STOP Those Spammers!

This is a solid approach that seems to work most of the time by reporting Spammers to their ISP and forwarding them to Spam Cop. You will need to sign up for a free Spam Cop account [SpamCop.net – Sign up for Spam Cop reporting](https://www.spamcop.net/anonsignup.shtml) .

Do not bother with the "Unsubscribe" as it will just yield your email address being sold to other Spammers and further increasing the amount of Spam you receive.

This method takes a bit of work, but it is worth it given how much Spam is eliminated from Mailchimp, direct spam, and others.

Configuring Outlook for Spam reporting.

1) If using Outlook, click the down arrow on the Quick Access toolbar, as shown in Figure 1 below circled in Red.



Figure 1

2) Select "More commands".

3) Click the dropdown and select "All commands", “Message Options”, “Add”, then “OK” as shown in Figure 2 below circled in Red.

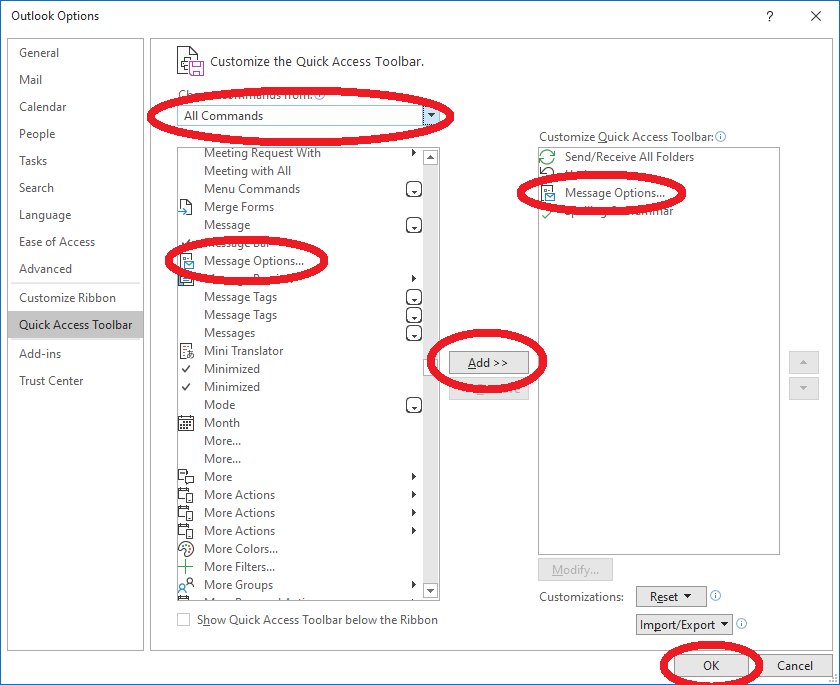


Figure 2

For other Mail Platforms, see the links located on Spam Cop’s website. Spam Cop covers most of the popular mail platforms in use today. [SpamCop.net - SpamCop FAQ: How do I get my email program to reveal the full, unmodified email?](https://www.spamcop.net/fom-serve/cache/19.html)

Reporting Spam

1) Upon receiving a Spam email in Outlook, click the message once (this assumes you have the reading pane off).

This will also work with the reading pane turned on, but the issue I have with the reading pane is it marks the message as “Read”. Depending on what hidden gems the Spammer has embedded in their Spam email, the reading pane could potentially advise the spammer your email address is valid. If your email address is verified as valid, rest assured the Spammers will use this information for additional Spam purposes and mailing list sales/abuse.

2) Select the "Message Options" button you added to your Quick Access Toolbar

3) Copy the entire "Internet headers" section, as shown in Figure 3 below, then close the window. This may look like a bunch of gibberish, and we will get to that in a moment.

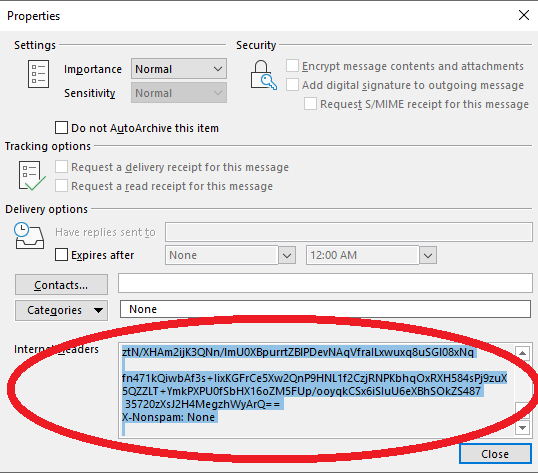


Figure 3

4) Right-click the suspect message and select "Forward".

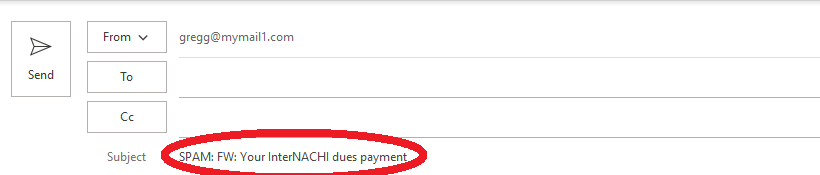
5) Right-click in the body of the message and select "Paste" or "Paste Options" to paste the Internet headers copied above.

Be sure to capture the entire Internet headers, as this is what the ISP expects and will use to verify the Spam came from their network and who the Spammer is.

6) Do not delete or change the subject line except as follows: add in front of the FW “SPAM:” so your subject line now appears as SPAM: FW: (Original Spam Subject)

7) Now, you need to pick through the Internet Headers to find the IP address the spam originated from. You will need to know your email host, and rest assured that this will become easier as you encounter this information over and over.

Usually, after the first few address lines, you will find the sending email systems IP address. The message which is shown below in Example 1 came from InterNACHI (This is a legit email, but all the same), so look for the outgoing, internachi and an IP like this; "Received: from o1.outgoing.internachi.org ([208.117.48.147])"



Received: (qmail 31392 invoked by uid 30297); 17 Dec 2020 05:01:33 -0000

Received: from unknown (HELO p3plibsmtp03-09.prod.phx3.secureserver.net) ([68.178.213.117])

(envelope-sender <bounces+62767-b211-gregg=mymail1.com@em8024.internachi.org>)

by p3plsmtp23-03-25.prod.phx3.secureserver.net (qmail-1.03) with SMTP

for <gregg@mymail1.com>; 17 Dec 2020 05:01:33 -0000

Received: from o1.outgoing.internachi.org ([208.117.48.147])

The above 208.117.48.147 is the spammers public IP address of interest. There may be other private range addresses before this, but this is the address we want. Private IP addresses you want to ignore are anything in the 10.0.x.x to 10.255.x.x, or 172.16.x.x to 172.31.x.x, or 192.168.0.x to 192.168.255.x – see this link: [Private IP Addresses: Everything You Need to Know (lifewire.com)](https://www.lifewire.com/what-is-a-private-ip-address-2625970) - these are just internal server/network IP addresses we don’t or care about.

(using TLSv1.2 with cipher ECDHE-RSA-AES256-GCM-SHA384 256/256 bits)

(Client did not present a certificate)

by CMGW with ESMTP

id plPwkrbG6SJ11plPxkhDzI; Wed, 16 Dec 2020 22:01:33 -0700

X-CMAE-Analysis: v=2.4 cv=N9rsq0xB c=1 sm=1 tr=0 ts=5fdae62d b=1 cx=a\_idp\_d

a=d9ChfnfsboirXitJ5rimZg==:117 a=d9ChfnfsboirXitJ5rimZg==:17

a=kj9zAlcOel0A:10 a=zTNgK-yGK50A:10 a=SSmOFEACAAAA:8 a=QsycGfSOAAAA:8

a=NzK0Cp3dAAAA:8 a=7jQJFEJsc2JFoVO\_OAoA:9 a=AUPQ-5AOrt4WBZEw:21

a=frz4AuCg-hUA:10 a=\_W\_S\_7VecoQA:10 a=CjuIK1q\_8ugA:10

a=0T8t5DThst0rWt21OuHD:22 a=wqHmUlg-O0Vzq69H9NdF:22

DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=internachi.org;

h=subject:from:mime-version:to:content-type:content-transfer-encoding;

s=s1; bh=hO6828CTfie2jZdscxnMDKB1GGZg1I6ffH9h+N5SIt8=;

b=T89MCW32ObFUsmHH/7CXRP/x9Dm3xMMyb58Jhiqpc9e3XaHOV7O17k0CNf1vTSIwNTLz

P+HjipSLLJi2wklJd0fp33Xnu3SkwzG6bBU6D/Pt394PtIPrO4VFGqzbt2/wvoVJlxXORo

RSlOEDQer046i5n9xv6ok1QV4IhQy0KhI=

Received: by filterdrecv-p3iad2-74bd9fb996-ckhwx with SMTP id filterdrecv-p3iad2-74bd9fb996-ckhwx-20-5FDAE62C-40

2020-12-17 05:01:32.544141558 +0000 UTC m=+539963.910662834

Received: from [127.0.0.1] (unknown)

by geopod-ismtpd-1-3 (SG) with ESMTP

id oPzUEW1JQAKO3cFf\_nG6fg

for <gregg@mymail1.com>;

Thu, 17 Dec 2020 05:01:32.491 +0000 (UTC)

Message-ID: <c0a315e27b2228c1d5ae2cf1e8a5e0ba@swift.generated>

Date: Thu, 17 Dec 2020 05:01:32 +0000 (UTC)

Subject: Your InterNACHI dues payment

From: InterNACHI <fast-reply@internachi.org>

MIME-Version: 1.0

X-SG-EID:

=?us-ascii?Q?wQsVFDSccCTE3EkRlDyU7KaldqJ7H4W55lqD9KUtbjAZJoHzYndh3Px5f24q69?=

=?us-ascii?Q?K8P4kvB4pidZ=2FkqVLVtc5QxZbdJkxlHYfeyMY8+?=

=?us-ascii?Q?kkzqvVPvVysHkNiv2kMjOpuNTjWznFl+9tWtz8R?=

=?us-ascii?Q?+AAKI89tLkMHNbSgMVtYSs4vdinGNa14obLQwbD?=

=?us-ascii?Q?gwMA7n+IHQNUBXu9HJ4gM8UYGt8x4+hFFknOUCz?=

=?us-ascii?Q?2oYHV09KFads3KGmLE7k8TJIbs1d4BKyeCI9ZK?=

To: gregg@mymail1.com

X-Entity-ID: H1nqNVphCpMoDGUtRspRFA==

Content-Type: text/html; charset=us-ascii

Content-Transfer-Encoding: quoted-printable

X-CMAE-Envelope: MS4xfE6F1LdesP5S05M04VSEfLIqWYlYnU6tMX03h1DGH9wlQ0R9HZTTQCwtLztN/XHAm2ijK3QNn/lmU0XBpurrtZBlPDevNAqVfraILxwuxq8uSGl08xNq

fn471kQiwbAf3s+IixKGFrCe5Xw2QnP9HNL1f2CzjRNPKbhqOxRXH584sPj9zuX5QZZLT+YmkPXPU0fSbHX16oZM5FUp/ooyqkCSx6iSIuU6eXBhSOkZS487

35720zXsJ2H4MegzhWyArQ==

X-Nonspam: None

**From:** InterNACHI <fast-reply@internachi.org>   
**Sent:** Thursday, December 17, 2020 12:02 AM  
**To:** gregg@mymail1.com  
**Subject:** Your InterNACHI dues payment

8) Now that you have the IP address of interest "208.117.48.147", go to this link: [https://bgp.he.net/AS32475#\_whois](https://bgp.he.net/AS32475%23_whois), enter the address, and select "Search".

9) Next, from the search results, select "Whois" and copy the "OrgAbuseEmail" address as shown below

OrgAbuseEmail: abuse@sendgrid.com

10) Paste the OrgAbuseEmail address from step 9 above in the "To field" of the message you have open and ready to forward.

11) In the to field, also add your Spam Cop reporting address in the "To" field, which should be something like "submit.7IHBqzOszRhBD@spam.spamcop.net" (The Spam Cop submit address will be unique to you when you sign up).

12 Hit send on your message.

This method is 99% effective. Sometimes, they host an IP address in a foreign country not required to provide an abuse address, sometimes the abuse address is invalid, and sometimes other things happen. However, these cases are rare, and typically this is a very effective method for stopping spammers in their tracks. You may find a spammer pops up on a new IP / ISP, but typically a few attempts at this, and they will get the message (no pun intended).

Typically, you will get a response from the ISP acknowledging receipt of your Spam complaint. If you find the message came from a Gmail account, Google wants you to use this form [https://support.google.com/mail/contact/abuse](https://support.google.com/mail/contact/abuse%20) for reporting but will require the same information you harnessed above.

Recognizing this method seems like much work. It is really not, and once you get comfortable; it becomes second nature. I have found the time spent is minimal in compared to the otherwise ridiculously lengthy list of SPAM messages I would have awaiting in my inbox daily.