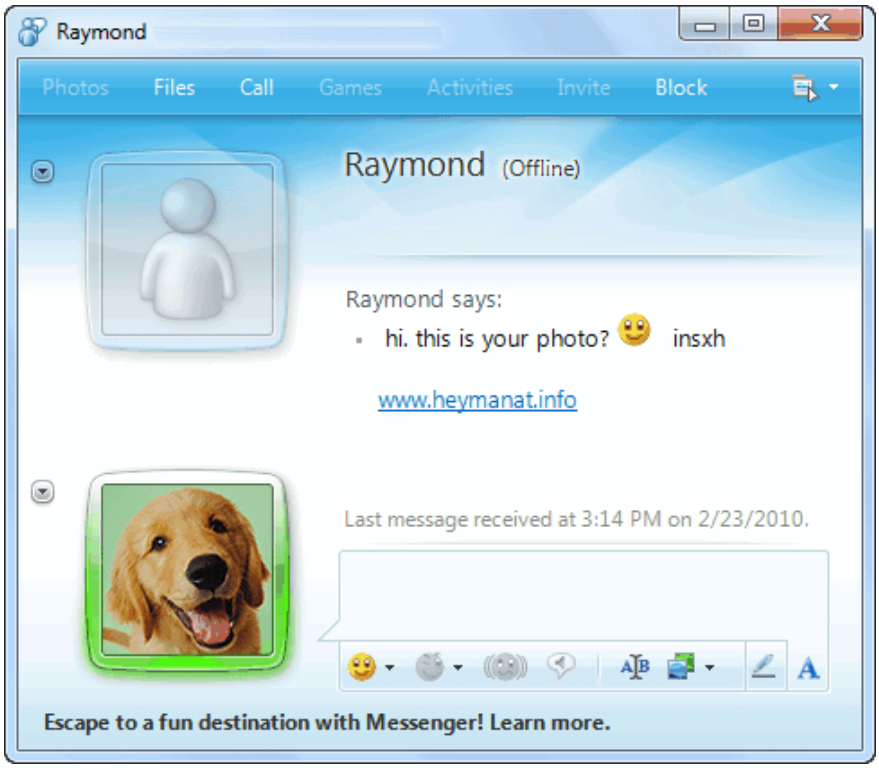
Beware of MSN virus' hi. this is your photo? '

For MSN users, the virus spread through offline messages is very common. Recently, a new virus has appeared in the form of this message

TipsMake.com - For MSN users, the virus spread through offline messages is very common. Recently appeared a new type of virus in the form of this message from friends on the list . These messages are generated by hackers (phishers) who want to steal everyone's MSN account.

These messages usually start with ' *hi* ' . *this is your photo?* 'along with 1 symbol and 1 string of 5 characters. In the next line is a path



If the user accidentally clicks on the link above, it will lead the user to a web page for the MSN account login details, but will automatically download a file named ' **Picture_2525.exe** 'is about 1.8 mb (this is a new virus). When activated in the system, the user will see a notice board titled ' *bedava Film indir. Hemen TIKLA 7* 'in Azerbaijani language.

If you continue to click on the bulletin board, an advertising website will appear on the user's browser. After analyzing the action of this virus program, the author discovered the main purpose of the virus is to automatically delete the file system in the ' *System32* ' *folder* and install, activate some additional services when

the system operating Windows startup. At the same time, it turns Internet Explorer's default startup site into a ' *www.googlesayfa.com/en* ' page with a very similar interface to Google. If the user trusts and continues to work on the site itself, a Google Adsense ad will appear with the content ' *this website unofficial Google Search Fan website* ', and the system will automatically connect to US IP address: **67.228.41.155** through port **6772** .

After analyzing the action of the ' **Picture_2525.exe** ' file using the *VirusTotal* online application, there are about 33 out of 41 identifiable apparatuses that are viruses. But it is also quite lucky for users because this virus is not equipped with the 'persistent' feature. Users can create batch files that automatically delete this virus or follow these simple steps:

- Open the **Task Manager** application, select **Tab Processes** and cancel the following processes: **svlost.exe** , **svlostSrv.exe** , **tasman.exe** by selecting ' **End Process** '

- Open **Run** (*Win + R*) and type: **sc delete svlostServices**

- Find and delete the following files in the ' *WindowsSystem32* ' system directory: **libeay32.dll** , **ssleay32.dll** , **svlost.exe** , **svlosta.dll** , **svlostb.dll** , **svlostSrv.exe** , **tasman.exe**

- Next, open the **Run** (*Win + R*) section and continue with the following two separate statements:

reg delete "hkcusoftwaremicrosoftinternet explorermain" / v default_page_url / f
reg delete "hkcusoftwaremicrosoftinternet explorermain" / v "Start Page" / f

After doing all of the above, you have completely removed the virus from the system, but it is best to change your MSN login password.

Besides, the author did a Reverse IP survey using *DomainTools* tool to track traces and discovered 52 domains under the same server:

And here is a complete list of malicious websites that spread viruses on:

 # Ahvalimsn.info
 # Ankemsn.info
 # Arabiamarabia.info
 # Arabimsnks.info
 # Asmsnas.info
 # Azrrufi.info
 # Baemsn.info
 # Burdamsns.info
 # Demlikciheymsn.info
 # Denimenter.info
 # Dubaimsn.info
 # Ehlenselamam.info
 # Elmsnulblock.info
 # Gerwhymsn.info
 # Habibimwhos.info
 # Habibmsnd.info

 # Habibulmsn.info
 # Hakmsns.info
 # Haydari.info
 # Heymanat.info
 # Hombilmombil.info
 # Kimbenibans.info
 # Kimbitr.info
 # Kimpetek.info
 # Leyyamsn.info
 # Lovemsnlove.info
 # Lovepoemswhy.info
 # Maishemsn.info
 # Menzilmsn.info
 # Msnbut.info
 # Msniblock.info
 # Msniblocki.info
 # Msnminepr.info
 # Msnmsntsn.info
 # Msnsenm.info
 # Mustarabis.info
 # Myfedorea.info
 # Mysoutchests.info
 # Nerdenmsns.info
 # Patlirafan.info
 # Peyamnetsd.info
 # Pirinces.info
 # Reddumsn.info
 # Senmsnen.info
 # Seyyarmsn.info
 # Seyyarmsnn.info
 # Tayyarmsn.info
 # Thisallfreegetit8.info
 # Turustum.info
 # Vasilios.info
 # Wheremerewhy.info
 # Zlanmsnm.info
 # Karamsns.info