Set Spam filter preferences and manage spams

Set Spam filter preferences

On this page

You can login to the user control panel inside WebMail. On the top right, click on **Control panel** link followed by the **Access Control Panel** button. You will be logged in automatically to your user control panel, just be sure your browser doesn't block any pop ups and permit them if that happens. For Enhanced accounts, there is a **Control Panel** link inside WebMail, also on the top right.

You can also access the user control panel directly:

- Go to

  Unknown macro: {link-window}

  https://cp.emailarray.com
- Log in using your full e-mail address (user@domain.com) and current password.

Notice you can also set spam filter preferences on the domain level, to define settings for users that don't have custom preferences saved, however, our goal in this FAQ is to detail the user level preferences and management.

After logging in and click on **Filtering**, on the top bar, the options are:

Accept e-mail from:

- **Everyone, Whitelist & Address book:** This is the default option and lets all messages reach you. Further down, we mention the option that controls if you want to send spams to your spam box, but it depends on this option being set.
- **Whitelist & Address book:** This option only allows messages present in the Whitelist & Address book to reach the Inbox, the rest will be sent to your spam folder.

> System default is to accept emails from everyone, but the option to accept only from whitelisted senders and contacts in your address book is a nice alternate way of receiving practically no spams in your inbox, at the cost of having to check your spam folder or spam reports, from time to time.

Blacklisted Messages: What to do with messages whose senders are in user's or domain's blacklist. The default is to delete them, but you can have them moved to your spam folder.

Enable autowhitelist: All e-mails sent by this e-mail account have the recipient's address of each e-mail added to the domain's auto-whitelist. Can be dangerous if a user account is compromised, sends spams and automatically all recipients of such spams are added to the domain level auto-whitelist (accessible in Filtering > Auto-Whitelist, in the admin panel), which would require cleaning up the auto-whitelist. This option is enabled by default.

Send spam to: this controls what happens to messages which are identified as Spam.

- **Spam folder:** Places the Spam messages in the Spam folder
- **Deliver to Inbox:** Delivers the Spam messages to the Inbox, basically same as disabling anti-spam for this user
- **Delete:** Deletes the Spam messages

Filter sensitivity: The filtering system can be adjusted on a scale from 1 to 10, with 10 being the most restrictive while 1 is the most permissive. We find that the default setting of Regular Sensitivity is just right for most users.

Keep Spam for: How many days to keep the Spam messages in your Spam folder.

Send Spam E-mail Report every: This defines how often you wish to receive in your Inbox the summary of Spam messages trapped over the past few hours (default is every 12 hours), or if you want it disabled. Using the report received via e-mail, you can easily click on the item in the Via column, which opens up the user panel and lets you deliver & whitelist an email/sender, just deliver the email (deliver only) or delete it. In the From column, click on the sender to preview the e-mail in the browser.

Spam E-mail Report Format: Lets you choose the format of the Spam Report message. Default is HTML and TEXT.

Detect Forged From: Creates a rule for user which checks if SMTP authentication has not occurred when the sender's e-mail address of a received e-mail is the same as the recipient account's address. Such messages are moved to user's spam folder. Click here for our wiki page about this topic.

After making any changes, click on the **Update Settings** button.

Managing spams

Note that e-mail accounts have a folder entitled "Spam", where messages detected by the system as spam are moved to. Such folder can be viewed via WebMail or using an email client with your account setup as IMAP, which may require right clicking the account root in your email program and subscribing to the Spam folder. If you use POP (not recommended), you should use the spam reports (described below), to release messages incorrectly detected as being spam (false positives) and you can also log o WebMail and view the Spam Folder, moving any false positive to your inbox.

Spam reports lead you to the user's control panel Spam quarantine and it is the best way to release false positives, as you can automatically deliver the email and at the same time, add the sender to your whitelist.

If you want to help us with undetected spam emails or emails incorrectly identified as spam, please contact our support. Consider also creating an account at SpamCop in order to use the system they provide to report spam.

Spam reports and Spam Quarantine

The system sends an email to your inbox, by default every 12 hours, detailing the emails caught in your spam folder, so you don't have to constantly check your spam box. The feature is extremely useful for those who use POP accounts with an e-mail client, since in that case, you cannot view the spam folder, except via WebMail.

Spam reports are sent from the sender "Spam Monitor" and let you click on the **Via** column of each e-mail listed, which opens your account's control panel. Login with your email address and password and you will be directed to the **Spam Quarantine** section. Click on the **Display** button to view the list of spams in your spam folder, being able to change the visualization criteria, such as view by **Date** (All or a specific date) or **filter by** text in the From, Subject or Unique ID fields.

Click on the **From** or **Subject** column on any of the listed e-mails to preview their content.

When you view the list of spams in your Spam quarantine/box, notice there's a checkbox next to each e-mail, which lets you select several e-mails at once and take some action, such as "**Deliver & Whitelist**", which delivers a message incorrectly detected as spam to your inbox and allocates the sender on your whitelist. Other options include "**Blacklist & Delete**", which can be useful to minimize the amount of spams received, as you can first deliver & whitelist the legit e-mails and then, possibly blacklist & delete from spam folder all the rest. Just be careful as, if there's some spam with a forged FROM address, you might end up blocking a legit sender. To check each senders FROM address, roll over the From field of each e-mail listed.

Other options include "**Delivery only"**, which only delivers a spam to your inbox but does not whitelist the sender, useful if you're unsure if the email is legit or not and just want to deliver the e-mail to your inbox and **"Delete"**, to simply delete the selected e-mails(s), which is the same as deleting them directly from your spam folder.

Remember you can always view all your blacklist and whitelist entries, as well as add new entries manually, as per our respective FAQ.

Tips

The Anti-Spam tips below are also very important to have better results.

- If you receive too much spam in your account, consider creating a new email address and preserve it. Use an alternate email address created on a free email service such as Hotmail, to be used when filling out forms in web sites, especially those that can expose your data, such as your domain's registries Whois.

Consider having an alternate address to promote socially, and maintain your own address domain restricted for work.

- When you create a new e-mail account, avoid common words before the @ sign, as John. Prefer to use, for example, johndoe@yourdomain.com.

- Use forms on your site, without publishing your email address explicitly. Forms allow you to be contacted without having to display your e-mail address, since spammers often track web pages looking for email addresses.

- If you want to publish your email address on web page, consider encoding it.

- Never reply to spam e-mails, since it is often a confirmation of the existence of your e-mail, as well as a trigger for auto-whitelisting, which adds all addresses to whom you send e-mail in your domain's auto-whitelist, feature which can be disabled in the Filtering section of your control panel.

- One interesting idea is to create aliases for your account and use them when informing your e-mail addresses in certain places, where you believe it could be exposed and spammed to. This way you can easily remove such alias, to stop receiving such emails. Another option is to create disposable addresses, such as a Dynamic (wildcard) extension.