

Managing Leech Protect in cPanel

Leeching occurs when users publicly post their username and password to a restricted area of your site, allowing other visitors to use the login information. cPanel can be configured to handle leeching, redirecting and potentially suspending the user. The protection function works by setting the maximum number of logins that can occur within a 2-hour time limit. If the login limit is exceeded, the user is presumed to be allowing other visitors to use his or her login information.

Enable Leech Protection

To protect your website from leeching:

1. Click the name of the directory you want to protect.
 - To navigate directories, use the folder icon located next to the name of the directory.
2. Enter the maximum number of logins you want to allow each user within a 2-hour period.
 - To redirect users exceeding the maximum number of logins, enter a URL to redirect them to.
 - If an email alert should be sent to your email address, click the *Send Email Alert to* checkbox and enter the email address.
3. To disable an account that exceeds the maximum number of logins in 2 hours, click the *Disable Compromised Accounts* checkbox.
4. Click *Enable*.

This page also provides a *Manage Users* button. Clicking this button takes you to the Password Protect Directories screen, where users can be added, edited, and deleted.

Disable Leech Protection

To disable leech protection, click *Disable* under the *Disable Protection* heading.