ORIGINAL ARTICLE

Physician use of updated anti-virus software in a tertiary Nigerian hospital

***Laabes E P** *FWACP*; ****Nyango D D,** *FWACS*; *****Ayedima M M**, *FWACS*; ******Ladep N G**, *FWACP*

*Departments of, *Family Medicine, **Obstetrics & Gynaecology, ***Surgery, & ****Internal Medicine; all of Jos University Teaching Hospital, PMB 2076Jos, Nigeria*

Abstract

Background: *While physicians are becoming increasingly dependent on computers and the internet, highly lethal malware continue to be loaded into cyberspace. We sought to assess the proportion of physicians with updated anti-virus software in Jos University Teaching Hospital Nigeria and to determine perceived barriers to getting updates.*

Methods: *We used a pre-tested semi-structured self-administered questionnaire to conduct a cross-sectional survey among 118 physicians.*

Results: *The mean age (±SD) of subjects was 34(±4) years, with 94 male and 24 female physicians. Forty-two (36.5%) of 115 physicians with anti-virus software used an updated program (95%CI: 27, 45). The top-three anti-virus software were: McAfee 40(33.9%), AVG 37(31.4%) and Norton 17(14.4%). Common infections were: Trojan horse 22 (29.7%), Brontok worm 8(10.8%), and Ravmonlog.exe 5(6.8%). Internet browsing with a firewall was an independent determinant for use of updated anti-virus software [OR 4.3, 95%CI, 1.86, 10.02; P< 0.001]. Busy schedule, 40(33.9%) and lack of credit card 39(33.1%) were perceived barriers to updating anti-virus software.*

Conclusion:*The use of regularly updated anti-virus software is sub-optimal among physicians implying vulnerability to computer viruses. Physicians should be careful with flash drives and should avoid being victims of the raging arms race between malware producers and anti-virus software developers*

Keywords: *Anti-virus software; Computer security; Updates; Physicians; Nigeria*

Date Accepted for Publication: 10th April 2010
NigerJMed 2010: 289 - 294

Introduction

A computer virus is defined as, "a program or piece of code that is loaded unto your computer without your knowledge and runs against your wishes." Viruses, Worms, Trojans and blended threats are terms used to describe malicious programs that damage computers with varying degrees of severity.

A typical *computer virus,* also known as a file virus attaches itself to a file or program which enables it to travel from one computer to the next, leaving infections in its wake. The typical computer virus would attach itself to an executable program, so that it can spread once the program runs; thus the continuing spread of a virus solely depends on human action (e.g., a mouse click). In contrast, a *worm* does not depend on human action to spread because it utilizes a computer's file and information transport system to travel unaided. What makes a worm lethal is its ability to replicate itself on a computer, so that it sends multiple copies of itself to any other computer with which its host communicates. In this fashion, a single worm can cripple several vulnerable computer networks. A *Trojan horse*, like a worm, represents another virus sub-class which masquerades as a desirable or legitimate software or file from a reliable source, but which inflicts damage once opened. [2] An additional feature of a Trojan horse is its ability to create a backdoor on a computer, allowing malicious software to collect personal information such as passwords, bank accounts and credit card information. Unlike typical viruses or worms, a Trojan horse does not replicate itself or infect other files. A *blended threat* combines the features of all virus sub-classes, capitalizes on all vulnerabilities, spreads through multiple routes and causes multiple harmful effects.

All malicious software is referred to as *malware*, with viruses and *Spyware* being the most common. Spyware refers to seemingly innocent software that embeds itself into a computer's browser and collects personal information such as e mails, passwords, and bank account or credit card details which it sends to a third party. A *Rootkit* is a special type of spyware in which a hacker takes control of a computer, and uses it to infect other computers.

In the year 2005 alone, the Storm Centre, a US organization dedicated to tracking online security threats, reported 7.6 million attacks in the US alone. As of the year 2006, about 1 billion people have internet access worldwide, with the internet being the major

Correspondence ***Dr Emmanuel P. Laabes,*** *E mail: laabes2002@yahoo.com +2348035860039*

reservoir for computer viruses. Other sources of infection include: external hard drives, flash drives, floppy disks and compact disks. Viruses may also be posted on an organization's local intranet by aggrieved employees.

Like human viruses, computer viruses may cause a spectrum of problems ranging from merely annoying effects such as changing the desktop background through data loss/operating system malfunction to severe effects such as deleting the master boot record of your computer or outright hardware damage. Furthermore, incapacitation of computer-based life support systems might results in a worsening of morbidity or outright mortality. In addition, viruses may affect an organization's billing software, resulting in massive revenue losses.

Anti-virus software is a program designed to conduct periodic checks on a computer, in order to remove the most common types of viruses.[1] Software developers continuously update their programs to counter the never-ending computer security threats. The development of anti-virus programs began in 1987 when the Internet precursor, Advanced Research Project Agency Network (ARPANET), a large network of computers belonging to the US Department of Defense, was infected by a virus.[1] Since then, many anti-virus software programs have been developed and made available to computer users worldwide. In Nigeria, most genuine anti-virus programs can only be obtained via on-line purchase; a situation made more precarious by non-availability and in some cases non-acceptance of credit cards from Nigeria. The free downloads available on-line do not contain most of the security features (add-ons) that come with the commercial packages. All anti-virus programs require updating on a regular basis as new malicious threats are continuously emerging: a ponderous requirement in Nigeria, owing to erratic and mostly crawling internet networks.

Medical practice has undergone a rapid transformation with the advent of computers and the internet. The proliferation of internet cybercafés and advancement in Wi-Fi technology has brought internet access even closer to the practising physician. Computers have found application in all aspects of medical care; from card issuance and booking of appointments to complex day-long surgical procedures. In addition, computers are at the centre of the current global move towards electronic medical records, the so-called 'paperless' practice. Furthermore, powerful statistical software packages and calculators provide invaluable aid to the practising physician, in the areas of data analysis and scientific publication, besides continuing professional development.

An informal survey has shown a recent surge in laptop computer purchase by physicians: laptop computers are expensive, need regular maintenance, and careful handling. It is widely accepted that physician ownership and usage of computers should be accompanied by use of up-to-date and efficient security software, but this hypothesis has not been tested. To our knowledge, the literature contains no report on the awareness and use of computer security software by physicians.

We designed the present study to assess physician use of updated anti-virus software in Jos University Teaching Hospital with the following specific aims: to determine the proportion of physicians using updated anti-virus software on their personal computers; identify the top three anti-virus software in use by physicians; identify recent and most common physician computer virus infections; identify any independent determinants for use of updated anti-virus software by physicians; and identify perceived barriers to physician use of updated anti-virus software. This report documents our findings from a cross-sectional sample of 118 physician computer users.

Subjects and Methods

Study area

Jos, the Capital of Plateau State in north central Nigeria, lies between latitude 9°55'N and longitude 8°53'E at an altitude of 1285m above sea level. Jos University Teaching Hospital is a 524-bed tertiary care referral facility within Jos Metropolis, with 557 physicians in its employment working in 14 specialty areas which comprises: anaesthesiology, chemical pathology, community health, family medicine, and haematology; others include, histopathology, internal medicine, microbiology, ophthalmology, obstetrics & gynaecology, paediatrics, psychiatry, radiology and surgery. Among JUTH Physicians, the advent of computer education and the accompanying explosion in use of information and communication technology is still in its early stages, as is the case in most countries of sub-Saharan Africa, where internet cybercafés with barely crawling networks are usually crowded.

Study design & Participants

We conducted a cross-sectional survey from July to November 2007. Physicians of either sex practising in Jos University Teaching Hospital and owning a personal computer (desktop or laptop) were eligible for recruitment into the study.

A sample size of 96 physicians was targeted for study which allows a 50% usage rate for updated anti-virus software to be detected with 95% confidence and 10% sampling precision. Adding 30% to cover for attrition on account of non-response and invalid responses resulted in an upward adjustment of the sample size to 125. Of the 125 questionnaires administered, 121 were returned, 3 of which were invalid, giving a response rate of 96.8%. Thus, 118 questionnaires were analyzed.

Consecutive eligible consenting physicians were recruited into the study until the desired sample size was obtained. A member of the research team requested participating physicians to fill a self-administered survey questionnaire soon after obtaining informed consent. Ethical clearance for study was duly obtained from the JUTH Ethical Committee.

Study Questionnaire

We designed a 33-item self-administered semi-structured questionnaire with closed and open-ended questions; which sought to establish baseline demographic information such as: age, gender, specialty and rank. In addition, we sought to establish the respondents' level of interest and familiarity with computing, including ownership and/or usage of flash drives.

Other questions sought to establish respondent's knowledge of computer viruses, any recent "computer viral infections" including the aftermath of such infections. Further questions sought to elicit responses pertaining to current anti-virus software on respondent's computer, preferred anti-virus software, how software was obtained, the frequency with which anti-virus software is updated and how often a full system scan for viruses is conducted. Equally, we sought to document perceived barriers to getting regular updates for anti-virus software in current use, to establish the type of operating system in use and the frequency of getting operating system updates. We also documented knowledge and use of a firewall online. We conducted an initial pilot testing of the study instrument in the Family Practice section, before commencement of the full-scale survey. This involved an assessment of the questions for clarity and acceptability.

Statistical analysis

Data analysis was conducted with Epi Info 3.4.3(CDC, Atlanta Georgia). Univariate analysis using the "frequencies" command was used to determine the proportion of doctors with updated anti-virus software, types of anti-virus software in use, recent types of computer virus infection(s), and physicians' perceived barriers to updating anti-virus software. The chi-square statistic was used to assess the relationship of various binary variables with the use of updated anti-virus software. We examined the independent determinants for use of updated anti-virus software with a multiple logistic regression model. A p-value < 0.05 was considered significant in all analyses.

Results

Characteristics of subjects

The mean age (±SD) of surveyed physicians was 34 (±4) years: range, 26 to 53 years. Ninety- four (79.7%) were male physicians and 24 (20.3%) were female physicians. Forty-seven (39.8%) were registrars, 42 (35.6) were senior registrars, 19 (16.1%) were senior house officers, 5 (4.2%) were house officers and 5 (4.2%) were consultants.

Of 118 physicians surveyed, 26(22%) were in surgery, 21(17.8%) were in Family Medicine, 19(16.1%) were in Internal Medicine, 19(16.1%) were in Obstetrics and Gynaecology, 14(11.9%) were in Public Health, 12(10.2%) were in Paediatrics and 7(5.9%) were in Anaesthesia.

Ninety-nine (83.9%) physicians owned a laptop and 18 (16.1%) owned a desktop computer. The top five computer models were: HP/Compaq, 41(34.7%); Dell, 23 (19.5%); Toshiba, 18(15.3%); Acer, 17(14.4%) and; Sony, 5(4.2%). Fourteen (11.9%) comprised of other models such as: Gateway, IBM, Mercury, Zinox, Rock, Siemens, Packard-Bell, and Cloned (unbranded). The median duration of PC ownership was 12.5months (range, 1-60 months; IQR: 7-24months). 116 (98.3%) physicians used Windows operating system, one (0.8%) used Linux, and one (0.8%) used both (dual boot). Seventy (59.3%) physicians surveyed reported failure to regularly download operating system updates in contrast to 48 (40.7%). We did not observe any sex-based differences in computing interest [OR 0.3, 95%CI 0.1 to1.3], P=0.12 [Fisher's Exact].Table 1 shows physician responses to questions on basic computing.

Table I: Responses of 118 physicians to questions on basic computing

Question	Response: no (%)	95% Confidence Interval
Own palm digital assistant?		
Yes	4(3.4)	0.9-8.5
No	114(96.6)	91.5-99.1
Computer savvy?		
Yes	28(23.7)	16.4-32.4
No	90(76.3)	67.6-83.6
Computing as area of interest?		
Yes	108(91.5)	85.0-95.9
No	10(8.5)	4.1-15.0
Familiar with computer applications?		
Yes	97(82.2)	74.1-88.6
No	21(17.8)	11.4-25.9
Familiar with computer hardware?		
Yes	71(60.2)	50.7-69.1
No	47(39.8)	30.9-49.3
Trained in computer applications?		
Yes	29(24.6)	117.1-33.4
No	89(75.4)	66.6-82.9
Trained in hardware repair& maintenance?		
Yes	1(0.8)	0.0-4.6
No	117(99.2)	95.4-100
Use a flash drive?		
Yes	108(91.5)	85.0-95.9
No	10(8.5)	4.1-15.0
Own a flash drive?		
Yes	100(84.7)	77.0-90.7
No	18(15.3)	9.3-23.0
Heard of computer viruses?		
Yes	116(98.3)	94.0-99.8
No	2(1.7)	0.2-6.0
Computer recently infected with a virus?		
Yes	74(62.7)	53.3-71.4
No	44(37.3)	28.6-46.7
Able to clean recent virus infection?		
Yes	55(74.3)	62.8-83.8
No	19(25.7)	16.2-37.2
Familiar with a firewall?		
Yes	55(46.6)	37.4-56.0
No	63(53.4)	44.0-62.6
Browse internet with a firewall?		
Yes	43(78.2)	65.0-88.2
No	12(21.8)	11.8-35.0

Types of anti-virus software in use by physicians

The top-three anti-virus software in use by physicians included: MacAfee anti-virus, 40(33.9%); AVG anti-virus, 37(31.4%) and; Norton anti-virus, 17(14.4%). Three (2.5%) physicians reported not having any anti-virus software on their PC. The top-three preferred anti-virus software included: MacAfee anti-virus, 40(33.9%); Norton anti-virus, 34(28.8%) and; AVG anti-virus, 23(19.5%). A sizeable number of physicians, 51(44.3%) were using free downloads, 27(23.5%) obtained anti-virus software from a vendor, 25(21.7%) were using factory-installed software and only six (5.2%) purchased anti-virus software online. Table 2 shows the reported types of anti-virus software in use, how these were obtained, and what software physicians preferred over the ones in use.

Table II: Anti-virus in use by surveyed physicians, how obtained, and anti-virus preferences

Anti-virus in use	No (%)	How Anti-virus obtained	No (%)	Preferred Anti-virus	No (%)
MacAfee	40(33.9)	Free download	51(44.3)	MacAfee	40(34.8)
AVG	37(31.4)	Software Vendor	27(23.5)	Norton	34(29.6)
Norton	17(14.4)	Pre-installed	25(21.7)	AVG	23(20.0)
Avast	13(11.0)	On line purchase	6(5.2)	Avast	6(5.2)
NOD 32	4(3.4)	Free gift	6(5.2)	NOD 32	4(3.5)
None	3(2.5)			Panda	3(2.6)
CA Anti-virus	1(0.8)			Sophos	2(1.7)
Kapersky	1(0.8)			CA Anti-virus	1(0.9)
Panda	1(0.8)			Kapersky	1(0.9)
Sophos	1(0.8)			Avira	1(0.9)

Physician use of updated anti-virus software

Only 42 (36.5%) of 115 physicians who had an anti-virus software on their computer reported using a currently updated anti-virus program [95%CI: 27, 45]. 73(63.5%) were using a non-updated anti-virus software. Despite the skewed male to female ratio in favour of male physicians, there was no gender-based difference in use of updated anti-virus software among surveyed doctors, although the O.R. showed a trend which did not reach statistical significance [OR 0.4, 95%CI 0.1, 1.2, P= 0.09]. Only 46(39%) physicians ran a full virus scan at least weekly, sixty-nine (58.5%) ran a full system scan at least monthly and, 3(2.5%) never ran a full system scan for viruses.

Recent physician computer virus infections, sources of infection, vectors of transmission and effects on personal computers

The top three reported computer virus infections were: Trojan horse, 22(29.7%; Brontok worm, 8(10.8%) and; Ravmonlog.exe, 5(6.8%). Computer virus infection with 'African-China' and 'Andre,' 1(1.4%) each, were infrequent. Interestingly, 27(36.4%) physicians whose PCs were recently infected could not remember the name of the virus. The top-three sources of PC infection were: offline computer, 32(43.2%); internet, 29(39.2%) and; flash drives, 11(14.9%). Table 3 describes the different types of virus infections including their sources and the 'vectors' responsible for transmission.

The reported effects of virus infection on physician PCs included: operating system malfunction, 25(33.8); hanging and slowing, 24(32.4%) and; data loss, 16(21.6%). Eight physicians (10.8%) reported no untoward effects following PC infection and only one (1.4%) had a system crash.

Table III: Frequencies of recent computer virus infections, sources of infection, and vectors of transmission

Recent virus infection	No (%)	Source of infection	No (%)	Vector of transmission	No (%)
Dont know	27(36.4)	Off line computer	32(43.2)	Flash drive	65(87.8)
Trojan horse	22(29.7)	Internet	29(39.2)	Floppy disk	4(5.4)
Brontok worm	8(10.8)	Flash drive	11(14.9)	Dont know	3(4.1)
Ravmonlog.exe	5(6.8)	Dont know	2(2.7)	External hard drive	2(2.7)
Ravmonlog.exe+ Trojan horse	4(5.4)				
Trojan horse + Brontok worm	4(5.4)				
Trojan Shipli + W32.rungbu	2(2.70				
African-china	1(1.4)				
Andre	1(1.4)				

Physicians' perceived barriers to updating anti-virus software

Top most on the list of barriers to updating anti-virus software by physicians was busy schedule, 40(33.9%).

Others included: lack of credit card facility for on line purchase, 39(33.1%); high cost of genuine software, 29(24.6%) and; lack of internet access, 2(0.7%). Interestingly, 8(6.8%) physicians cited lack of awareness as a barrier to updating anti-virus software.

Determinants for use of updated anti-virus software

We assessed the relationship of physician characteristics and use of updated anti-virus software through bivariate analysis with the chi-square statistic [Table IV]. To control for confounding, all physician characteristics significantly related with use of updated anti-virus software (P<0.05) were entered into a step-wise logistic regression model and backward elimination conducted to identify independent determinants for use of updated anti-virus software. We identified browsing the internet with a firewall as an independent determinant for use of updated anti-virus software: OR 4.3, 95%CI, 1.86, 10.02; P< 0.001, suggesting that physicians who routinely browsed the internet with a firewall were four times likely to use updated antivirus software.

Table IV: Unadjusted determinants for use of updated anti-virus software by 115 physicians

Variable	Updated anti-virus software		
	Odds ratio	95% Confidence Interval	P-Value
Computer type (Desktop/Laptop)	5.76	1.26 - 26.3	0.023
Computer savvy(yes/no)	2.69	1.12 6.41	0.025
Cleaned recent virus infection(yes/no)	2.25	1.05 4.86	0.038
Regularly updates OS (yes/no)	3.38	1.54 7.44	0.002
Knows what a firewall is(yes/no)	3.08	1.40 6.76	0.005
Browses the web with a Firewall(yes/no)	5.2	2.31 11.85	<0.001
Fully scans PC[‡] weekly for viruses(yes/no)	2.78	1.27- 6.08	0.010

Os[†] = operating system
PC[‡] = personal computer

Discussion

In many developing countries of sub-Saharan Africa, physician ownership of a personal computer has witnessed a rapid transformation from a social status symbol in the last decade, to a near-physiologic necessity in recent times. The current state-of-affairs with respect to the ponderous and ever-increasing requirements for cutting-edge medical practice is occasioned by the overwhelming load of professional information which physicians must access and acquire for continuing professional development, and renewal of practicing licenses. Of late, physicians are also becoming increasingly aware of the internet as a veritable tool for economic empowerment. Since computer viruses constitute a formidable threat to successful web browsing, the increasing dependence of physicians on the internet makes the use of genuine and regularly updated anti-virus software mandatory.

The main finding of our study was that just over a third of surveyed physicians reported current usage of updated anti-virus software. Even more striking was the finding that three physicians had no anti-virus program on their computers. The top-three anti-virus software in use by surveyed physicians included: MacAfee anti-virus, AVG anti-virus and Norton anti-virus in decreasing order of frequency. Equally, Trojan horse, Brontok worm and Ravmomlog.exe were reported as frequent computer virus infections. With regard to perceived barriers to getting updated anti-virus software, frequent responses included: a busy schedule, lack of credit card for on line purchase, the high cost of genuine software and a lack of internet access. To our knowledge, no study examining the anti-virus usage habits of physicians exist in the literature, making comparison with previous reports impractical.

Physicians with currently updated anti-virus software were less susceptible and more likely to have cleaned any virus infections compared with those without updated software. Anti-virus software makers recommend regular updates of installed anti-virus software. The availability of virus definition updates depends on the software maker and range from hourly to monthly updates. It is recommended that a full system scan be conducted at least once weekly. However, only customers with genuine software are able to access such updates and will therefore remain protected. Free anti-virus software does not truly provide acceptable cover against emerging virus infections. For added security, Microsoft provides regular updates of its windows operating system, which can be downloaded by users with genuine Microsoft products. Physicians should configure their computers for automatic updates so that any available updates to the operating system are automatically downloaded once on line.

Surveyed physicians tended to use any available anti-virus software, with most reporting preference for software other than the one in use. The choice of which software to use should be determined by ease of use and effectiveness. In this regard, the TopTen Antivirus Reviews[3] provide a succinct on line guide to the choice of anti-virus software. The review outlines the strengths and weaknesses of the top-ten anti-virus software on the market. Similarly, the current PC Antivirus Reviews 2008 reports the top-four anti-virus software as: BitDefender anti-virus 2009, Kapersky anti-virus 2009, Norton anti-virus, and McAfee VirusScan Plus in decreasing order of effectiveness. BitDefender Antivirus earned a score of 97% and emerged as the

best antivirus of 2009 after rigorous independent laboratory testing of all antivirus software compared.

Most physicians who reported recent virus infections cited the Flash drive as the vector of transmission, which seriously calls to question the utility of the Flash drive as data storage and transfer medium. Flash drive-borne virus infections have remained extant despite the recent emergence of newer brands of Flash drives preloaded with anti-virus software meant to address this vulnerability, probably because users are unaware that the preloaded software requires activation on line.

In terms of significance, our findings demonstrate a rather lackadaisical attitude on the part of most surveyed physicians with regards to personal computer security. With increasing availability of affordable mobile internet access, a busy schedule should no longer be accepted as a plausible excuse for inability to obtain genuine anti-virus software. Equally, genuine software can be purchased on line via credit card and in rare instances be obtained from a software vendor. The current provision of credit card facilities by most banking institutions should increase physician access to genuine anti-virus software.

Our data indicate a heightened vulnerability to computer viruses amongst surveyed physicians. This apparently self-inflicted vulnerability has far reaching consequences for clinical practice, research and continuing medical education, in addition to avoidable financial expenses that might be incurred in the wake of a computer virus infection.

In retrospect, our study had a few limitations: our cross sectional sample may not be truly representative of the population of physicians because of unavoidable volunteer bias. Equally, differential reporting bias with regard to use of updated anti-virus software might have skewed the results in favor of the group with currently updated software, however the low proportion who reported using an updated software suggested that such bias if present was at best minimal. Our use of a semi-structured non-validated questionnaire might have limited response options largely to those on the questionnaire. However, we believe that all pertinent information was captured following initial pre-testing of the questionnaire.

In light of our limitations, future surveys should offer real time-time scans of physician computer systems to ascertain anti-virus software type and update status, including any computer virus infections.

We conclude that the use of updated anti-virus software is sub-optimal among physicians, implying increased vulnerability to computer viruses. Physicians who routinely browse the internet with a firewall are likely to be more security conscious and to be less susceptible to computer virus infections. The Flash drive is a major driving force in the transmission of computer virus infections amongst physicians. A combination of high cost, lack of credit card facility and a busy schedule constitute the main obstacles to updating anti-virus software by physicians in resource-limited settings. Physicians should avoid being caught in the cross fire of the raging arms race between malware producers and anti-virus software developers.

References

1. What is a virus- A word definition from the webopedia computer dictionary. http://www.webopedia.com/TERM/v/virus.html. Accessed 12/10/08.
2. Vangie B. The difference between a Virus, Worm and Trojan horse. Http://www. Webopedia.com/DidYouKnow/Internet/2004/virus.asp. Accessed 12/10/08.
3. Anti-virus Software Review 2008. http://www.toptenreviews.com.html. Accessed 15/10/08
4. Mehta S. computer security: Is anti-virus software enough? http://www.physiciannews.com.html. Accessed 15/10/08. 2007 Anti-virus reviews. http://www.antivirus-software.6starreviews.com. Accessed 23/04/08.
5. Krever C. Electronic Medical Records, Chatham-style. In: Technology for Doctors. April 2005 Issue. http://www.canhealth.com/doctors.html. Accessed 23/04/08
6. Climate and Daylight chart for Jos, Nigeria. Find at http://www.Climate Charts.com/countries/Nigeria.html. Accessed 23/09/08.
7. Microsoft Update. http:www.microsoft.com. Accessed 17/10/08.
8. PC Antivirus reviews 2008. http://www.pcantivirusreviews.com. Accessed 17/10/08.
9. PC Anti-virus Reviews 2008. http://www.pc antivirus reviews.com/reviews/bitdefender antivirus.html. Accessed 17/10/08.