Spam

Overview

Things to look for:

- Unprofessional profile pictures
- Non-Hub related information in the Bio
- Unprofessional URLs/links to outside websites
- Inappropriate language
- Selling ads or promotional information
- Non-Hub related content
- Components on the Hub with links in the text box

Disable Accounts for Spam

1. Find the account that created the Spam, and then on the backend of the Hub navigate to **Users** and then click on **Members**. Click on the name to open up account details
   a. **Note:** You can usually be sure that the account is a spammer if they have a Hub nonrelated website link in the URL and an unprofessional profile picture.
2. If the **Public Profile** box is checked, uncheck it. It is important to make the profile not available to the public incase they have Spam links in their account
3. Uncheck the **Confirmed** box if the user had confirmed their account. If it is not checked leave it unchecked
4. Change the **Contact me** drop-down to the **Receive email updates?** option
5. Change the spam account password by typing into the **New Password** field a long and random password that the spammer could not figure out
6. Check the box beside the user's name and then click **Block** to block the user from the Hub
7. Click **save and close**
8. After disabling the spammer's account, find the spam that the individual has put on the Hub and delete it
9. Make sure that they account has been deactivated prior to deleting the Spam. This way the spammers will not receive emails about their content being deleted

Antispam Plugins

To keep your Hub from being abused by spammers, enable these antispam plugins to give your site the fighting edge.

How It Works

For most content on the site, when a user presses **save** to submit a new entry—be it a blog post, forum comment, wish, etc.— a **before save** event is triggered. That event allows the system to validate and run any desired pre-processing or checks on the content before it is stored within the database. When any anti-spam plugins are enabled, the content is handed off to each plugin, in their defined order (see the **Plugins Manager**), where the plugin in turn has a chance to evaluate the content for likelihood of being spam. If a plugin flags the content as being spam, the process stops (i.e., the content is not passed along to the next plugin), an error is raised, and the content fails to be stored to the database.

Enabling

To enable these plugins, follow these steps:

1. Navigate to the backend of the Hub and locate the **Extensions** tab
2. Click on **Plug-in Manager** from the drop-down
3. Inside of the **Plug-in Manager**, locate a plugin through search and click on the title
4. Inside the plugin, change the status to **Enabled** and provide any API keys or change the settings then click **Save & Close**

Available Antispam Plugins:

- **Antispam-Akismet**: This plugin uses the remote Akismet service to scan posted content and determine if the content has a high probability of being spam. Akismet digests massive amounts of data from hundreds of sites a day to learn about how to protect sites from spammers. Learn more at: http://akismet.com.

  Usage of this plugin requires API credentials provided by having an Akismet account.

- **Antispam-Baba Ji Spam Detector**: This plugin provides content spam section of the mass spammer Baba Ji.

- **Antispam-Bayesian Filter**: This is a spam detector that employs a basic Bayesian filter which looks for spam headers and character strings.

- **Antispam-Black List**: This is a spam detector that detects black-listed words; inside the plugin words can be added to a list to build the black list inventory.

- **Antispam-Link Rife**: This is a spam detector that detects link frequency in a body of text. This spam detector has three configuration options for determining if submitted content is likely spam:
  1. **Link Frequency** - Maximum number of links allowed in a text before it is considered spam.
  2. **Link to Text Ratio** - Ratio (In Percentage) of the number of links to the number of words in the string. If the percentage ratio is greater than the specified ratio, it is considered a **Link Overflow**.
  3. **Link validation** - Check found links against known blacklists.

- **Antispam-Mollom**: This plugin uses the remote Mollom service to scan posted content and protect a Hub from users who post abusive content like profanity and will learn as it grows. Learn more at: https://www.mollom.com.

  Usage of this plugin requires API credentials provided by having a Mollom account.

- **Antispam-SpamAssassin**: This plugin scans posted content with SpamAssassin to determine if the content has a high probability of being spam. SpamAssassin is an Open Source antispam platform which allows administrators to filter and classify bulk spam. Learn more at: http://spamassassin.apache.org.

Testing Content

Sample content may be tested against enabled plugins to further examine which plugin may have flagged content as potential spam and why. The testing interface may be found by:

1. Navigate to the **/administrator** interface of the Hub and locate the **Components** tab
2. Click on **Support** from the drop-down
3. Inside of the **Support Manager**, locate the sub-menu item for **Abuse**
4. Inside of the **Support Manager > Abuse** panel, locate the sub-sub-menu item for **Spam Check**

A form with a single text box will be present. Paste content into the box and click the

Check button in the toolbar. The interface should update to display a list of all anti-spam plugins the content was passed through and the results of said plugins.

Not a spammer but a normal user what was flagged as one?

Sometimes when a user repeats actions on a Hub in a rapid function or tries to submit a flagged item multiple times, they end up in Spam jail. In order to reset the Spam jail count and free them, follow these steps:

1. Navigate to the **/administrator** interface of the Hub and locate the **Users** tab
2. Click on **Members** from the drop-down
3. Locate the user and click on their name
4. Locate the **Lifetime Spam Incidents** and click **Reset**
5. Click **Save & Close** and notify the user that they are out of Spam jail

If this user is a habitual offender and you are tired of bailing them out of Spam Jail or you would like to whitelist the Administrator user group, you can Whitelist a user group or a specific user by completing these steps:

1. Navigate to the **/administrator** interface of the Hub and locate the **Extensions** tab
2. Click on **Plug-in Manager** from the drop-down
3. Inside of the **Plug-in Manager**, locate the **Content - Antispam** plugin and click on the plugin's title
4. Click on the **Whitelist** section and change the access group or add the user's username to the list in order to Whitelist all users in that access group or that specific user
5. Click **Save & Close**