Cyber criminals are found creating various forms of scams to frighten computer users into purchasing fake antivirus software with a seemingly genuine security warning, which is one of the fastest-growing types of Internet fraud today. When users choose to buy this program, they will find that it will either do nothing or it could compromise their computers by installing malicious software onto their system. To avoid falling victims to this type of scam, users should know this: few legitimate Internet security companies use ads to tell you about a virus on your computer.

XP Internet Security Pro 2013 is such an instance. It is a fresh rogue program that was designed by inventors of Vista Security Plus 2013 and Win 7 Internet Security Pro 2013. It tries to frighten you into purchasing fake security software with a fake security warning. The inventors of this fake security program uses networks of compromised computers under their control-to push out the fake software and the criminal also masquerades as legitimate Internet security companies and buy ads on other websites, but when you click on the ads to purchase the products, you will be redirected to websites controlled by the bad guys.

When this rogue program is installed, it will mess up your system in many other ways. For example, it stops your real antivirus from working and installs Trojans or spyware on your computer, which allow the hacker to access your entire system. So when you see a pop-up message telling you your computer is infected with a virus and that to get rid of it, all you have to do is order XP Internet Security Pro 2013, don't be scared by this message. Instead, you should take actions to uninstall this program from your system.

XP Antispyware Pro 2013 is a rogue antivirus that belongs to Fake Rean/Braviax family. It targets computers having Windows XP operating system. As all of this family rogues, XP Antispyware Pro 2013 is known to disable existing computer security, legitimate programs and browser sessions. The aim of this fake antivirus program is to trick people's money away by trying to convince an infected computer user that her PC is badly damaged. Since cyber criminals use prepaid payment systems for collecting money, it is particularly difficult to trace the amounts paid.

For those not familiar with fake AV it might be difficult to identify that a computer is infected. XP Antispyware Pro 2013, just like many rogue AVs, shares several main features:

- its graphic user's interface (GUI) looks professional in order to create an impression of a legitimate antivirus;
- after infiltrating into the system fake AV imitates a computer scan and presents a list of threats found;
- as a solution to any of the problems found rogue AV offers purchase of its full version.

XP Antispyware Pro 2013 might get installed after browsing through corrupted websites and pressing on advertisements. It is also distributed in attachments of spam e-mails. Malware uses Adobe, Java or other software vulnerabilities to get inside a computer. In a case of infection, you should remove XP Antispyware Pro 2013 as soon as noticed. There are reputable antivirus and antispyware tools available. If one tool is not enough to get rid of rogue AV, use multiple tools.

To protect your computer from XP Antispyware Pro 2013 attacks you should follow safe computer usage and internet browsing tips. An advice number one listed on many Lists is reliable and legitimate antivirus software. But it is not enough to have it. You must check regularly if your computer security is up to date. Also make sure that your computer operating system is updated. Another point to consider is having your web browser up to date since fixes of security holes are being identified and eliminated constantly. It is not recommended to download shareware or freeware files from untrustworthy sources because these might be a reason of many infections. In a case of downloading a file, you should scan it first before using it. When navigating through the Internet, leave the webpage if it looks suspicious. Note that even those pages that you use regularly and have been safe before might be infected one day. If you let other people use your computer, create another account for this with limited rights especially when it concerns downloading and installing of programs.

How to remove the fake security tool?

Some users may wish to get rid of the fake security tool by doing a system restore. However, the reality is that things will get worse if you perform a system restore to remove this rogue program. The system restore may cause computers freeze and the loss of your precious data. The worst thing is that the fake security tool may remain in your computer. Hence, it is recommended that using the manual approach below to remove this nasty virus.

1. Restart your computer to safe mode with networking.
2. Press Ctrl+Alt+Del keys together to open the Windows Task Manager and stop the process of the fake security tool.
3. Delete associated files from your PC completely as follows:
%AllUsersProfile%random.exe

%AppData%RoamingMicrosoftWindowsTemplatesrandom.exe
%Temp%random.exe
4. Click on Start menu -> Run. Type "regedit" into the Run command and press OK to open the Windows Registry Editor.
5. Access to the following registry entries and remove them one by one:
HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersionPoliciesSystem
"DisableRegedit" = 0
HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersionPoliciesSystem
"DisableRegistryTools" = 0
6. Restart your computer to put the steps above into effect.

To get rid of XP Internet Security Pro 2013 quickly and safely, it is recommended to use some of our recommended antivirus suites. It is a professional and powerful tool that provides you with effective and secure way of uninstalling any fake antivirus programs and other unwanted programs, saving you much time and reducing the risk of lose important data that may happen when you delete registry entries. What's more, it is very user-friendly, which allows you to manage unwanted programs easily.

telefon dinleme