# Securing an OpenSimulator DreamGrid to Prevent Attacks

By Marianna Monentes.

Griefer attacks can be a major issue in virtual environments by causing harm and disruption to users and their creations. There are several steps that can be taken to mitigate these attacks and ensure a safe and secure virtual experience in OpenSimulator and DreamGrid.

* **Verify Your Members:**  Check your Members list regularly to see who your new members are.  The known griefers can easily be disabled so that they cannot gain access to your grid as a new member.
* **Limit Group Access:**  Griefers often join groups with loose membership requirements to gain access to your grid and its resources. To prevent this, make sure that your grid has strict membership requirements for all groups, and consider disabling or limiting the permissions of any groups that are not essential to the operation of your grid.
* **Restrict Building and Scripting for Guests** : Guests are often griefers, so it's important to limit their access to building and scripting functions. Consider disabling building and scripting for guests entirely. Limit their permissions so that they can only use these functions in designated areas. This can help prevent griefers from using these tools to cause harm to other users or their creations.

**Implement Anti-Grief Tools**: There are various ways to implement anti-grief tools available for OpenSim grids. Anti-grief tools mitigate the risk of attacks.  Using your Firestorm or Singularity Viewer.

Region Monitoring such as:

* **Access Lists:** Add the avatars who you would like to enter your Sim on a Whitelist or Banned on a Blacklist
* **Object Permissions:** Set to no copy, no modify.
* **Limit The Ability to Move Objects:** Make sure "Anyone can Move" is off on your Objects.
* **Object Locking:**   Object Locking is an anti-grief tool in OpenSim that allows estate managers to restrict modifications or movements of specific objects in virtual regions. Research your viewer to see what Anti-grief tools it has. When an object is locked, users are prevented from making changes to its properties, such as size, color, and position.
* **Estate Ban System:** If you wish to prevent people from accessing the region/estate, they may be added here.
* **Object Auto return:** Allows a timed return of objects other than owner or group owned. If set to 0 the timer is off, otherwise will return items after a set number of minutes.  Before setting this please make sure all items on your land are set to the same group the land is deeded to.  Then when anything is left on land not belonging to you or group it will delete after the time indicated.
* For example, auto-return can be used to automatically return items that are left in inappropriate locations.
* **Monitor User Activity** : Regular monitoring of user activity can help detect and prevent grief attacks before they cause significant harm. Consider using tools like log files and network monitoring tools to track user activity, and take action if you see any suspicious behavior.
* **Bans** may be set for Grids, IP addresses, Viewers, and MAC addresses, and In V 3.53 and greater, for Disk ID's. MAC addresses are a serial   number found in Ethernet cards. These bans shut off incoming traffic by using Robust  capabilities, and by adding entries to the Windows Firewall. They are not a total solution but can work in many cases. This may not be effective as the login name can be changed, the Viewer Name can be tweaked, they may have another PC with a different MAC or they may have changes it, and the IP may change by the ISP or come from a VPN. You can get the Login Name and Grid http://name:port, IP address, and MAC address of people from the Robust log as it happens. You can also look in the menu system at Help ->View Logs->Robust to view the log with Baretail.exe or Notepad.

**DreamGrid has many tools to help with griefers:**

The Regions List has a column that shows you Parcel Permissions.  It shows if the script, rez or land editing are enabled. These permissions should be off.

The Setup->Settings->Region form has a button named "Make Regions No Rez".  This will set the database so visitors cannot rez objects or run scripts.  You must reboot the region for this to go into effect.

DreamGrid has special features that prevent loading OARS with these permissions set.  After loading an OAR, the safe permissions take effect on next boot.

New regions will have Rez and Scripts off by default.

**Tips:**  If you are griefed with many items strewn about ---->Please do not delete everything named "Object'!

You can get the UUID of any griefer from the prim Information. Then you can delete all Griefer prims from the console using these commands:

* delete object owner <UUID> - Delete a scene object by owner
* delete object creator <UUID> - Delete a scene object by creator
* delete object name  <name> - Delete a scene object by name.
* delete object name [--regex] <name> - Delete a scene object by name.  A regex is a regular expression. Example:  you have seagulls named ‘seagull1, seagull2, etc.’. I would use –regex /seagull\d/  to delete any with a digit. Or /seagull.\*/ to do any seagull with extra text.  This last one will also delete seagull\_by\_ferd, so it’s best to be very careful here!

If you are griefed and you have a lot of regions, you can add any of the above commands into Opensim\bin\startup\_commands.txt. Then restart the grid and all those bits will go poof.

**Keep software updated**: Regularly updating the software and plugins used on your OpenSim grid can help prevent security vulnerabilities from being exploited by malicious actors.

In conclusion, taking these steps can help secure your OpenSimulator grid and prevent griefer attacks. By verifying user identity, limiting group access, restricting building and scripting for guests, implementing anti-grief tools, and monitoring user activity, you can create a safe and secure virtual environment for your users.