

Virtual Identities; Real Threats

4th Annual ID & Access Summit
11 March 2009, Sydney

Stephen Wilson
Lockstep Group



European security report

Virtual Worlds, Real Money

2007 was the year of online gaming fraud with ... over 30,000 new programs aimed at stealing online game passwords.

Such malware is invariably aimed at the theft of virtual property and its sale for real money.

*With nearly 1 billion registered users of MMO/VWs and **real-money sales of virtual objects estimated at nearly US\$2 billion worldwide at the end of 2007, this is a serious issue.***

Nov 2008



Real money



Site	Users	Revenue	Valuation (USD)
Habbo hotel	100M		\$1250M
Second Life			\$500-1000M
MindArk <i>Entropia Universe</i>		\$360M	
Blizzard <i>World of Warcraft</i>	10M	\$1100M	
QQ	350M	\$523M	

- No. MMOG subscribers: 14 million in 2008 (ref: www.mmogchart.com)
- Second Life Marketplace: US\$35M traded per month
- LindEx: US\$100M exchanged 2008
- Club NEVERIDE: bought for \$100,000 in 2005; valued at \$1,000,000 in 2008

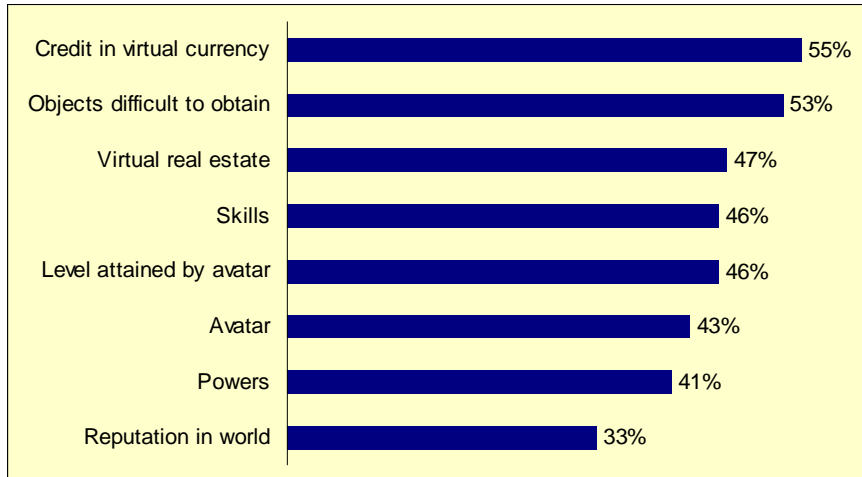
ENISA: Risks



1. Avatar identity theft and identity fraud: theft of account credentials (username and password). The main motivation is real-money financial gain, but identity fraud can also be used to damage reputation (real-life or, more commonly, in-world) and to avoid responsibility for crime.
2. MMO/VW privacy risks: In privacy terms, avatars are no different from other forms of online persona. Users may even disclose more personal data because the MMO/VW gives a false sense of security. There is also a trend towards behavioural marketing by "eavesdropping" on avatars.

Virtual Worlds, Real Money, November 2008.

Which virtual assets matter?



Adapted from Fig 1, *Virtual Worlds, Real Money*, ENISA 2008

Related risks & threats

- Facebook, MySpace and other OSNs under political pressure in US to verify age of users
- New ACMA rules require restricted access to MA15+ content and R18+ content either hosted in Australia or provided from Australia, from Jan 2008
www.acma.gov.au/WEB/STANDARD/pc=PC_310905
- VIPs & Celebrities suffering ID theft;
e.g. James Packer LinkedIn profile hijacked, 2008
- Age verification services in the US are booming, and yet US District Court Judge Lowell Reed, ruling in March 2007 on the Child Online Protection Act wrote:
“There is no evidence of age verification services or products available on the market ... that actually reliably establish or verify the age of Internet users”

ENISA: Recommendations



To MMO/VW providers

1. *The five most important technical issues ... include item-duping, **end-to-end security** and MMO/VW specific denial of service. In general, providers should create an appropriate balance between security measures aimed at detection & response and those aimed at prevention. Detection & response is often a more effective means of addressing security in MMO/VWs than prevention*
- ...
4. *Any initiative which increases the **strength of user authentication** (while maintaining an appropriate balance between usability and cost) should be encouraged.*

Virtual Worlds, Real Money, November 2008

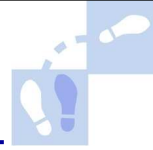
Opportunities



Drawing inspiration from the fact that Citi bank and MySpace have recently partnered on a social loyalty card, and that World of Warcraft and Entropia Universe each offer Two Factor Authentication ... we can envisage banks offering their smartcards for protected logon to OSN/VW/MMOG, to help resist profile & avatar theft, while preserving users' ability to name their own handles

Drawing inspiration from the fact that the New Queensland Driver Licence smartcard technology will be used for a counterfeit resistant Over-18 card ... we can envisage such smartcards holding anonymous proof-of-age certificates so that individuals can prove themselves to MA15+ and R18+ content servers, online liquor merchants, Internet dating services and so on.

Discussion



Stephen Wilson
Lockstep Consulting
swilson@lockstep.com.au
0414 488 851