Attackers use JavaScript URLs, API forms and more to scam users in popular online game “Roblox”

By Tiago Pereira

Published: 2023-11-02 · Archived: 2026-04-05 21:26:13 UTC

Thursday, November 2, 2023 07:58

- Online video games often make use of in-game virtual currency and give players the ability to purchase, trade or sell items. While these features are often selling points for players and potential revenue streams for the companies that make them, they also inevitably draw bad actors and scams.
- One of these games is “Roblox,” a highly popular gaming platform, especially among children. We curated a short list of scams that have been reported online, such as on user support forums, YouTube videos and scammer Discord channels, explaining how they work and providing advice on how to detect and avoid them.

Roblox is a gaming platform composed of “Experiences,” which is “Roblox’s” name for user-created 3-D worlds where players can interact with each other and their surroundings. The creator, which can be any user, builds the scenarios, the game logic, items and overall interactivity of the experience.

Roblox is free to play but contains an in-application currency called “Robux” that can be used to purchase clothes, weapons or other items for a user’s avatar, some of which exist in limited quantities and can be worth tens of thousands of real-world dollars. Items can also be traded for other items or Robux using a built-in trading system. This creates a potentially profitable market and even though trading for real money is prohibited by the terms of service, some users negotiate outside the platform and trade using real money.

Where there is a potential for profit there are also people trying to scam others. “Roblox” users can be targeted by scammers (known as “beamers” by “Roblox” players) who attempt to steal valuable items or Robux from other

players. This can sometimes be made easier for the scammers because of “Roblox's” young user base. Nearly half of the game’s 65 million users are under the age of 13 who may not be as adept at spotting scams.

How to identify scams

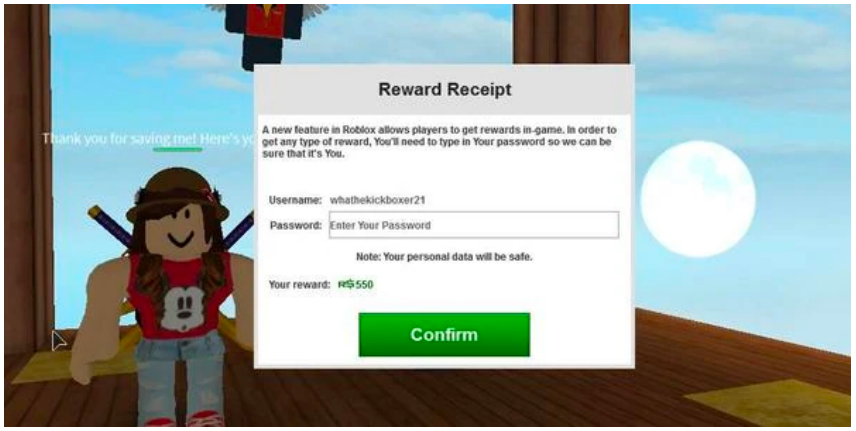
Having knowledge of common scams and how they work is key to spotting them, even if you’ve never heard of a particular tactic before. The following are some of the most common scams that have been seen targetting “Roblox” users.

Offering free Robux/phishing

The scammer sends a message using “Roblox’s” in-game chat or another messaging application, to the victim offering a way to earn free Robux. In the most common variation of this scam, the user receives a link to a web page containing “Roblox”-related themes or images. The site offers the victim free Robux and asks the victim to enter their username and password so that they can receive the Robux in their account. After inserting their username and password, instead of receiving the Robux, the scammer logs into the victim’s account and steals all Robux and valuable items.

In-experience phishing

In Roblox, any user can create experiences, including scammers. In this case, the scammer creates a malicious experience that promises to deliver free Robux and prompts the victim to fill out a form with their username and password. The victim’s credentials are sent to an actor-controlled server, allowing the adversary to log in to the user’s account and steal all Robux and valuable items.



source: https://roblox.fandom.com/wiki/Scam/Gallery?file=Reward_scam.jpg

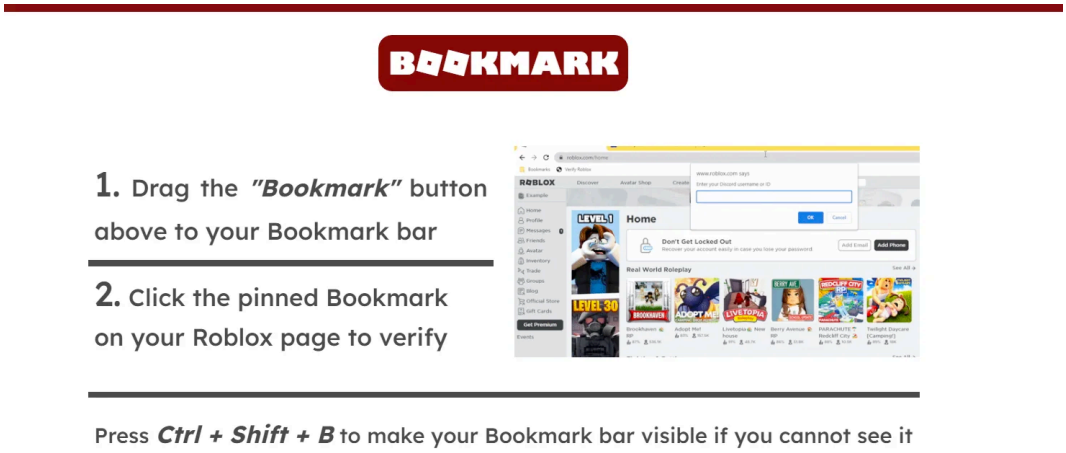
JavaScript method

The scammer asks the victims to copy and paste a link containing JavaScript code into the browser’s address bar. There are many variations that use this method. In one common variation, the scammer pretends to be developing an experience and asks the user to use their avatar image in the experience. To receive the details of the avatar automatically, the scammer asks the victim to copy and paste the link containing the JavaScript code into the browser’s address bar. That code then steals the victim’s session ID, allowing the scammer to use the platform to

log in to the victim's account and transfer all items and Robux from the victim's account to the scammer's account.

Bookmark method

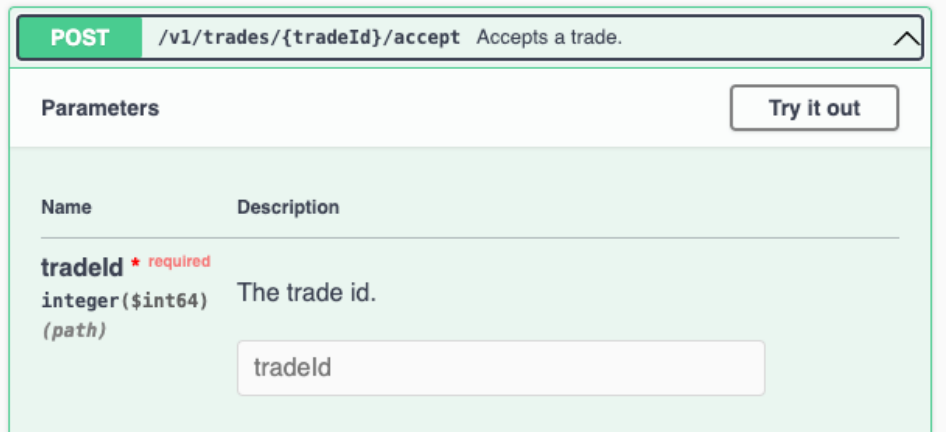
The bookmark method is a variant of the JavaScript method. Instead of asking the victim to paste a link into the address bar, the victim is asked to drag and drop the bookmark into the bookmarks bar and then click on it. The bookmark contains JavaScript code that steals the victim's session ID.



source: https://www.reddit.com/r/robloxhackers/comments/11eofbr/possibly_new_roblox_scam/

API method

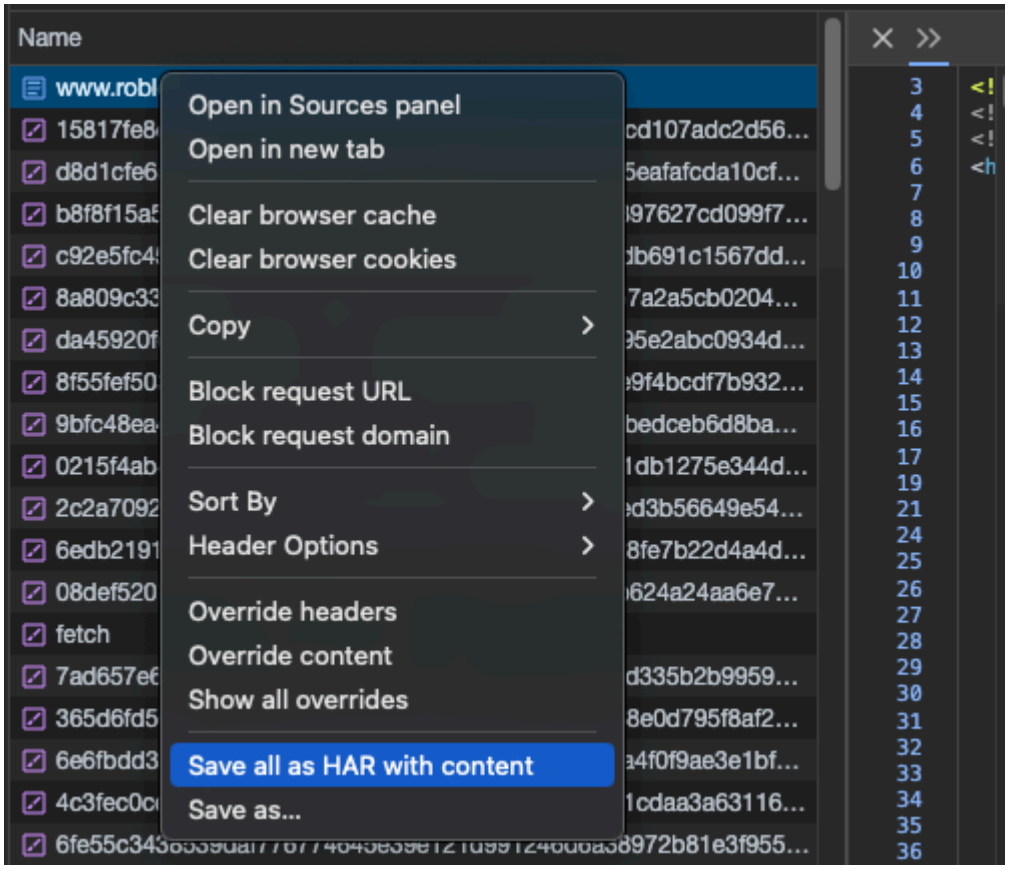
The scammer proposes a trade that is usually too good to be true to the victim. Then, the attacker says that before continuing with the trade, they would like to check if the victim's items have not been stolen. To do this, they say, the victim must visit a special page in Roblox and insert an ID. They then give the victim the URL for a page that is actually part of the Roblox domain and contains the following form, among other things.



This page is part of the Roblox API documentation and is used by developers to test the API. While talking with the victim, the scammer creates a trade request that, if accepted, would transfer all the victim's items to the scammer. The scammer then sends this ID to the victim and instructs him to insert the ID in the form and click "Try it out." This will cause the user to accept a trade with the specified ID and transfer all their items and Robux to the scammer.

HAR file method

The scammer offers to create a free GFX (a 3-D, realistic version of the victim's avatar) under the pretext that they are learning to do this and could use the practice. If the victim accepts, the scammer says they need a file to complete the development and gives the victim a tutorial or video explaining how to obtain the file. The tutorial requests that the victim open their browser developer tools and save the network request as a HAR file, as shown below.



Once saved, the victim is instructed to send it to the scammer. This file contains the session ID of the victim, which allows the scammer to use the platform logged into the victim's account and steal all items and Robux.

Double trade

The scammer approaches the victim proposing two trades. One trade is good for the scammer and one is good for the victim. The victim comes out with a clear advantage from this trade. The scammer puts the condition that the victim either accepts both trades or rejects both trades. However, while they chat, the scammer removes some Robux from their account, making the trade that favors the victim fail for lack of Robux in the attacker's account. When the victim accepts both trades, only the bad trade goes through, making it a bad deal for the victim.

Malware installation

This method is as simple as requesting the victim to install some software or a browser extension as a way to receive free Robux or to help the scammer perform some development that is of interest to the victim. The installed software is malware, designed to steal the victim's session ID, which allows the scammer to use the platform logged in to the victim's account and steal all items and Robux.

5 ways to avoid being scammed

Knowing the common scams is an important step in using the platform safely. The following recommendations help players not fall into scams:

- **If it seems too good to be true, it is:** This is probably the most important recommendation. If a stranger or a website is claiming to offer free currency or free items, it is almost certainly a scam.
- **Don't open links or download files sent by unknown sources:** These links can be phishing or malware delivery lures. If you don't know the other player, it's generally a good idea to not open the link.
- **Be suspicious of requests to perform unusual actions**: Some scams rely on the user performing more or less technical actions. These are a good indicator that it may be a scam. For example:
    - Copy-pasting into the browser address bar.
    - Creating and clicking in bookmarks.
    - Opening browser developer tools.
- **Be suspicious of unusual trades**: When trading some attention to some red flags, such as:
    - Trades that are conducted outside the platform.
    - Trades where the trader creates unusual rules such as double trades.
    - Requests to perform actions on the web browser during a trade negotiation, such as using the API form.
- **Use the platform's built-in security features**: Roblox takes security seriously and provides security guides and several features to increase security. For example:
    - Enable multi-factor authentication.
    - Configure account privacy.
    - Configure who, if anyone, can trade with the player.
    - Configure the trade quality filter to help avoid suspicious trades.
    - Enable a mandatory PIN to change settings.
    - Exploring and using these can help better protect minors. The following links contain additional information and guidance:

https://corporate.roblox.com/parents/

https://en.help.roblox.com/hc/en-us/articles/203313380-Keep-Your-Account-Safe

---