Find out who really sent you an email

By Vince Pontorno, Komando.com, November 4, 2019

No doubt, you've been bombarded with your fair share of suspicious emails. Each of these messages leads down the same road, which ends with a phishing scam or some sketchy request to reveal your personal data. If there's one thing you've learned from Kim after all of this time, it's this: don't open it!

If you really want to check the credibility or authenticity of an email, you'll need to dig deeper and establish where the email originated from — a virtual *69 if you will. This may seem a bit daunting at first, but thankfully there are resources available that can help.

Find the IP address

It's actually pretty easy for anyone to send an anonymous email. Oftentimes these emails can be made to look like they came from another person's email address. While some anonymous emails can be deemed harmless or even playful, there are times when they have more malicious intentions.

Getting to the bottom of where these emails come from is the most crucial step to ending the constant harassment. Thankfully, email platforms from Google, Yahoo and others make it simple for you to find the email headers of any unwanted messages. If you're a regular user, these platforms are rather easy to navigate, but let's go through the steps together.

Gmail

1. Start by logging into your Google Gmail account and selecting the specific email in question.
2. Click the down arrow next to the reply button on the right. A drop down list will appear. Click Show Original. This triggers a new window to open with the full email header.
3. From here, you'll want to launch an IP tracking site or email tracking site. Copy and paste the original IP or the full email header.
4. Record any results the tracking site comes back with.

Yahoo

1. Launch your Yahoo email and open the anonymous email you wish to trace.
2. Click the gear icon or the arrow pointing downward to open the More Actions menu. Click the View Full Headers option
3. Launch an IP tracking site or email tracking site. Copy and paste the original IP or the full email header.
4. Save any and all results the tracking site comes back with. This info will come in handy later.

Outlook

1. Start by logging into your Outlook account and selecting the specific email in question.
2. Highlight the email and right-click on the email, then hit Options.
3. At the bottom of the Options box, click Internet Headers. Scross until you see Received: from (sender's IP address).
4. From here, you'll want to launch an IP tracking site or Email tracking site. Copy and paste the original IP or the full email header.
5. Once again, record and file whatever data the tracking site reveals and keep them saved in your archives.

After receiving an anonymous email, don't get rid of them. You should save them and keep a detailed record of everything you find. If the emails are abusive or threatening in nature, you should immediately contact the authorities. Always stay calm and respond in an appropriate manner to anonymous emails. This will prevent you from escalating a conflict or even landing in legal trouble.

Tools for tracking IP and email headers

By now you're probably asking, "Where can I find an IP tracking site?" or "Which one should I use?" Glad you asked. We have a credible options for you to consider. MXtoolBox is one of the leading online IP tracking sites. The platform allows you to track if anyone may be sending emails from your domain. Additionally, it can track the reputation of a senders IP, as well as the location of the sender and what their blacklist reputation is, if any.

Go to mxtoolbox.com and click on Analyze Header. Simply copy and paste the email's header into the search bar and MXToolBox will give you the rundown.