FAQs on "Virtual Worlds, Real Money"

1. Q: **What is meant by online gaming fraud?**
   A: Online gaming fraud is fraud aimed specifically at online games and virtual worlds. This is usually done with malicious programs that steal online game passwords, thereby enabling the cyber criminal to steal the virtual property accumulated in a user’s account and its sale for real money. Another important cause of fraud is duping – the unauthorised duplication of valuable objects in MMO/VW, usually by exploiting a software bug.

2. Q: **What is meant by a virtual game world?**
   A: We define the virtual and game worlds covered by this paper according to these criteria:
   - They are shared and persistent – all participants of the world see the same world (even if from different perspectives) – and the data defining the world is usually stored in a central database controlled by the service provider.
   - Interactions occur in real-time.
   - There is an underlying automated rule set, the “physics” that determine how individuals effect changes.
   - Individuals are represented within the world as “avatars”

   ENISA has looked at four different classes of worlds and the security-relevant features of each type:
   - Civic Worlds, e.g., Second Life
   - Game Worlds, e.g., World of Warcraft, Entropia Universe
   - Social Worlds, e.g., There, Habbo
   - Corporate Worlds, e.g., Qwaq, Forterra

3. Q: **What are the main risks concerning fraud for online gamers?**
   A: The main risks include:
   - Theft of identity credentials (abuse of authentification) and their use to sell virtual assets inside or outside the game.
   - Exploitation of flaws in the in-world economy. This includes so-called “duping” (illegal duplication of objects), and other forms of cheating such as illegal automation using bots and “gold farming” the virtual equivalent of sweatshops where low paid workers work long hours to produce valuable assets within worlds. All practices of this kind usually result in inflation of in-game currency and loss of value to bona-fide players.
• In-game theft – the exploitation of a game features to defraud another player of an asset. For example, in 2007, a flaw in the implementation of QuickTime within the world Second Life allowed hacker to carry out virtual pickpocket attacks on their world residents.

4. Q: Why should this problem of online game fraud be taken so seriously?
A: The Internet security company Kaspersky Labs named 2007 as the year of online game fraud. Over 30,000 new malicious programs specifically targeting online games were developed in 2007 - an increase of 145%. Such malware is invariably aimed at the theft of virtual property accumulated in the user’s account. The crucial factor motivating this form of cyber crime is that virtual items can be sold for real-world money, either legitimately or on the black-market. Although amounts stolen from each individual may be smaller compared to Trojans that steal credit card numbers (at least for now), prosecutions are low or non-existent and volume is high. Virtual worlds are an easy target for cyber criminals because they fall outside many of the measures taken to protect other online assets. With nearly 1 billion regular users of online games worldwide and real-money sales of virtual objects estimated at nearly US$ 2 billion at the end of 2007, this is no doubt a serious issue. It is also important to note that the spread of malware is an issue even for non-gamers, since malware often targets internet users indiscriminately on the basis that a few victims will have the relevant software installed.

5. Q: What is malware?

6. Q: What is the cause of the sudden surge in fraud aimed at multiplayer online gamers?
A: There are several reasons. Online games have quickly become increasingly popular, drawing a growing number of users worldwide. As a result, online games have gained the attention of cyber criminals that can exploit a relative immunity against punishment that is the norm prevalent for online games.

7. Q: What is an example of ENISAs security advice to the users of MMO/VWs?
A: The use and collection of in-game data plays an increasingly important role in the economic models of most providers. Whilst this is in many cases necessary to maintain service, users should nevertheless be made aware of the possible privacy threats from playing online games. In particular:

• The use of an avatar is not necessarily a protection against the disclosure and collection of sensitive personal information.
• Sensitive data, such as chat messages, may be eavesdropped by other characters or even in-world objects.
• Actions carried out in-world may often be linked to a real-world address, sometimes even when false registration information is given.

8. Q: Why did ENISA write a report on this topic?
A: The security threats that this report highlights are serious - there are 1 Bn registered players of online games worldwide and the malware targeting them affects everyone with a computer connected to the internet. They affect a huge and growing constituency of people. The real-money at risk is reaching six or even seven figure sums. One of the functions of ENISA's position papers is to highlight threats which people are not aware of and in that respect, this is an especially important topic. You may not be able to touch the goods that get stolen, but then you can't touch your bank balance or stocks and shares either. Virtual goods represent an investment of time and effort to the people who own them just as much as any other so-called "intangible asset". Annual real-money sales of virtual goods are estimated at nearly 1.5 Bn Euro worldwide, but users currently can do very little if their virtual property is stolen. This paper aims to find ways to change that.

9. Q: What is ENISA's recommendation for tackling the threats listed above?
A: One of the most important countermeasures is to raise awareness of the potential threats to MMO/VW-users. In general, it is important to use in-context methods to raise awareness. For example, when logging in, a link could be provided to a video about how to detect account compromise, or about the advantages of stronger authentication methods. When creating in-world content, a link could be provided to a user-friendly explanation of the user's IP rights.

The report lists numerous recommendations for handling this issue to both the European Commission and National Governments (Government Policy Recommendations), and, also to MMO/VW providers. See page 5-6 in the report for a summary of the recommendations.

10. Q: Who contributed to this position paper and how was the data collected?
A: 16 experts from all over Europe contributed to this position paper. In addition, we also conducted a survey of 1 500 end-users of MMO/VWs in the UK, Sweden and Germany. This survey gave us valuable information about habits, preferences and attitudes, specifically towards security in MMO/VWs, among end-users.