues mentioned already. Patches for vulnerabilities are being released fairly quickly but it is up to the user to apply the patches when they become available. Automatic updating may help, but as with end point protection, it needs to be maintained and monitored.

Incidences of data loss via breaches and the mishandling of personal data are increasing [10]. In cases where the lost data on CDs or laptops are never found, what has happened? Has the data ended up with

criminals? This personal data could be used in highly targeted phishing attacks where detailed information is known. Showing known private details reassures the users and then they become a victim by acting upon the phishing request.

## 3.2 Consumer Usage Threats

I carried out research to identify consumer user habits in the following areas: Internet security, computers setup and Internet applications. The research was based on a user survey along with a literature review of relevant materials.

I conducted the survey to identify consumer computer and Internet usage habits. The survey was web based and was posted out to candidates via email and a social networking website. The candidates were made up of individuals from the following age group: 40 percent were 22-34, 52 percent were 35- 44 and 8 percent were over 45.

### 3.2.1 Network Security

80 percent of the survey candidates connected to the Internet with a router. 55 percent always kept their router on. 55 percent of the candidates were either not sure if the router had a password, or if the default router password had been changed.

60 percent of the survey candidates using Internet router had WIFI capabilities. 31 percent had WEP wireless security enabled but 46 percent were unsure what security, or if any security was used. WEP was confirmed as the most common wireless security in a simple evaluation of WIFI access points, which I performed. The results show in figures 1 and 2 that 58 percent of access points were found with WEP security. I used an access point scanner tool on a laptop to show the security on access points in range. I performed a scan at my work location where I am based on the 7<sup>th</sup> floor in an area where there are numerous residential flats nearby. I also performed a scan my home location, which is an area of terraced houses.

Name	Security	Ch.	Signal	Noise	Best	% Avail.	MAC	Last Contact
khkwestminster	WPA-PSK	10	-60	-96	-58	96%	00:14:80:03:00:00	26/02/2008 14:53:06
home	WEP	1	-77	-96	-76	26%	00:14:77:00:00:00	26/02/2008 14:53:06
dolcis	WEP	9	-73	-96	-72	73%	00:0F:30:AC:F1:28	26/02/2008 14:53:06
TalkTalk	WEP	1	-67	-96	-67	80%	00:14:03:00:7C:00	26/02/2008 14:53:06
TalkTalk	Unknown	11	-60	-96	-60	92%	00:14:03:03:00:00	26/02/2008 14:53:06
TalkTalk	WPA-PSK	12	-73	-96	-73	57%	00:14:03:00:03:27	26/02/2008 14:53:06
TPP	WPA-PSK	5	-77	-96	-77	15%	00:14:03:00:03:28	26/02/2008 14:53:06
SKY	WPA-PSK	1	-69	-96	-68	96%	00:14:03:03:02:04	26/02/2008 14:53:06
Pete	WPA-PSK	6	-75	-96	-75	34%	00:14:03:03:03:78	26/02/2008 14:53:06
Mango_Tree	Unknown	11	-75	-96	-74	26%	00:14:03:00:04:00	26/02/2008 14:53:06
Fenwick	WEP	11	-71	-96	-69	100%	00:14:03:00:04:02	26/02/2008 14:53:06
BTHomeHub-1000	WEP	7	-75	-96	-75	53%	00:14:77:00:C2:00	26/02/2008 14:53:06
BTHomeHub-1001	WEP	1	-65	-96	-65	88%	00:14:77:00:11:00	26/02/2008 14:53:06
BTHomeHub-1002	WEP	7	-76	-96	-76	76%	00:14:03:00:04:00	26/02/2008 14:53:06
BTHomeHub-1003	WEP	11	-75	-96	-74	80%	00:14:77:00:04:00	26/02/2008 14:53:06
BTHomeHub-1004	WEP	11	-71	-96	-71	84%	00:14:03:03:04:00	26/02/2008 14:53:06
BTHomeHub-1005	WEP	8	-74	-96	-72	100%	00:14:77:00:04:00	26/02/2008 14:53:06

Figure 1: Access point scan from work location

Name	Security	Ch.	Signal	Noise	Best	% Avail.	MAC	Last Contact
waysomenet	WPA-PSK	11	-76	-96	-73	50%	00:00:00:00:00:00	26/02/2008 19:22:37
cool-net	WPA-PSK	11	-58	-96	-23	100%	00:14:80:03:00:00	26/02/2008 19:22:37
belkin54g	Unknown	13	-61	-96	-51	100%	00:17:3F:78:33:28	26/02/2008 19:22:37
SKY	WPA-PSK	1	-77	-96	-76	50%	00:14:03:00:03:00	26/02/2008 19:22:37
SKY	WPA-PSK	11	-71	-96	-71	50%	00:14:03:00:7C:00	26/02/2008 19:22:37
NETGEAR	WEP	11	-69	-96	-63	100%	00:14:03:00:03:00	26/02/2008 19:22:37
Home Wireless	WEP	2	-59	-96	-57	100%	00:14:77:00:00:00	26/02/2008 19:22:37
BTHomeHub-1000	WEP	1	-72	-96	-72	100%	00:14:77:00:00:00	26/02/2008 19:22:37
BTHomeHub-1001	WEP	1	-75	-96	-75	100%	00:14:77:00:00:00	26/02/2008 19:22:37

Figure 2: Access point scan from home location

The results showed that Wired Equivalent Privacy (WEP) wireless security was used on all the BT (British Telecom) Hub access points found in the scan. The BT Hub product support guide [11] states that WEP is the default security. However, the BT Hub also supports WPA security. The main reason for making WEP the default security is compatibility. This is because WEP is the most commonly supported security on wireless adaptors.

Weaknesses in WEP security have been known since 2001. The weakness is due to the weak Initial Vectors (IVs) which can be exploited with the Fluhrer-Mantin-Shamir (FMS) attack. This attack along with other WEP vulnerabilities can be exploited with numerous free tools [12]. In today’s environment WEP security is very trivial to break and shouldn’t be used.

The weakness of WEP, the BT hub default security setting and the results found in the survey and access point scan are concerning. BT has more than a quarter of the market share in residential and small business broadband connections. (BT had a 26.5 percent market share in Q4 of 2007 [13]).

It is clear that the network security employed on consumer networks is insufficient. This is major threat area as we have inadequate WIFI security on routers, which are always on. We also have routers, which still have the default password enabled.

### **3.2.2 Internet Security Software**

100 percent of the survey candidates claimed to have anti-virus software installed but 24 percent were not sure if it got updated. 68 percent claimed to have anti-spyware installed but as before, 12 percent were not sure if it got updated. 88 percent claimed to have a firewall enabled.

The good awareness is possibly due to the constant reminders about Internet Security. For example it is difficult to buy a new computer without being required to buy an Internet security product. This is true of PC World, Comet and purchasing online from Dell. Problems arise if the user misunderstands what the product does, or if they don't act when the product subscription expires.

These results are good and show that consumers are aware of Internet security products. But is this really true? An online safety study [14] carried out by McAfee and the National Cyber Security Alliance (NCSA) showed a mismatch between the perceived and actual security on consumer's computers. While 87 percent claimed to have anti-virus installed, only 51 percent had the latest update. 70 percent claimed to have anti-spyware installed, but only 55 percent actually had it. 63 percent had their firewall enabled against 73 percent who claimed to have a firewall installed.

This is another major threat area. Utilising Internet security is the one the security start points. Consumer may be aware of the need for Internet security but they have a false reality thinking they are protected when they are not.

### **3.2.3 Access Control**

The survey candidates reported that 24 percent of their computers had no passwords. 40 percent of their computers had multiple users, which used the same logon. 70 percent of these used a logon, which had administrator access. 25 percent of computers had users under the age of 16 yr old, which were not monitored. These findings match what is commonly believed about user accounts. They also show that the default computer setup and a lack of knowledge are being used to define consumer computer access controls.

48 percent of the survey candidates use social networking websites, 80 percent use web based email (Gmail, Hotmail and Yahoo Mail). 76 percent use work place systems, which are accessed with a password. Almost all the candidates claimed that they log on and off the various web applications once they had finished using them. This is, as opposed to staying logged on for the entire time that they are using their computer. This particular finding is interesting because of way that browsers handled logons to websites and the lack of detail gathered from the survey. Is the user actually logging out or just navigating away from the site? If so, the session will still exist. Has the website logon credentials been saved in the browser? Also, has the user instructed the website to remember there logon?

The way users behave with their logons is critical to their security. In particular, the not so obvious security with JavaScript based websites (Gmail, MySpace and Facebook) which are subject to XSS attacks. This is where a user clicks on a link on a random webpage and it performs a malicious action on the social networking or webmail application, which they are logged into [15].

### **3.2.4 P2P Software**

Peer-to-Peer (P2P) software is used by 40 percent of the survey candidates. 90 percent use P2P software on same computer that they use for online shopping, online banking or to access their work place system. Lime Wire and Bit-Torrent were the most popular P2P applications with 70 and 50 percent of these candidates.

Lime Wire is one of the most popular P2P applications available. It is claimed that it is installed on a third [16] of all computers in the world. Being the most popular, it is also the most dangerous. A study [17] of malware found that the Lime Wire network contained a significant amount of malware. Bit-Torrent is also subject to malware problem in a different form. It has suffers from hijacked torrent client software [18]. Password protected downloads, which require the user to visit a website with malicious content to retrieve the password. Also, there are downloads, which require the user to download and install specific software, which contains trojans [19].

To reduce the threat, users must perform an anti-virus scan of everything downloaded and ensure that the sharing settings are set to the most restrictive. They should delete anything, which requires activation via obtaining a password or downloading an application. All of this however, is subject to the adeptness of the users and whether they have an Internet Security products employed, which is maintained correctly.

### 3.2.5 Website Status and Warnings

The results show that a third of survey candidates did not check for the padlock icon on the website they are purchasing from. Also, the same number of candidates ignored certificate warnings like the one shown in figure 3.

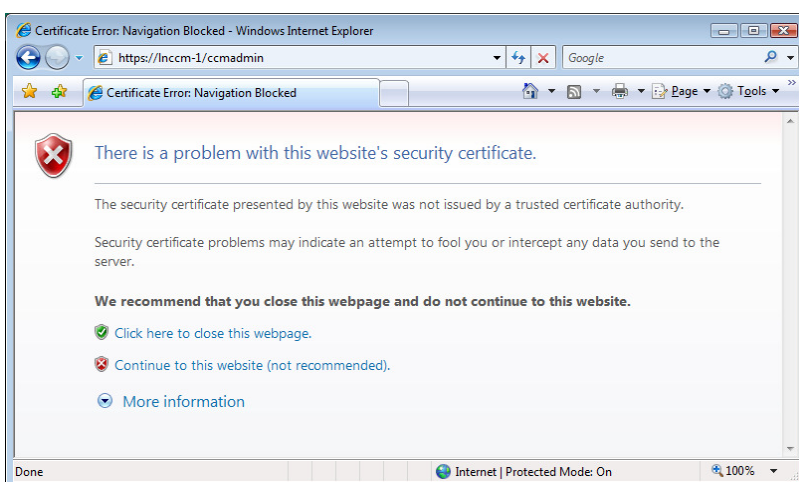
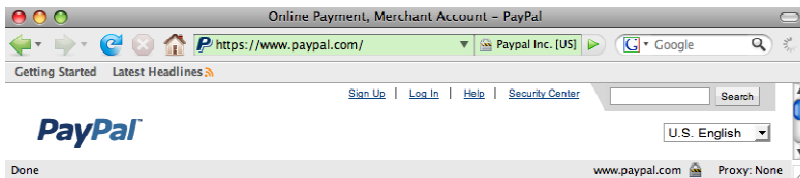


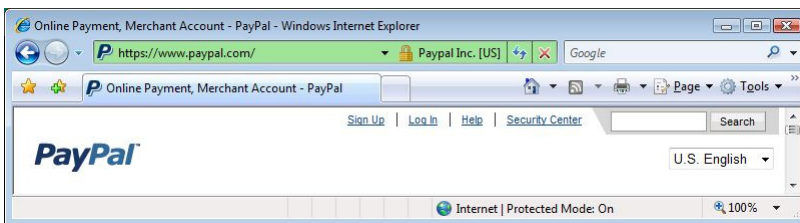
Figure 3: Certificate warning - Internet Explorer 7

Certificate Authorities have attempted to improve the validity of certificates with extended validation. These certificates identify the owner of the certificate in the address bar of the browser and turn the

address bar green. This is shown in figures 4 and 5. Extended validation works by default with Internet Explorer 7 or with a plug-in with Firefox 1.5 and 2. This, in theory should provide a limited form of authentication to the user that they are using the legitimate website. However, research in the evaluation of extended validation and phishing attacks [20] concluded that users who hadn't received training in browser security did not notice the extended validation features.



**Figure 4: Extended Validation - Firefox 2 with the VeriSign plug-in**



**Figure 5: Extended Validation -Internet Explorer 7**

Research [21] has shown that users commonly ignore certificate warnings. The most common reason is that they do not understand the warning. Browser phishing or forgery warnings also suffer from the same problem. These warnings come from anti-phishing tools, which aim to combat the proliferation of phishing. These tools are built into browsers and are available as add-on toolbars. The tools will warn against known websites that are forgeries or malicious. They check against a list, which is constantly updated. Or they connect directly to Google (Firefox) or Microsoft (Internet Explorer) to actively check each site visited.

This shows a threat area where users are diminishing the underlying security by ignored the warnings. Also there is a general lack of awareness of features that provide assurance.

### 3.3 The Uncontrolled Environment Defined

To conclude we can say that the uncontrolled environment is the perfect breeding area for the common threats to propagate. Unsecured PCs exist on open or unsecured networks. End point protection is employed on a good percentage of PCs but is not sufficiently maintained. Users are unaware of their actions and unaware of their lack of actions. For example using P2P software without proper end point protection on the same PC used for e-banking, also ignoring certificate and phishing site warning. Then there are the threats that users just wouldn't know about from XSS.

Clearly users need to be better educated. But it is not all their fault. Major providers such as BT need to improve the level of security provided as consumers are relying on them for assurance.

- 
- 1 National Statistics. First Release Internet Access, Households and Individuals, August 2007, <http://www.statistics.gov.uk/pdfdir/inta0807.pdf>
  - 2 Enterprise Nation. Home Business Report, Oct 2007, <http://www.enterprisenation.com/downloadfile.aspx?ID=83>
  - 3 Holmes, J., Euromonitor International. Online shopping sees fraud clouds, July 2007, [http://www.euromonitor.com/Online\\_shopping\\_sees\\_fraud\\_clouds\\_ahead](http://www.euromonitor.com/Online_shopping_sees_fraud_clouds_ahead)
  - 4 APACS. Internet banking outstrips telephone banking for first time, Dec 2006, [http://www.apacs.org.uk/media\\_centre/press/06\\_28\\_12.html](http://www.apacs.org.uk/media_centre/press/06_28_12.html)
  - 5 Young, T., Computing. Home workers pose security threat, Feb 2008, <http://www.computing.co.uk/computing/news/2208912/home-workers-pose-increasing>
  - 6 The Department for Business, Enterprise & Regulatory Reform (BERR), Flexible Working and Work-Life Balance, <http://www.berr.gov.uk/employment/workandfamilies/flexible-working/index.html>
  - 7 Gemalto, Gemalto Supports Barclays' Large-Scale Roll Out of Two-Factor Authentication Solution for Online Banking in the UK, <http://www.gemalto.com/press/archives/2007/04-18-2007-Barclays.pdf>
  - 8 F-Secure, IT Security Threat Summary for H2 2007, <http://www.f-secure.com/2007/2/index.html>
  - 9 Symantec, Symantec Internet Security Threat Report - Trends for July-December 07 (p2,p7), [http://eval.symantec.com/mktginfo/enterprise/white\\_papers/b-whitepaper\\_exec\\_summary\\_internet\\_security\\_threat\\_report\\_xiii\\_04-2008.en-us.pdf](http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_exec_summary_internet_security_threat_report_xiii_04-2008.en-us.pdf)
  - 10 Harrison, D., The Telegraph, Government's record year of data loss, Jan 2008, <http://www.telegraph.co.uk/news/newsttopics/politics/1574687/Government's-record-year-of-data-loss.html>
  - 11 BT, The BT Hub Product Support Guide - BT Fusion, (accessed June 2008), <http://www.btbroadbandoffice.com/BTHubProductSupportGuide%5BFINAL%5D.pdf>
  - 12 Ossmann, M., Security Focus, WEP Dead Again: Part 1 & 2, Dec 2004, <http://www.securityfocus.com/infocus/1814>, <http://www.securityfocus.com/infocus/1824>
  - 13 Office of Communication (OFCOM), Telecommunications Market Data Update Q4 2007,

---

[http://www.ofcom.org.uk/research/cm/tables/q4\\_2007/q42007.pdf](http://www.ofcom.org.uk/research/cm/tables/q4_2007/q42007.pdf)

14 McAfee, NCSA Online Safety study, Oct 2007,

[http://staysafeonline.org/pdf/McAfee\\_NCSA\\_analysis.pdf](http://staysafeonline.org/pdf/McAfee_NCSA_analysis.pdf)

15 Wesemann, D., SANS, Cross-Site Scripting (XSS) bug in Gmail, Jan 2007,

<http://isc.sans.org/diary.html?storyid=1995>

16 Azuri, C., TMCnet Contributing Editor, LimeWire Installed on One-Third of PCs Worldwide, Dec 2007,

<http://www.tmcnet.com/ce/articles/16950-limewire-installed-one-third-pcs-worldwide.htm>, (Account registration required for access),

17 Kalafut, A., Acharya, A., M,Gupta., Indiana University, Bloomington Indiana, USA, A study of Malware in Peer-to-Peer Networks, IMC 2006, <http://www.imconf.net/imc-2006/papers/p33-kalafut.pdf>

18 TorrentFreak, Hijacked Bit-Torrent Client, Dec 2007, <http://torrentfreak.com/shareazacom-hijacked-and-turned-into-a-scam-site-071224/>

19 TorrentFreak, DomPlayer, Oct 2007, <http://torrentfreak.com/domplayer-rips-off-axxo-bittorrent-fans-071017/>

20 Jackson, C., Barth, A., (Stanford University, Stanford, CA), Simon, D.R., Tan, D.S., (Microsoft Research, Redmond, WA), An Evaluation of Extended Validation and Picture-in-Picture Phishing Attacks, <http://www.usablesecurity.org/papers/jackson.pdf>

21 Biancuzzi, F., Security Focus, Phishing with Rachna Dhamija, Jun 2006, <http://www.securityfocus.com/columnists/407>