Journal of Virtual Worlds Research
jvwresearch.org ISSN: 1941-8477

Vol. 1. No. 1
ISSN: 1941-8477
"Virtual Worlds Research: Past, Present & Future"
July 2008

Help – Somebody Robbed my Second Life Avatar!

By James Elliott, Elliott Security Group

Abstract

Virtual worlds are fantastic places for people all over the world to come together and collaborate, socialize, as well as buy and sell goods. Unfortunately, criminals have discovered that virtual worlds can be used to commit crimes and violence against the citizens of the virtual worlds. This paper reviews many of those crimes and steps users must take to protect themselves from becoming a victim of fraud or other crimes that occur in Second Life.

Keywords: second life, virtual crimes, griefing, phishing.

Help – Somebody Robbed my Second Life Avatar!

By James Elliott, Elliott Security Group

Fraud, Violence, Theft – Just the Beginning

As history shows, criminals have always been eager to take advantage of unsuspecting victims using any means available. When the internet emerged, criminals quickly sprung into action to take advantage of this new media. Criminals have carried out Nigerian e-mail scams (419), auction fraud, hacking into websites to steal information, credit card fraud, phishing, stock "pump and dump" scams, and the list goes on and on.

Criminals see that millions of people are online and are easy targets to exploit. Bank robbers are an excellent example case study. These criminals realized that instead of walking into a bank, holding up a gun, and demanding money, it was much less risky to hire a person with computer skills to sit thousands of miles away and hack into the bank's infrastructure. The bank robbers were effectively still robbing the bank, except instead of walking away with physical cash (and probably a dye pack), the robbers were obtaining account numbers, social security numbers, and other valuable personal information. This information could then be converted into cash through re-selling or purchasing goods online. Criminals knew it would be much harder to be prosecuted if thousands of miles away from where the crime was committed. On top of this, not all law enforcement agencies are technically savvy and many do not have the manpower to investigate computer crime; and this does not even take into consideration cyber legislation and potential extradition issues.

Activist groups such as People for the Ethical Treatment of Animals (PETA) and the Earth Liberation Front (ELF) have also recognized the power of the internet. Instead of having to round up thousands of people to go out and protest in public, they have found it is easier to create "electronic disturbances" (Earth Liberation Front, 2007). Distributed Denial of Service (DDoS) is attack software that has been widely utilized by these as well as other groups to launch crippling attacks on many organizations' websites. These attacks have caused tremendous financial losses to the victim organizations.

Linden Labs (LL) was founded by Philip Rosedale in 1999. LL's mission is "to connect us all to an online world that improves the human condition" (lindenlab.com, 2007). LL's major development was Second Life (SL), a virtual world that began in June 2003. It is not a game, but a place to socialize, build local and regional environments, and engage in a virtual economy (Mennecke, Terando, Janvrin & Dilla, 2007). SL users interact through "avatars," also known as "residents," a computer representation of oneself that can be customized. Registering and creating an avatar is an anonymous process unless a membership is purchased (not required). In December 2005, the 100,000 registered user milestone was reached. At the time of this writing, SL's website shows that there are approximately 1.3 million members that have logged in within the last 60 days (lindenlab.com, 2007). SL purports that there are more than 12 million registered avatars. This number can be misleading because some are inactive and individuals may have multiple accounts or avatars. The official currency used is called Lindens; the exchange rate is approximately US$1 to L$265 to EUR$.678 (Reuters, E., 2007). Approximately $1.2 to $1.7

million US Dollars are exchanged for Linden Dollars on a daily basis within this virtual world. Figure 1 shows the volume of Lindens exchanged during the last 27 months (Second Life, 2008).

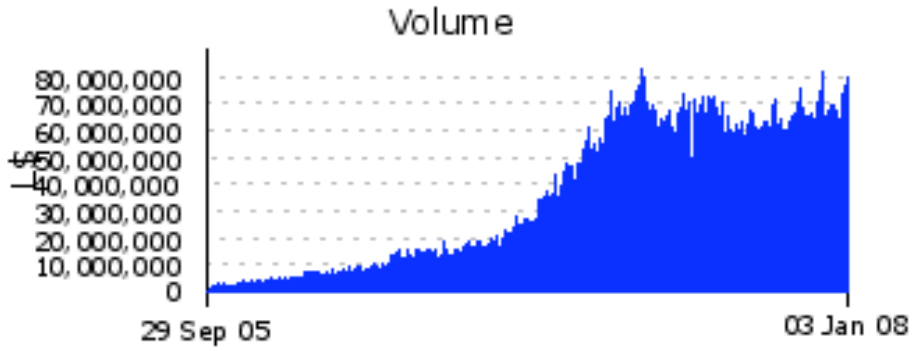

Figure 1 – LindeX Market Volume (Second Life, 2008)

Corporate use of SL to sell goods and services includes external research, marketing and communications, and internal and external collaboration. All of these bring additional security risks to the organization and users must exercise caution in uncontrolled virtual worlds, such as SL. All communications are transmitted over public networks, even if meetings are held in "private" locations (Carr, 2007; Prentice, 2007). Current business uses of SL include IBM, once they decided to use SL, they had more than 3,000 employees in-world in less than 3 months (Kirkpatrick, 2007); a job fair was held for real-life jobs recruiters from Accenture, EMC Corporate, GE Money, and US Cellular (Schalch 2007); BP has developed a program for employee ethics and compliance in SL (Monahan, Harvey, & Ullberg, 2007); the medical community is using SL with people suffering from Asperger's syndrome, often referred to high-functioning autism, to help with their condition (Phillips, 2008); and Zora, another virtual experiment was used to foster civic engagement in participants aged 11-17 (Bers & Chau, 2006). Just a few of the other businesses that currently participate in SL include: Adidas, American Apparel, Circuit City, Cisco, Dell, Reuters, Sears, Starwood Hotels, Sun Microsystems, Sundance, and Toyota (Hemp, 2006; LaPlante, 2007; Stein 2007). Educational institutions are also involved in SL; Cheal (2007) found that SL is not just a fad, but part of a continuum of instructional technology. Educational examples of SL include practice nursing at Tacoma Community College (Carnevale, 2007), public health preparedness at University of Illinois Chicago (Ullberg, Monahan, & Harvey, 2007), economics lectures at Chicago's law school (Foster, 2007), and architecture classes by Terry Beaubois at Montana University (Newitz, 2006). Many other universities have a presence, including University of Idaho, New York University, Vassar, La Cittadella, Bowling Green State University, DePaul University, and University of Southern Denmark. Politicians are also getting involved in SL. Hillary Clinton has an avatar, both a democratic headquarters (place) and republican headquarters (place) have been established, and a Dick Cheney Hunt club (group) has even been set up.

Recognizing there is money to be made and disturbances to cause, criminals and attackers have entered into virtual worlds such as SL. These malicious users have quickly caused many problems. From carrying out thefts, fraud, pyramid schemes, and even a form of denial of service attacks called "griefing," these users are causing headaches for LL and for the virtual

residents of SL (Weslander, 2006). Unfortunately, there appears to be no fix in sight for stopping many of these crimes. The types of crimes being carried out will be described in the next section.

Types of Crimes, Fraud, and Disturbances in Second Life

As noted in the previous section, online attackers have found SL to be a fantastic place to steal, cause disturbances, and commit various crimes. Some of the crimes being carried out in SL are described below.

Griefing. Griefing is defined as "purposefully engaging in activities to disrupt the gaming experience of other players" (Mulligan & Patrovsky, 2003) or "a player of malign intentions… will hurt, humiliate and dishevel the average gamer through bending and breaking the rules of online games… want glory, gain or just to partake in a malignant joy at the misfortune of others" (Rossingol, 2005). Accidentally bumping or pushing other avatars are not included as a griefing, although it often happens unintentionally with new users (Gregson, 2007). As noted in multiple SL Herald articles, griefing incidents have risen drastically over the past year (Ludwig, 2006). One simply needs to review the SL Police Blotter to see that the number of incidents involving harassment, vandalism, and specifically griefing are up tremendously (Second Life Website, 2007a).

Griefers have even formed "invasion groups" that work to cause public disruption and annoyance (Griefing in Second Life, 2007). A few examples of recent griefing attacks performed by the SL Invasion Group include:

- Blocking the exit doors on a disco's private rooms and filling the dance floor with an annoying large box.

- Building walls containing swastikas.

- Detonating nuclear bombs in crowded areas.

- Using a weapon called "the Cosby Block" which fills an area with hundreds of posters of Bill Cosby.

- Mario mosh pit – an attack that floods an area with images of Nintendo's Mario character.

Images showing these attacks are available by visiting Griefing in Second Life, 2007 reference Need this reference here. Without a required registration process that involves users entering a credit card or other mechanism that validates user id's, these attacks will continue to occur.

Phishing. Phishing is a combination of a real world and virtual crime. There are now approximately 12 million SL avatars at this time and criminals have found that the established technique of phishing is working well. Phishing is described by the Anti-Phishing Working Group (2007) as*:*

> using both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials. Social-engineering schemes use 'spoofed' e-mails to lead consumers to counterfeit websites designed to trick recipients into divulging financial data such as credit card numbers, account user names, passwords and social security numbers.

To "phish" end users, criminals will e-mail potential victims, posing as a LL employee and ask the user for their username and password for SL. Many times, users receive an e-mail stating there is a problem with their account and that they must click on the link provided by the attacker to validate their account. Once the user does this, they have effectively provided the attacker with their credentials. Now that the attacker possesses the user's credentials, the attacker can transfer funds out of the end user's account, assume the user's identity, change their avatar, or perform any other action as if they are that person (for example, committing crimes).

Money laundering. Although a virtual world, SL has a real economy in which users can buy and sell items using Linden Dollars (lindenlabs.com, 2007). As noted on the SL website, there are several online resources that allow residents to convert Linden Dollars into US Dollars or other currency, and vice versa. Rates fluctuate based on supply and demand. Currently, no Federal agency like the Financial Crimes Enforcement Network (FinCEN) is monitoring transactions being converted from Linden Dollars to other currencies (Koster, 2007). This provides an excellent back channel for terrorists, organized crime, and even regular business owners to transfer funds to parties undetected. The scenario that Kenneth Rijock suggests is just one example of how criminals can use virtual worlds to funnel money illicitly (Rijock, 2007). The scenario starts by first opening 15 to 25 accounts at SL's website, all with counterfeit identification. Next, fund the accounts with narcotics proceeds, all patiently deposited at the available ATMs by smurfs and then purchase some virtual real estate from a co-conspirator. This co-conspirator is just one of the bogus identities. Next, funnel all the virtual purchase money into this account and then the "seller" can access these funds, either through ATMs or through a bank. Perhaps the criminal can open a small bank account, using a bogus ID, and obtain cashiers' checks with the now-converted "virtual" profits (Rijock, 2007).

LL realizes that there are many legitimate Linden dollar exchanges and has developed an Exchange Risk API in an attempt to cut down on fraud (Second Life Website, 2007b). However, the Federal regulating bodies such as FinCEN need to start reviewing money transfers conducted in virtual worlds such as SL.

Pyramid schemes. Pyramid schemes or "Ponzi" schemes have been around for many years. In a Ponzi scheme, the promoter promises huge returns to investors on short term investments. The scheme works by paying older investors with funds from newer ones. The first few people who invest in a Ponzi scheme usually receive the interest promised, but Ponzi schemes eventually collapse as they do not actually generate money and require an ever increasing number of new investors to keep up the interest payments owed. A virtual bank called Ginko Financial emerged in SL and through much investigation, was found to be running a pyramid scheme. The bank promised 0.10 percent daily accrued interest, which works out to approximately a 44 percent annual return. Interviews conducted by Reuters with the bank's owner, Nicholas Portocarrero (avatar name), have exposed the fact that Portocarrero will not answer questions clearly as to whether or not his bank is a pyramid scheme (Reuters, A., 2006a). As noted in Wired Magazine recently, Ginko Financial finally ceased operations, causing losses

of approximately 750,000 US Dollars to SL residents that had invested in the bank (Gardiner, 2007). After many complaints regarding fraudulent banks in SL, LL announced the following statement on their blog (Linden, 2007):

> it will be prohibited to offer interest or any direct return on an investment (whether in L$ or other currency) from any object, such as an ATM, located in Second Life, without proof of an applicable government registration statement or financial institution charter.

While this statement may deter some miscreants, this traditional scheme will most likely continue to emerge as more and more avatars inhabit SL's virtual world.

Money transfer fraud .This type of fraud occurs when goods or services are promised in exchange for money. The buyer "wires" or transfers money to the seller and then the seller is expected to deliver the promised goods. SL has now experienced multiple cases of wire fraud being reported. In some of the instances, a seller will create a shop and will collect funds from buyers but will not deliver goods. Real estate is another area where this fraud has occurred. A seller promises a parcel of land in exchange for money, but when the money is wired, the rights to the land are not transferred. These cases are quite interesting for they are spilling out from the virtual world into the real world. The fraud may have been committed in a virtual world, but the money is real and the court systems are starting to hear their first cases that involve crimes being committed in virtual worlds (Millstone, 2007).

Vandalism and theft. Vandalism is defined as "willful or malicious destruction or defacement of public or private property" (Merriam-Webster, 2007). Vandalism has been carried out in SL, with users defacing buildings, placing obscene structures in public places, and even building walls with swastikas on them. John Edwards' campaign headquarters was recently vandalized in SL and the "Gay Yiffy," a virtual nightclub for homosexuals, was also vandalized (Brownlee, 2007). While mainly a minor annoyance, vandalism can quickly spawn into a more serious problem.

Theft has also proved to be an issue. Kevin Alderman, owner of Eros LLC, tracked down the real person that illegally copied and sold SexGen Platinum, violating copyright and trademark protections. SexGen allows purchasers to have realistic body parts and sexy moves (Wolfe, 2007).

Attacks on the Second Life grid. Multiple attacks have occurred on the SL grid, leaving the virtual world inaccessible and forcing SL administrators to kick off all users until they are able to restart the grid (a process that can take up to three hours). These attacks are becoming more widespread and, as noted in the griefing section above, can cause major headaches.

One of the biggest attacks to hit SL was dubbed the "Grey Goo Attack" (Lemos, 2006). As noted by The Register, this attack filled SL with golden rings and the distinctive two-tone ding of Sega's popular Sonic the Hedgehog games. As a result of the attack, LL's servers responded slowly causing a variety of side effects, including unreliable account balances, disappearing clothes, and an inability to teleport (Lemos, 2006).

The LL security team has reduced the time it takes to get the grid up and running again after a major attack but security will be a major issue as more users join SL. The LL team has stated that they referred the Grey Goo attack to the Federal Bureau of Investigations (FBI) for investigation, but LL is spending more time researching for ways to combat viruses and malicious code that is unleashed to disrupt the SL.

Slot machine fraud / game tester fraud. This scam preys on new users in SL that are unaware of how fraud is carried out. In this case, the scammer approaches a new SL user in a free area, such as a junkyard. The scammer will ask the user if they will assist in testing a slot machine game they have created. Then they will place a slot machine down next to the new user and instruct them to pay the machine. While the machine will make noises and sound like the new user has won money, the machine will not pay out and the scammer will have taken money from the new user (Panther, 2007).

The slot machine scam as well as minor deviations of this scam are very common and there is no way to stop them other than by banning the scammer. This action only temporarily stops the scammer as they can register another avatar and continue to carry out the fraud.

Fake Second Life Exchange Terminals. This fraud occurs when an attacker places a fake terminal over an actual SLExchange Terminal. Once this is done, the attacker sits back and waits for victims to use the terminal. The victim comes along and deposits money in what they believe is their SLExchange account. Instead, the money is deposited into the attacker's account and the victim does not know about this until the money is long gone. This attack has also been labeled as the "Invisible Prim Over Vendor" scam by Panther (2007). While not the most creative attack, many users have become victims. Users should pay close attention when using SLExchange Terminals to ensure that they are not using a fake terminal.

Linden Labs Responds to Crimes and Disturbances in Second Life

LL does have an acceptable use policy that is required of all new residents, however, most criminals ignore this. LL has the daunting task of trying to stop crimes and disturbances in SL. Unlike the real world that has a police force, SL has no authoritative body to crack down on crimes, fraud, and disturbances being committed. At the present time, when a report is received of suspicious activity from a SL user, the LL team may choose to temporarily suspend the offending user for a set period of time. This does not stop the crime, for the perpetrator can simply obtain a new avatar and continue to carry out crimes.

LL has begun to issue a police blotter which highlights the following information pertaining to incidents (Second Life Website, 2007a):

- Date of incident
- Violation
- Region
- Description

• Action Taken by LL

Overall, the policing system in effect in SL emulates the neighborhood watch concept. The virtual world relies on its citizens to protect each other and to be on the lookout for potential problems. Without a police force or authoritative mechanism to crack down on crime, crimes will continue to be carried out in SL.

Steps for Protecting Yourself From Becoming a Victim

Since there is no formal police force or authoritative body monitoring the virtual world of SL, it is up to you to protect yourself and ensure you do not become a victim of fraud. The following is a checklist of recommended actions that will reduce your risk of becoming a victim if properly followed:

• Never give out your username, password, account numbers, or personal information

• If an offer is too good to be true, it is (don't take it).

• Read security blogs associated with SL to be educated about current illegal activities such as http://slcaveatemptor.blogspot.com.

• Read the SL newspapers to keep abreast of new and emerging issues http://www.secondlifeherald.com.

• Use caution and good judgment when making purchases, using exchange terminals, and so on.

Most importantl, report issues and crimes to LL immediately. If LL does not know about a fraud being committed, they cannot take action to stop it. Incidents can be reported by sending an e-mail to support@lindenlabs.com.

Conclusion

Virtual World crime is here to stay. Criminals have found a new viable way to swindle electronic users and steal real world money. LL needs to take a hard look at crimes being committed in SL to ensure that its virtual world citizens are educated and protected from becoming victims of crimes. LL should also partner with existing law enforcement agencies (FBI, USSS, for example) to work together to reduce virtual crime and disturbances that have severely affected the SL grid. Failure to do so could result in users no longer visiting the virtual world and the eventual collapse of SL.

Bibliography

Anti-Phishing Working Group Website. Retrieved November 17, 2007 from http://www.antiphishing.org/

Bers, M. U. & Chau, C. (2006). Fostering civic engagement by building a virtual city. *Journal of Computer-Mediated Communications, 11*, 748-770.

Brownlee, J. (2007, March 3). John Edwards meets Second Life 'Feces Spewing Obscenity.' *Wired Blog*. Retrieved March 30, 2007, from http://blog.wired.com/tableofmalcontents/2007/03/john_edwards_me.html

Carnevale, D. (2007, November 13). To save a Second Life. *The Wired Campus*. Retrieved January 17, 2008, from http://chronicle.com/wiredcampus/index.php?id=2541

Carr, D. F. (2007, March 1). Second Life: Is business ready for virtual worlds? *BaselineMag*, *Wired*. Retrieved January 19, 2008 from http://www.baselinemag.com/article2/0,1540,2098902,00.asp

Cheal, C. (2007). Second Life: Hype or hyperlearning? *On the Horizon, 15*(4), 204-210.

Denning, D. E. (2007) Activism, hacktivism, and cyberterrorism: The Internet as a tool for influencing foreign policy. Retrieved December 30, 2007, from http://www.iwar.org.uk/cyberterror/resources/denning.htm

Earth Liberation Front Website. Retrieved March 22, 2007, from http://www.earthliberationfront.com/main.shtml

Foster, A. L. (2007). Virtual worlds as social-science labs. *Chronicle of Higher Education, 53*(44), A25.

Gardiner, B. (2007, August 15). Bank failure in Second Life leads to calls for regulation. *Wired.* Retrieved January 9, 2008, from http://www.wired.com/gaming/virtualworlds/news/2007/08/virtual_bank

Gregson, K. (2007, October). Bad avatar! Griefing in virtual worlds. *M/C Journal, 10*(5). Retrieved December 15, 2007, from http://www.journal.media-culture.org.au/0710/06-gregson.php

Griefing in Second Life. (2007, March 5). Retrieved December 3, 2007, from http://news.com.com/2300-1043_3-6163932-1.html?tag=ne.gall.pg

Hemp, P. (2006, June). Are you ready for e-tailing 2.0? *Harvard Business Review*, DOI: F0610F .

Kirkpatrick, D. (2007). It's not a game. *CNN Money, 155*(2), 56. Retrieved January 19, 2008 from http://money.cnn.com/magazines/fortune/fortune_archive/2007/02/05/8399120/

Koster, R. (2007). Is Second Life being used for money laundering? Could it be? Retrieved on January 3, 2007, from http://www.secondlifeherald.com/slh/2007/01/is_second_life_.html

LaPlante, A. (2007) Second Life opens for business. Information Week, Wired February 24, 2007. Retrieved on January 15, 2008 from http://www.informationweek.com/industries/showArticle.jhtml?articleID=197008342

Lemos, R., (2006, November 24). Second Life plagued by 'Grey Goo' attack. Retrieved January 5, 2008, from http://www.theregister.co.uk/2006/11/24/secondlife_greygoo_attack/

Ludwig, F. (2006, August 23). Negative coordinates: Griefing in the unverified age. *Second Life Herald*. Retrieved November 23, 2007, from http://www.secondlifeherald.com/slh/2006/08/negative_coordi.html

Lindenlab.com (2007). What is Linden Lab? Retrieved December 15, 2007 from http://s3.amazonaws.com/download.grid.secondlife.com/Fact_Sheet_LL_Overview.pdf

Linden, K. D. (2008). New policy regarding in-world 'Banks.' Retrieved on January 8, 2008, from http://blog.secondlife.com/2008/01/08/new-policy-regarding-in-world-banks/

Mennecke, B. E. Terando, W. D. Janvrin, D. J. & Dilla, W. N. (2007). It's just a game, or is it? Real money, real income, and real taxes in virtual worlds. *Communications of the Association for Information Systems, 20*, 134-141.

Merriam-Webster Online Dictionary. (2007). Retrieved on December 14, 2007, from http://www.m-w.com/dictionary/vandalism

Millstone, K. (2007, March 8). Pixilated property dispute a real issue in court. Retrieved on January 8, 2008, from http://www.azcentral.com/ent/vgames/articles/0308vglaw0308.html

Monahan, C., Harvey, K., & Ullberg, L. (2007). BP tries Second Life for employee ethics and compliance. *Second Life Education Workshop*, August 24-26, 2007, 93-95.

Newitz, A. (2007). Your Second Life is ready. *Popular Science, 269*(3). Retrieved January 17, 2008 from http://www.popsci.com/popsci/technology/7ba1af8f3812d010vgnvcm1000004eecbccdrcrd.html

Panther, M. (2007, October 10). Second Life terminal fraud. *Caveat Emptor - Buying & Selling in Second Life*. Retrieved on March 23, 2007 from http://slcaveatemptor.blogspot.com/

Phillips, A. (2008, January 15). Asperger's therapy hits Second Life. *ABC News*. Transcript available at http://abcnews.go.com/print?id=4133184

Prentice, S. (2007). Enterprises face security and risk management issues in virtual worlds. Gartner, Inc. July 13, 2007, ID number: G00149677.

Reuters, A. (2006a, October 12). Interview: Ginko CEO Nicholas Portocarrero. Retrieved on October 14, 2007, from http://secondlife.reuters.com/stories/2006/10/12/nicholas-portocarrero/

Reuters, A. (2006b). Outcry as 'copybot' threatens copyright protection. Retrieved on October 14, 2006, from http://secondlife.reuters.com/stories/2006/11/14/outcry-as-copybot-threatens-copyrightprotection/

Reuters, E. (2007, December 18). Second Life performance improves, but residents don't feel it. Retrieved on January 8, 2008, from

http://secondlife.reuters.com/stories/2007/12/18/second-life-performance-improves-but-residents-dont-feel-it/

Rijock, K. (2007, January 2). Virtual money laundering now available on the World Wide Web. Retrieved on January 2, 2008. Available http://www.world-check.com/articles/2007/01/02/virtual-money-laundering-now-availableworld-wide-/

Rossignol, J. (2005, November 15). A deadly dollar. *The Escapist*. Retrieved on December 15, 2007, from http://www.escapistmagazine.com/articles/view/issues/issue_19/121-A-Deadly-Dollar

Schalch, K. (2007, August 22). Virtual recruiting for real-world jobs. *NPR*. Retrieved January 15, 2008 from http://www.npr.org/templates/story/story.php?storyId=13851345

Second Life. (2008) LindeX market data. Retrieved January 4, 2008, from http://secondlife.com/whatis/economy-market.php

Second Life Website. (2007a). Community: Police Blotter. Retrieved January 20, 2008, from http://secondlife.com/community/blotter.php

Second Life Website. (2007b). Linden Labs exchange risk API. Retrieved on January 23, 2008, from http://secondlifegrid.net/programs/api/risk

Stein, J. (2006, December 16). My so-called Second Life. *Time, 168*(26), 76. Retrieved on January 14, 2008 from http://www.time.com/time/magazine/article/0,9171,1570827,00.html

Ullberg, L., Monahan, C., & Harvey, K. (2007). New face of emergency preparedness training: Using Second Life to save first lives. *Second Life Education Workshop*, August 24-26, 96-99.

Warner, D. E. & Raiter, M. (2005). Social context in massively-multiplayer online games (MMOGs): Ethical questions in shared space. *International Review of Information Ethics, 4*, 46-52.

Weslander, Eric. (2006, November 12). Virtual-Reality crimes present literal challenge for real life police. Retrieved November 30, 2006, from http://www2.ljworld.com/news/2006/nov/12/virtualreality_crimes_present_literal_challenge_re/

Wolfe, A. (2007, October 28). Second Life lawsuit over cybersex toy theft. *Information Wee*k. Retrieved January 19, 2008 from http://www.informationweek.com/blog/main/archives/2007/10/second_life_law.html