

Forum:[Hack Forums](#)

Thread: [MSN, HF Account, and Gmail account hacked - Just checking](#)

Banks? - February 18, 2012, 3:47 pm

1. My issues are: MSN, HF Account, and my main gmail account were hacked.

2. My MBAM log: <http://pastebin.com/XZRWEH6x>

3. My OTL log: <http://pastebin.com/M4AiEMCh> - Main
<http://pastebin.com/XFWCCTZb> - Extras

4. My GMER log: <http://pastebin.com/HKPCZnhZ>

Issues encountered: None so far.

Brandenx781 - February 18, 2012, 6:36 pm

Hi, your logs are looking okay.

Step 1:

Download Combofix from either of the links below, and save it to your desktop.

[Link 1](#)

[Link 2](#)

Note: It is important that it is saved directly to your desktop

--

IMPORTANT - Disable your AntiVirus and AntiSpyware applications, usually via a right click on the System Tray icon. They may otherwise interfere with our tools. If you have difficulty properly disabling your protective programs, refer to this link [here](#)

--

Double click on ComboFix.exe & follow the prompts. When finished, it will produce a report for you.

Please post the C:\ComboFix.txt for further review.

Notes:

1. Do not mouse-click Combofix's window while it is running. That may cause it to stall.
2. Do not "re-run" Combofix. If you have a problem, reply back for further instructions.
3. ComboFix may reset a number of Internet Explorer's settings, including making I-E the default browser.
4. Combofix prevents autorun of ALL CD, floppy and USB devices to assist with malware removal & increase security. If this is an issue or makes it difficult for you -- please tell your helper.
5. CF disconnects your machine from the internet. The connection is automatically restored before CF completes its run. If CF runs into difficulty and terminates prematurely, the connection can be manually restored by restarting your machine.

Banks? - February 18, 2012, 6:56 pm

(Feb 18, 2012 07:36 PM)Brandenx781 Wrote: [\[CITE\]](#) Hi, your logs are looking okay.

Step 1:

Download Combofix from either of the links below, and save it to your desktop.

[Link 1](#)

[Link 2](#)

Note: It is important that it is saved directly to your desktop

--

IMPORTANT - Disable your AntiVirus and AntiSpyware applications, usually via a right click on the System Tray icon. They may otherwise interfere with our tools. If you have difficulty properly disabling your protective programs, refer to this link [here](#)

--

Double click on ComboFix.exe & follow the prompts. When finished, it will produce a report for you.

Please post the C:\ComboFix.txt for further review.

Notes:

1. Do not mouse-click Combofix's window while it is running. That may cause it to stall.
2. Do not "re-run" Combofix. If you have a problem, reply back for further instructions.
3. ComboFix may reset a number of Internet Explorer's settings, including making I-E the default browser.
4. Combofix prevents autorun of ALL CD, floppy and USB devices to assist with malware removal & increase security. If this is an issue or makes it difficult for you -- please tell your helper.
5. CF disconnects your machine from the internet. The connection is automatically restored before CF completes its run. If CF runs into difficulty and terminates prematurely, the connection can be manually restored by restarting your machine.

Thank you. Here is the ComboFix log:

<http://www.pastebin.com/nEU2118w>

Brandenx781 - February 18, 2012, 7:05 pm

Hi,

Step 2:

We will be doing a ComboFix Script

Please open Notepad and copy/paste this code into the notepad:

Code FCopy::

c:\windows\Ubuntu Skin Pack\Backup\comres.dll | c:\windows\system32\comres.dll

c:\windows\winsxs\amd64_microsoft-windows-explorer_31bf3856ad364e35_6.1.7600.20910_none_ae79ed04ac56c4a9\explorer.exe | c:\windows\explorer.exe

Save this as CFScript.txt and change the "Save as type" to "All Files" and place it on your desktop. Make sure your AV is disabled while we do this.

[img]http://users.pandora.be/bluepatchy/miekiemoes/images/CFScript.gif[/img]

Referring to the screenshot above, drag CFScript.txt into ComboFix.exe.

ComboFix will now run a scan on your system. It may reboot your system when it finishes. This is normal.

When finished, it shall produce a log for you. Copy and paste the contents of the log in your next reply.

Step 3:

Please download and run a free online scan with ESET Online Scanner from here:

[LINK 1](#)

Note: You will need to use Internet Explorer for this scan. Tick the box next to Yes, I accept the Terms of Use.

Click Start

When asked, allow the ActiveX control to install

Click Start

Make sure that the options Remove found threats and the option Scan unwanted applications is checked

Click Scan

Wait for the scan to finish

Use Notepad to open the logfile located at C:\Program Files\EsetOnlineScanner\log.txt

Copy and paste that log as a reply to this topic

Step 4:

Please click [here](#) to download AVP Tool by Kaspersky. Save it to your desktop.

Reboot your computer into SafeMode. You can do this by restarting your computer and continually tapping the F8 key until a menu appears. Use your up arrow key to highlight SafeMode then hit enter.

Double click the setup file to run it.

Click Next to continue.

Accept the License agreement and click on next.

It will, by default, install it to your desktop folder. Click Next.

It will then open a box There will be a tab that says Automatic scan.

Under Automatic scan make sure these are checked.

Hidden Startup Objects

System Memory
Disk Boot Sectors.
My Computer.
Also any other drives (Removable that you may have)

Leave the rest of the settings as they appear as default.

Then click on Scan at the to right hand Corner.

It will automatically Neutralize any objects found.

If some objects are left un-neutralized then click the button that says Neutralize all

If it says it cannot be neutralized then choose the delete option when prompted.

After that is done click on the reports button at the bottom and save it to file name it Kas.

Save it somewhere convenient like your desktop and just post only the detected Virus\malware in the report it will be at the very top under Detected post those results in your next reply.

Note: This tool will self uninstall when you close it so please save the log before closing it.

Banks? - February 19, 2012, 9:50 am

I accidently uninstalled the ESET Scanner before I got the log. It had 35 detections, and it said it removed them all.

I will post the Kaspersky one when it's done.

Is the Kaspersky scan supposed to take 7 hours normally? ._.

Is there an alternative to this? I don't really feel like waiting this long to be honest.

[img]<http://screensnapr.com/e/fNINer.png>[img]

Brandenx781 - February 19, 2012, 10:39 am

Depending on how many files you have, yes it can take up to 7 hours. There is no alternate.

Banks? - February 19, 2012, 10:43 am

Oh, I almost forgot, here's my ComboFix log:

<http://pastebin.com/QKicZRCi>

Brandenx781 - February 19, 2012, 10:44 am

Good. Please be patient for AVP. It's better to be safe.

Banks? - February 19, 2012, 3:04 pm

Only another 3 more hours. ?

[img]<http://screensnapr.com/e/z25HFI.png>[img]

Brandenx781 - February 19, 2012, 7:54 pm

Hi, how is everything going for you and that scan?

Banks? - February 19, 2012, 8:01 pm

37 Minutes left.

[img]http://screensnapr.com/e/e5soBk.png[/img]

The log file is HUGE... 456 MB.

[img]http://screensnapr.com/e/nsexom.png[/img]

But here's what it said:

[img]http://screensnapr.com/e/HEuYZM.png[/img]

Brandenx781 - February 20, 2012, 1:13 pm

Looking good.

Step 5:

Download [SuperAntiSpyware](#) Load SuperAntiSpyware and click the Check for updates button.

Once the update is finished click the Scan your computer button.

Check Perform Complete Scan and then next.

SuperAntiSpyware will now scan your computer and when its finished it will list all the infections it has found.

Make sure that they all have a check next to them and press next.

Click finish and you will be taken back to the main interface.

Click Preferences and then click the statistics/logs tab. Click the dated log and press view log and a text file will appear.

Copy and paste the log onto the forum.