# TABLE OF CONTENTS

Executive Summary ........................................................................................................................................................................... 3  
Sidebar: Virtual World Glossary .................................................................................................................................................................. 3  
Introduction: Security Threats are Real in Virtual Worlds .................................................................................................................. 4  
In-World Threats ..................................................................................................................................................................................... 5  
  - Identity Masking .................................................................................................................................................................................. 5  
  - Phishing ............................................................................................................................................................................................... 5  
  - Money Laundering .............................................................................................................................................................................. 5  
  - Theft .................................................................................................................................................................................................. 5  
  - Gangs .................................................................................................................................................................................................. 6  
  - Unique Threats Due to Open Code ..................................................................................................................................................... 6  
Sidebar: Virtual World Best Practices ..................................................................................................................................................... 6  
External Threats ......................................................................................................................................................................................... 7  
  - Keyloggers and Password Stealers ........................................................................................................................................................ 7  
  - Spoofing ............................................................................................................................................................................................. 7  
  - Third-Party Sites .................................................................................................................................................................................. 7  
  - Plug-ins and Extensions ...................................................................................................................................................................... 7  
Increased Business Use of Virtual Worlds ............................................................................................................................................. 8  
  - Identity and Access Management ....................................................................................................................................................... 8  
  - Confidentiality ..................................................................................................................................................................................... 8  
  - IT Risks .................................................................................................................................................................................................. 8  
Sidebar: Cisco and Second Life ............................................................................................................................................................... 8  
Multi-Layered Security and Virtual Worlds ........................................................................................................................................ 9  
  - User Awareness .................................................................................................................................................................................. 9  
  - Protection in the Cloud ......................................................................................................................................................................... 9  
  - Gateway Protection ............................................................................................................................................................................. 9  
  - Endpoint Protection ........................................................................................................................................................................... 9  
Conclusion ............................................................................................................................................................................................................. 10
VIRTUAL WORLDS

EXECUTIVE SUMMARY

As companies adopt telecommuting and workers become more mobile, work PCs are increasingly used for various non-work related activities. These activities expose employees to myriad online threats, and when the computer connects to company networks, the threats can increase corporate risk as well. The increasing popularity of virtual worlds and massively multiplayer online role-playing games (MMORPGs) adds another dimension to these threats and risks.

To help protect employees from these threats and maintain corporate IT systems free from malware, a multi-layered approach to security is needed. This approach combines protection methods in the cloud, at the gateway, and at endpoints with user awareness and education programs. This white paper introduces the kinds of threats that virtual world members and MMORPG players may encounter and suggests protection approaches and best practices for individuals and businesses.

Virtual World Glossary:

Virtual World
A virtual world is an online world that simulates the real world in which “residents” can interact. Residents participate in the creation of the virtual world, contributing virtual objects and social constructs like clubs, stores, real estate, and much more. Examples of virtual worlds include Second Life, IMVU, Google Lively, and Twinity.

MMORPG
A massively multiplayer online role-playing game is similar to a virtual world, but usually includes a goal (e.g., accumulate points) that players try to achieve in a game. Examples of MMORPGs include World of Warcraft, Lord of the Rings, Eve Online, and Final Fantasy.

Avatar
An avatar is a representation of a resident in a virtual world, or a player in an online game. The actions of an avatar (e.g., the creation of an object) persist in a virtual world even when a resident is offline. A virtual world user may create more than one avatar in any given virtual world.
INTRODUCTION: SECURITY THREATS ARE REAL IN VIRTUAL WORLDS

A virtual world is a computer-simulated environment intended for users to inhabit and interact via “avatars.” An avatar is a text-based or graphical representation of the player in the virtual world. Users can manipulate elements of the modeled world and explore it using the avatar as an online self. Virtual worlds might appear similar to the real world or they can represent fantasy worlds. Users in-world can communicate with each other via chat, instant messaging, graphical icons, visual gestures, and voices. Massively multiplayer online games render a world similar to the real world, including real world rules, actions, and communications.

The rapid growth in popularity of online games and persistent virtual worlds has attracted the unwanted attention of both hackers and organized crime. Trend Micro security experts have seen and expect to see an increase in attacks on trusted virtual worlds like Second Life and MMORPGs like World of Warcraft (see Figure 1).

While hackers generate havoc, cybercriminals exploit these trusted online environments, using them for fraud and other illegal activities, including money laundering. Many virtual worlds and MMORPGs allow players to conduct real money transactions in virtual worlds, using real credit cards and other payment methods to purchase and then exchange virtual credits with other players across the globe. The link between real world currency and virtual world trade attracts the organized criminal element.

Figure 1. Trend Micro showed a significant increase in the volume of threats in virtual worlds in 2008.
IN-WORLD THREATS

Many of the threats users experience online in the real world exist also in virtual worlds. The threats may look and feel slightly different from those in the real world, but they exist nonetheless.

Identity Masking
Users can create any number or kind of avatars. As a result, determining the true identity of an avatar is almost impossible, although users can post a profile that more or less represents their true identity. Virtual worlds harbor fake characters that interact with real characters using social engineering techniques to acquire items of value in-world. For dedicated players, losing precious objects they spend hours developing or winning can be upsetting. In-world, when an unknown avatar presents an offer that seems too good to be true, that is likely the case. Awareness and common sense can protect users from identity masking and social engineering attacks.

Phishing
Phishing attempts to acquire sensitive consumer information fraudulently, such as usernames, passwords, and credit card details. Phishers masquerade as a trustworthy entity in an electronic communication and can appear both in-world and out-of-world. In-world phishers communicate through chat or instant messaging and typically direct users to provide account details at a third-party website that appears legitimate, but actually harbors malware that stealthily and methodically steals information. Once an account is compromised in this way, a cybercriminal can empty it or use its associated credit card information for other purchases.

Money Laundering
While not a threat in the usual sense, users can unwittingly become party to money laundering. Because avatars can trade currencies and goods inside the virtual world and then sell them into secondary markets for real money, crime is difficult to trace. If an avatar requests help purchasing or selling in-world currency, players should refuse, to avoid becoming party to a crime.

Theft
In games such as World of Warcraft, avatars build up virtual assets that players can exchange or purchase in the real world. Two kinds of theft can occur, including the theft of virtual assets for use in the virtual world, or their theft for conversion to real world cash. The more sophisticated syndicates focus on the latter, because virtual currencies and goods are not regulated. Therefore, the legal implications for theft are unclear, though people in the real world have sued for theft in the virtual world.
Gangs
In some MMORPGs, groups of avatars known as gangs wait for new players to come online. The gang kills the unsuspecting, novice avatar with virtual swords or other weapons. When the avatar dies, assailants assume their assets. To guard against gangs, users form in-world guilds to work with known avatars and friends to ensure safety.

Unique Threats Due to Open Code
To allow players and third-party developers to participate in the creation and modification of objects, some virtual world programming languages are open and therefore more vulnerable to hacking. Three years ago, a virtual illness killed thousands of World of Warcraft avatars when a design flaw spread through low-level players. Similarly, user-generated code caused a terrorist attack in Second Life.

In another example, the “grey goo” virus replicated objects too many times, resulting in program crashes and strange account problems, such as disappearing in-world currency. This virus occurred in Second Life because of user-contributed programming. Game and virtual world developers have begun to “police” their worlds. The grey goo incident resulted in player expulsions and code alterations, making the replication algorithm less vulnerable to misuse.

While these kinds of threat are less defensible, users should be aware they exist. When strange program behaviors occur, users should read the virtual world and game bulletin board warnings that apprise players about new hazards and misuses.

Virtual World Best Practices
Never use a virtual world login or password outside of the virtual world viewer or website. Hacked or “cheat” viewers can easily pass login credentials to a fraudster. Only deal with known and trusted developers if you choose to use a non-authentic viewer.

Never provide password or security answers via chat or instant messaging to anyone in-world.

Never buy in-world dollars for someone claiming to be unable to buy them.

Never sell in-world dollars on behalf of someone claiming to be unable to sell them.

If possible, join an in-world guild for safety when first exploring a new virtual world.

Read official site bulletin board warnings.
Avoid third-party offers; only use in-world services initially.
EXTERNAL THREATS

Keyloggers and Password Stealers
In the real online world, the use of keyloggers has diminished, but not so in the virtual world. Many Trojans and worms targeted towards online gamers and residents of virtual worlds contain keyloggers. Keyloggers aim to capture account verification credentials when a user launches a game. The keylogger records keystrokes typed at sign in and then submits them to the attacker via email or a web request. Hackers and criminals hide keylogger and related password stealer code in seemingly harmless files, executables, and on websites through URLs embedded in emails or instant messages. Because developers often update games and virtual worlds, phishers typically present a code update through a website URL or as an attached executable in an email. The so-called update contains malware instead.

For example, TSPY_ONLINEGA.KB, a password stealer Trojan, collects user credentials and information on users of the Chinese MMORPG Zhengtu. TSPY_ONLINEGA.KB drops a DLL component into the WindirSystem32 folder and installs itself into a newly created Windir uninstall folder. The Trojan injects the DLL into Windows Explorer (Explorer.exe) and other running processes. Outgoing network connections may be spoofed to appear to be coming from Windows Explorer. Variants of TSPY_ONLINEGA and TSPY_LINEAGE, which steal user information for the Lineage II game, are some of the most widely reported Trojans targeting online gamers during the past year. Trojans can lurk inside user blogs, bulletin boards, and other webpages as well.

Spoofing
Virtual world users should be wary of the potential for spoofed sites, as they may closely resemble the official game or virtual world site. If a user is invited to visit a site for a code update, through a URL embedded in an email, instant message, or chat session, following the link may route them to a malicious URL. For example, www.world0fwarcraft.net and www.wor1dofwarcraft.com (note the number “1” instead of the letter “l”), which at a glance appear to be legitimate World of Warcraft sites, actually host malicious files. To protect against spoofing, users should resist the urge to follow embedded URLs, particularly blind URLs, and follow the practice of typing a known URL.

Third-Party Sites
Virtual worlds such as Second Life have spawned a proliferation of related businesses. For example, users can purchase third-party objects to import into the virtual world. Some of these sites may not be legitimate, including those that provide currency exchanges for in-world dollars. Established exchanges have solid reputations built in part on their in-world longevity and contributions in other areas of the virtual world. Without in-world experience, discerning legitimate third-party sites from frauds is difficult. Hence, new users (referred to as noobs meaning newbies) should strictly adhere to in-world services until they build a social network and gain the experience that allows them to assess the status of third-party offers.

Plug-ins and Extensions
Attackers have begun to use virtual worlds and MMORPGs to trick victims into installing malicious software under the pretense that it provides entirely new or improved functionality. Hackers may use the automated in-world tools to incorporate keystroke loggers, password stealers, and other malicious code that infects unsuspecting player systems.
INCREASED BUSINESS USE OF VIRTUAL WORLDS

Companies are beginning to take advantage of public virtual worlds for external and internal communications – particularly in large, distributed enterprises (see the sidebar for one example).

While most businesses set up private areas that only authorized avatars can access, hackers can penetrate these, exposing users to all the same threats described in the previous two sections of this white paper. A number of challenges for implementing virtual business worlds exist, including identity and access management, confidentiality, and IT risks.

- **Identity and Access Management**
  The lack of verifiable identity control or access management – a deficiency in public virtual worlds – is impacting potential use of virtual worlds for communication and collaboration purposes. As a result, companies should evaluate the benefits of private virtual-world environments, hosted internally, and existing entirely inside the enterprise firewall.

- **Confidentiality**
  Most companies seek to ensure that discussions involving confidential and commercially sensitive information do not take place inside a public virtual world, or on an open, social-networking site. By moving to an internally hosted, private virtual world, the issues of privacy, confidentiality, and identity can be controlled from within the enterprise (although some of the benefits of a public virtual world are lost as a result).

- **IT Risks**
  Virtual worlds require complex client applications, evolve rapidly, and are typically updated frequently. This can lead to staff member use of multiple versions of the software, complicating update management. At worst, end-users may fall prey to downloading an infected version from a non-authenticated site.

  The trend toward business use of online virtual worlds, virtual events, and MMORPGs is growing. As a result, Trend Micro believes that business will inevitably adopt these technologies for their many benefits, including increased collaboration, communication, and marketing potential.

---

**Cisco and Second Life**

Cisco Systems has a few hundred employees resident in Second Life. They have created office building, meeting room, and conference hall “sims”, or simulations, which they use for internal international and user-group meetings. They perform customer education and training, and elicit feedback from customers on products. They even hold events that combine people in the real world with avatars in Second Life – a type of event called “mixed reality.”
MULTI-LAYERED SECURITY AND VIRTUAL WORLDS

Implementing policy compliance software for virtual worlds helps ensure that users cannot install unauthorized client software on corporate computers. Another approach involves disabling access to popular sites at the perimeter. However, with the increase in virtual worlds and MMORPG popularity and the blurring of the use of computers for work and personal use, these methods seem draconian and in the second case, only work when a user accesses the Internet through a corporate network.

Because threats in virtual worlds are similar to real world online threats, security system designers can adopt a multi-layered approach to protecting corporate assets. Whether a company decides to make use of a public virtual world for corporate use, or if the company allows workers to visit virtual worlds with corporate computers, a multi-layered approach is paramount.

User Awareness
Forewarned is forearmed, and teaching users what to expect in virtual worlds is a prudent approach to protection. Users inside “trusted” sites may grow careless and succumb to malicious tactics that would be ineffective in the real world. Security awareness training can help protect the enterprise from Internet-based attacks. Employees and executives alike should increase their awareness of threats that exist and learn how to guard against them. Applicable security policies should be created, adopted, periodically reviewed and updated, and communicated to all relevant parties.

Protection in the Cloud
URL filtering and reputation analysis services provide a layer of protection in the cloud outside the corporate gateway. Reputation services rate URLs based on the likelihood they harbor malware or send spam. Databases fed by information from end users and corporate systems continuously identify and track millions of potentially harmful pages and sites. Reputation-based protection is essential today when so many threats originate from website and email vectors.

Gateway Protection
Assuming that workers in the organization visit virtual worlds working behind corporate firewalls, gateway security appliances and software can perform content and URL filtering, as well as reputation analysis, and provide anti-phishing, anti-spam, and antivirus protection.

Endpoint Protection
Many users visit virtual worlds and MMORPGs from non-work locations, using less secure and less protected network connections. As mobility increases, protection should focus on protecting mobile devices. However, hackers and criminals continuously adapt and invent new techniques. User behavior can be unpredictable – especially inside a trusted world. As a result, companies should also invest in high-quality endpoint security products. These include virtual browsing environments through which users can access virtual world, file behavioral analysis, reputation management, and restore point technologies. If an individual machine is well protected, this forms a critical line of defense.
CONCLUSION

To avoid the threats posed by virtual worlds and MMORPGs, Trend Micro recommends that users and organizations be vigilant and proactive in protecting their information and systems. Best practices include using commonsense practices; employing multiple, overlapping, and supportive protection systems; increasing awareness of the threats; applying caution when file-sharing; and keeping systems up-to-date. Using these and related measures, businesses can safely take direct advantage of the opportunities virtual worlds offer, build them into their business practices, and protect corporate assets from employee exposure to their threats.