Playing it Safe:
Avoiding Online Gaming Risks

ERIC HAYES

Introduction

New technologies and high-speed internet connections have helped online gaming become a popular pastime on the internet. While gamers invest large amounts of time and money in today's sophisticated games for enjoyment, others see an opportunity for mischief or illicit profit. The technological and social risks of online games should be understood by anyone who plays them. These include the following:

- risks from social interactions with strangers who may trick you into revealing personal or financial information
- risks from computer intruders
- risks from online and real-world predators
- risks from viruses, Trojan horses, computer worms, and spyware

The following sections discuss the risks of online gaming and how you can safeguard against them.

Online Gaming Risks

An abundance of choices exist in today's online gaming environment. Online gambling games are played by people all over the world. Another popular genre of games has emerged called Massive Multiplayer Online Role Playing Games (MMORPGs or MMOs). Most allow players to create online identities as game characters who participate in virtual adventures, which sometimes cross into the real world. For example, gamers sell virtual game items for real-world money in markets such as eBay. In some games, there is a user-created, virtual world where people use real money to create or purchase personal property in their online world. This has created an opportunity for a new type of criminal activity called "virtual crime," in which traditional crimes, such as theft or extortion, are carried out in online game environments.

In general, online gaming may involve both social risks and technological risks. Thus, many online gaming risks are similar to those computer users may have already encountered, but they may not have realized that the games pose another opportunity for the compromise of their privacy or computer security. In this paper, we describe both types of risk.

Technological Risks

Online gaming can involve the following technological risks to your computer system or the systems of gamers with whom you interact.

Viruses and Worms

Viruses may arrive as attachments in email messages or via instant messaging programs, and corrupt or malicious programs may be hidden in game files you download or software you install.

Malicious Software

Viruses and worms may be used to install malicious software on your computer. Malicious individuals may also take advantage of the social networks associated with online games that rely on chat, email, or even voice communication to entice you to visit bogus web sites or open email attachments containing malicious software and install this software on your computer. They then use this software for a variety of illicit purposes.

Insecure or Compromised Gamer Servers

Gamer concerns: If the software on the game server has been compromised, computers that connect to it can be compromised also. The CERT Coordination Center[1] has documented cases of game vulnerabilities in its vulnerability database. Essentially, *any* game with a network connection carries some level of risk to computer security, especially compared to playing a computer game that does not require a connection to another computer or a link to the internet. By exploiting vulnerabilities, malicious users might be able to control your computer remotely and use it to attack other computers or install programs such as Trojan horses, adware, or spyware, or gain access to personal information on your computer.

Server operator concerns: Operating a computer server to run a gaming application involves the same challenges and risks associated with operating a server for other applications. Intruders may break into or crash your server if its security profile or level of protection is insufficient.

Insecure Game Coding

Some game protocols – the methods for communicating game information between machines – are not implemented as securely as other protocols. Game code may not be as well scrutinized as more popular commercial software. Consequently, game software may sometimes cause "buggy" behavior on your computer or introduce unknown vulnerabilities.

1 CERT and CERT Coordination Center are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

Social Risks

Although computer games were once solitary activities, most now have an online community whose members talk, chat, or send instant messages during the games. Some computer intruders may use the social interaction of the online gaming environment in an attempt to exploit software vulnerabilities. Others may try to gain access to unprotected computers connected to the internet. The intruders may want to do any of these:

- capture your personal information
- steal your identity
- steal credit your card information
- inappropriately contact children by pretending to be another child, setting up meetings, or tricking them into revealing personal information

The following sections highlight social risks associated with online gaming.

Social Engineering

Malicious individuals may try to trick you into installing software on your computer that they can use to control your computer, monitor your online activities, or launch attacks against other computers. They may, for instance, direct you to phony web sites offering bogus patches or game downloads that, in reality, are malicious software. For more on social engineering, see the US-CERT Cyber Security Tip "Avoiding Social Engineering and Phishing Attacks" < http://www.us-cert.gov/cas/tips/ST04-014.html>.

Identity Theft

If a malicious individual can gather information about you from the profiles you create in games and other sources, they may be able to use it to establish accounts in your name, resell it, or use it to access your existing financial accounts. For example, in South Korea, more than a thousand gamers had their identities compromised[2] through a fantasy game called "Lineage." Game accounts were created in their name without their knowledge. The suspected motivation was that people were trying to earn money selling virtual weapons and abilities used in the game. For more on identity theft, see the US-CERT Cyber Security Tip "Preventing and Responding to Identity Theft" <http://www.us-cert.gov/cas/tips/ST05-019.html>.

Protection Schemes

The gaming community has also seen the emergence of protection rackets. A common tactic is for a virtual extortionist to threaten weaker players in a game or warn them of negative consequences unless they pay virtual or real protection money.

[2] http://www.post-gazette.com/pg/06052/658467.stm

Cyber Prostitution

In the game "The Sims Online," an MMO, a "cyber-brothel" was developed by a 17-year old boy using the game alias "Evangeline."[3] Customers paid sim-money ("Simoleans") for cybersex by the minute. His account was canceled, but no legal action was taken.

Virtual Mugging

The term "virtual mugging" was coined when some players of Lineage II used bots[4], which are software programs often used to gather information or perform specific function, to defeat other player's characters and take their items. Japanese police arrested a foreign exchange student in August 2005 following the reports of virtual mugging and the online sale of the stolen items. The number of game players who have experienced some manner of virtual crime is already large. South Korea, a country with many active gamers, had over 22,000 reported cases of various types of virtual crime involving games in 2003.[5]

Virtual Sweatshop

The virtual economies of some online games and the exchange of virtual items and currency for real money has spawned the virtual sweatshop, in which workers in the third-world countries are economically exploited by people seeking to find new ways to profit from the new online economies.[6]

How to Protect Against the Risks

Internet gaming can be a safe and enjoyable online activity if your educate yourself and practice the basic principles of good computer security.

General Security Practices

Many computer security principles are the same as those you may have practiced in other computer applications. See the resources section at the end of this paper to locate more information about computer security. Key practices of good personal computer security include the following:

- Use antivirus and antispyware programs.
- Be cautious about opening files attached to email messages or instant messages.
- Verify the authenticity and security of downloaded files and new software.
- Configure your web browsers securely.
- Use a firewall.
- Identify and back-up your personal or financial data.

[3] http://en.wikipedia.org/wiki/Virtual_crime
[4] http://en.wikipedia.org/wiki/Internet_bot
[5] http://en.wikipedia.org/wiki/Virtual_crime
[6] ibid.

- Create and use strong passwords.
- Patch and update your application software.

US-CERT has published a number of Cyber Security Tips corresponding to the items in the above list. To view a complete list of US-CERT Cyber Security Tips, visit < http://www.us-cert.gov/cas/tips/>.

Gaming-Specific Security Practices

Recognize "Administrator Mode" Risks

Some games require you to use your computer in "administrator mode." If this is the case, it is important to make sure the game vendor is reputable and download the game from a site you believe you can trust. Free downloads of games sometimes conceal malicious software. This includes "plug-ins" sometimes required to run certain games. By operating in "administrator mode," you open yourself to the risk that an attacker could gain complete (administrator-level) control of your computer. Web browsing from a user account is generally safer than using administrator mode. If you choose, you can keep the administrator password private and supervise the online game time of your children.

Recognize ActiveX and JavaScript Risks

Some web games are played via a web browser and require ActiveX or JavaScript to be enabled. If this is the case, be aware that enabling these features can lead to some vulnerabilities. For more information, read the CERT document on securing your web browser.[7]

Play the Game at the Game Site

When playing an online game, it is best to play it at the game site and save web browsing for later. This way, when you are done playing, you can switch back to a user account to browse the web. This may reduce your risk if you end up on a malicious web site.

Pay Attention to Firewall Management

Home users often use firewalls to help protect their computers. Playing a multiplayer internet game sometimes requires an exception in the rule set for the firewall to allow information from the game to get through to your computer. Remember that anytime you allow more permissive security settings on your firewall, you increase the chance of a computer security problem. Firewalls may also allow you to designate specific IP addresses of fellow gamers as "trusted" to reduce the possibility of interaction with a malicious individual or of a malicious program infecting your computer.

[7] http://www.cert.org/archive/pdf/browser_security0601.pdf

Conclusion

Online gaming has many positive aspects. It has become a major source of entertainment, developed new industries and sources of revenue, and introduced new uses of the human imagination to millions of people. However, it is important to know and guard against the risks associated with the internet gaming world to keep it safe and enjoyable for all.

Resources

Securing Your Web Browser
http://www.cert.org/archive/pdf/browser_security0601.pdf

Sources of Security Information
http://www.cert.org/other_sources/

Home Network Security
http://www.cert.org/tech_tips/home_networks.html

Cybersmart
http://www.cybersmart.org/home/

A Parent's Guide to Internet Safety
http://www.fbi.gov/publications/pguide/pguidee.htm

Know the Risks – Gambling
http://www.media-awareness.ca/english/teachers/wa_teachers/safe_passage_teachers/risks_gambling.cfm

Computer and Video Game Addiction
http://www.mediafamily.org/facts/facts_gameaddiction.shtml

Internet Filters: Making Web Surfing Safer For Children
http://www.mediafamily.org/facts/facts_internet.shtml

Resources about Children and the Media
http://www.mediafamily.org/facts/index.shtml#ic

Learn how the right user account can help your computer security
http://www.microsoft.com/athome/security/online/logoff_admin_account.mspx

TechNet Security Center
http://www.microsoft.com/technet/security/default.mspx

Security in the Online Game World
http://www.microsoft.com/windowsxp/using/games/learnmore/gamerparenting.mspx/

Keeping Kids and Teens Safer on the Internet
http://www.netsmartz.org/

Child Safety on the Information Highway
http://www.safekids.com/child_safety.htm

Computer Security Resources from US-CERT
http://www.us-cert.gov/reading_room/