Occasionally you may notice that you are no longer receiving emails from familiar senders. Here are some common answers to the question:

Why am I no longer getting ACSW emails?

The Alberta College of Social Workers sends email to your primary email address on file.

We would like to suggest that you add the following email addresses to your contact list to avoid missing important emails that may concern your registration:

- **registration@acsw.ab.ca** – All emails will pertain to your registration and continued renewals
- **acsw@acsw.ab.ca** – auto emails from the database when renewing or updating your member profile, paying invoices, status changes, etc.
- **acsw.mail@acsw.ab.ca** – Newsletters, Advocate and area specific emails. You can login to your member profile and update the communications section and choose the options for how you would like to receive these communications. You do have the option to opt out of these types of emails only.

To opt out:

- Go to your member portal
- Under the Action Menu
- Click on View/Edit My Profile
- Click on Edit and scroll down to Communication Preferences and choose the options for each type. (If you do not choose a preference, you automatically receive the emails.)

Some Emails are marked as SPAM

Good email service providers have sophisticated SPAM filters that detect which emails are legitimate and which are not. However, they are not always 100% reliable and sometimes legitimate emails can get caught in the net. To avoid this, you should check if any emails from people you know are getting moved to your SPAM folder and, if so, mark them as safe.

The emails contain an attachment or a link

Emails that contain attachments or links can sometimes be blocked too. Although common file types such as Word docs, PDFs and Excel spreadsheets usually get through; even they can sometimes cause problems. When Word/Excel documents contain macros, they are blocked but this is for good reason as there is a very real danger of malware being smuggled in through the macros. In the case of large attachments, it is highly recommended that you use a secure file transfer application rather than zipping them. This is because ZIP files can be used to deliver and unpack malware such as CryptoLocker and CryptoWall. This can also be true of hyperlinks. Please note, links contained in official ACSW correspondence have been reviewed prior to sending to ensure their safety.

Email settings

You should check that you don't have any rules set up in your email program (such as Outlook) that might be moving or blocking the email or quarantining it. Check your Junk and Clutter folders to see if certain emails are being moved there. If they are, it will often be because they contain SPAM words or attachments that the program doesn't trust or because Clutter is attempting to 'de-clutter' your inbox by 'learning' what you do and don't want. You can even ask the sender to send just a blank email to check if it arrives successfully.

If you are missing an email from a particular sender, there is a chance their message was marked as spam.

All incoming emails are filtered for spam using state of the art anti-spam technologies. Keep in mind that it is possible for legitimate messages to trigger spam filtering, and it is possible for legitimate companies to be publicly blacklisted. There is a chance that DNS or server settings on the recipients' end may be causing delivery issues. In short, a number of factors determine whether a message is delivered to your Inbox, your Junk E-mail folder, or blocked by your server as spam. Here are a few guidelines to remember:

- If an email has enough characteristics of spam, it will be moved into the Junk E-mail folder.
- If an email has strong characteristics of spam, it will be deleted at the server level before ever reaching your inbox.
- If the sender is blacklisted by a public blacklist, it will be blocked by our server. There are several ways to get blacklisted: virus infected or hacked PCs sending out spam, an email / web hosting company that allows spammers to send spam from their network, or a network / IP address that has been compromised by spammers.
- If the sender's DNS records are not set up properly, they may be inadvertently violating their own security protocols, resulting in delivery rejection/failure.
- Misconfigured mail servers are also blocked by our server. Most misconfigured email servers do not have reverse DNS, or they are trying to spoof (forge) a domain name.

Blocking legitimate mail

Legitimate email can get blocked in error for a couple of reasons:

- The receiving system thinks your email looks too much like spam.
- The receiving system thinks you have a reputation for sending spam.

Spam typically doesn't bounce

Because bouncing email flagged as spam would give the real spammers too much information about how to bypass the spam filters, it is simply not done. Email flagged as spam is simply not delivered, or is delivered to the recipient's spam folder, where they may or may not find it.

A quick test to make sure that any email can get through is to use another provider — for example, a friend's email account on a different service, or a free account on another service.

What to do about a missing message

Step 1: If you are not getting emails from specific people, the first step is to check your Junk E-mail folder. Often, such emails will end up in this folder. If you do not see the message in any of your folders, their message may have been blocked for strong characteristics of spam.

Step 2: To prevent emails from a particular sender from being moved to the Junk E-mail folder or being blocked in the future, you will need to add the sender's email addresses to your Trusted Senders list. Have senders resend email message after making this change.

Step 3: If you added an email address to the Trusted Senders list and are still not receiving any emails from that specific sender, then they are most likely on a public blacklist, their email server may be misconfigured, and/or they are being blocked on a server level.

Adjusting spam settings in Shaw email

Through Shaw Webmail you can adjust your spam settings to allow you to discard messages immediately so that they will not appear in your inbox or in your trash folder.
To adjust your spam settings in Webmail:

- Go to https://webmail.shaw.ca
- Log in using your email address and password.
- Click Preferences and select Spam.
- Select a spam mail option:
    - Label message as not spam and keep in Inbox
    - Discard message immediately (will not appear in trash)
    - Label message as spam and send to Junk
- Click Save at the top left of the page

More information: Shaw Webmail: Email filters and spam settings If you logon via Shaw WebMail, while the E-mail program on your computer is inactive, you should see 100% of your "incoming" E-mails -- before your E-mail program can view/block/discard any messages.

Looking like spam

Spam filters look at the email and assign points for various behaviours associated with email that "looks like" spam. As soon as an account collects too many points (where "too many" is arbitrary, and up to the receiving system or the individual recipient to define), the email is flagged as spam. Some things to watch for in your email include:

- Sexually explicit terms or phrases.

- Certain drugs (typically linked to sexual performance or characteristics)
- SHOUTING. Spam filters often consider shouting (typing in all caps) as sales copy.

- Fake, inconsistent, or illegal return addresses; or, a “reply-to” address that does not match the “from” address. (If you don’t know how to even make that happen, don’t worry about it.)
- HTML email. It is not a huge mark against it, but some spam filters still consider HTML or “rich text” email as having a higher likelihood of being spam when compared to plain text email.
- Marketing terms. Because so much spam is an attempt to get you to buy something, many filters look for various words and phrases associated with sales and marketing efforts.

It is important to realize that no one is saying that any of those things in the email are bad, or that any one of those things will cause the email to be blocked. The unfortunate reality of the situation is that the more an email looks like spam, however innocuous, the more likely it is to be treated as spam.