# Overview

This is an email overview that we wrote to help you uncover problems when one of your customers reports that he does not receive your Pure Harvest emails.

Email is an electronic file that is transferred through a network of computers to reach a specific person. It requires a sender, a sending server, a receiving server and a recipient.

A lot of work has been done to stop Spam, but that can sometimes capture innocent emails. A sender can properly send an email, yet the recipient never sees it.

# Identifying Spam

The battle to stop spam starts at the receiving server. The server may examine an email and reject it by bouncing it back, or by just throwing it away. In either case, there is a single line entry in the servers email log that shows what was done with the email. This log is held on the receiving server, and the recipient **cannot see it**. Only the techies at the ISP can see this log.

If the receiving server allows the email to go through, then the end user can see it. If the receiving server tags it as SPAM, then the end user may never see or open it. If the receiving server tags it as SPAM, the end user can usually remove the SPAM tag by adding the sender to a "white list" of emailers that the recipient wants to receive. If the end user sees it, usually they can tag it as spam themselves so as not to see it again.

The receiving server has many tools that can be used to identify SPAM. The server can look for hints in the emails "headers". For example, SPAM email usually has a "From" address that does not match the Senders address. This is because the sender wants you to think it was sent by someone you recognize. This can be valid, like with Pure Harvest emails, or it can be fraudulent, like emails that try to get you to provide your banking information.

If you apply them too strictly, you will throw away useful, even important, emails.

# Checking Spam Folders

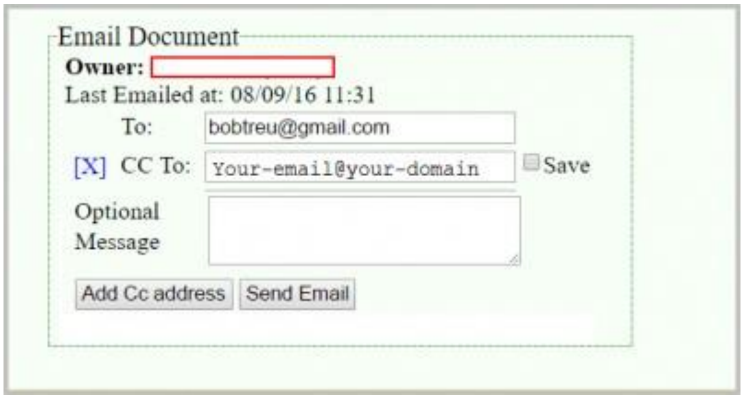
The easiest and most obvious step is to ask your customer to check their spam folder. Their spam folder may be internal to their email client ( like outlook or thunderbird ), or it may be held on the server and reported as a daily Spam Log. Either way, the customer can check these two places and change a setting so the email is not blocked. If that doesn't locate the missing email, it gets more complicated.

# Tracking a missing email

It's not possible to know what the fix is unless we know the cause. In order to know the cause, your customer needs to work with their ISP and their local tech support to know what happened to a specific email.

Every email that goes to a customer is either accepted or rejected by that customers mail server. If is rejected, it is either thrown away or bounced back to the sender. In either case, there will be a single line entry in the servers email log that shows what was done with the email. This log is held on the receiving server.

You can create a test case by going to the Reports screen and manually sending a report. Send a copy to your customer and to yourself. If you get the copy and your customer doesn't you know it is on their end. You also have identifying information you can send to the customer's ISP so they can track it down.



Email Document

**Owner:**

Last Emailed at: 08/09/16 11:31

To: bobtreu@gmail.com

[X] CC To: Your-email@your-domain □Save

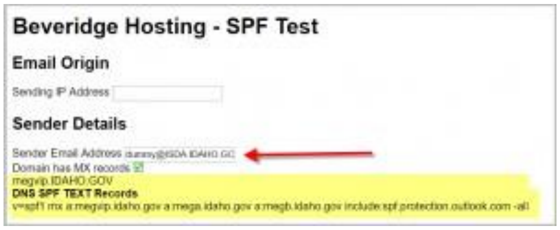
Optional Message

Once you have the line from the customers ISP's email log that shows how the email was handled, then you can track down the fix.

# Debugging Tools

Send an email from your email address ( the one used as “From” when we send lab report emails) to check-auth@verifier.port25.com. Your email will bounce back with lots of information that will help diagnose the problem.

If you're checking an email address that you don't have access to, then fill in the email address at http://tools.bevhost.com/spf/ [http://tools.bevhost.com/spf/]. The SPF record will be looked up when you tab out of the email fiel



**Beveridge Hosting - SPF Test**

**Email Origin**

Sending IP Address

**Sender Details**

Sender Email Address dummy@ISDA.IDAHO.GO

Domain has MX records ☑

megvip.IDAHO.GOV

**DNS SPF TEXT Records**

v=spf1 mx a:megvip.idaho.gov a:mega.idaho.gov a:megb.idaho.gov include:spf.protection.outlook.com -all

d

DNS SPF TEXT Record for Idaho. The “-all” (a minus sign) at the end means to HARD FAIL and BLOCK any email that comes from a server not in the given list.

```
 v=spf1 mx a:megvip.idaho.gov a:mega.idaho.gov a:megb.idaho.gov
include:spf.protection.outlook.com -all
```

If you look up the SPF record for Washington, you won't see anything. As of 8/26/16, they do not use the SPF control protocol.

The forest service, at USDA.gov uses “~all” (a tilde sign) at the end, which indicates a “SOFT FAIL”. The message may be marked as possible spoofing by the end user mail server, but it is not blocked.

```
 v=spf1 include:mailproxy1.usda.gov include:mailproxy2.usda.gov
ip6:2610:20:10bb:bb90::15 ip6:2610:20:1085:e229::22 ip4:96.127.52.98 ~all
```