**Virtual Worlds - Real Money. Multiplayer online gamers ‘soft target’ for cybercriminals - EU Agency report warns.**

**Serious real-world money locked up in the 1.5 Bn Eur virtual goods market is leading to a wave of malware threatening ca 1 Bn users worldwide. The EU Agency’s report includes 12 recommendations for governments, game providers and users.**

**Virtual worlds-real money.** Online gaming fraud is an increasingly serious threat– according to a new [ENISA report](http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_security_privacy_virtualworlds.pdf). The failure to recognise the importance of protecting real-money value locked up in this grey-zone of the economy has lead to a 'year of online-world fraud'. A [survey](http://ievooj.notlong.com/) in the report shows that 30% of users have recently lost some form of virtual property through fraud. In less than a year, more than 30,000 new malicious programs have been detected specifically targeting accounts and property in online games and virtual worlds – “this is a jump of 145%”, says Kaspersky labs.

Such malware is invariably aimed at the theft of virtual property accumulated in a user’s account and its sale for *real money*. “While annual *real-money* sales of virtual goods is estimated at nearly 1.5 Bn Euro worldwide, users can do very little if their virtual property is stolen. They are a very soft target for cybercriminals,” says Giles Hogben, editor of the report put together by a group of industry, academic and government experts. ”There are 1 Bn registered players of online games worldwide and the malware targeting them affects everyone with a computer connected to the internet.”

**Privacy and personal data**. Another important area is the misuse of personal data. The survey of 1.500 respondents in the UK, Sweden and Germany shows that most people think their avatar cannot reveal anything about their real identity. But an avatar is no different from using any online persona, particularly in so-called “social worlds”, i.e. hybrids between online games and social networks. “People should take just as much care of their personal data in these environments as in any other online context,” says Mr. Andrea Pirotti, Executive Director of the Agency. Bots can be sprinkled within virtual worlds to spread spam or advertise products, for example, and these sites are vulnerable to novel variants of denial of service attacks. “Multiplayer online games are especially vulnerable to denial of service attacks because of their centralized architecture and poorly authenticated clients," the report says. The report identifies 12 recommendations to tackle these problems, e.g.;

* An industry-wide forum for service providers to share best-practice on security vulnerabilities
* Clarification of virtual property rights for more adequate theft protection
* A checklist of key technical issues for service providers/developers
* Awareness-raising campaigns for users eg., on child-safety and privacy risks.

**For full report and survey see:** [**http://www.enisa.europa.eu/doc/pdf/deliverables/enisa\_pp\_security\_privacy\_virtualworlds.pdf**](http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_security_privacy_virtualworlds.pdf)or [the survey](http://ievooj.notlong.com/): **For further information**: Ulf Bergstrom, Press and Communications Officer, ENISA, [http://www.enisa.europa.eu/garnish/mail/press.gif](mailto:press@enisa.europa.eu), Mobile: ulf_handy, or **Giles Hogben**, ENISA Expert, [positionpapers@enisa.europa.eu](mailto:positionpapers@enisa.europa.eu) **Have your say!** To influence the future of European Network and Information Security: please give your opinion in the online [public consultation](http://ec.europa.eu/yourvoice/ipm/forms/dispatch?form=InfsoNis): [**http://ec.europa.eu/yourvoice/ipm/forms/dispatch?form=InfsoNis**](http://ec.europa.eu/yourvoice/ipm/forms/dispatch?form=InfsoNis)