

# Content Risk Services

The advanced email builder has built-in functionality to help you avoid triggering spam filters. Certain keywords can trigger these filters, which send your email straight to your contact's junk folder, where it sits unread. You can check your emails for these keywords by clicking the "Spam" icon in the email builder. These keywords will also be flagged when you click "Review and send" before sending your email.

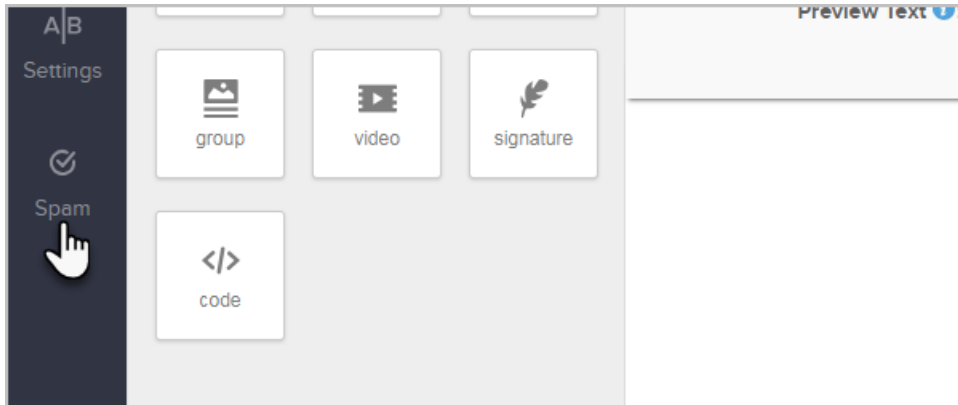
In most cases the Spam Filters will warn and simply advise that certain content be edited to have a better chance of hitting the contact's inbox (rather than junk). In some cases the system will not allow you to send until these issues are resolved. This should be seen as advice rather than punitive as we reflect (through 3rd Party Industry tools and knowledge) how the receiving Email Provider will analyze this content.

**Please Note:** This is currently only available when sending an email broadcast

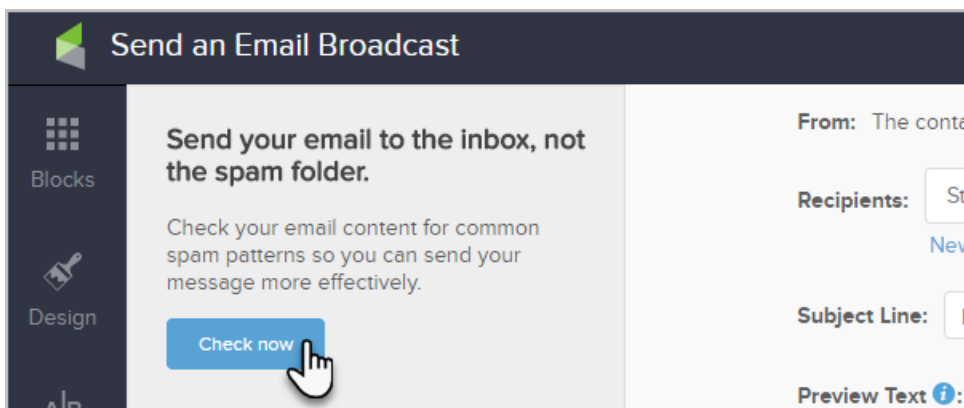
In order to ensure high deliverability, Infusionsoft will restrict sending an email if the content is too risky. You will have to remove the offending content prior to sending.

## Using the Spam Filter

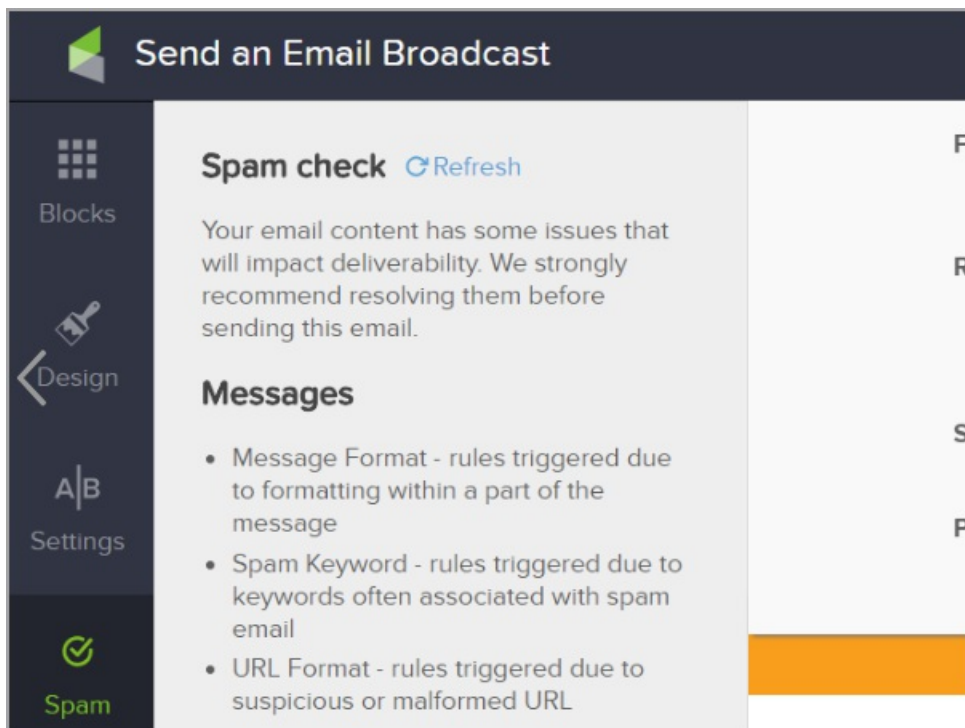
1. To manually check the contents of an email click the **Spam** button.



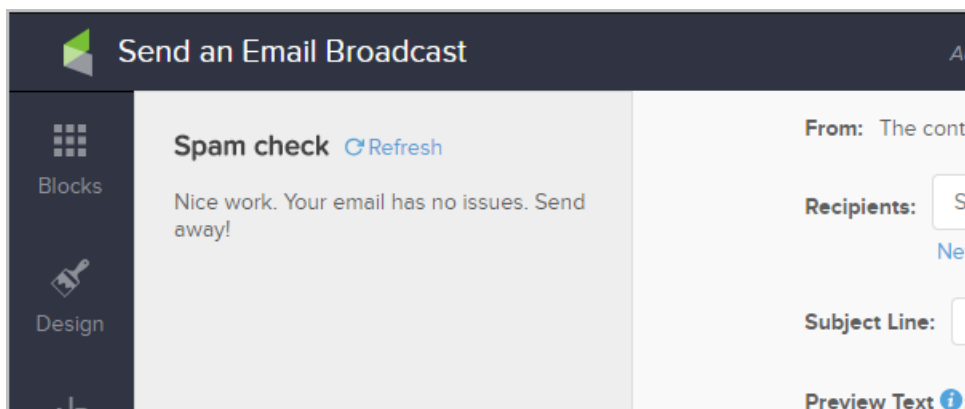
2. Click **Check now**



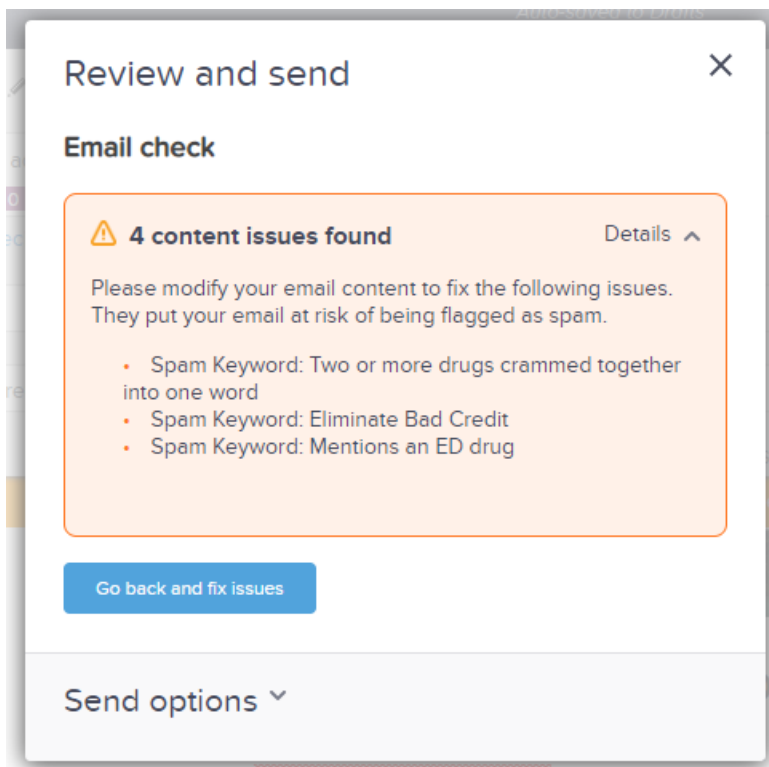
3. You will see an alert message detailing the issues to resolve prior to sending the email



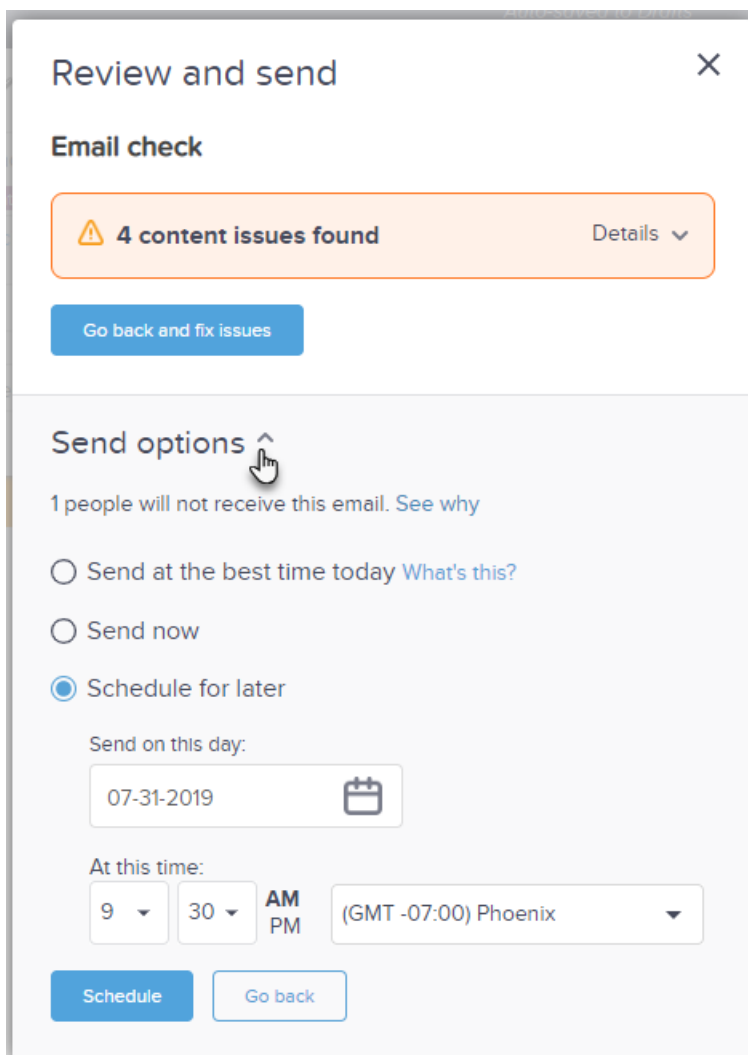
4. You will also be notified if there are no issues found



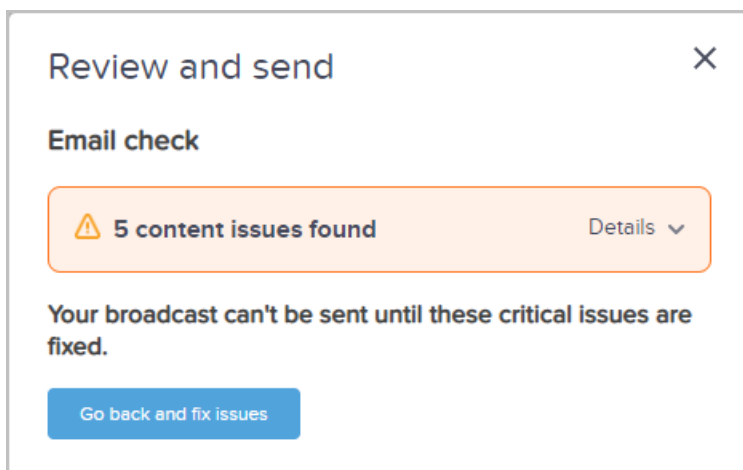
5. When you click **Review and Send**, you will automatically be presented with a window that will check your email prior to sending.



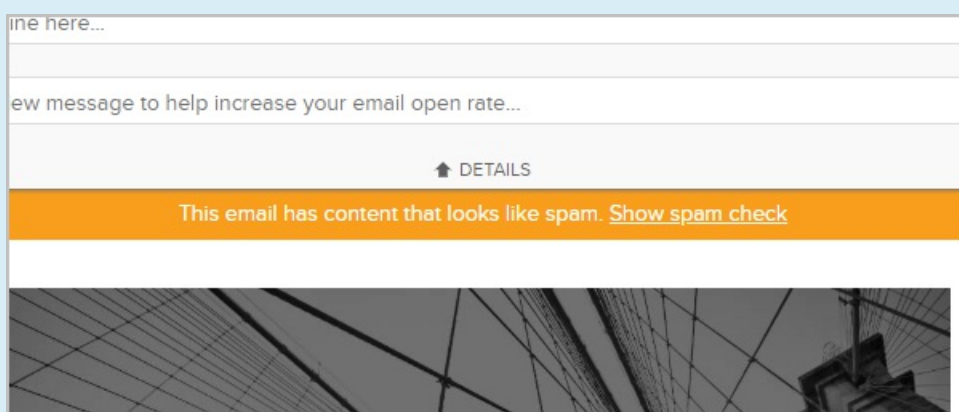
6. Click the **Send options** link if you are ready to send the email.



7. Your email may be blocked from being sent if it has a high risk of being flagged as spam. You will need to return to your email and fix the issues before the email can be sent.



**Note:** If you are working in an email that has been flagged for Spam content, you will see an orange banner at the top of the email. Clicking the **Show spam check** link simply brings you back to the **Spam** check section of the Email Builder



## Most Common Triggered Messages

Analysis of real world usage of the Spam Filter shows these messages are triggered the most often. Here is a further description and reasoning why these may have been triggered and the effects of keeping them in your email template:

**Note:** In very rare edge cases where auto generated links (for example Social Media links) contain a series of characters that, when analyzed by the Spam filter, fires a warning. If this occurs you should still be able to send the email but the Spam filters at the receiving Email Provider may still flag this as Spam. In this rare

case we recommend linking to a different social media page or edit the page so the link is re-generated.

**1. Ratio of whitespace to non whitespace is too large:**

Having a lot of line breaks (and other whitespace) alerts the ESPs that critical information, for example the unsubscribe link, may be attempted to be hidden way down the email (with a lot of space between the end of the content and the Unsubscribe link). Also, ESP's are moving towards promoting shorter emails that fit on a mobile device so keeping the content concise will help inboxing.

**2. Huge... sums of money:**

Most of us have been fortunate enough to be selected by the Nigerian Prince who has too much money and needs your help spending it and requires your bank account details ;-). ESP's obviously protect their customers from phishing attacks such as this and editing large monetary values is recommended if this warning is triggered.

This rule has been known to fire a false positive when phone numbers are used with a specific suffix, for example; [+12345678](#) US or [+1 234 5678](#) US. To avoid this either leave off the 'US' or use 'USA'. We are currently investigating a workaround to this issue.

**3. Message Format: X% of a lot of money for you:**

Similar to the above. Offering free money seems too good to be true and ESPs have found that it actually is. We've seen this triggered in Real Estate emails such as: "House prices increased an average of 8% last year and the average house price increased to \$750,679." Keap will still allow you to send this email but in this case if our system is flagging this then the ESP's will as this is from a 3rd Party System that is widely used. In cases like this it's better to have the contact confirmed (double-opt in) and have good engagement (opening emails <15 days).

**4. Message Format: Subject is in all capital letters:**

Analysis shows that 30% less people open emails where the subject line is all capitals. Historically most emails that do this are considered Spam and the ESP's will likely junk this email. A critical email with a subject of "URGENT: READ NOW" will be less likely to make it to someone's Inbox compared to an email with a less 'urgent' subject line.

**5. HTML Format: Message contains one or more shortened URLs:**

The potential issue occurs when both a spammer and you use the same link shortener in your emails. If one or more ESPs start blocking emails that include the link shortening domain (to block the spammer), they may block your emails as well. This is a warning and you can still send.

**6. Porn detected:**

Our AUP states that porn is not to be sent. That said this warning will be triggered on 'xxx'. Again, this is advice that ESP's may also pick up on this and wrongly infer that porn is included in the content.

**7. Trading options or Crypto detected:**

These types of email are against our AUP and should not be sent. Analysis shows that content including 'Bitcoin' have a large number of complaints and are regarded by the ESP's as Spam. Removing references to

Crypto currencies will give the email a better chance of inboxing. Including Trading Options, will cause a Compliance Issue and you may be blocked from sending.

**8. Domain/IP Reputation - 1 or more links in content has reputation issues:**

This is a message surfaced from one of the 3rd Party systems we integrate with to assist in providing content advice. We cannot specify which link in the email points to a site with a reputation issue. It is advisable to remove the links and add them back one at a time to identify the problem link. You can then decide to remove or change the link flagged.

**9. COVID content will likely go to Junk folder:**

Unfortunately nefarious individuals are attempting to launch phishing attacks on individuals concerned with COVID. ESP's have seen a large number of fraudulent emails and are scrutinizing email using this content and, in our analysis, sending most marketing email using this keyword to junk.

---