# Chapter 71
# The Cyber Awareness of Online Video Game Players:
## An Examination of Their Online Safety Practices and Exposure to Threats

**Soonhwa Seok**
*Korea University, Seoul, South Korea*

**Boaventura DaCosta**
*Solers Research Group, FL, USA*

## ABSTRACT

*The cyber awareness of online video game players (n = 183) was investigated by examining their online safety practices and the degree to which they were exposed to threats. With findings revealing that gamers engaged in poor online practices, despite expressing concern for their safety, this investigation supports the view that gamers are unaware of the possible consequences of their online actions, and/or continue to show resistance to cybersecurity practices perceived to hinder gameplay. While the findings should be regarded as preliminary, game developers and publishers, policymakers, and researchers may find them valuable in obtaining a clearer understanding of gamers' cyber awareness and online practices. Coupled with ongoing research, these findings may also prove valuable for the identification of strategies that may be used to curb risky online behavior.*

## INTRODUCTION

Video gameplay has become an everyday activity, available on a multitude of platforms, from computers to mobile devices. While these games can offer rich interactive experiences, their connectivity raises concern about safety. Massively multiplayer online role-playing games (MMORPGs), for example, have been described as breeding grounds for hackers and cybercriminals. Further, mobile games are believed to expose gamers to cyber threats through vulnerabilities that, when coupled with granted permissions, can create opportunities for unintentional access to device features. With video games anticipated to

DOI: 10.4018/978-1-6684-7589-8.ch071

grow in popularity and sophistication, it is important to understand the cybersecurity risks associated with this form of entertainment.

This study investigated the cyber awareness of online video game players (hereafter referred to as "gamers") by examining their online safety practices and the degree to which they were exposed to online dangers. With findings revealing that gamers engage in poor online practices, despite concern for their safety, this investigation offers empirical data in preliminary support of the argument that gamers are unaware of the possible consequences of their online actions and/or continue to show resistance towards cybersecurity practices perceived to hinder gameplay.

## BACKGROUND

### Cybersecurity Gaming Threats

Although cybersecurity-related gaming threats are not new (Cook, 2016; Dickson, 2016), the popularity and growth of online games have created new opportunities for cybercriminals (Dickson, 2016), who see these games as a way to make money using a variety of methods. For example, data breaches have seen yearly growth that is not confined to a particular sector, but targeting everything from retail to government. The video game industry has not been excluded from this trend, with large breaches reported in just the past few years. One of the most noteworthy was the PlayStation Network breach in 2011, which resulted in 77 million accounts being compromised (Paganini, 2016). In addition, Valve revealed in 2015 that 77,000 Steam accounts were hacked for months (Dickson, 2016; Makuch, 2015) using malware that is readily available on black markets for as little as US$3 (Dickson, 2016).

Such breaches often result in compromised gamer accounts that can be looted for personally identifiable information and sold to other cybercriminals (Rashid, 2013; Trend Micro, 2015, 2016) for the purposes of identity theft or fraud (Trend Micro, 2015, 2016). Gaming accounts typically include name, birth year, mailing address, email, mobile number, payment information, and even social networking data (Trend Micro, 2015, 2016). With the average gamer's age 18 to 30 years old, these accounts are attractive to cybercriminals (Rashid, 2013) with far-reaching implications, particularly for those who use the same password for their email, social media, and banking. Furthermore, data found in compromised accounts may be mined beyond financial gain, putting lives at risk. For example, social engineering tactics might be employed to determine if account owners hold significant positions or have access to important information, such as U.S. intelligence (Rashid, 2013).

Money may also be made through the sale of virtual goods. For example, some online games are intensely played (Cimpanu, 2016; Cook, 2016) to amass in-game items (e.g., weapons, armor) or currency that can be sold for real-world money (Cook, 2016). A DFC Intelligence (2010) study in cooperation with Live Gamer helps illustrate the popularity of such sales. Of the 4,816 mostly male U.S. and European gamers surveyed, approximately 60% purchased in-game goods (that was not a full game), with nearly 50% specifically buying power-up items believed to offer a gameplay advantage. While the sale or trade of legitimately attained in-game items is not prohibited (although the practice is considered cheating by some and thus frowned upon), in-game goods associated with compromised and stolen accounts can be illegally sold or purchased with a linked credit card for subsequent sale (Trend Micro, 2015, 2016). This was the case with the aforementioned Steam data breach, where cybercriminals targeted assets to be resold on Steam Trade (Dickson, 2016). In fact, according to *The New York Times,* the sale of in-game