What to do if you have been scammed.

If you have been scammed, you need to report the incident to the local police. Hopefully you kept details on the incident, otherwise it makes no sense to report it to anyone.

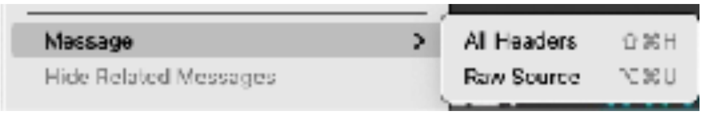
Here is a list of government offices to contact:

AARP Fraud Watch Network:
    877-908-3360 www.aarp.org/fraudwatchnetwork
Internal Revenue Service:
    800-829-1040 www.irs.gov
Medicare:
    800-633-4227 www.medicare.gov/fraud
Social Securit Administration:
    800-772-1213 www.ssa.gov
Federal Trade Commission:
    202-326-2222 www.ftc.gov, www.identifytheft.gov

In addition, your financial institution that was involved needs to be notified.
If your computer has been compromised, notify all of your financial institutions to have your accounts frozen and new credit cards issued.
If someone claimed to be representing a company, then that company needs to be notified as well.

When including any email content, it is best if you set the mail content to expose the raw content of the header information as this shows the path that the email went through to get to you. It might not reveal the sender's actual location, but enough information like this could help the authorities to narrow down the location.

On the Mac with Apple Mail, to reveal the full header information, click on View in the Menu Bar of Mail, then click Message, then click "All Headers." Clicking on "Raw Source" reveals every detail of even the content of the message, and that might not be necessary.



Copying the full header information revealed like this to include in a report can be tricky, but it is better than forwarding an email or copying just the content of an email for a report. In fact, forwarding an email actually loses all traceable information about the sender of the email being forwarded.

Using the “Raw Source” option creates a text file containing every piece of information about the sender and the content. That information might only be useful to the FBI. So just in case, save all email that you get on possible scams that you want to report on for a couple of months - just to have it on hand if some authority wants more detailed information.

Some clues as to how people are being scammed:

1. You get an email or phone call asking for money.
2. You get an email or phone call claiming to be a friend or relative who needs some information or is in a desperate situation and needs money.
3. You get an email or phone call claiming that you computer has been compromised. No one can possibly know this.
4. You get an email or phone call claiming that you are being sued. If you are being sued, you will get a snail mail letter from a lawyer that you can turn over to your lawyer to handle. Never handle claims like this on your own.
5. You get an email or phone call that asks you to provide some personal information to confirm that you are the recipient of some award or legacy. Never give out any personal information to someone or some company out of the blue like this. If it is a company that you have done business with, contact them by phone to confirm that the claim is real.
6. You get an email or phone call claiming that you have won a prize, but you must pay something to get it.
7. The IRS, Medicare, and Social Security will never ask you for any information out of the blue and will never call you for anything.

Use two factor authentication on all of your accounts to prevent scammers from accessing your accounts.

When sending and receiving email to and from a group list of people, if one of the persons in the list has a compromised computer that is collecting information, then that leads to everyone in that group list getting scam phone calls and email. Be sure that your computer is protected with the best anti-virus and malware protection available. Sophos Home, Avast, and Malwarebytes are options, but my recommendation is just for Sophos Home (the free or paid version). If you have the paid version of Sophos Home, you are also protected against being locked out of your computer (ransomware).

The two most favored methods of scammers are 1) preying on your sympathies, and 2) preying on your fears. Getting messages that evoke these feelings in you are clues that you are being scammed.

Security is your personal responsibility. Never trust a phone call or an email or a letter. If you suspect that there might be something real about the call or email, do what you can to confirm who is contacting you. Never send money or give out personal information without you verifying the authenticity of the caller. And NEVER let anyone whom you don’t know have remote access to your computer, especially anyone claiming that you have a problem that they can fix. If you don’t know that your computer has a problem, how can anyone else know?

If you suspect that you are being scammed, call the local police department and let them do the research for you.

-o-