Email Compromise and Redirection

September 4th 2015

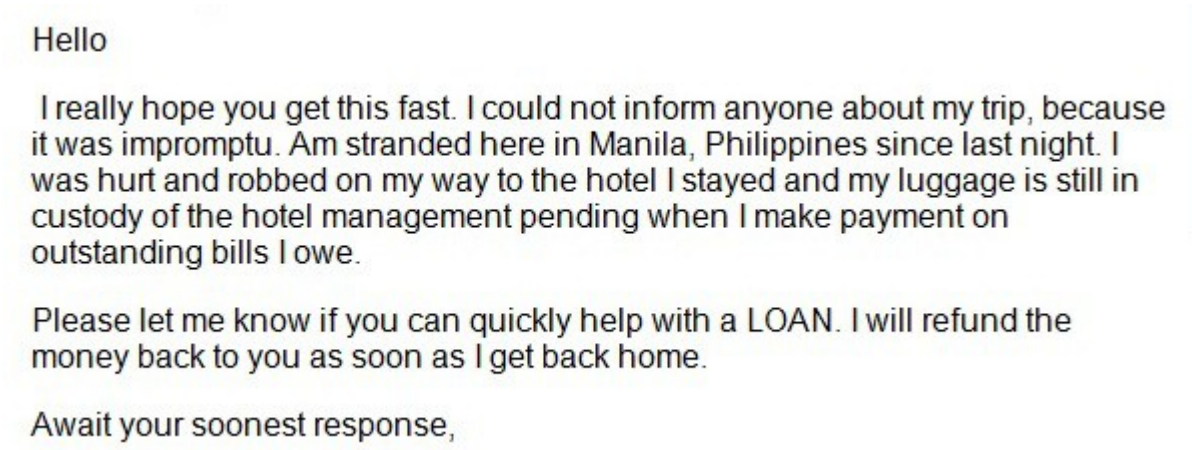
At UG-CERT we are receiving an increasing number of cases where peoples email accounts are being compromised by hackers. The hackers send emails to the owners contacts impersonating the owner, claiming that they are in an emergency situation and are in need of money.

The hacker usually edits the settings in the owners email account so that all emails that the owner receives are instead sent to the hacker. Therefore the hacker maintains communication with the owners contacts without the owner even knowing.

1. How do you know if you are affected?

If your email contacts have received emails from you which request for money (see image below), then your email account has most probably been compromised.

Additionally if you have stopped receiving emails or are receiving some emails but not from certain people whom you are expecting to recieve from, then the hacker has most probably changed the settings in your email account to redirect these emails to his own email address.



Hello

I really hope you get this fast. I could not inform anyone about my trip, because it was impromptu. Am stranded here in Manila, Philippines since last night. I was hurt and robbed on my way to the hotel I stayed and my luggage is still in custody of the hotel management pending when I make payment on outstanding bills I owe.

Please let me know if you can quickly help with a LOAN. I will refund the money back to you as soon as I get back home.

Await your soonest response,

A typical email sent by a hacker using an innocent persons email account

2. How do you correct this problem?

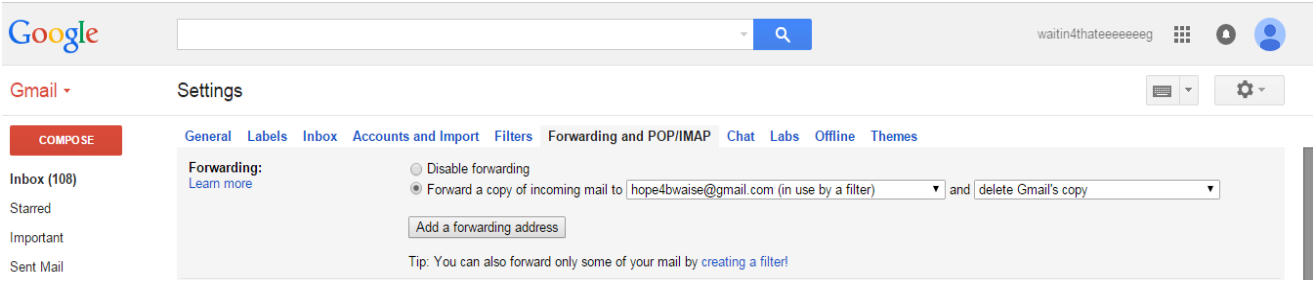
1. The hacker most probably has the password for your email account so the first thing you should do is **change your password**.

2. The next thing you should do is to check your email forwarding and filtering settings. If they have been changed then you should reset them to their original settings.

How to do this in **Gmail**:

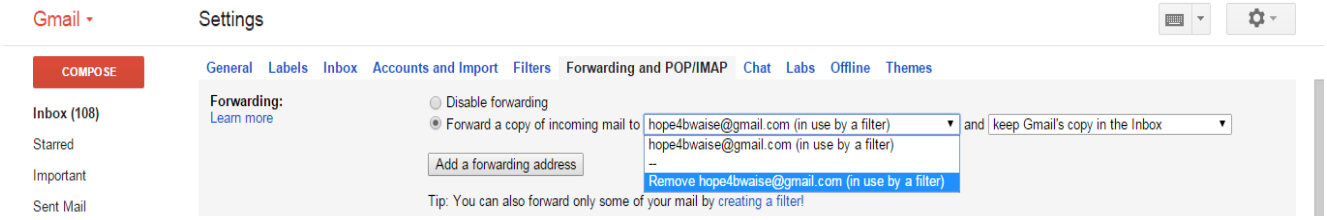
Go to **Settings** -> **Forwarding and POP/IMAP**

If you did not enable forwarding and filtering previously but the Forwarding section looks something like this:



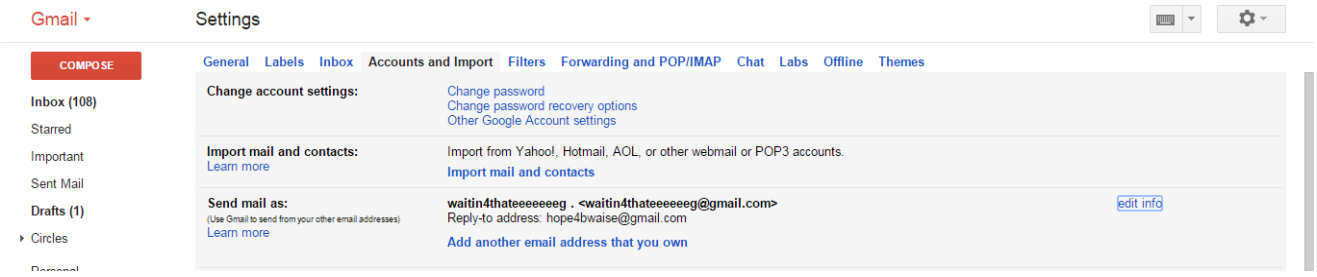
then it means that the hacker has changed your settings so that all or certain emails you receive will go to his email instead.

Disable this setting by clicking on the email address and then click on **Remove** [**the email address**].



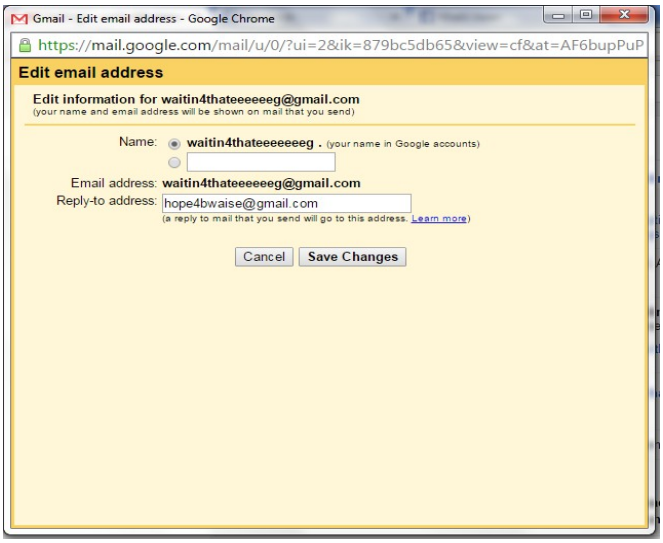
Click **OK** on the warning box that appears. You are done with this part.

Next go to **Accounts and Import**.



In the '**Send mail as:**' section click on '**edit info**'.

A screen will appear like this:



If the hacker changed this setting then you will see a different address from yours in the **'Reply-to address:'** section.

Delete this email address (by clicking on it and pressing the delete key or Backspace key) and click **Save Changes**.

You have now fully disabled the settings created by the hacker and have returned them back to how they were before.

How to do this in **Yahoo Mail**:

Go to **Settings**.

On **Mail version** check **Basic** so that you can see all of the settings clearly.

Click **Save.**

On the new Basic screen go to the top right hand corner and click on **Profile**. Choose **Options** and then click **Go** next to it.

Click **POP & Forwarding**.

If '**Forward Yahoo Mail to another email address:'** is checked (and you did not previously enable forwarding) it means that the hacker is forwarding all emails that you receive to the address that is shown.

To disable this setting delete the address (by clicking on it and pressing the delete key or Backspace key) and check **Access Yahoo Mail via POP**.

Scroll to the bottom of the page and click **Save** to save your changes.

Next Click **Mail Accounts**.

Make sure that the email address next to '**Reply-to address:**' is actualy your email address.

Hackers usually change this to their email address so that when someone replies to your email it instead gets sent to the hackers email address.

Once you have made sure that the address next to '**Reply-to address:**' is yours, scroll down to the bottom of the page and click **Save** to save your changes.

You have now disabled the settings created by the hacker and can switch back to the Full featured version of Yahoo Mail.

3. Let your email contacts know that your email account was compromised

The email addresses that the hackers use are usually very similar to the victims email address. For example if the victims email address is jmugisha@yahoo.com the hacker will create an email address named jmugisha@hotmail.com or jmugisha@outlook.com and they will use the victims names as well. Therefore it is very difficult for someone replying to your email to recognise that she is replying to a different address.

It is therefore important to let your contacts know about what happened so that they can recognise the phony email address and stop communicating with the hacker.

4. How can you prevent this from happening to you?

1. **Avoid typing your password in public computers.** Criminals can secretly install programs on public computers that record all the passwords that are typed. Therefore if you log in to your email account or your online bank account the password that you type in will be recorded by this program. The criminal will then come back later to retrieve it.

Note: Remember that the criminal does not need to work in the internet Cafe to be able to do this. He can simply install the program or leave a flash disk plugged into the computer which runs the program. He can then come back later to retrieve all the passwords that were stored. Therefore **even if you** trust the owner of the Internet Cafe, it is still unsafe to log into your important accounts on them.

2. **Whenever you log in to your email account or do any email activity make sure HTTPS is always in the address bar and that there is a green lock next to it.** This means that the website you are on has been verified by a Certificate Authority and is therefore not a fake one created by a haker to steal your credentials.

   This also means that your communication with this website will be encrypted at all times (meaning that anyone who intercepts information that you send to or receive from the website will not be able to decipher it) as long as HTTPS and a green lock are in the address bar.

HTTPS and a green lock in the address bar

3. **Enable 2-step Verification for your email account.**

   When 2 step verification is enabled, every time you log in to your email account from a new computer/device a code is sent to your phone. Only when you enter this code into the email website can you then proceed to your email account.

   This means that even if a criminal has your password he cannot log in to your email account because he does not have your phone to receive this code.

   To learn how to enable 2-step verification in your **Gmail** account go **here**.

   To learn how to enable 2-step verification in your **Yahoo Mail** account go **here**.

   To learn how to enable 2-step verification for **other popular websites** go to **twofactorauth.org**

Feel free to contact us for further information or assistance on our Toll Free line 0800 133 911, or you can send us an email at info@ug-cert.ug.