



# Cybersecurity Digest

Bi-Weekly update by the CISO Section of Meghalaya Rural Bank

Volume 2 Issue 15

Date: 01.11.2025

## Video games: A gateway to online money laundering

Online video games have become a popular pastime for people of all ages. However, the rise of the virtual economy and the increasing value of in-game items and currencies (in-game items and in-game currencies) have also made them a target for money launderers. Money laundering is the disguise of proceeds from illegal activities as legitimate funds, and criminals use virtual currencies and in-game items in online video games to launder their illicit funds. The anonymity and global reach of the Internet make it an attractive option for money launderers, as it allows them to move money across borders and through different financial systems with relative ease.

## What are in-game currencies?

An in-game currency is a virtual currency created specifically for a video game to fuel its virtual economy. This type of currency can either be earned in-game by winning challenges or acquiring new abilities, converted into real funds or traded between players. There are two common types of in-game currency: convertible



and non-convertible. With the more convertible currency, a player can exchange real currency for in-game currency and then back again. Many of these types of currencies have a fluctuating exchange rate and a specific exchange platform. A player can use this type of currency to create, sell, or trade items with other play-

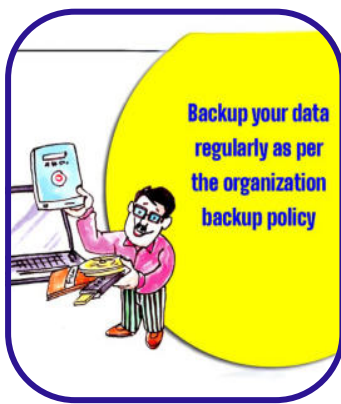
ers in the game, or to invest in the game's virtual properties or assets. With non-convertible currency, a player can exchange real money bills for in-game currency, but not back. This currency can only be used within the game to purchase skins, weapons, or power-ups for the player's avatar to personalize their in-game character, but cannot be traded with other players or officially invested.

## Why cybercriminals use the video game industry for money laundering.

The video game industry, particularly the market for online multiplayer games, has seen a rise in nefarious activity in recent years due to the lack of regulation by local and international organizations, few to no customer identification rules, ease of transferring in-game currency, and crowded platforms that allow criminal transactions to get lost in the myriad of legitimate transactions. For money launderers,

traditional methods of money laundering pose higher risks than in the past as AML regulations become tighter. As a result, cybercriminals are looking for new avenues. The video game industry is one of those new avenues. The video game industry poses a money laundering risk due to in-game commerce, as game materials can be purchased with real money in some video

games. The key factor that makes money laundering through online games possible is that virtual items in the game sometimes have real value outside the game. These include, for example, artifacts that give the game character additional powers (e.g., swords, armor, and potions) or "currencies" that can be used to purchase them.



## Examples of money laundering in online games

The use of convertible and non-convertible virtual currencies in the video game industry and the anonymity offered to players have created an environment for criminal activity. When purchases are made for the game in online video games, users enter their credit card information into the system. Criminals can steal these credit card details and conduct money laundering activities through these accounts. In addition,

cybercriminals typically log into accounts without two-factor authentication and use stolen credit card information to purchase in-app money. These game materials and purchased currency can then be sold on an online marketplace at a lower price. Game owners can only find a solution if they are aware of this event.

Some common methods are:

- Buying virtual currency or in-game items by illegal means

and then selling them for profit on third-party marketplaces.

- Using virtual currency or game items to purchase real goods or services, such as weapons, drugs, or other illegal items.

- Creating multiple accounts in a game and using them to transfer virtual currency or game items between accounts.

- Gambling with virtual currency or game items in online games.

- Creating fake virtual items in a game and selling them to other players

## How are values acquired?

The normal way to acquire new game values is to simply play the game. But the game is not fast enough for those who want to make money by trading values from the game. Criminals have found out that it is not difficult to gain access to a computer and the game using phishing, Trojans or simply hacking the PC. Once they gain access, there are several ways criminals can get game assets. Basically, it's not diffi-

cult using common phishing techniques, such as emails that entice people to click on a link that downloads malware, gaining access to the player's name and password. The criminals discovered that it was quite easy to take over a computer in this way and went one step further. They refined the malware so that it also gave access to bank and credit card information and even took over the player's ac-

cess to the banking system. After that, the easiest way to empty the bank account was to make large or multiple purchases. However, they also discovered that they could use the account to transfer illegal funds. By buying game assets directly from the account and immediately reselling them to an exchange or RTM (real money trading) website, they could make the money virtually untraceable.

MINISTRY OF HOME AFFAIRS

# DIAL 1930

## FOR ONLINE FINANCIAL FRAUD

### REPORT ANY CYBERCRIME AT

## WWW.CYBERCRIME.GOV.IN

FOLLOW CYBERDOOST ON SOCIAL MEDIA FOR UPDATES ON CYBER HYGIENE