Cybercrime in Online Gaming

4

Boaventura DaCosta
https://orcid.org/0000-0003-0692-2172
Solers Research Group, USA

Soonhwa Seok
Korea University, South Korea

INTRODUCTION

Video games are readily available on several platforms, including computers, dedicated game consoles, handhelds, and mobile devices. While these games offer rich interactive experiences, their global connectivity is increasingly raising concerns about safety. For example, massively multiplayer online games (MMOs) have been described as breeding grounds for hackers and cybercriminals. Mobile games are also of interest in this connection, because they may expose players to vulnerabilities through unauthorized access to device features. With video games anticipated to grow in popularity and sophistication, it is vital to have a clear understanding of the most current forms of online risks associated with this form of entertainment.

Considerable information on the Internet speaks to cybercrime as it relates to online gaming. However, there does not appear to be much consensus on the extent to which cybercrime has impacted the video game industry and its gamers, to include conflicting views about specific forms of illegal activity. The belief that today's cybercriminals are using virtual currency in online game economies to launder money is one such example. This idea has been presented by some as a serious problem (e.g., Richet, 2013), with the game industry unknowingly being a pawn in online criminal activity. Conversely, others have contended that the premise makes for an interesting story, but that carrying out such an act would be impractical given the challenges involved (e.g., Messner, 2018).

This chapter extends the work of Seok and DaCosta (2019), who examined the online safety practices of video game players and the degree to which they are exposed to online threats, by offering a deeper understanding of the types of cybercrime that affect the video game industry and its players. Although considerable effort was made to capture peer-reviewed materials, the great majority of the content comes from Internet news articles, to include reports and commissioned studies on the video game industry. Finally, online criminal activity is ever changing, with video games in a constant state of technological advancement. Though it is expected that this chapter will be of value to educators, practitioners, researchers, and game developers and publishers, it should by no means be considered an all-inclusive reference, but rather a catalyst for discussion, debate, and future research.

DOI: 10.4018/978-1-5225-9715-5.ch059

CYBERCRIME IN ONLINE GAMING

Cybercrime is not new to the video game industry (Cook, 2016; Dickson, 2016). Nevertheless, the popularity and prolific growth in the number of online games have produced new opportunities for cybercriminals (Dickson, 2016), who have come to view these games and their players (hereafter referred to as "gamers") as easy targets for making quick money through a multitude of techniques. Given that the size of the game industry rivals that of the movie industry in terms of gross revenue, and that hacking techniques are anticipated to grow in sophistication, it has been argued (Cook, 2016, 2017) that the potential for increasingly complex and dangerous online threats is a serious problem.

In the subsequent sections of this chapter, data breaches, compromised accounts and stolen data, the theft and sale of in-game items, and money laundering are discussed. Other forms of cybercrime facing the video game industry, such as the highly debated practices of piracy and reverse engineering, are not discussed. Although these threats are also important, this chapter focuses on the most deliberate types of cybercrime impacting the video game industry in recent years.

Data Breaches

At the time of this writing, data breaches seem to have become commonplace, to such an extent that data privacy and online security have become part of the national conversation. Take the two related incidents involving the U.S. Office of Personnel Management (OPM). The OPM reported that in 2015, the personal data of 4.2 million current and former federal government employees were compromised. The data included names, birth dates, home addresses, and Social Security Numbers (SSNs) (OPM, n.d.). Later the same year, the OPM reported that the background investigation records of current, former, and prospective federal employees and contractors had also been compromised. This included the SSNs of 21.5 million individuals (19.7 million of whom had applied for a background investigation; and 1.8 million non-applicants, primarily comprising spouses or co-habitants of the applicants) (OPM, n.d.). Compounding matters, the OPM reported that some of the stolen data also included findings from interviews conducted by background investigators as well as fingerprints (OPM, n.d.).

Even though victims of large data breaches have sometimes been offered identity-theft protection coverage for a few months, or even a few years (in the OPM breach, for example, victims were given coverage through 2026 [OPM, n.d.]), in many cases the data stolen do not expire. That is, while banks and financial institutions can issue new credit cards to mitigate unauthorized purchases, other stolen personal information, such as SSNs, continues to pay dividends to cybercriminals. Four years after the OPM breach, for instance, two people pleaded guilty to using stolen OPM data in identity theft cases (Weiner & Hawkins, 2018), showing the long-term consequences of such incidents.

Regrettably, the OPM breach is by no means the largest to date. The Equifax breach in 2017 resulted in the exposure of 143 million American consumer accounts (FTC.gov, 2017). The data included names, birth dates, addresses, SSNs, and in some instances, driver's license numbers (FTC.gov, 2017). The credit card numbers of approximately 209,000 and dispute documents (with personal information) of 182,000 consumers were also stolen (FTC.gov, 2017). Further, in 2013 Yahoo admitted that the information of one billion account holders had been stolen (Burgess, 2016). Yahoo later acknowledge that the actual number of compromised accounts was three billion (Burgess, 2017).

While these hacking events specifically targeted government, finance, and telecommunications, such incidents are by no means isolated to a specific sector, and the video game industry is seeing its own share of large-scale occurrences. The most noteworthy is perhaps the PlayStation Network breach in 2011,